University of Strathclyde

Department of Computer and Information Sciences

Exploring the Organisational, Social and Cultural Factors Influencing those Employee Attitudes and Behaviours That Impact the Implementation of an Information Security Culture within Omani Organisations

A thesis submitted in fulfilment of the requirements

For the degree of Doctor of Philosophy

By

Fathiya Hamed Salim Al Izki

2019

Declaration of Authenticity and Author's Rights

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.

Signed: 

Date: 18th JUNE 2019

"If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees." - (Kahlil Gibran, 1883-1931)

Acknowledgments

My first and foremost thanks go to Almighty God for giving me the opportunity, patience, and courage to conduct this research study. Without his blessings, this achievement would not have been possible. Secondly, my journey of pursuing doctoral studies made me realize how lucky I am to have many people who consistently provide me with support and encouragement. I would like to take this opportunity to express my gratitude to all of them.

I would like to express my most sincere thanks and appreciation to my employer, the government of Oman, for their generous funding of my scholarship and their continuous support that enabled me to pursue this PhD research. Further and as always, I am deeply appreciative of my family, especially my parents, for their endless love, prayers and for providing me with inspiration, encouragement, and continuous support to complete this work successfully and in all the walks of my life. My sincerest thanks and gratitude go to my brothers and sisters, my brothers-in law and sisters-in law and all other family members for their unconditional support, encouragement and love and without which I would not have come this far. My very special and sincere thanks go to my dearest and best friend, who has been there for me from the beginning of the research until the end, Widad, a source of great emotional support, understanding, encouragement, and motivation.

My deepest and sincere thanks, gratitude and unrestrained appreciation go to my supervisor Dr. George R.S. Weir, for his creative input and endless guidance, advice, support, and patience throughout my research years. I have been very fortunate to have him as a supervisor. I extend my thanks and gratitude to my second supervisor Dr. John N. Wilson, for his constructive comments and invaluable guidance, advice and feedback during my research study. Further, I am very grateful to Dr. Ali Sharaf Al-Musawi, my local supervisor from the Sultan Qaboos University for his support, guidance, and many comments that assisted me in successfully completing this thesis.

Finally, my deep appreciation and heartfelt thanks go to each interview and questionnaire participant, who was generous with their time and provided detailed discussion and valuable insight, for sharing their valuable experiences. My thanks and appreciation also go to my work colleagues, Said A. Al Hashmi, Saleh Al Masoudi, Sami Al Sulimani, Sami Al Mamari, Bader Al Khatri, and Ibrahim Al Zadjali, who have helped in diverse ways with conducting the interviews used in the thesis.

Abstract

Research has strongly established that the success of an information security program is heavily dependent upon the actions of the members of organisations that interact with the information security program. An appropriate information security culture is required to effectively influence and control the actions of the members within an organisation because of this interaction between people and the information security program.

This thesis seeks to explore and study the current state of information security behaviour and discipline in public and private organisations in the context of Oman and investigates the challenges in developing an information security culture within these organisations. The key focus of the study is on an investigation and identification of the critical socio-cultural and organisational factors that affect the successful development and maintenance of a culture of information security within public organisations in the context of Oman. The study also aims to examine the difference between public and private organisations in Oman regarding information security practices.
Although many organisations in Oman have implemented technical solutions to protect information resources from adverse events, internal security breaches continue to occur. For this reason an emphasis on a culture of information security within organisations is required in order to make security an integral part of employees' daily work routines. Although, it is important in practice to address both technical and non-technical aspects when dealing with information security, the research described in this thesis concentrates upon non-technical approaches, and excludes consideration of the technological aspects.

To achieve the study aim, the research reviewed and compared the roles of national culture; information security culture; organisational culture and employee behaviour within organisations, in order to determine the socio-cultural and organisational factors that potentially hinder an organisation in implementing, integrating, and maintaining a successful organisational information security culture. A review of related academic work was undertaken. In addition, the research used both quantitative and qualitative research methods to collect, analyse and integrate data from a survey questionnaire of 155 respondents semi-randomly selected from different Omani public and private organisations. The survey results formed the basis of hypotheses about the critical factors in developing effective information security practices in these organisations.

The IBM Statistical Package for the Social Sciences (SPSS version 22) with multiple regression was used to analyse the relationship between a dependent variable and several independent variables. To validate the identified critical factors further, thematic analysis was carried out using semi-structured open-ended interviews with specialist Information Technology (IT) and Information Security (IS) senior managers in fifteen selected public and private organisations.

The data analysis indicates that security of information in Omani public organisations is not optimal. The findings show in general that these organisations have inadequate information security cultures. These organisations are facing several challenges. These include the remoteness of those in power from the issue and therefore a lack of senior management support and involvement. There is a lack of training and awareness. There is an absence of policies to develop a respect for collectivism, avoiding uncertainty and building a high level of trust, which would all help to support security of information.

The current study contributes in a number of ways to discussions and actions around these issues. Firstly, the findings can serve as a basis for Omani public organisations to reform their information security programs. The study identifies and investigates the most critical factors influencing the effectiveness of information security practices. There has been little research conducted to date that assists an understanding and management of the culture of information security within Omani public organisations. The researcher hope that this study will expand the body of knowledge in this area. Furthermore, this study is the first and only one to my knowledge that explores the influences of critical socio-cultural and organisational factors on employee behaviours and attitudes regarding the security of information in Omani organisations. However, further research is needed to improve our insight into information security in the context of Omani organisations. In addition, research which compares Omani organisations with other Gulf country organisations would provide further insight into information security in Oman.

Contents

List of Figures

List of Tables

List of Charts

List of Abbreviations

CA	Culture Assessment
CEO	Chief Executive Officer
CERT	Computer emergency response team
COP	Child Online Protection
EGDI	E-Government Development Index
EISC	Employees Information Security Culture
GCC	Gulf Corporate Council
ICT	Information Communication Technology
IS	Information Security
ISACA	Information Systems Audit and Control Association
ISBP	Information Security Best Practice
ISC	Information Security Culture
ISCA	Information Security Culture Assessment
ISD	Information Security Division
ISP	Information Security Policy
ISRM	Information Security Risk Management
ISSA	Information Security Strategy Alignment
ISTA	Information Security Training and Awareness
IT	Information Technology
ITA	Information Technology Authority
NC	National Culture
NRI	Network Radiance Index

OC	Organisational Culture
OCERT	Oman National Computer Emergency Readiness Team
Org	Organisation
PD	Power Distance
PKI	Public Key Infrastructure
Priv	Private
Pub	Public
RA	Risk Assessment
RM	Risk Management
SD	Security Division
SDT	Self- Determination Theory
SET	Social Exchange Theory
TPB	Theory of Plan Behaviour
TRA	Theory of Reasoned Action
UA	Uncertainty Avoidances
UN	United Nations

List of Publications

4. Management attitudes toward information security in Omani public-sector organisations

Al-Izki, F., & Weir, G. R. S. (2016, August). Management Attitudes Toward Information Security in Omani Public Sector Organisations. In Cybersecurity and Cyberforensics Conference (CCC), 2016 (pp. 107-112). IEEE.

4. Gender impact on information security in the Arab world

Al Izki, F., & Weir, G. R. S. (2015, September). Gender Impact on Information Security in the Arab World. In International Conference on Global Security, Safety, and Sustainability (pp. 200-207). Springer, Cham.

4. Information security and digital divide in the Arab world

Al Izki, F., & Weir, G. R. S. (2014, June). Information security and digital divide in the Arab world. In Cyberforensics 2014-International Conference on Cybercrime, Security & Digital Forensics (pp. 15-24).

Chapter 1. Introduction

"The art of writing is the art of discovering what you believe."

-(Gustave Flaubert, 1821-1880)

1.1. Introduction

Information security good practice should be an integral part of every employee's daily work routines and organisational systems (Schlienger and Teufel, 2002). Martins and Eloff (2002) believe that an information security culture is about what is acceptable and what is not acceptable in relation to information security. Thus, the absence of a proper information security culture will increase the inherent risks of inconsistent employee security behaviour with regard to handling the information assets of organisations. Developing an information security culture can help promote security best practices amongst employees, thereby helping to reduce internal security incidents within an organisation.

Public organisations in Oman face a wide range of information security threats caused by insiders, so that securing organisational information has become a crucial function. The researcher decided to investigate this problem through the current study that seeks to answer the following questions: *What is the current state of information security culture and practices in public and private organisations in the context of Oman? What are the critical socio-cultural and organisational factors that may affect the information security performance and hinder the development and maintenance of an effective information security culture in these organisations?* These questions are addressed with a view to providing useful recommendations for the managers of organisations and implementers of information security programs in the context of Oman.

According to Van Niekerk and Von Solms, (2010), information is a sensitive factor and is considered one of the most valuable assets of any organisation; it is not only important for completing work, but it is a prerequisite for operations to continue. Most current organisations cannot function professionally without access to their information. This exists in many different forms including printed or written on paper, stored electronically, transmitted by post or electronic means, shown on film, or spoken in conversation. Regardless of the form of information or how it is shared and stored, it should always be appropriately protected (Calder & Watkins, 2008). Furthermore,

organisations should not view information security only as a technological issue but should look holistically at its organisational context (Grand & Ozier, 2000; Martins & Eloff, 2002). As well as its technological and procedural components, information security should also involve people. These three components, the people involved, the organisation of the process involved in securing the environment, and the technology used, are equally important for an organisation's efforts to meet its business objectives (Kark et al., 2007; DeLone & McLean, 2008).

Figure 1-1: Information Security Components
Source: Schneier, 1999

Dutta and Roy (2008), state that information security has been perceived as a technical issue, which has led organisations to focus solely on technical solutions to solve problems related to information security. However, recent studies indicate that insiders are intentionally or unintentionally the weakest link in the security chain and the root cause of most security breaches. (Verizon, 2009; da Veiga & Eloff, 2010; Wipawayangkool, 2009). Regardless of the number of technical controls in place, organisations will continue to experience security breaches (Schultz, 2005; Besnard & Arief, 2004), because information security is primarily a 'people' problem (Schulz, 2005). People have a tremendous impact on the success or failure of efforts to secure and protect businesses, services, systems, and information (Orshesky, 2003). Researchers are particularly interested in the impact of the behaviours of insiders within an organisation upon information security within the organisation (Boss et al., 2009; D'Arcy & Hovav, 2007; Moore et al., 2012), and the potentially negative influence of insider behaviour upon organisational information security efforts. (D'Arcy et al., 2009; Straub, 1990; Warkentin & Willison, 2009; Whitman, 2003; and Willison & Siponen, 2009). On the other hand, employees will adopt consistent security practices when the organisation establishes a culture of security. (Corriss, 2010; Thomson, von Solms, & Louw, 2006; von Solms & von Solms, 2004).

Instilling an information security culture represents one of the necessary foundations for effective information security in an organisation. Such a culture requires an organisation's members to have knowledge and understanding of their information security responsibilities and to be committed to those responsibilities (Siponen, 2000). However, this culture cannot be achieved without appropriate effort from top management to develop good information security policies: security awareness; training and education for all the members of the organisation. Moreover, even when employees have sufficient knowledge about their roles in the security process, there is no guarantee that they will adhere to their required security roles.

Contemporary research shows that establishing an information security culture within an organisation can help address the human factor problem in security management. Aligning organisational and employee attitudes, beliefs and values is key to establishing a culture of information security. (Kolkowska, 2011; von Solms & von Solms, 2004). Programs within an organisation that are congruent with attitudes, beliefs, and values, serve to motivate employees to embrace security controls. (Lacey, 2010). In their seminal work on security culture, von Solms and von Solms (2004, p.277) concluded, "…if management wants their employees to act in a specific way that is beneficial to the organisation, they need to dictate the behaviour of the employees, this can be done by expressing collective values…". Von Solms (2000) and Schlienger and Teufel (2002) explain that security culture covers social, cultural, and ethical measures to improve the security-relevant behaviour of organisational members, and it is considered a subculture of organisational culture.

Organisations are encouraged to build a culture of information security; such that information security becomes a natural aspect of the daily activities of all employees. By establishing an information security culture, employees can become a security asset instead of a risk (Von Solms, 2000). In addition, most failures of information security systems are due to an organisation's lack of information security strategies that align information security with the business. An organisation's top management has direct responsibility for ensuring that all the information assets of an organisation are secure (Von Solms &Von Solms, 2004). When the goal of leadership is to align the organisation's information security values with the values of its employees, the organisation becomes well positioned to succeed in developing effective information security practices. (Corriss, 2010; Furnell & Thomson, 2009; von Solms & von Solms, 2004). When these practices become habitual, a culture of security is established. (Baggett, 2003; Chang & Lin, 2007; Thomson, von Solms, & Louw, 2006).

Furthermore, when individuals within a group share values, these values influence security behaviour within the organisation, (Alfawaz, Nelson, & Mohannak, 2010; Dhillon & Torkzadeh, 2006; Killingsworth, 2012) and continue to influence employees throughout their employment with the organisation (Ostroff, 2005). These findings suggest that if employee and organisational values can be aligned, not only will the organisation influence employees to adopt a security culture, but the employees will also influence each other and so strengthen the security culture.

This chapter proceeds to give an overview of the research including the context for the research, the research problem, the research aim and the approach including the research questions and hypothesis. The chapter finally provides an outline and structure of the thesis. Section 1.2, below, sheds light on the context of the current study the sultanate of Oman.

1.2. Research Context

The main goal of this study was to investigate how Omani public organisations were addressing information security issues. This section provides a brief overview of the Sultanate of Oman in the context of the current study. Oman, officially known as the Sultanate of Oman, is the oldest independent state in the Arab world, and is one of the more traditional countries in the Gulf region. The Sultanate of Oman is a member of the Gulf Co-operation Council (GCC) along with the United Arab Emirates, the kingdom of Saudi Arabia, Kuwait, Qatar and Bahrain. Covering an area of 309,501 km², it is the third largest country in the Arabian Peninsula after the Kingdom of Saudi Arabia and the Republic of Yemen. The country is situated at the strategic crossroads of Europe, Asia, and Africa, extending along the southern coast of the Arabian Peninsula for 1,700 km.

The growth of information and communication technology (ICT) has offered the government in Oman an opportunity to reshape traditional approaches to public service delivery. Oman's transformation into a knowledge-based economy was emphasised by His Majesty Sultan Qaboos bin Said Al Said, the Sultan of Oman, whilst addressing the Council of Oman in November 2008. Oman's ICT strategy is embodied in the e-Oman strategy, which forms the blueprint for the growth in ICT usage as well as connectivity. e-Government services have become prevalent with the recent radical improvement in the ability of citizens and residents to communicate, interact and transact digitally. There is a high mobile penetration rate of 156.73%; the Internet penetration rate is at an all-time high (Fixed Internet at 60.1% and Active Mobile Internet at 92%), coupled with

a high PC penetration rate of 87.54%. (ITU, 2017). Nevertheless, the growth of ICT and the ease of internet access contributes greatly to the existence of information security risks in Omani public organisations especially as many of the processes involved in information security are dependent on people's behaviour.

The particular impact of human factors on information security in public organisations arises from the socio-cultural context in Oman. There has been little research into the impact of socio-cultural and organisational factors upon information security in Oman, which this study aims to identify and explore.

1.2.1. Oman Vision and Strategy

Oman has made transformation technology a national priority since the early 1970s under the direction of His Majesty Sultan Qaboos. In 1995 Oman launched a national long-term plan, 'Oman 2020' (1996-2020) which focuses on ICT alongside other economic and social aspects. ICT received a great deal of attention in establishing the major fundamentals of a knowledge-based economy, in an effort to increase the productivity of the Omani economy and improve the livelihood of citizens. The government of Oman sees a knowledge based society, as one in which government operations and information are made transparently and efficiently accessible to all sections of society and are regularly updated. The plan also aims to use enhanced ICT capabilities to harness potential strengths in society and so build the required skills to advance and transform Oman. (Information Technology Authority (ITA), 2006a).

Oman, like other countries in the world, has realized the importance of moving toward the ICT era. The adoption of an e-government strategy reflects this interest. 'Towards Digital Oman', launched in 2003 and later shortened to 'e-Oman' was the first official initiative in e-government. Besides developing the provision of e-services to the public, the 'e-Oman' strategy also considered the development of information technology awareness, IT skills and IT businesses (Al-Ruzaiqi & Baghdadi, 2016). The government implemented the 'e-Oman' strategy by establishing the Information Technology Authority (ITA) by the Royal Decree No. 52/2006 promulgated on May 31, 2006. The ITA is responsible for overseeing 'e-Oman' infrastructure projects, and has an essential role in providing technical services for those projects during their execution. Moreover, it offers consultation services for government entities during mutual collaboration projects. One example of a large electronic transformation initiative is the Invest Easy Project, an online one-stop shop that integrates different Omani government entities that offer e-services such as commercial registration and licensing processes. In 2010 ITA

launched the Sultan Qaboos Award for Excellence in e-Government, a competition to honour government project achievements, to encourage the provision of e-services and to assess the adoption of e-government.

1.2.2. Information Security Bodies in Oman

One of the activities that ITA has focused on since its establishment in 2006, is to provide a secure environment for ICT users within Oman. Research by Sharma revealed that security issues could affect the usage of the government's e-services in Oman. (Sharma, 2014). Al-Busaidy and Weerakkody (2009) agree with Sharma and emphasise the importance of firmly embedded security practices in enhancing users' trust in e-services. (Al-Busaidy & Weerakkody, 2009). In this regard, for example, a public key infrastructure (PKI) has been established to secure e-service communications of government and private entities by providing digital encryption capabilities. The administrative structure of ITA, includes the Information Security Division (ISD), and the National Computer Emergency and Readiness Team (OCERT) in order to secure the cyber environment in Oman. They seek to provide a trustworthy environment for users whether they are a public or private institution.

Oman National CERT

OCERT, established in 2010, is responsible for securing the cyber space for individuals and public or private entities. Its task is to develop information security strategies and policies to ensure the online viability of these institutions. OCERT works in real time to monitor and respond to any cyber threat or attack. In 2015, for example, OCERT responded to almost six thousand serious attack against Oman cyberspace (Information Technology Authority Annual Report, 2015). Along with these efforts, OCERT has an essential role in raising public awareness of cyber security.

Information Security Division (ISD)

Information Security Division (ISD) functions follow international security standards to ensure a secure ICT infrastructure for government entities. This includes securing government's portals and networks as well as Internet access. (Information Technology Authority Annual Report (ITA), 2015). In 2015, for example, ISD managed to stop around 398,000 attacks against government portals and almost five million attacks against government networks. (ITA Annual Report, 2015). ISD provides technical consultation services to all communications channels within government and end customers to raise security awareness.

1.3. Research Problem

According to Perry (2012), the reason for carrying out research is usually a research problem that acts as a catalyst to the commencement of the research. In this study, the researcher tries to provide a better understanding of the association between human elements and the culture of information security in the context of Oman.

Information security is a concept that emerged from the recognition that information is valuable and needs to be protected. Information flow is no longer restricted within the boundaries of an organisation; rather, information is shared with other people, other organisations, and the establishments that are linked to the organisation, which may be in or outside of the country. Despite the growing appreciation of the need for effective information security and the more proactive approaches by organisations towards achieving appropriate information security, the number of information security breaches and incidents is still rising (Garrison and Ncube, 2011). This may be because many organisations have upgraded their technological approach towards information security, without realising that inappropriate information security behaviours by employees are also a source of vulnerability. Upgraded technological responses to information security threats and vulnerabilities may lead to a false sense of security and complacency. (Parsons et al., 2010). According to Liagkou and Spirakis (2010), most IT security solutions suggest a set of security tools for addressing security issues. However, they fail to present a security model that includes developing a security culture.

The researcher believes that the behaviour of employees is the key factor in the quality of information security within Omani public organisations. Therefore, a solution is needed in which information security is no longer viewed as a nuisance to be ignored, or an add-on to be marginalised, but is instead considered a core component of the human resource, processes, and technologies of an organisation. The human aspect of information security must be addressed, including the attitude that insiders have towards information assets and the way they comply with information security programs and practices. Lack of compliance with the security program can occur if employees do not know or understand security procedures, or if they resist following them. (Kolkowska and Dhillon, 2013).

A few public organisations in Oman have tried to achieve compliant employee behaviour by enforcing information security instructions and technical obligations. However, this type of enforcement may have a negative effect on employee compliance, as it induces stress, which reduces willingness to comply with the rules (Lee et al.,

2016). Other studies emphasise that cultivating an information security culture can improve employee compliance with security policies (Da Veiga & Martins, 2015b). Therefore, mitigating insider threats in these organisations involves strengthening security behaviour and security culture within the wider human resources and organisational culture. (Chang & Seow, 2014; Chang & Ho, 2006; Lacey, 2010).

There are many unresolved problems associated with ineffective information security in developing countries such as Oman, where the threat posed by organisation insiders continues to be one of the main issues facing public organisations. This research is concerned with studying the critical organisational and socio-cultural factors affecting the development of an information security culture and employee security best practice in Omani public organisations. Thus, the research addresses:

- Ongoing concerns about the lack of information security culture in Omani organisations, leading to ineffective information security.
- The increasing importance and significant investment made by the Omani government in information and communication technology (ICT) in these organisations, indicates a need to investigate information security culture from the perspective of Omani public organisations. Sasse et al. (2007) stated that further investigation is required into how to develop and maintain a healthy security culture in an organisation.

The research explores and analyses the current state of information security practices in Omani public organisations, and helps identify major information security gaps in them.

Figure 1-2: Information Security Vulnerabilities and challenges facing Omani organizations: Source: Self

Figure 1-2 above, illustrates some of the information security vulnerabilities and challenges that might hinder the development of a secure information security culture

in Omani public organisations. The researcher identified these challenges during the research planning and initial literature review phase, together with the researcher's professional experience, that enabled her to visit a number of organisations in Oman and observe their levels of information security. Subsequent results of survey and interview data analysis confirmed most of the sources of information security vulnerability referred to in figure 1-2.

It is worth mentioning that these challenges do not all apply to any single organisation, rather they are an accumulation of challenges across many public organisations, as explained in more detail in chapter two (the related work review chapter) and chapter six (the discussion chapter).

1.4. Research Aim

The main aim of this research is to investigate and explore the current state of information security practices in Omani public and private organisations, and to identify and study the critical socio-cultural and organisational factors that may inhibit the development of an information security culture within organisations, resulting in impairment of employee attitudes and behaviours towards information security discipline. The study also aims to examine the difference between public and private organisations in Oman regarding information security practices and behaviour.

1.5. Research Approach

Employee attitudes toward security requirements and controls are determined several factors, including an individual's knowledge, the attitude and behaviour of colleagues and management, and the way that Information Security Policies (ISP) and procedures are implemented and maintained by any security awareness program in place. Many public organisations in Oman struggle with leakages of data and important work documents. Such incidents have recently increased.

To meet the research aim, the following key steps were undertaken:

1. The researcher conducted a review of related academic work to produce a synthesis of current ideas and research techniques around topics such as: socio-cultural and organisational factors; issues related to employee behaviour and compliance; risk assessment (RA) and risk management (RM); information security controls and countermeasures; social engineering.

2. The researcher investigated the current state of information security practices in Omani public organisations. The researcher identified and discussed the possible socio-cultural and organisational factors that may influence employees' attitudes and behaviours towards information security discipline, and hinder the development of a successful information security culture. The researcher used the data analysis results derived from an applied integrated mixed-methods approach.

    - A quantitative approach, justified by the need for a wide spread survey questionnaire with hypothesis testing. *and*
    - A qualitative approach based on the opinions and perceptions of senior security and IT managers in Omani organisations to assess the level of ISC and practice in their organisations. *and*
    - The researcher's personal observation and professional experience.

3. The survey data was used to compare information security practices in public and private organisations in Oman.

4. The researcher set out a set of recommendations to help cultivate an information security culture within Omani organisations.

1.6. Research Questions and Hypotheses

The following questions were posed to address the research problem, and achieve its aim. (RM= Research Main Question, RS= Research Sub-Question):

RM-Question: What is the current state of information security culture and practices in public and private organisations in the context of Oman? What are the critical socio-cultural and organisational factors that may affect the information security performance and hinder the development and maintenance of an effective information security culture in these organisations?

The research main question was resolved through the following sub-questions, and hypotheses.

RS-Question#1: What is the current level of compliance with information security best practices in Omani organisations? What is the difference between public and private sector organisations in this regard?

RS-Question#2: What are employees' attitudes towards the role of rewards and punishment in motivating personnel to commit to good information security practices in Omani organisations?

RS-Question#3: How does the social factor "education" affect information security performance in Omani organisations?

This sub-question was resolved through the examination of the following hypotheses:

1- Hypotheses related to the organisation's education level factor:

H#1: Education level positively affects information security performance in the Omani organisations.

The following sub-hypotheses are drawn from the previous (H#1) main hypothesis:

H#1.1: Education level is positively associated with information security policy in Omani organisations.

H#1.2: Education level is positively associated with information security training and awareness in Omani organisations.

H#1.3: Education level is positively associated with managerial support for information security in Omani organisations.

H#1.4: Education level is positively associated with employee commitment to information security disciplines in Omani organisations

H#1.5: Education level is positively associated with an organisation's information security practices in Omani organisations.

RS-Question#4*:* What is the relationship between critical organisational factors and information security performance; and the development, and maintenance of an information security culture in Omani organisations?

This sub-question was resolved through the examination of the following hypotheses:

2- Hypotheses related to some critical organisational factors:

H#2: Lack of management support and involvement negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#3: Lack of information security awareness and training negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#4: Lack of information security policy negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

RS-Question#5*:* What is the relationship between the development and maintenance of an information security culture, and information security disciplines and practices in Omani organisations?

This sub-question was answered through the examination of the following hypotheses:

3- Hypotheses related to information security disciplines and practices:

H#5: There is a positive correlation between the information security culture and employee commitment to information security disciplines in Omani organisations.

H#6: There is a positive correlation between the information security culture and information security practices in Omani organisations.

RS-Question#6*:* What is the relationship between critical cultural factors and information security behaviours and practices; and the development, and maintenance of an information security culture in Omani organisations?

This sub-question was answered through the examination of the following hypotheses:

4- Hypotheses related to the critical cultural factors:

H#7: High power distance negatively affects the development and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#8: A high propensity to avoid uncertainty distance negatively affects the development and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#9: High Collectivism distance negatively affects the development and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#10: High Trust negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

1.7. Research Structure

This thesis is organised into seven chapters. Each chapter presents an introduction, major concepts, and a summary, as described below:

Chapter one	This chapter starts by providing background information about the context of the study, and then introduces the research problem, aim, approach, and research questions and hypotheses, followed by an outline of each of the remaining chapters.
Chapter Two	This chapter analyses and reviews the existing academic and research work related to the study. It explores significant issues relevant to information security: information security culture; national culture; organisational culture; information security behaviour and compliance of employees. This chapter also discusses the social and organisational factors that impact employee behaviours related to information security compliance, and addresses the importance of aligning information security with the wider business.
Chapter Three	This chapter discusses the general methods and approaches of the research methodology. The chapter also provides justification for adopting the tool (mixed-methods) and the processes used to collect the data and selected samples, as well as the reliability and validity of the research. The chapter also addresses the ethical considerations related to this study.
Chapter Four	This chapter presents the data analysis and research findings for the statistical quantitative (survey questionnaire) methods phase of the research, and for testing the research hypotheses as part of the research investigation. The quantitative method was conducted to investigate the level of employee compliance with information security best practices in Omani organisations, and to explore the difference between public and private-sector organisations in this regard. In addition, hypotheses were applied

to the analysis of the survey results, to help examine the relationship between organisational factors and information security aspects in Omani organisations.

Chapter Five

This chapter presents the data analysis and research findings from the qualitative (Interviews) method, where data was collected through open-ended semi-structured interviews with fifteen information technology and information security managers from public and private organisations in Oman. The results derived from this method answer the second part of the research question and confirm the result obtained from the quantitative method.

Chapter Six

This chapter discusses and explains the study's results and draws conclusion from the quantitative and qualitative data collection methods. It includes a discussion around the key findings presented in chapters four and five, considering the comparison between public and private organisations regarding information security practices in Oman.

Chapter Seven

This final chapter presents the main conclusions derived from the research and its key achievements. In addition, this chapter summarises the main outcomes of the research, and sets out recommendations to improve the information security culture within Omani organisations. The chapter also includes the main contributions and limitation of the research and closes by suggesting areas for future research on information security culture in Oman.

Chapter 2. Related Work Review

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."
- (Bruce Schneier, 2011, p.9)

2.1. Introduction

This chapter aims to build the theoretical foundation of this study, by presenting a review of the existing academic work related to the research problem introduced in Chapter One, concerning the deficiencies in the information security culture (ISC) and practice in Omani public organisations.

The research problem is addressed by answering the following research questions:

What is the current state of information security culture and practices in public and private organisations in the context of Oman? What are the critical socio-cultural and organisational factors that may affect the information security performance and hinder the development and maintenance of an effective information security culture in these organisations?

Research into the information security culture existing in Omani public organisations is largely lacking. Consequently, this overview of the field of research deals broadly with some relevant characteristics of the Arab world in general and Oman in particular, as well as considering related research work which emphasises the social, cultural and organisational aspects of information security.

The chapter is in two main parts. The first part reviews earlier research studies that formulated an understanding of the elements and concepts that are fundamental to the issues around security of information. These include: vulnerabilities arising from human factors, both within and outside an organisation (Insider and social engineering); information security in public and private organisations; risk assessment and risk management; information security controls and countermeasures. This literature review helps to locate the current study within previous and ongoing research in the field.

The second part discusses the socio-cultural and organisational factors that are relevant to the thesis, and identified in the diagram 2.1 on the next page. They include: the support of senior top management; a culture of information security; a clear information security policy; information security training and awareness; power distance; uncertainty avoidance; collectivism level; trust and reward; and punishment sanctions for non-compliance. These variables emerge in the quantitative and qualitative data

analysis in Chapter Three of this dissertation. Each of these variables in the diagram also derive from the academic literature in this field. This provides a useful theoretical perspective to underpin the research problem introduced in Chapter One.

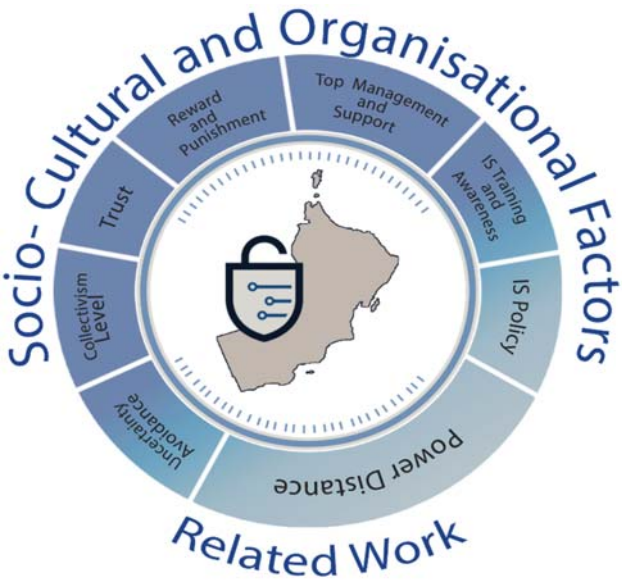

Figure 2-1: Research Interests Related Work. Source: Self

The review of the related work that is relevant to this study facilitated an understanding of the topics relevant to this study, identified the relationships that exist between those topics, and ensured that the thesis is firmly rooted in the knowledge and insights of other researchers. Leedy (2005) indicates that the related work review serves to support the discovery of issues and variables that are critical to the study and provides a general background of previous studies that are relevant to issues related to the study in question as well as acting as a foundation for explaining the results of the study.

The following sections briefly discuss part one topics, starting with an introduction to information and information security.

2.2. Information and Information Security

Information, knowledge, and information security play an important role in people's lives and they are indispensable to ensuring the effectiveness of organisations. An organisation needs people who have adequate information and knowledge to run its business. People use information to make decisions, knowledge to create new insight, and information security to protect information assets. Any lack of information, knowledge, and information security will jeopardise an organisation and have a negative impact on organisational effectiveness.

2.2.1. The Importance of Information Security

In the current knowledge-based economy, information is more powerful and valuable than it has been in the past, as it is essential for daily business operations. Nevertheless, accessing this information and its associated resources has become easier due to developments in distributed processing and advanced technology, which means the various tasks performed by an organisation's staff, and the critical work and personal information stored on computer, must be secured (Mindful.com, 2009). Public and private organisations rely on this advanced technology to conduct business and cannot afford disruptions in their operations. Their information may be compromised or breached by unauthorized persons if not adequately protected and secured. Furthermore, recovery from a breach of information takes many years and the financial damage is significant (Ponemon Institute, 2014). These breaches and data loss incidents are becoming unavoidable for organisations of all types and sizes. Therefore, public organisations need to be confident that their information assets are safely and securely stored, processed, transmitted, and destroyed, whether they are managed within the organisation or by delivery partners and suppliers.

Although information security is important for protecting organisation and individual information against accidental or deliberate modification, and against unauthorized disclosure for legal and competitive reasons, determining the factors that contribute to information insecurity is challenging and complex. People and organisations responsible for critical assets and business survivability have used different terms to refer to the activity of protecting an organisation's critical assets (Torres et al., 2006). A desirable level of information protection against threats involves establishing, as a high priority, an information security program that addresses the risks that organisations face. This will mitigate business risks and protect information assets. The definition of information security discussed further in the next section.

2.2.2. Information Security Definition

Information security traditionally aims to provide appropriate and effective tools and mechanisms to protect the confidentiality, integrity, and availability of information and systems, which may be vital to protect an organisation's operations from unauthorized access and attacks. (da Veiga et al., 2007; Tipton & Krause, 2009; Andress, 2014; Pieters, 2011; Kruger & Kearney, 2006, Peltier et al., 2005; Avizienis et al., 2004; Cherdantseva & Hilton, 2012; ISACA, 2012).

The mnemonic CIA (Confidentiality, Integrity, Availability) is used to summarise these elements, and they are frequently referred to as "the CIA triangle". According to

Whitman and Mattord (2012), the computer security industry originally developed the concept of the CIA triangle and it has been used since the development of the mainframe.

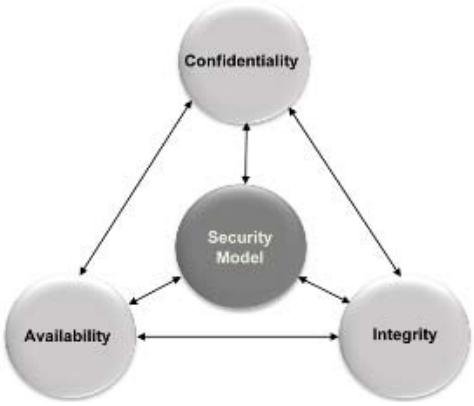

Figure 2-2: Information Security Elements (CIA Triangle). Source: Marzigliano, 2013

Confidentiality refers to preventing the unauthorized disclosure of information. Humphreys et al. (1998, p8) stated that ensuring confidentiality involves "protecting sensitive information from unauthorized disclosure or intelligible interception". Thompson and von Solms (2003) mention that confidentiality of information may be preserved by applying one of two approaches: either restricting access to confidential information or encrypting sensitive business information. Confidentiality is also referred to as secrecy. (Krige, 1999; Bruce & Dempsey, 1997).

Integrity is the ability to guarantee the accuracy and consistency of data and information throughout its entire life cycle, such that management can be assured that the information on which decisions are based has not been modified dishonestly by unauthorised parties or in an unauthorised way. (Krige, 1999; Bruce & Dempsey, 1997; Ritchie & Brindley, 2001).

Availability, according to Afyouni (2006), and Whitman and Mattord (2008), means that the system should be accessible to those who are authorized to access it, such that they can reach the required information at the right time. According to Gerber and von Solms (2001), ensuring the availability of information is important because without timely information, an organisation would be incapable of continuing normal operations.

Alves et al. (2006) argue that it is not always necessary to combine these three elements to reach an acceptable information security level. For example, it is necessary to guarantee the availability and integrity of information that is classified as public, whereas confidentiality is not required. Although there is no hierarchy for the importance of these three elements, the importance of each depends on the context within which it is applied (Tettero, 2000).

On the other hand, some information security experts argue that the information security triangle is not sufficient to provide a foundation for information security. Anderson (2001) asserts that information security includes more elements than those of the CIA triangle. He suggested a multidimensional approach to information security, arguing that people, and institutional and economic factors are no less important than technological factors.

Likewise, Parker (1998) and Whitman and Mattord (2012) state that the scope of information security extends beyond the CIA triangle which is no longer adequate for a complex interconnected environment. Consequently, Donn Parker proposes an alternative information security model to the classic CIA triad in 2002, which he calls the Six Atomic Elements or the Parkerian Hexad. It consists of six foundational elements: Confidentiality, Possession, Integrity, Authenticity, Availability, and Utility.

Figure 2-3: The Information Security elements; Parkerian Hexad. Model. Source: Mrzigliano, 2013

This study adds the following three secondary attributes to support the CIA and strengthen the security of organisational assets:

Accountability: This refers to the level of availability of the identity of a person who performs an operation, such as storing an entry in a database, and the integrity of that person. In other words, the identity should be known and available if needed.

Authenticity: This is the integrity of a message and the metadata related to it, such as the origin. It is a way to ensure that data, systems, communication processes, and information are genuine. Authenticity is also responsible for validating that both parties involved in a communication process are who they claim to be.

Nonrepudiation: This means that a party within a communication process cannot deny having received specific information, and the other party cannot deny having provided specific information.

According to Hagen et al. (2008) and Reinhardt (2007), information security also includes several other elements, such as legal aspects, best practice applications,

technology, institutionalisation elements, and security technologies. For McDaniel (1994); Ferrari and Thuraisingham (2006); and Merkow and Breithaupt (2006), information security includes the concepts, techniques, technological measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use. Furthermore, Pfleeger (1997); Von Solms and Eloff (2004); Doherty and Fulford (2006); and Von Solms (1999, 2005) define information security in terms of the following five security services: identification and authentication; authorisation; confidentiality; integrity; and non-repudiation. These services are required to ensure that information is protected and secured at all times during transmission or usage. Heiser (2004) views information security as an operational risk that is growing in importance, but managed in an immature way. Moreover, Whitman and Mattord (2012, 2009) describe information security as "the protection of information and the systems and hardware that use, store, and transmit that information" (Whitman and Mattord, 2012, p.588, 2009, p.8).

Anderson (2003) states that information security provides a well-informed sense of assurance that information risks and controls are in balance. The primary assumption behind Anderson's definition is that information security is about one's perception of information security, as reflected in the use of the terms "assurance" and "balance". These terms imply a sense of the state of being rather than absolute knowledge of the state of information security. In the business context, the (ISO 17799) standard defines information security as the protection of information assets from a wide range of threats, ensuring business continuity, minimizing business risk, and maximizing return on investments and business opportunities.

The term "information security" originally referred to a technique, but its meaning has expanded over time to a business orientation in organisational contexts (Anderson, 2003), and a comprehensive social–technique–philosophy view. (Zafar & Clark, 2009). Since organisations brought technology into business environments in the 1960s and 1970s, information security in the industry of IT has evolved, and agencies needed better information security to protect their assets. (Bennett, 2009). Organisational information security now faces a higher risk of identity theft, stolen passwords, fraudulent emails, and inadequate network practices. (Mensch & Wilki, 2011).

Solutions based only on technology are not sufficient to guarantee the protection of organisational assets. Information security involves human beings who do not always

act as they are supposed to while interacting with information systems. (Aytes & Connolly, 2004). Therefore, understanding which factors motivate users to adopt security practices is fundamental to solving problems of information security. (Bulgurcu et al., 2010). Social rules and interactions in the workplace influence an individual's understanding of information security. (Albrechtsen, 2007).

The security of information has been an area of great concern and its importance has intensified exponentially. However, information security arrangements must achieve a balance by allowing reasonable access while providing protection against threats. (Whitman & Mattord, 2009). Potential security risks can also come in different forms, both externally and within organisations. The next section presents an overview of the sources and classification of information security threats.

2.3. Information Security Threat Sources

According to Howard (1997) and Benson (2000), there are two sources of security threats; from natural disasters (e.g. floods, fire, and earthquake) and human threats. Other researchers have also included physical risks (e.g. power failure, network failure, hard/software failure). Most researchers see the threats from human behaviour as having a strong impact on the success or failure of an organisation's efforts to secure and protect their businesses, services, systems, and information. (Orshesky, 2003).

Human threats may be malicious or non-malicious. Malicious threats consist of inside attacks by dissatisfied or malicious employees, and outside attacks committed by non-employees who are looking to harm and disrupt an organisation. (MS TechNet library, 2009). Non-malicious threats arise from the ignorance of employees or users, such as data entry clerks, system operators, and programmers who make unintentional errors that directly and indirectly contribute to security problems. Sometimes the errors caused by ignorant or careless employees are threats that can create vulnerabilities. In fact, researchers have found that one of the top threats to information security is errors committed by employees. (Von Solms et.al 2004; Whitman & Mattord, 2005).

Figure 2-5 in the next page, illustrates risky human behaviours that are Malicious, Negligent or Accidental.

Malicious behaviours require a motive to harm and a conscious decision to act inappropriately. Such acts include leaking confidential information, sabotaging networks, and using work privileges for personal benefits. Employees who cause

damage use their knowledge and access to information resources for a range of motives, including greed, political protest, terrorism, revenge for perceived grievances, and resolution of personal or professional problems. These acts maybe performed to challenge their skills, express anger, impress others, or a combination of these. (Elliot, 2011; Sakar, 2010; Shaw et al. 1998).

Malicious motivations are illustrated in Figure 2-4 below.

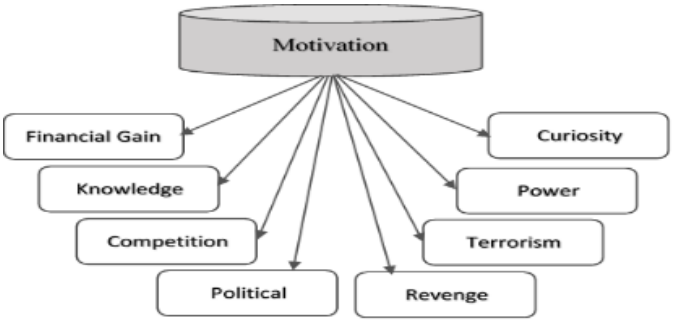

Figure 2-4: Information Security Malicious Motivations.
Source: Sakar, 2010

Negligent behaviour does not involve a motive to harm, but it does involve a conscious decision to act inappropriately. The act is usually well intentioned (e.g. using unauthorised services or devices to save time, increase productivity, or enable flexible working), and the behaviour often includes the knowledge that the action is bypassing a control or circumventing a policy. Despite the lack of malicious intent, negligent insiders knowingly accept a risk that is outside their organisation's risk acceptance.

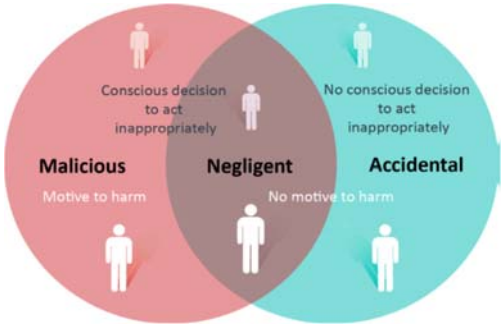

Figure 2-5: Information Security Threats Sources. Source: ISF, 2014

Accidental behaviour involves no motive to harm and no conscious decision to act inappropriately. Emailing information to the wrong people, opening malicious attachments, and publishing private data on public servers can all happen accidentally. The first time an employee behaves in this way can be considered accidental; however, repeated accidental behaviour may be considered negligent.

It is obvious that humans play a significant role in information security and that security controls must work in a variety of environments and be designed, and implemented with

human behaviour in mind. Unfortunately, most of the above-mentioned behaviour types are present in Omani public organisations, and most probably, in many organisations around the world. The next section explores human factor vulnerabilities.

2.3.1. Human Factor Vulnerability

Technology is often falsely perceived as the immediate answer to information security problems. (Hinson, 2003). However, several researchers have acknowledged that the human factor plays a significant role in information security. (Parker, 1998, 1999; Siponen, 2000, 2001; Alnatheer, 2012; Schultz, 2005). Dutta and Roy (2008, p.352) argue that "Information security has been understood as a technical subject and that only recently has it been recognized that information security involves a complex interaction between technical, organisational and behavioural factors".

In his research on data security problems, Alagar (1986) argues that security is a human problem because human decisions and interventions are most significant in information security. Trcek et al. (2007) mention that technology alone cannot provide appropriate levels of information safety. In addition, Vroom and Von Solms (2004) state that employee behaviour is critical to any organisation. Further, Kankanhalli, and Xu (2009) explain that technological control is necessary to assure information security, but this security also depends on an individual's security behaviour.

Almost all information security solutions rely on the human element, while employees continue to be the most severe threats to organisational information security. (Mitnick & Simon, 2002; Berti & Rogers, 2004). Therefore, information security should involve more than implementing an assortment of technical controls; it should also address the behaviour and resulting actions of employees, (Berti & Rogers, 2004) since the human factor issue is often referred to as the weakest link of a security chain. (Angel, 1993).

Many researchers have shown that technological solutions are not sufficient to control human threats, but that changing the security culture and increasing awareness is necessary. (Flynn et al., 2014; Shamir, 2011). The following sub sections discuss insiders and their threats to information assets of an organisation.

2.3.1.1. Insiders and Insider Threats

Evidence suggests that more information security incidents occur from internal employee actions (Richardson, 2008) than from external individuals. An insider can be defined as "anyone with knowledge of operations or security systems and who has unescorted access to facilities or security interests". (Biringer et al., 2007, p.55). It can

also be anyone who has access to the organisation's information systems and networks, such as employees, contractors, and consultants (Butavicius et al., 2012). Insiders may also include third-party business partners and their employees, temporary help (Schultz, 2002), and supervisors and managers. Insiders also include previous employees who have had access to the network and systems. (DHS, 2014).

Insiders can be more dangerous than people outside an organisation because of their intimate knowledge of organisational information systems and access to data during their routine work activities. (Herath & Rao, 2009a, 2009b; Bulgurcu et al., 2010; Johnston & Warkentin, 2010; and Siponen & Vance, 2010). Their actions or ignorance can potentially lead to incidents ranging in severity from lost staff hours to negative publicity and financial damage such that the organisation may not survive. (Kowalski et al., 2008). Therefore, "insiders should be monitored closely because they have exceptional access to data". (Magnuson & Sicard, 2015, p.10). Insider threats have become a common trend targeting private and public organisations for reasons such as financial gains, IT sabotage, business advantage, or industrial espionage. (Barrios, 2013).

The problem of insider threats is viewed as one of the most difficult problems to address, as motivations differ between organisations as well as between countries. This further complicates the problem of insider threats as it becomes difficult to address the source of a threat completely. Although some researches emphasise that internal threats are more pressing than external threats (Leach, 2003), not every organisation considers their employees a serious source of threats. Humans are often afraid of the unknown and do not usually suspect colleagues as potential criminals. For example, people fear hackers and usually do not fear people who they know well such as IT support people, which can make them react inappropriately when dealing with information security issues. (McIlwraith, 2006). Liu et al. (2009) report that organisations are struggling with how to protect information that must be shared with insiders to perform business processes.

Most organisations in Oman rely on log monitoring tools and traditional access control mechanisms to combat insider threats, and these techniques cannot withstand emerging insider threats that are becoming highly sophisticated. A root cause of the insider threat issue in Omani organisations stems from the fact that these organisations do not seem to have adequate non-technical security defences in place to detect and prevent insider attacks. In addition, most employees have access to valuable information assets, which encourages them to abuse this privileged access intentionally or unintentionally by causing data and information leaks.

Having defined insider threats, it is necessary to discuss the categories of this type of threat, and the actions that the individuals in these categories carry out. Sarkar (2010) categorises insiders as: pure insiders; insider associates; insider affiliates, and outside affiliates.

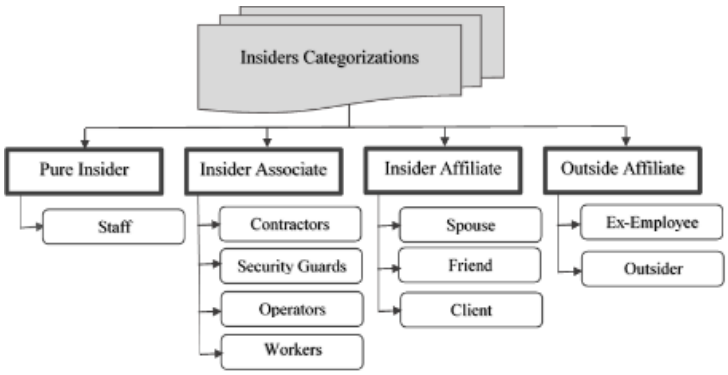

Figure 2-6: The Insiders Categories. Source: Sakar, 2010

Pure insiders are full-time and part-time employees with necessary privileges such as, keys, access cards, and network logons made available to them to perform their job functions. (Sarkar, 2010). Employees pose the greatest risk to organisations in terms of access and potential damage to sensitive and private information. As inspected members, employees are trusted and expected to be interested in the productivity and success of their organisation. After recruitment, employees are considered 'members of the family' and are often the last to be suspected when systems malfunction or fail. (Shaw et al., 1998).

Insider associates are often third-party personnel, such as contractors, partners, consultants, cleaners, security guards, and suppliers with limited authorised access, a facility, employees' desks and bins and restricted access to networks. They may find sensitive information and documents on desks, such as usernames and passwords left on bits of paper, under keyboards, and stuck on monitors, or they may plant key logging devices to retrieve sensitive information.

Insider affiliates are often the spouse, friend, or client of an employee with no direct access privilege, but who can use the credentials of the employee to gain access. This type of insider can be a client who enters the building and wanders around the facility or a malicious imposter pretending to be an employee. It can be a spouse borrowing the office laptop to access the Internet, or who is provided with access details such as a username, password, or access card to collect papers from the office.

Outside affiliates, are outside threats from external intruders who are referred to as hackers or attackers and who are not registered as individual users. They may gain access to the organisation's network through open access such as a wireless access that is unprotected, or impersonate or copy the credentials of authorised employees. These

attackers no longer only attempt to exploit vulnerabilities in systems or applications; they also attempt to exploit vulnerabilities in the behaviours of employees.

A common way to exploit human vulnerabilities is to deceive and manipulate employees to perform actions that benefit the attackers. This type of information security threat that relies on the psychological manipulation of humans is called social engineering. The next sub section briefly discusses social engineering as an example of an outside threat that uses an organisation's employees to gather information that can be used to harm the organisation.

2.3.1.2. Social Engineering

Social engineering (SE) is a term used to describe how one person persuades another person to give him information. In the context of information security, social engineering is effective as it can utilise strategies that bypass computer security technology. (Schneier, 2000). According to Mouton et. al. (2016) and Espinhara and Albuquerque (2013), the art of influencing people to divulge sensitive and confidential information is known as social engineering and the process of doing this is known as a social engineering attack. Social engineering is predominantly concerned with finding and exploiting vulnerabilities, and in most organisations, the most vulnerable element is the employees. (Schneier, 2000).

There are various definitions of social engineering, and the most popular definition is by Kevin Mitnick. In his book 'The Art of Deception', he defines social engineering as using influence and persuasion to deceive people and take advantage of their misplaced trust in order to obtain insider information. (Mitnick, 2002). Another popular definition provided by Harl (1997) states that: Social engineering is the art and science of getting people to comply with your wishes. It is not a way of mind control, it will not allow you to get people to perform tasks wildly outside of their normal behaviour and it is far from fool proof. (Harl, 1997). Samani & McFarland (2015, p.6) define social engineering as "The deliberate application of deceitful techniques designed to manipulate someone into divulging information or performing actions that may result in the release of that information".

Cialdini (1984) identifies several different 'relational cues' that are used for persuasion, including reciprocity, scarcity, commitment, consistency, liking authority, and social validation. Hadnagy (2010, p37) defines social engineering as "The act of manipulating a person to take an action that may or may not be in the target's best interest. This may

include obtaining information, gaining access, or getting the target to take certain action". According to Mitnick and Simon (2001), social engineering exploits human behaviour idiosyncrasies to form an attack from the outside that leads them to gain inconspicuous entry into protected areas of the organisation for their own illicit use. According to Sood (2014) and Granger (2001), social engineering involves techniques for manipulating the system user's psychology by exploiting trust, and often exploiting a user's poor understanding of technology. System users may be unable to determine or fail to understand the attack patterns used in targeted attacks. Mouton et al. (2014, p269) define social engineering as "the science of using social interaction to persuade an individual or an organisation to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity" (Mouton et al., 2014, p.269).

Social Engineering attacks are challenging to counter since they depend on human behaviour and involve taking advantage of vulnerable employees. At the same time, social engineering is also a major concern for organisations due to its effective results in compromising systems by exploiting users. (Newbould & Furnell, 2009). This may cause a major breach through which the social engineer can have complete control of the system, allowing privilege escalation or launching a denial of service attack. (Liu & Cheng, 2009). The victims often do not notice during and after the execution that they are victims of a social engineering attack, which makes social engineering attacks dangerous and challenging to manage. Mitnick and Simon (2005) believe that social engineering attacks are difficult to detect and almost impossible to defend against.
They classify social engineering attacks into three main categories: direct requests, contrived situations, and personal persuasion.

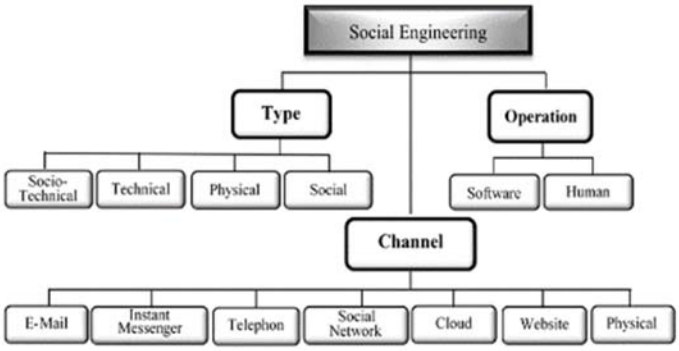

Figure 2-7: Social Engineering Types, Operation and Channel of Attacks .
Source: Sakar, 2010

Social engineering techniques often rely on a medium to attack human weaknesses. The medium could be direct interactions such as face-to-face interviews, telephone communication, or indirect interactions through letters, or using information and

communication technology (ICT) such as sending phishing e-mails, and exploitation through the digital domain (Mohebzada et al., 2012; Workman, 2008; Parrish et al., 2009; Vishwanath et al., 2011; Darwish et al., 2012). Other means include social media, websites and unidirectional interactions such as leaving a USB or CD on the ground and waiting the victim to pick it up (Krombholz et al., 2015 and Mouton et al., 2016).

Impersonation and false authorisation are considered the most suitable techniques for deceiving people. (Hanan et al., 2009). According to Mitnick and Simon (2002), impersonation is pretending to be eager for information or help through the telephone, email, or instant messages. The hacker deceives the victims in this scenario by requesting urgent help to solve a specific issue while useful information is leaked during the conversation. As in other parts of the world social engineering is very active in the Arab world including Oman, but most attackers target individuals through social media by blackmailing the victims for financial purposes.

To protect information from social engineering attacks, organisations must utilize a combination of technology solutions and user awareness. (Dimensional Research, 2011). Thus, employees must be aware of potential attacks and learn the appropriate tools for reducing their chances of becoming targets and victims. Further social engineering attacks can be reduced using security defence measures to fix the human weaknesses and decrease the risk. The awareness function also includes efforts to integrate up-to-date policy compliance and enforcement feedback as well as current threat information, to make the awareness information as topical and realistic as possible.

The next two sections provide a brief description of risk assessment and risk management.

2.4. Risk Assessment

The objective of risk assessment (RA) is to support organisations with assessing their risk and help them make decisions regarding strategies for coping with those risks. It is primarily an exercise in measurement. Risk assessment typically requires data about the current impact of risk and potential loss in the organisation, and the likelihood or probability of a risk event actually occurring.

Organisations should carry out an information security risk assessment that allows them to ‘know themselves’ with respect to their risk exposures. Each part in a project or system may have a different set of risks to which it is exposed, or a different perspective

on risks and alternative actions. (Burke, 1999; Sherwood, 2000; Wood, 1995). Many authors raise this point including Karyda et al. (2005), the IT Governance Institute (2007), Im and Baskerville (2005), and the ISO 27001 standard.

In addition, Lund et al. (2011), classify risk assessment approaches into two main categories: offensive approaches and defensive approaches. Offensive approaches refer to risk assessment that is concerned with balancing potential gain against the risk of investment loss. This kind of analysis is most relevant to finance and political strategy making. Defensive approaches include risk assessment that is concerned with protecting existing assets. An organisation without a risk assessment process cannot identify or measure their risks, and their level of exposure will remain uncertain.

According to Syalim et al. (2009) and Stephenson (2004), risk assessment is a complex process that is generally composed of four steps: threat identification, vulnerability identification, risk determination, and control recommendation.

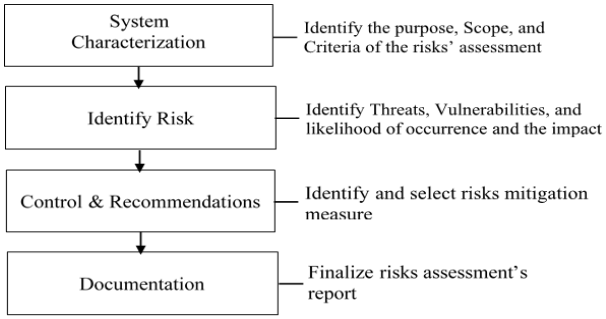

Figure 2-8: Information Security Risk Assessment Process.
Source: Syalim, et al., 2009; Stephenson, 2004

Shedden et al. (2010) argued that risk assessment in the information security domain is often performed by people who have sufficient knowledge in information security or risk management. Such knowledge would ensure that the controls and expenditures needed to implement and support these controls are commensurate to the risk to which an organisation's assets are exposed. This way of risk assessment not only allows the organisation to provide an appropriate level of security, but also helps determine the acceptable level of risk that the organisation is willing to accept based on the effort or expenditure involved in the application of the control or safeguard. Organisations are ultimately responsible for that level of risk management, which enables them to successfully manage all the risks affecting their information assets. (Stoneburner et al., 2002; Gerber & Von Solms, 2005; Farahmand et al., 2005).

In Oman and in most Arab countries, organisations lack risk assessment in regards to information security, and that explains the continuous high level of information security threats and vulnerabilities in these organisations. Although risk management is common

to most organisations, risk assessment is only undertaken intermittently. The following section explains Information security risk management.

2.5. Risk Management

The main goal of risk management is to help organisations manage the particular risks associated with their operations. Using risk management, organisations can reduce the losses that might result from security problems. (Dubojs et al., 2010). Risk management is a process that aims to achieve an efficient balance between realising opportunities for gains and minimising vulnerabilities and losses. Since information security incidents are a form of adverse events that may cause losses for organisations (Blakleyetal., 2002), information security is a risk management discipline. (Blakley et al., 2002; Spears, 2005). Enterprise risk management, in this context, is a process systematically applied across an entire organisation to manage risks, from all sources, that may affect the ability of the organisation to execute its strategy and conduct operations effectively and efficiently. Business The management of a business is ultimately responsible for a risk management strategy that should enable them to manage successfully all the risks affecting their organisation's information assets. (Stoneburner et al., 2002; Gerber & Von Solms, 2005; Farahmand et al., 2005). While the information security department may manage the risk management program, it is necessary for them to consult organisational leadership about handling complex risks that cannot be easily reduced or mitigated.

Within Arab countries, including Oman, there are particular challenges facing the implementation of successful information security risk management (ISRM). Information risk managers may face challenges in supporting their organisation and boards of directors to meet corporate governance obligations in full. This may require fundamental changes to the risk management structure within which they are working. In addition, a lack of employee information security awareness and education in processes and procedures means there is a higher risk that an employee will make an intentional or unintentional error that causes a continuous information security violation and leads to ISRM failure.

To manage and control such information security risk, organisations need to apply different types of countermeasures. The next section briefly explains information security risk controls and countermeasures.

2.6. Information Security Controls and Countermeasures

Controls, safeguards, and countermeasures are terms that describe mechanisms used for information protection. (Whitman & Mattord, 2008). These may avoid, reduce, or mitigate risks related to information security. According to Schneier (2000), countermeasures to reduce risk and vulnerability consist of three mutually dependent elements: protection, detection, and reaction. Since protection cannot be guaranteed, a greater emphasis should be placed on detection and reaction to increase the chance that an organisation will know when a security breach has occurred, such that actions can then be taken to address the threat (Schneier, 2000).

A security countermeasure is defined by Harris (2013, p.98) as "a control, measure, technique or procedure that is put in place to prevent a threat agent from exploiting a vulnerability". He provides examples of security countermeasures including strong password management, firewalls, access control mechanisms, encryption, and security-awareness and education. Such countermeasures can be categorised by type (i.e. administrative, logical, or physical). According to Whitman and Mattord (2008), there are three general categories of countermeasures: policies, programs, and technical countermeasures. Some researchers such as Schultz et al. (2001) consider security countermeasures as only technology and procedural. Others state that informal norms have a serious impact on employee information security behaviour and that it is possible to formalise norms to reduce internal threats. (Frank et al, 1991; Da Veiga & Eloff, 2010).

This study agrees with the related research literature regarding the importance of countermeasure to protect organisation assets from any security threats. Omani public organisations are similar to any other organisations in their need to apply information security countermeasures to protect their information assets from insider adverse behaviours. Beside technological countermeasures, this thesis identifies other non-technical countermeasures to help organisations mitigate any risks to which their information might exposed. These include:

- Organisations must commit to protect their valuable information assets, and create a culture of valuing and protecting information through:
    - Strong management leadership and commitment.
    - Responsibility of everyone for protecting information.
- They must focus on the human aspects and implement emphasis awareness, and training programs.

- Organisations must improve visibility within the organisation and focus on incident detection and response.
- They must share threat intelligence with other organisations within the same sector and with other national organisations.
- Organisations must adhere to the policies and standards published by regulators and other entities.

Most public and private organisations have some form of controls in place to manage information security. However, the effectiveness of such controls is determined by how well they are organised and monitored. Many organisations introduce security controls randomly. Such random security controls will only address certain aspects of IT or data security, and can leave valuable non-IT information assets such as paperwork and proprietary knowledge less protected and vulnerable. The next section gives a brief introduction to public and private organisations.

2.7. Public and Private Organisations

Many people believe that there are not many differences between public and private organisations regarding information security, while others disagree. Before proceeding further, it is important to define these two types of organisations. Public organisations are engaged providing government goods and services to the public, such as education, health, and social services. They are fully owned, controlled and run by the government, while, private organisations are not owned by or part of the government.

Much related work has been published on this topic by Caudle et al. (1991); Fryer et al. (2007); and Joia (2003), and several characteristics have been identified. For many decades, organisation theory has identified differences between public and private sectors. Most studies in this field focus on specific variables to differentiate between these two sectors. (e.g. Ring & Perry, 1985; Perry & Rainey, 1988; Nutt, 1993; Scott & Falcone, 1998). However, few have tried to describe the sectors from a global and integrated perspective (Perry & Rainey, 1988; Rainey & Bozeman, 2000; Boyne, 2002).

Hvidman and Andersen (2013) study of public and private organisations concluded that three dimensions are theoretically important.

The first dimension is their ownership. (Rainey et al., 1976). Public organisations are owned by the government and their ownership rights cannot be easily transferred among entities (individuals or organisations), which gives rise to diffused risks. On the other

hand, private firms are subject to clear risks, as they are owned by entrepreneurs or private individuals (shareholders) who can easily transfer their property rights.

The second dimension is funding; public organisations are largely funded by taxes, rather than fees paid directly by customers. (Niskanen, 1971; Walmsley & Zald, 1973) There is no link between resource generation and resource consumption. This link is present in private organisations, which are funded by the prices of the goods they deliver to the market.

Finally, the third dimension is control. Public-sector organisations are controlled predominantly by political agencies or multiple stakeholders (e.g. politicians and bureaucrats) at different levels of a politically constituted hierarchy in which control is mainly executed through rules and directives, and not market forces. In other words, the primary constraints are imposed by the political system rather than the economic system. (Dahl & Lindblom, 1953). In contrast, private organisations are controlled by the market through selling goods and receiving sales revenues.

Beside the above-mentioned dimensions, the researcher states a fourth dimension, that of the organisational culture. This performs two critical functions in organisations: it integrates members such that they know how to relate to one another, and it helps organisations adapt to the external environment. (Daft, 2001).

Organisational cultures are embedded in, and shaped by, national cultures. Unlike private organisations, public organisations cannot readily change their operational norms, which might lead to shaping or reshaping people's behaviour or patterns of consumption. Thus, traditional organisational cultures in the public sector are likely to impede public service modernization and innovation. (O'Donnell & Boyle, 2008). Hooijberg and Choi (2001) argue that new leaders and managers can emerge in the private sector in response to the situation or environment, but this is difficult for public sector leadership and managers. Laws, rules, and oversight activities remove more discretion from leaders in the public sector than from leaders in the private sector. In fact, public-sector leaders have less autonomy in exercising leadership than private sector managers. (Hooijberg & Choi, 2001).

A number of public and private organisations have set up guidelines or procedures, to help them protect the organisation's assets. However, these guidelines are generic in scope and thus unable to ensure an adequate level of security is maintained, that resources are used in the right way, or that the best security practices are adopted in the organisation. There is a digital divide in information security between organisations,

with regard to levels of information security skills and knowledge, perceptions of information security, social norms, and interpersonal relationships, any or all of which can result in differences in information security performance between organisations. The next section briefly explains some facts about the digital divide

2.8. The Digital Divide and Information Security in Arab Countries

The digital divide (DD) is a term used to describe the growing gap between those who have access to, and the skills to use, information and communication technology (ICT) and those who have limited or no access, for socio-economic and geographical reasons. The digital divide and information security have mutual effects on each other. Many scholars have shown that digital literacy affects the security divide. For example, Norris (2001) describes a consequence of the urgent need for a society to purchase increasingly complex computer equipment to avoid being 'off-line', and ignoring the implications, responsibilities and learning processes imposed by the technology. Similarly, Ghernaouti-Helie (2008) stresses the need to ensure that the digital divide is not exaggerated by a security divide.

The ICT infrastructures deployed in developing countries are inadequate. If developing countries are to have the advantages of an information society at the same level as developed countries, they should integrate their security needs at the same time as they develop their ICT infrastructure. The rapid growth of information technologies may leave those newly entering information societies unaware of the full social and technological implications, further widening the information security divide.

Addressing the digital divide in information security within Arab organisations requires not only technological solutions or access to information systems which incorporate adequate information security technology, but also requires a consideration of skill and knowledge differences as well as the nature of responsibilities, perceptions, and interpersonal relationships between the various members of an organisation. From this perspective, several digital divides may exist within information security related to age, gender, IT experience, education, or occupation. Warschauer (2002) states that the digital divide is about physical access to computers and connectivity, as well as people's ability to use the systems. Jung et al. (2001), Harittai, (2002), and DiMaggio et al. (2004) argue that the question of unequal access must be expanded to address people's skills, scope of use, autonomy, and ability to maximise the utility of the technology to achieve their goals.

Oman is working towards bridging the digital and security divide by involving the entire community as partners in its mission towards creating a secure digital society. Efforts are underway to raise IT and security literacy levels through formal training and the inclusion of certified IT and security qualifications, especially in the public sector. Nevertheless, regardless of the training programs that have been delivered or the security technology tools that have been implemented in Oman public organisations, information security still faces the risk of security breaches due to weak ISC and lack of organisational and national information security strategies.

This completes the first part of this chapter dealing with the general aspects of information security. The following second part of this chapter focuses on the critical socio-cultural and organisational factors that are related directly to the research question. Related work in this field shows that aspects of culture, lack of management support, lack of information security policies and guidelines, and lack of awareness and training programs, all hinder an effective information security culture. (Casmir & Yngström, 2005).
The following sections briefly explain the topics that form the second part of this chapter, starting by exploring the influence of socio-cultural factors.

2.9. The Influence of Socio-Cultural Factors on Information Security

The impact of social influences on individual behaviours and beliefs has been widely acknowledged. (Cialdini & Goldstein, 2004; Leenders, 2002). Social influences are often referred to as subjective norms. (Ajzen, 1991) these can take the form of introjection motivation. (Gagné & Deci, 2005). For instance, in the theory of planned behaviour (TPB) as posited in (Ajzen, 1991), subjective norms refer to the end users' beliefs about the normative expectations and social pressures that are expected to determine intentions and behaviours in a security context. Similarly, self-determination theory (SDT) suggests that people complying with security requirements under introjection processes are driven to perform actions to maintain their ego, which is itself associated with the surrounding social climate. (Gagné & Deci 2005).

A study by Ifinedo (2014) discloses that social bonds have a positive, though indirect effect on employee security behaviour through social pressure. People generally follow group norms. Therefore, if information security is considered an important and serious problem within the group, then it is more likely that the individuals within that group will value and follow the security policies and procedures that are used by their organisation. Conversely, if risk taking is accepted within the group, then it is likely

that greater risks will be taken. Drawing on the notion of social control and social bond theory (Hirschi (1969), Cheng et al. (2013) investigate the influence of informal controls on security policy violations, and conclude that social pressure has a significant impact on employees' intentions to violate security policy, suggesting that expectations of immediate supervisors are important determinants of employee security behaviour.

A social effect known as the *bystander* effect could also influence the way people respond to or perceive risks. This effect is based on the idea that people will shift their responsibility as the number of people present increases, such that the likelihood of any one person responding decreases. In large groups, individuals may feel less personal responsibility for security. These social and group factors are strongly related to organisational culture, although social bonds, including attachment, commitment, involvement, and belief, have mixed influences on security violation intentions. Cheng et al. (2013) stress that managers should aim to strengthen the relationships between employees and an organisation in a number of ways, including offering employees a sense of achievement and satisfaction, to enhance their loyalty to the organisation.

Figure 2-9 bellow, illustrates some critical socio-cultural factors that have a direct influence on information security culture and compliance.

Figure 2-9: Research Related Work: Critical Socio-Cultural factors. Source: Self

The following sections explain in more detail the critical socio-cultural factors that are highlighted in figure 2.9 above that are believed to have an impact on information security culture development and practices in Omani public organisations.

First the study briefly explains the different types of culture.

2.10. Culture

The concept of culture has a number of different meanings which include: collectively shared forms of ideas and cognition; symbols and meanings; values and ideologies; rules and norms; emotions and expressiveness; the collective unconscious; behaviour patterns, and structures and practices. (Alvesson, 2002). Scholars share no precise agreement on what is meant by the term culture because of its complexity, importance, and strong influence on social science and management studies. The term is frequently used in everyday language to explain several different concepts; sometimes to explain concepts such as societal culture or organisational culture, as well as artistc culture. (Dahl, 2004). Culture has been studied for over a hundred years in various disciplines and, as Straub et al. (2002, p.14) state, "culture has always been a thorny concept and an even thornier research construct" (Straub et al., 2002, p.14).

There is a wide range of definitions by many social scientists and management theorists. The definition of culture crosses many disciplines including history, linguistics, literature, anthropology, sociology, psychology, and more recently, economics, business, management science, information systems, technology, and management information systems. Each field has its own approaches and methodology for dealing with the concept of culture. (Srite et al., 2004). Furthermore, definitions of culture vary from general to specific, depending on the discipline and level of analysis. Kilmann (1985) identifies culture as a separate and hidden force that controls behaviours and attitudes in organisations. House et al. (2004, p.15) suggest that "culture is a set of parameters of collectives that differentiate the collectives from each other in meaningful ways". Hofstede (2001) compares culture with an onion consisting of multiple layers; values are the inner layer of the onion and the core element of culture. They are invisible until they become evident in behaviour. In addition, Philips (1984) portrays culture as a set of tacit assumptions that guide acceptable perceptions, thoughts, feelings, and behaviour among members of a group.

There is a general agreement that culture works at different national, organisational, industry, professional (occupational), and individual levels. (Chen et al., 2012; Pizam, 1993). Hofstede et al. (2010) believe that the national level is the most fundamental level and is at the heart of the primary socialisation process in early childhood, giving people their values and beliefs.

2.10.1. National Culture

National culture is a way of behaving. It is a common belief system that exists among people in the same society. Despite the variety of group and individual values, national culture is a 'large frame' of thoughts and inherited beliefs. (Larsson & Risberg, 1998).

According to Beck and Moore (1985), national culture is the belief, values, and assumptions that people gain in early childhood. These attitudes distinguish one group from another. Indeed, national culture can be viewed as a guideline that people use in their everyday life. Regarding information security Hofstede's cultural model is the most predominantly used model. (Srite & Karahanna, 2006). Further, several studies (Hofstede, 2001; Hall, 1990; Harris and Moran, 1996; Rosseau, 1990) use the term culture and nationality interchangeably, implying that nation states comprise populations with a shared history and experience, and therefore have homogeneous cultures. When ethnic and religious sub-groups are discussed in a cultural context, several studies (Hofstede, 2001; Fang, 2003; Munter, 1993; Hofstede and Bond, 1988) show contradicting perspectives about whether national culture is a nationality dimension, a religious dimension, or a combination of nationality and religion.

Although Hofstede (1991, p.5) defines national culture as "the collective programming of the mind which distinguishes the members of one group or category of people from another", it does not follow that this is the only role of national culture. In fact, cultural influences extend beyond simply distinguishing one country or nation from another, to include factors that exert a powerful influence on the characteristics of management and business entities. In his later work, Hofstede (2001) emphasises that external influences on culture, such as economics and trade, can eventually shift cultural perspectives.

However, there are wide variations in culture between countries. Geography, ethnicity, religion, gender, generation, and class all define the national culture of an individual country. (Hofstede, 2005). Therefore, what one country or culture finds acceptable may not be received in the same way by another country or culture. Alas (2006, p.237) emphasises this point as follows: "What one ethnic group thinks about what is right or wrong depends on culture and environmental circumstances and is different across the cultures. National culture plays a fundamental role in forming cultural values" (Alas 2006, p.237). Ali and Brooks (2008) define national culture as a shared set of core values, norms, and practices in a society that shapes the behaviour of individuals within that society.

The most recent version of the Hofstede cultural framework contains the following six distinct dimensions: Power Distance (PDI), Individualism versus Collectivism (IDV), Masculinity versus Femininity (MAS), Uncertainty Avoidance (UAI), Long-Term versus Short-Term Orientation and Indulgence versus Restraint. (Hofstede & Minkov 2010). These dimensions are defined in Table 2-1. Some authors (Miller et al., 2006;

Smith & Bond, 1998) prefer alternative frameworks such as Schwartz's (1994) framework. Hofstede believes that the national level is the most fundamental level and is at the heart of the primary socialisation process in early childhood (Hofstede et al., 2010), giving people their values and beliefs.

(see Table 2-1 Below)

Table 2-1: The Six Dimensions of Hofstede's Culture. Source: Hofstede & Minkov, 2010)

S	Dimension	Meaning
1	Power Distance (large versus small)	The basic issue involved within this dimension is human inequality. A national culture characterized by large power distance is more willing to accept inequalities (e.g. those between a manager & her/his subordinates) within an Organisation than cultures with small power distance.
2	Uncertainty Avoidance (strong versus weak)	The uncertainty avoidance index is defined as "the extent to which the members of a culture feel threatened by uncertain or unknown situations" (Hofstede, 1991). Strong UAI cultures try to minimize the possibility of uncertain, unexpected situations by strict laws and rules, safety and security measures. Cultures with a weak UAI are less rule-dependent and are more trusting (De Mooij, 2000).
3	Individualism versus Collectivism	In cultures that are considered highly individualistic, individuals are loosely tied and are expected to look out for themselves and their family. In collectivist cultures, people are integrated into strongly cohesive in-groups, and group loyalty lasts a lifetime. In individualistic cultures, time, punctuality and schedules are considered highly important, whereas in collectivistic cultures personal relationships and contacts prevail.
4	Masculinity versus Femininity	In a feminine society values like quality of life, tenderness and modesty prevail. In a feminine culture, individuals don't like to stand out or be unique, whereas in a masculine society success and career are valued highly.
5	Long-Term versus Short-Term Orientation	Every society has to maintain some links with its own past while dealing with the challenges of the present and the future. Societies who score low on this dimension, for example, prefer to maintain time-honored traditions and norms while viewing societal change with suspicion. Those with a culture which scores high, on the other hand, take a more pragmatic approach: they encourage thrift and efforts in modern education as a way to prepare for the future. In the business context, this dimension is referred to as "(short term) normative versus (long term) pragmatic" (PRA).
6	Indulgence versus Restraint	Indulgence stands for a society that allows relatively free gratification of basic and natural human drives related to enjoying life and having fun. Restraint stands for a society that suppresses gratification of needs and regulates it by means of strict social norms.

The many definitions of national culture can be summarized as a certain set of values, beliefs, behaviours, and attitudes, which is shared, interpreted, and transmitted over time within a collective group; it makes the collective unique and distinguishable from other groups. (Bik, 2010). Arab countries share the same cultural attributes. Rees and Althakhri (2008, p.128) characterise Arab culture as "strongly group oriented". Arab and Omani culture will be discussed further in the following sub-sections.

2.10.1.1. Arab National Culture

Arab culture applies to those countries for which the official language is Arabic. It is difficult to define Arab culture more precisely because it is diverse and determined by the union of several ethnicities, cultures, and philosophies under the umbrella of Islam. Arab societies share close cultural characteristics. Some distinguishing traits of Arab personality could render Arab employees more vulnerable than others to information security threats. Cultural elements such as religion, tribalism, and family play a major role in establishing Arab values, norms and behaviours (Mohamed et al., 2008; Rees and Althakhri, 2008), that are clearly manifested in workplace practice. When discussing the importance of national culture in forming management practices, Al-Yahya et al. (2009), describe Arab culture as sharing relatively high collectivist and power-distance orientations, as well as highly centralised hierarchical decision-making.

Furthermore, the national culture is highly dominant in and shapes the culture of organisations within the country. (Lindholm, 2000). The predominant Arab culture is derived from regional, national, generational, social, gendered, and organisational cultures, and it influences work values in most Arab societies. Additionally, tribalism is an important factor that has a great impact upon social systems. (Rees & Althakhri, 2008). Arabs generally share the same cultural attributes. Rees and Althakhri (2008, p.128) characterise Arab culture as "strongly group oriented, male-oriented and dominated by large power distance, strong uncertainty avoidance, and long-term orientation". Dedoussis (2004) argued that, while Arab managers respect friendly relationships and group harmony, they assert the importance of loyalty and obedience from their employees.

Privacy is a commonly shared element in Arab culture. In certain circumstances, individual privacy may have a lower priority than the needs of the community or family. (Chadwick, 2002). Since Arab culture respects elders and seniority (Koocher, 2009), private details may be divulged in circumstances involving seniority requests.

In the next section, the researcher addresses the most important elements, in the formation of Omani societal culture and characteristics of Omani personality.

2.10.1.2. Oman National Culture

Societal and institutional influences are always interacting in Arab societies, including Oman, and can hardly be separated from each other. (Hutchings &Weir, 2006b). As an Arab country, Oman shares many cultural influences with other Arab nations, such as

the Islamic religion and the Arabic language. In particular Oman shares many of the characteristics of Arab culture with its Arab neighbours in the Gulf Cooperation Council (GCC), due to their tribal origins and their highly collectivist behaviour. (AlTwaijri and AlMuhaiza, 1996). However, there are important factors that make Oman unique in the Middle East, that are products of its geography, history, and economic change. Furthermore, Oman's cultural diversity is much greater than that of its Arab neighbours. There is a degree of cultural heterogeneity within its national boundaries, arising from its historical expansion to East Africa and the Indian Ocean, which differentiates Oman from other Arab Gulf States.

Oman's strategic location, combined with a sustained history of interaction with people of distant lands, robust trade relations, and extensive imperial exploitation, contributes significantly to its rich cultural mosaic. Further, since 1970, Oman has changed demographically, externally and environmentally due to new educational processes, modernisation and development. However, despite such external changes, family 'stickiness' and the tribal structure remains strong (Al-Hamadi et al., 2007).

Cultural elements, such as religion and tribalism, play a major role in establishing Omani values, norms and behaviours. (Mohamed et al., 2008; Rees and Althakhri, 2008). This spills over into workplace practices. In common with other Arab states, Islam is constitutionally the country's official religion and that has been clearly declared in the Basic Law of the state. Oman is a remarkable example of a culture where people are tolerant of various beliefs from Islam's different forms. Many scholars believe that religious practices have a considerable impact on the culture of states. Tayeb (1997) states that religions in many countries, with either secular or religious constitutions, have a certain degree of influence on the cultural characteristics of their people and their institutions. Islam is a way of life that aims to produce a unique personality and a distinct culture in a society. (Haneef, 1979; Esposito, 1991). In Islamic countries, these influences can be observed in many aspects of life, such as: family relationships, social and economic affairs, the judicial system, etc. This is valid for Oman.

Omani culture is steeped in Islamic thought and beliefs. Additionally, individuals who behave according to Islamic instructions create a group with common values and norms. Moreover, religion can affect the attitudes of people in a society and this can manifest itself as collectivism where the interest of the group comes before the interest of the individual (Al-Twaijri & Al-Muhaiza, 1996; Hofstede, 2001). In turn, this can facilitate the flow of knowledge, cooperation and interaction between individuals. Furthermore,

Ali (1996) and Jasim (1978), also note the importance of the Islamic work ethic, and its influence on both individuals and organisations.

Further, Islam, and the tribal model, enhances the importance of the family in social and organisational life. As Haddad and Esposito (1998) state: 'Islam, in time, became an integral part of tribal society. Therefore, all issues such as loyalty, marriage and divorce, friendship, tolerance, justice, and any other kind of life and work experiences were all surrounded by the Islamic way of living (Ali et al., 1997). Tribalism as well as Islam continues to play a crucial part in shaping the society in Oman (Neal et al., 2007).

Omani tribal systems are effective and efficient within small population. (Rugh, 1999). The tribe is presided over by a chief called 'sheik', and he is responsible for helping tribe members and dealing with their various demands. He acts a mediator and represents his tribe in regard to its social and economic needs. Neal et al. (2007) describe the relationship between the sheik and the tribe members as follows: '……(it) is not merely 'top-down', however, but is characterized by high degrees of embedded interaction and consultation'. (Neal et al., 2007). Furthermore, Barber (2007) states that tribalism remains strong in Oman, though not unchanged. (Barber, 2007). Landen (1993) postulates that tribalism in Oman is a state requirement; the major role of the tribe is to serve society and its values. Thus, the official system and social structure have played a significant role in preserving tribalism. Supporting such a view, Rabi (1997) asserts that tribal practice provides a critical counterweight to economic and technological change. Oman's social landscape comprises over a hundred tribes that belong to the main Arab tribal blocks: Qahtani and Adnani. The Al Bu Said tribe, the ruling tribe in Oman since 1744, belongs to the Qahtani block. Many Omani citizens still remain loyal to their tribes which are considered as the source of glory and protection. For instance, tribal connections have a great impact on Majlis al-Shura (the elected consultative council) voting results. (Barber, 2007).

A study conducted by Alarifi, Tootell and Hyland in 2012, to examine the level of information security awareness among the general public in Saudi Arabia found that 35.8% of the participants of the survey share their password with their family members. (Alarifi et al., 2012). They suggest that this tendency is related to the tribal nature of Saudi culture where tribe members trust each other. They also mention the patriarchal element in tribal culture influences the belief that the information security is a responsibility of the information provider. Therefore, in the context of this literature, it is important to consider any negative impacts of Omani tribal affiliation and loyalty

upon information security, and whether such affiliation can lead for example to disclosure of confidential information or sharing of passwords, for the purpose of tribal interests and advantages.

The tribal characteristics of Omani society have strong connections with social and family orientation, where the responsibility to family is the primary concern of its people. Furthermore, the government system in Oman has created a country that has a unique style, where tribal and modern state systems both exist in one dynamic culture, as an example of useful and healthy interaction between two different orientations. (Pederson, 2002). Given that Oman consists of many different tribes and ethnic groups and has many expatriates from around the world, the country presents an excellent research opportunity.

Research by Al-Twaijri and Al-Muhaiza (1996) to measures Hofstede's cultural dimensions in GCC countries. They find that, compared to those Arab countries studied by Hofstede, Oman scores higher on the dimensions of Power Distance, Uncertainty Avoidance, and Collectivism, whereas it scores low on Masculinity Vs Femininity. However, Mujtaba et al. (2009) argue that such variation could be related to processes of cultural change and increased participation of Omani females in the workplace.

The first three dimensions and their relationships with the culture and practice of organisation information security are explained in brief below.

High Power Distance (HPD):

Power distance is defined as the extent to which the less powerful members of organisations expect and accept the unequal distribution of power within an organisation. Therefore, power distance, as described, is based on the value system of the less powerful members. Power distribution is usually explained by the behaviour of the more powerful members, the leaders and managers, rather than those led. In high power distance cultures, such as Omani public organisations, power hierarchy is obvious, and individuals respect their superiors without questioning their authority. In low power distance cultures, individuals tend to favour personal responsibility and autonomy, and power is shared and well dispersed. Low power distance implies greater equality and empowerment.

Figure 2-10: The Relationship between High Power Distance and Information Security Culture in Omani organisations. Security Culture. Source: Self

High Uncertainty Avoidance:

Individuals in Omani culture are likely to have more concerns about ambiguity and uncertainty and less tolerance for diverging opinions. Cultures with a high uncertainty avoidance are less willing to take risks and accept organisational change. Regarding information security: public organisations in Oman should have clear information security polices, rules, and procedures that act as guidelines and constant reminders for employees to maintain behaviour awareness.

Figure 2-11: The Relationship between High Uncertainty Avoidance and Information Security Culture in Omani organisations. Security Culture. Source: Self

Individualism vs Collectivism:

This refers to how individuals value themselves, their groups and organisations. High individualistic cultures tend to care more about self-actualisation and career progress whereas people with high collectivistic values tend to value group benefits over their self-interests. Oman is a collectivistic society, which is manifested in fostering strong relationships with a close long-term commitment for fellow members of their group, and high preferences for a tightly knit framework and strong group cohesion. This may have practical implications for an individual's daily security practices.

Collectivism can act as a double-edged sword in respect of those information security culture and practices where the culture is highly collectivistic, characterised by strong, cohesive groups who continue to protect each other in exchange for unquestioning loyalty. One the one hand, collectivist societies are more trusting towards each other and his may lead to undesirable behaviour, compromising the principle of confidentiality in an information sharing environment (Chang & Lin, 2007), and more likely to commit information security violations such as password sharing and illegal sharing of copyrighted material. (Al-Mukahal & Alshare, 2015).

Figure 2-12: The Relationship between Collectivism Value and Information Security Culture in Omani organisations. Source: (Self)

On the other hand, collectivism would assist an information and knowledge sharing culture within an organisation if individuals are willing to share security information

and knowledge. Thus, the effectiveness of an information security system faces paradoxical requirements in balancing opposing cultural orientations. While Collectivism implies that people in a collective society may tend to follow information security rules and procedures to protect the interest of the group (organisation), the organisation should nevertheless provide awareness and training programs to limit the negative aspects.

2.10.2. Organisational Culture

The terms organisational culture (OC) and corporate culture refer to "the way things are done here". (Valga & Eloff, 2010; Lundy & Cowling, 1996). It defines the specific or unique personality of an organisation. (Robbins & Judge, 2008). It establishes the norms within which people are used to think, act, and feel. The concept of organisational culture has been defined in many ways since its evolution in the mid-twentieth century. The common idea of all these definitions is that organisational culture consists of shared values, beliefs and assumptions that are communicated among members, (Deshpande, 1989; Gregory, 1983b; Schein, 2010), guide behaviour, and facilitate shared meaning. (Alvesson, 2013; Denison, 1996).

Culture also incorporates a group of rules that must be followed, i.e. all newcomers must understand them to become a member. (Maanen & Schein, 1979). Researchers such as Geertz (1966; 1973), Schein (1988; 1996a; 1996b), Deal and Kennedy (1982), Hofstede (1980; 1984), and Hall (1959), all discuss the concept of organisational culture at a high level, as a construct that deals with beliefs and behaviours of employees in the organisation as a whole.

The conceptualisation of organisational culture has also been applied to, and is suitable to, explaining organisational issues such as marketing culture (Deshpande, 1989; Webster, 1993), innovative culture (Van de Ven, 1986), and knowledge management culture. (Banks, 1999). Furthermore, organisational culture can be seen and recognised in mission statements, vision statements, strategic plans, sales materials, web sites, architectural and interior office styles, employee clothing, how employees treat each other, job specifications, and how employees use their time. It is not difficult to notice the uniqueness of a firm, which can be recognised by experiencing how daily activities are performed. (Brock, 2007).

According to Chang and Lin (2007), an organisational culture is one factor in the failure or successes of organisations. Robbins and Judge (2007) argue that organisational culture can serve as a sense-making control mechanism that guides and shapes the

attitudes and behaviours of employees. A strong organisational culture increases behavioural consistency and creates predictability, orderliness, and consistency. Employees share values and beliefs with other employees in an organisation's culture. (D'Arcy & Greene, 2014). According to Schein (1996), the way to conceptualise organisation culture is to examine the different levels at which it exists. He characterised an organisation's culture as consisting of physical artefacts and behaviour.

2.10.2.1. Organisational Culture Models

Various models have been adopted to study the phenomena of organisational culture. Two generally accepted models include Schein's (1985) cultural model, and Cameron and Quinn's (2005) competing values framework. The first of these two models is by researcher Edgar Schein, who describes organisational culture as a pattern of basic assumptions and beliefs that an organisation has learned, and that is taught to new members as they join the organisation.

He names three levels for organisational culture:

Level One: Artefacts

Artefacts are factors that can be seen, heard and felt in an organisation (Schein, 1999), including processes and organisational structures. "Artefacts are what actually happens in an organisation". (Van Niekerk & von Solms, 2010, p.114).

Level Two: Espoused Values

An organisation's espoused values are the reasons that an employee provides for why activities of the organisation are done in a certain way. These values are often expressed in documentation about the organisation's vision, principles, ethics, and values. Teamwork and the belief that everyone is important in the decision-making process are typical espoused values that can be perceived as organisational management's 'visible' contribution towards the cultural direction of the organisation. (i.e. what the organisation *wants* to live up to; Van Niekerk & von Solms, 2010). How the espoused values are interpreted and implemented strongly depends on the shared tacit assumptions of the employees (Schein, 1999).

Level Three: Shared Tacit Assumptions

Shared tacit assumptions are the beliefs, assumptions, and values shared and taken for granted by the organisation's employees; they form the essence of an organisation's culture. Moreover, tacit assumptions act as a filter when interpreting the organisation's espoused values. (i.e. the policies and principles).

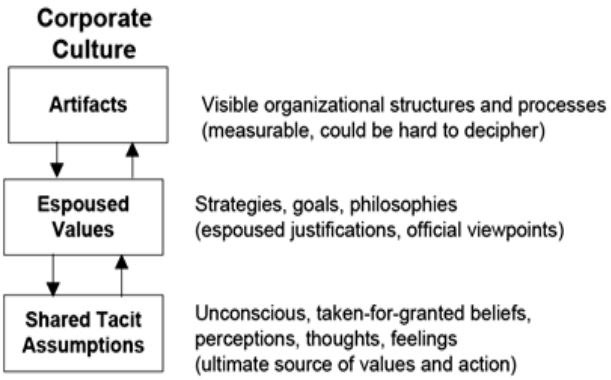

Figure 2-13: Schein's Three Levels Culture Model. Source: Schein, 1985

Van Niekerk and Von Solms (2006) further enhance the definition adopted by Schein's model and add a fourth level of 'information security knowledge', which supports the other three levels. Information security knowledge is necessary for employees to behave in a secure manner, as it cannot be assumed that the employees already possess such security knowledge. (Van Niekerk & Von Solms, 2010).

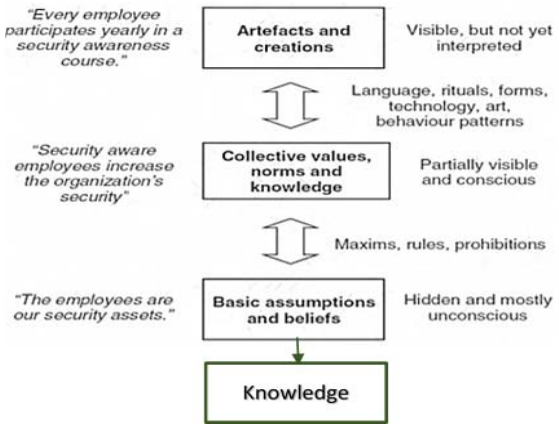

Figure 2-14: Schein's Three Culture levels + Knowledge.
Source: Van Niekerk & Von Solms, 2006

Hofstede (2004) mentions that culture can be distinguished from both general human nature, and one of a kind individual identity. A unique personal set of mental programs comes from the identity of a person, which is not shared with any other individual. This unique personality depends on the characteristics that are mostly inherited from the individual set of genes of individual's or from individually learned experience. In this context, learning represents the influence of shared culture along with unique personal understandings.

The other view of organisational culture, is Cameron and Quinn's (2005) competing values framework, which focuses on the values of an organisation. The model considers how organisational values align with two different sets of dimensions: internal or

external focus and stability or flexibility focus. The model explains how four types of culture exist (clan, market, rational, and hierarchical), depending on the primary orientation towards the four dimensions.

These four types of culture are theoretical, as organisations typically do not fall into a single culture type, but tend to be more dominant in one cultural type than another (Cameron & Quinn, 2005). The competing values framework of Schein's culture model focuses only on organisational values and does not consider how social structures affect human behaviour. It does not address how culture can be changed through power struggles, sanctions, or communication channels. Nevertheless, all the models and perspectives mentioned above should be considered when trying to find out how to improve information security culture and practice in an organisation.

The next subsection describes the relationship between national culture and organisational culture.

2.10.2.2. The Correlation between National Culture and Organisational Culture

The national culture as a macro culture has a strong relationship with organisational culture as a micro culture. Organisational culture mainly influences values and roles inside the organisation. However, national culture directs organisational culture and deeply influences the personal values of both leadership and employees. Furthermore, the relationship between organisational culture and national culture affects leadership, employees, job satisfaction, and the commitment to the organisation. (StudyMode.com, 2011). Buchanan and Huczynski (2004) point out that the organisational culture, influenced in some way by the particular national culture, shapes employee behaviour. This idea is supported by Jung et al. (2008), who also indicates that the employees of a multinational organisations' subsidiary will be largely influenced by the national culture of the subsidiary in terms of that country's values, beliefs, customs rather than the values and assumptions of the organisation itself. Levitin (1973) agrees with Robbins (2003), who reports that the formation of an organisational culture stems from the ideologies of the organisation's founders, which are based on the values, beliefs, and assumptions of those founders.

Cultures at the national level exert a subtle, yet powerful influence on individuals and organisations. (Lee et al., 2013; Leidner & Kayworth, 2006; Sagiv et al., 2011). Further, Sagiv et al. (2011) note that organisations are nested within nations, and as such, organisations and their employees tend to develop and evolve in ways that are

compatible with the surrounding national culture. This demonstrates that each national culture is characterised by a range of attitudes, values, and beliefs, reflected in its members' behaviour, which determine how individuals behave in specific situations and roles.

This research proposes the idea that in any organisation, national culture influences the way that information security is handled, how information and knowledge is valued and used, and the overall success of information security systems. Therefore, an understanding of these differences in national culture may help organisation managers develop more effective approaches to managing the information security culture in their organisations. Schlienger and Teufel (2002) emphasise that an organisation must establish a culture of security as a socio-cultural measure to promote security-cautious behaviour and address the human factor problem in the area of information security.

2.10.2.3. Organisational Culture, Organisational Value and Employee Value

In their study of the challenges of information technology management, Werlinger, Hawkey, and Beznosov (2009) conclude that organisational culture influences security practices and that an understanding of an organisation's culture is an important factor in influencing the adoption of best practice. The concept of value congruence provides an explanation for reasons employees adopt a security culture and how behaviour is associated with values. (Lamm et al., 2010). Kalliath et al. (1999) define the concept of congruence as, "the degree to which an individual and an organisation's culture share the same values". (Kalliath et al., 1999, p.1176).

The greater the alignment between employee and organisational values, the greater the value congruence. Greater value congruence then leads to higher levels of organisational commitment and more employees who will behave in a manner that is consistent with the organisation's values, goals, and culture. (Kalliath et al., 1999; Ostroff et al., 2005). Much of the research on value congruence examines its usefulness in predicting employees attitudes (Lamm et al., 2010; Meglino et al., 1989; Posner, 2010), and commitment (Amos & Weathington, 2008; Kalliath et al., 1999). Posner (2010) reports the usefulness of value congruence for predicting employee attitudes across disparate ages, genders, education levels, functional disciplines, and level of management experience. This finding suggests that value congruence related to security attitudes could be consistent across organisations with diverse employee populations.

The alignment of employee and organisational values is a fundamental component of security culture. (Thomson et al., 2006; Van Niekerk & von Solms, 2010). However, obstacles to building a program based on aligned values have been identified, including conflicting employee values (Kolkowska, 2011) and inconsistencies between actual and espoused security behaviour when policy and employee values conflict. (Hedström et al., 2011; Suar & Khuntia, 2010). However, research based on a value congruence framework has proven useful for predicting employee behaviour (Lamm et al., 2010; Meglino et al., 1989), and it may be useful for predicting behaviour associated with security culture.

The next section explores information security culture.

2.10.3. Information Security Culture

A security culture within an organisation can overcome threats and risks associated with keeping information secure. One reason that people are the greatest threat to information security is that individuals in the organisation do not understand information security. (Ilvonen, 2011). The level of understanding of information security impacts the success of an information security culture. (ISC) (Ilvonen, 2011). Dhillon (1995) defines information security culture as the totality of human attributes such as behaviours, attitudes, and values that contribute to the protection of all kinds of information in a given organisation. Malcolmson (2009) argues that security culture could have potential impact on the security of that organisation; it could affect how employees interact with the organisation's systems and procedures at any point in time and result in acceptable or unacceptable behaviour. Alhogail & Mirza, (2014), define information security culture as the collection of perceptions, attitudes, values, assumptions, and knowledge that guide the human interaction with information assets in an organisation with the aim of influencing employees' security behaviour to preserve information security.

Creating a security culture within organisational settings is important because the human dimension in information security is always considered the weakest link. (Da Veiga. & Eloff, 2007; Martins & Eloff, 2002; Maynard & Ruighaver, 2002; Schlienger & Teufel, 2003; van Niekerk. & von Solms, 2005). Therefore, the creation of an information security culture is necessary for effective information security management. (Eloff & Eloff, 2005; Eloff & Von Solms, 2000). O'Dell (2012) states that creating a security culture in an organisation could minimize the information security incidents caused by employee behaviour. In information security, culture is defined as the way activities are performed to protect information assets. (Dhillon, 1997). It reflects the perceptions, attitudes, assumptions, and beliefs of the employees

regarding information security. (Martins & Eloff, 2002; Da Veiga et al., 2007; Valga & Eloff, 2010).

The research of Rastogi and Von Selms (2012) indicates that the establishment of an information security culture supports the development of security policies and procedures, which ultimately drive the implementation of an information security awareness program. (Rastogi & Von Solms, 2012). Shaw et al. (2009) note that a program of information security awareness is an excellent channel to distribute information about a new information security culture.

An information security culture may include a variety of elements beyond information security awareness, such as elements and programs to instil information security best practices in its employees. One such item that is simple and inexpensive is an information security code of ethics. (Harrington, 1996). An organisational code of ethics supported by senior management can have a direct and positive effect on employee security threats and risks. The visible and regular support of information security by top management is also an effective method to reduce information security threats and risks.

2.10.3.1. Correlation Between Organisational and Information Security Cultures

An information security culture develops from the information security behaviour of employees in the same manner that an organisational culture develops from the behaviour of employees in an organisation. (Martins 2002). An information security culture is based on the interaction of employees with information assets and the security behaviour they exhibit, driven by cultural, social, and ethical values.

An instrumental view of organisation's culture is that of a tool to drive the behaviour of employees. (D'Arcy & Green, 2014). Cultures within organisations can change but before change can occur, employees must be included in the implementation, or at least notified of the upcoming change. (Puhakainen & Siponen, 2010). This will lead to positive attitudes and behaviours towards the adoption of the change, as Chang et al. (2007) explain that the culture affects all levels of an organisation.

Several information security scholars connect organisational culture and information security culture. For example, Kolkowska, (2011) and Solms and Solms, (2004), state that security culture is achieved by aligning organisational and employee attitudes, beliefs, and values. Schlienger and Teufel (2002) emphasise the importance of a strong organisational culture to create a culture of information security in an organisation.

Peters and Waterman (1982) explain that in organisations with strong cultures, people mostly know what tasks they are supposed to perform. These organisations do not completely rely on policies, procedures, and rules. Thus, a strong security culture within an organisation promotes the security-adequate behaviour of employees without employing radical security compliance measures, such as punishment. Cultures that promote good security-related human behaviour through knowledge, artefacts, values, and assumptions are far more effective than regulations that simply mandate employee behaviour. It is apparent that security can only be effective if employees know, understand, and accept the necessary precautions.

Information security culture includes all socio-cultural-organisational measures that support technological security methods to make information security a natural aspect of employees' daily activities. (Schlienger & Teufel, 2003). It involves identifying the security-related ideas, beliefs, and values of the group that shape and guide security-related behaviours. (Ramachandran et al., 2008). Since the most influential factor regarding employee beliefs and attitudes is the working environment, a change of culture must originate from the senior management. (Drennan, 1992). The implementation of information security should start with the top management and continue downwards in the hierarchy. Furthermore, many studies suggest that implementing an information security culture involves providing guidance and structure to the interaction of humans with an organisation's sensitive information to avoid actions that may create risks. (Bess et al., 2010; Furnell & Thomson, 2009; Knapp et al., 2006; Ruighaver et al., 2007; Zakaria, 2006).

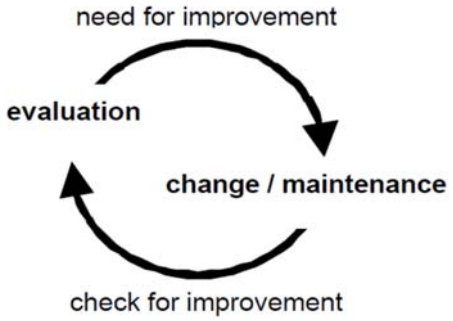

Figure 2-15: Information Security Culture Management Cycle
Source: Schlienger & Teufel, 2003

These studies suggest that organisations must take formative steps to create an environment where security is ''everyone's responsibility'' and where doing the right thing is the norm. (Alfawaz, et al., 2010). Further, to ensure that information security culture corresponds with the targets of the organisation and maintains a high profile, that culture must be continually created, maintained, or changed.

In addition, information security culture should not be treated as a monolithic construct, because it is not the same throughout the organisation. Recently, scholars in organisational studies have argued that cultures in organisations can vary across different groups within an organisation, and that subcultures can exist under the umbrella of an official organisational culture. (Chatman 1998; Jermier et al. 1991; Martin et al. 1983). Vroom and Solms (2002) state that these human factors play an important role in ensuring that policies and procedures are followed properly and effectively. Indeed, employees adopt habitual and consistent security practices when an organisation establishes a culture of security. (Corriss, 2010; Thomson et al., 2006).

2.10.3.2. Information Security and Compliant Employee Behaviour

There is an increasing focus on enforcing information security compliance. (Boss & Kirsch, 2007; Siponen et al., 2007). This is referred to as the effective implementation of information security standards and policies for protecting information in public organisations. (AlKalbani et al., 2014; Von Solms, 2005; Herath & Rao, 2009). The adoption of information security compliance ensures that information security mechanisms can work together effectively to protect critical information in the organisation. It satisfies the information security requirements, improving users' confidence and trust.

Several studies explore alternative approaches to improving information security compliance. For example, Bulgurcu et al. (2010) investigate the role of information security awareness in changing users' attitudes towards complying with information security requirements. Pahnila et al. (2007) and Bersz (2004) suggest that to improve employee compliance with policies and guidelines, employees need to receive appropriate awareness, education, and training. Furthermore, D'Arcy et al. (2008) find that employees' awareness of security procedures, security education, training, and awareness (SETA) programmes, and computer monitoring may deter information security misuse. Sasse et al. (2001) analyse employee interactions with security mechanisms to strengthen information security compliance. In addition, Lee et al. (2004) explore the use of sanctions to increase information security compliance in public organisations. Siponen et al. (2010) examine factors related to normative beliefs, threat appraisal, self-efficacy, and visibility that influence employees' intentions to comply with information security standards and policies in organisations.

This research thesis agrees with the findings of the above-mentioned studies, and suggests that the success of an information security program depends on the employees'

security related behaviour. If employees are offered good security training and awareness programs, they will gain a better understanding about security threats and vulnerabilities. The study believes that the behaviour of employees needs to be directed and monitored to ensure compliance with security requirements. Recent studies have used the 'theory of reasoned action' (TRA) and the 'theory of planned behaviour' (TPB), to explain information security compliance. (Bulgurcu et al., 2010; Herath & Rao, 2009; Hu, Dinev, Hart & Cooke, 2012; Pahnila, Siponen & Mahmood, 2007). According to Ajzen (1991), behaviour stems from the theory of reasoned action and the theory of planned behaviour. He suggests that actual behaviour should result from the intention to perform a certain behaviour, and these intentions involve motivation. (Ajzen, 1991).

The intention to comply may reflect a rational state of mind, which itself may affect actual behaviour in situations where an individual must decide whether or not to comply. (Becker, 1968).
Compliance intentions are determined by the following three variables:

(1) Attitudes towards the compliance behaviour measures in terms of the degree to which individuals evaluate compliance behaviour positively.
(2) Normative beliefs, which measure a person's judgment about whether close colleagues would stick to compliance management requirements.
(3) Self-efficacy, which is defined as a measure of the extent to which an individual has the skills, knowledge, and competencies to adhere to compliance management requirements. (i.e. it describes the ease or difficulty with which the individual complies) (Ajzen, 1991).

According to TPB, the greater these three determinants are, the higher the intention. Self-efficacy in this regard tests whether a compliance program and training increase the knowledge and skills that enable all employees to fulfil the program's requirements. Therefore, if employees feel they can achieve the compliant targets, they are more likely to be compliant. Employees who believe that their close colleagues will stick to the compliance program, may show greater compliance intentions than those who believe that their colleagues will not stick to the compliance program. (Bulgurcu et al., 2010). In addition to discussing one's own subjective norm, the perceived attitude of other colleagues towards rules may show that compliance can be seen as a collective activity. (Pinto et al., 2008). If the collective relevance of compliance decreases, this may hinder internalisation since collective non-compliance may be the cause of individual non-compliance.

Another area of individual interest is personality and how it influences and is influenced by the work environment. (Szilagyi & Wallace, 1990). Thus, the behaviour of individuals plays an important role in the development and evolution of organisational culture, and factors that affect this behaviour should be conducive to information security. A group that is composed of individuals develops characteristics beyond those of each individual's personal contribution. Group values and norms play an essential role in how groups of employees act and behave while engaged in organisational duties. Organisations can be compared according to common characteristics such as their size, and whether they influence their surrounding environment, which also influences employees and internal operations. (Szilagyi & Wallace,1990). These aspects of organisational behaviour are not mutually exclusive, as they influence each other to form the culture of a business. Each level in an organisation has a different type of behaviour. The way individuals act to situation may be different from how the group to which they belong.

Figure 2-16: National Culture Influences on Employee Behaviour
Source: Szilagyi & Wallace, 1990

To improve information security compliance within organisations, issues related to organisational security culture and the external environment need to be investigated (Warkentin et al., 2011). The organisation must be changed at three levels where organisational behaviour occurs. Different factors affect each of the following three levels mentioned by Szilagyi and Wallace (1990): the individual, the group, and the formal organisation. As each person brings different characteristics into the organisation, there are assorted organisational forces that affect individual employee attitudes, motivation, and job satisfaction. Information security scholars acknowledge the crucial role that an information security culture within organisations can play in promoting security through the prudent behaviour of employees. (Schlienger & Teufel, 2002; da Veiga & Eloff 2010).

The overall result of changes in awareness at each of the three levels will create a culture of compliance'. (Furnell et al., 2000). An organisation with this type of culture has a level of compliance that is demonstrated by its leadership, and includes norms for

security guidelines that are invariably followed by everyone in the organisation.

The next sections present a brief review of information security within the context of developing countries and within Arab culture.

2.10.4. Information Security within the Context of Developing Countries

The literature on the challenges facing Information Security management in developing countries is very limited. Niels, (2016, p5) referres to the new societal vulnerabilities emerging from digitalisation in developing countries as “a less-studied issue". He states, "While there is wide agreement about the need to bridge the gap between the connected and the disconnected, the pitfalls are many, especially concerning cyber security - a topic often neglected, also in the recent World Bank report Digital Dividends". Hu et al., (2012), also argue that studies investigating the effect of key organisational constructs in the literature related to Information Security are very few.

Several authors such as Posthumus et al., (2004) and von Solms et al., (2005), identify information security as a priority for executive management, including the Board of Directors, and therefore should be a key element in corporate governance responsibility. This establishes the need to integrate information security in corporate operations through the development of a framework for information security governance. In the same vein, information security governance, according to von Solms (2006), should be an integral part of corporate governance, consisting of:

- The commitment and awareness of senior management to the management and leadership of good information security practices.
- The appropriate organisational structures which reinforce information security best practice.
- Knowledge of legal and regulatory requirements regarding privacy of data and information security.
- Optimal implementation of policies, procedures, processes, technologies and necessary compliance mechanisms that promote best practice, improve shortcomings and avoid the negative consequences of negligence.

Additionally, Connolly et al., (2013) argue that very little cross-national research into information security has been conducted. He points out a need for a broader understanding of differences in information security behaviour arising from factors inherent within national culture. According to Von Solms (2000), good information security practices, from the national perspective, are a compilation of combined

information security experiences of many influential international companies. These practices reflect international experience in operating relevant control measures, procedures and techniques, and provide an adequate or acceptable level of information security.

Robert et al. (2013) also highlight the paucity of research on behavioural information security in developing countries. They state: "One of the biggest issues and limitations of behavioural information security research is that the majority of it has been conducted in Western cultures, with occasional studies being conducted in Asia and elsewhere. Most of the rest of the world has been overlooked; and little has been done to examine cross-cultural considerations involved with insider behaviour, IT security compliance, hacking, security violations, and so forth". They argue that current studies may need to be adapted to account for many cross-cultural differences, among which is so called collectivism.

2.10.5. Information Security within the Context of Arab Culture

There are many examples showing that confidential information may be disclosed in circumstances that exploit Arab traits (Alizki & Weir, 2016). According to Nydell (2006), password sharing can be considered a sign of trust in a group or a family, and therefore, refusing to share a password can be perceived as a sign that a person does not trust his family. Furthermore, when an Arab person receives a call related to confidential information, he or she will continue talking without considering the attendance of a relative, because moving to another area while talking could be a sign of mistrust.

Al-Kaabi and Maple (2012) note the prevalence of respect for elders and seniority in Arab culture and suggest that a significant aspect of Arab culture is its tendency not to prohibit privacy sharing among peers or with superiors. (Al-Kaabi & Maple, 2012). For instance, an Arab helpdesk employee will not easily turn down a request for important information if it comes from people who refer to themselves as ‘directors’ and need information for the future of the organisation. In Arab culture there is also no separation between professional and personal lives. Doing business revolves around personal relationships, family ties, trust, and honour. There is a tendency to prioritise personal matters above all else. Therefore, it is crucial that business relationships are built on mutual friendship and trust. A social engineer could construct several ways of attack to exploit this characteristic of Arab personnel to build mutual friendship and trust. Furthermore, an Arab person will not easily turn down an invitation from a person who could be a social engineer on Facebook or other social network site, and who shows interest in being a friend, especially if they have mutual friends. As soon as social

engineers become a member of a network or group, they may start exploring the data or information presented in each profile or account of group members for their own benefit or for criminal purposes.

It is not wise to generalise the fore-mentioned observed Arab traits as a consistent cultural pattern among Arab personnel of different cultural origins, especially for those involved in information security practices. It would not be surprising to find a group of Arabs with similar reactions to a situation, but this may be a coincidence. Nonetheless, Arab scholars in different Arab countries have addressed issues of information security culture from many perspectives.

For instance, in the context of Saudi Arabia, Hend Alkahtani's (2018) research reveals the existence of significant cultural issues affecting information security awareness that had made information systems in Saudi Arabia vulnerable. In her work, she suggests that there are no obvious policies or laws to protect information security other than the single Saudi Crime Act, of which she observes, few people in Saudi Arabia are aware. Her work reveals the existence of ignorance on the part of information security users, user misuse of information, and a lack of awareness of the threat and danger associated with their actions. She suggests that regional culture factors, such as language, management hierarchy, gender communication, fear of losing face and nepotism, influence the level of information security awareness, with resulting strong impacts on the success and security of information systems. The findings of this research show that the majority of users have high expectations of and trust in each other, which can, in turn, adversely affect the security of information.

Her analysis leads to a recommended framework that focuses on minimising culture issues and raising the information system users' security awareness level. The framework design aims to engage information system users in:

- Development of information security policies,
- Auditing of information systems,
- Identification of threats and associated risks,
- Reporting of attacks,
- Classification of information and risks,
- Collaborative work to raise awareness of information security.

She suggests that this culturally aware information security framework could be useful for the Middle Eastern countries, Gulf Cooperation Council countries (GCC) and any developing or developed county that has similar hierarchical culture and management.

Similarly, by reference to Saudi Arabia, AlGarni, Khaled (2015) affirms that the existing government laws and policies make e-government applications unsafe. The ways in which poor information security threatens e-government services include lack of education, poor training, and low staff awareness of information security. He suggests that there is a continuing need for improvement in every field of public management. His work shows that information security staff in Saudi Arabia have inadequate requisite skills. He highlights key elements of the policy framework such as education, training & awareness and the rules and regulation, as areas that adversely affect the condition of information security in Saudi e-government. He also suggests there is an insufficient IT infrastructure. He identifies hacktivists, software errors and terrorists as the most significant threats to the information security of Saudi Arabian e-government, while lesser threats include environmental influence, government intrusion, and foreign state notations. He points out that citizen trust in e-government applications is low, despite all the attempts to supply information. He recommends that Saudi government must give priority to awareness programs.

Further, Alhogail, (2015), suggests that establishing a culture of information security in organisations affects employee perceptions and security behaviour in such a way as to guard against many of the information security threats posed by insiders. In her work, she presents an information security culture framework (ISCF) based on five dimensions through which various issues of information security are integrated. The dimensions are Strategy; Technology; Organisation; People and Environment. The framework incorporates the four main domains of the human factor diamond: Preparedness, Responsibility, Management, and Society & Regulations. It also incorporates change management principles that inform the cultivation of an information security culture. She suggests that this framework can assist organisations to develop an effective information security culture that protects their information assets.

Additionally, Alnatheer (2012), suggests that there are strong correlations between security culture and security culture reflection (Awareness and Ownership). He also identifies a strong relationship between factors influencing security culture and top management involvement, policy enforcement and training. The qualitative study he conducted reveals that lack of a security culture is a major concern in Saudi Arabian organisations. He argues that, many factors influence the security culture, such as top management involvement in information security, enforcement and maintenance of information security policy, security training and ethical conduct policies. In addition,

his work underlines the direct influence of national and organisational culture on Saudi Arabian organisations.

Alnatheer & Nelson (2009) investigated the extent to which security culture has evolved into practice in Saudi Arabian organisations. They produce an information security model to focus on the cultural factors influencing the processes of implementation and adoption of information security.
They suggest that these factors are corporate governance, legal and regulatory environment, and corporate citizens. They conclude that information security culture in Saudi organisations is affected by the organisational culture, which is affected in its turn, by the national culture. However, these conclusions are not studied in depth in their work.

In the context of Egypt, Loch, Straub, and Kamel. (2003), examine culture-specific inducements and impediments to using the internet in the Arab world. They investigate the extent to which the process of technology acculturation on the one hand and social norms on the other affects the acceptance of the internet. Their work shows how culture can both inhibit and encourage technological innovation and how Arab cultures can move their economies more quickly into the digital age. They claim that cultural obstacles to the diffusion of information technologies in the Arab world are significant. They suggest that technological acculturation is a process that seems to overcome certain cultural inhibitors. When individuals are exposed to the beneficial uses of the internet in other cultures, they are more favourably inclined toward adoption. This effect seems to occur whether the trainers are Arabs educated in these technologies or foreigners from the technology-originating cultures. They argue that more top-level support from the government and the involvement of the private sector could spread knowledge of and ability to use the internet to hundreds of thousands of new users. They assert, that although culture can be a barrier to information technology transference in Arab cultures, they believe that this can be overcome through certain critical mechanisms.

In the context of UAE, Al-azazi (2008) says that the security aspect of information sharing is always a concern as although information leaves a government department through the internet or a public network with a certain level of classification, it might be mishandled or declassified for any number of reasons. He believes that maintaining the classification of the information, as well as its confidentiality, integrity, and availability will require more than a policy or a technological solution. He claims that

the misuse of information arises from technological flaws, weak policies, lack of competencies and awareness on the part of security practitioners or users, a lack of operational management, and wrong decisions on how to handle governmental classified information. He suggests that implementing appropriate security measures will assist in mitigating the multiple threats of information sharing. He addresses the different security issues using a multiple layer model. He proposes this model as a tool to assess the level of security readiness of government departments, to provide a checklist for required security measures, and as a common reference for the security in government departments in Dubai. He considers his new model to have a high level of flexibility with sub layers representing technologies, policies, competencies, procedures or decision making, which can be updated with new trends in the security field and in the light of future needs.

In the context of Oman, Al-Kalbani, Ahmed (2017) suggests that the development of e-government increases the possible exposure of critical information, and thus affects the confidence and trust of e-government stakeholders. His study develops a compliance-based framework for information security in public organisations in the context of e-government development in Oman. This framework consists of four main dimensions including (a) Organisational security culture, (b) information security processes, (c) security technologies, and (d) environment pressures. It hypothesises the critical factors for effective information security compliance in organisations, and is tested and validated using structural equation modelling with the use of survey data collected from Omani public organisations. His study reveals that management commitment, awareness and training, accountability, organisational loyalty, audit and monitoring, process integration, technology capability, technology compatibility, technology reliability, legal pressures, and social pressures are critical to the development of effective information security compliance in Omani public e-government. He claims that his research demonstrates how socio-organisational factors influence information security compliance in public organisations to promote e-government. He also provides an in-depth investigation of the critical factors for information security compliance, which provide the Omani government with useful guidelines on ensuring public information security in e-government. Such guidelines are also useful for other developing countries in their e-government development endeavour.

Every organisation needs information security solutions to protect their information assets and to be able to achieve an effective information security culture. Kraemer, Carayon, and Clem (2009) explore the human and organisational factors that lead to

information security vulnerabilities. They recommend an integrated, multi-layered approach to improve information security culture.

The next part of this chapter addresses critical success factors that influence organisational information security culture.

2.11. Organisational Information Security Critical Factors

Critical factors are defined as measures of key areas in organisations that, if they are satisfactory, will assure success within and outside of the organisation. (Rockart, 1979). Leidecker and Bruno (1984) define CSFs as events that must go as planned for the business to reach its goals. Vedder (1992) argues that managers may use CSFs as descriptions, predictors, and guidelines for achievement levels. This research focusses on what the researcher considers the most important organisational factors that affect the development and maintenance of information security culture and practice in Omani public organisations. This section briefly discusses critical organisational factors, believed to have a direct impact on the successful development and maintenance of a culture of information security in Omani public organisations.

Figure 2-17 illustrates these factors, which are top management support, information security policy, and training and awareness programs.

Figure 2-17: Research Related Work: Critical Organisational Factors. Source: Self

The research field review identifies significant agreement around the impact these factors on information security and information security culture. Although this thesis identifies more than three critical factors that have an impact on the development of an information security culture in Omani organisations. Nevertheless, the factors discussed

in the first three sections are considered the most critical ones. The hypothesis study tests these three factors in the findings chapters.

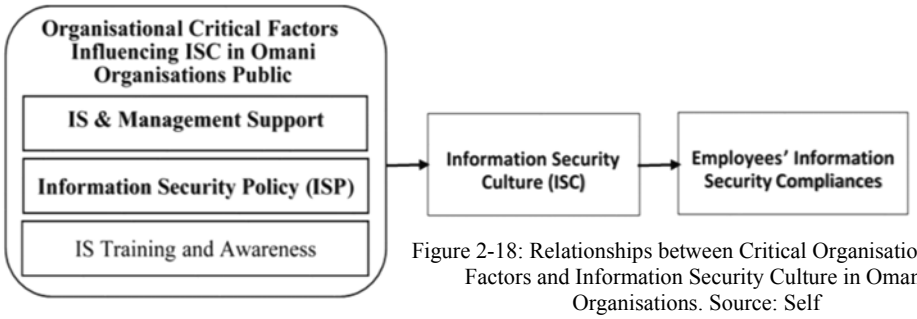

Figure 2-18: Relationships between Critical Organisational Factors and Information Security Culture in Omani Organisations. Source: Self

The literature field review demonstrates that senior managers have important responsibilities, such as the aligning of business with information security strategies (Hall et al., 2011; Johan & Rossouw, 2006), and their support for information security is considered an important organisational factor essential in promoting the information security culture in their organisations.

The following section examines the relation of top management to a successful information security culture.

2.11.1. Top Management Support and Commitment

The information security literature identifies constructive top management support as the most frequent variable hypothesised to contribute to Information Security implementation success. (Markus, 1981; Sharma & Yetton, 2003). Ruighaver et al. (2007) argue that information security is primarily a management problem within an organisation, and how management deals with information security is a direct reflection of an organisation's culture. Management can ensure a sufficient allocation of resources and act as a change agent to create a favourable environment. (Kankanhalli et al., 2003). Creating a safety culture within the organisation may encourage employees to take an interest in helping shape effective information security within an organisation. (Van Niekerk & Von Solms, 2010).

Top management involvement is critically essential to the design, implementation, effectiveness and success of information security management within organisations. (Barton et al., 2016; Alavi et al., 2014; Sharma & Dash, 2012; Van Kessel, 2012; McFadzean et al., 2006; Liang et al., 2007). Moreover, top management support and commitment can drive organisational changes and improve employee compliance. In addition, top management plays a major role in developing and enhancing an

appropriate working culture. (Van Niekerk & Von Solms, 2010; Chang &Lin, 2007; Kritzinger & Smith, 2008).

Effective information security requires top management to have clear expectations about information security programs, the ability to evaluate the organisation's risk posture, and the vision to define information security objectives that are in alignment with the strategic direction and goals of the organisation. Furthermore, Alizki and Weir (2016) argue that the role of management is important to the development of organisational culture and cultural change. They add that, while management need not focus on organisational security culture as an explicit perception, the attitude they display to their subordinates through their involvement in daily operations regarding information security will influence employee compliance with security rules and practices.

The field research review also identifies top management support as the most frequently cited factor in establishing a security conscious organisation. In recent years, many studies have investigated the importance of management support, including the research conducted by Knapp, Marshall, Rainer, & Ford (2006). Using a grounded theory approach, the authors questioned 220 certified security professionals, considered industry experts in information security (CISSP), from across 23 countries and multiple industries. They set two open-ended questions, as follows:
What are the top five security issues facing organisations today? And.
What are the top five security policy related issues facing organisations today?
Two major themes emerged on analysing the answers. The first theme was the positive influence of top management support on the security culture and the second theme was the positive influence of top management support on the level of security policy enforcement. These two themes were validated as significant findings with strong support from the quantitative data analysis carried out as part of this thesis. In particular, top management support was found to have a great impact on information security compliance in Omani organisations.

Top management commitment is a prerequisite for effective development, implementation, and maintenance of information security programs within organisations. (Barton et al., 2016; Kayworth & Whitten, 2010). Additionally, top management has the authority to influence other employees and is more likely to succeed in overcoming organisational resistance and cultural barriers, (McCrohan & Dutta, 2002), and their involvement and commitment to an information security

program is vital to promoting compliant, proactive, and security-conscious users. (D'Arcy & Greene, 2009). When managers demonstrate a behaviour that reflects their deep concern and prioritise information security, their employees will follow them. When employees believe that management cares about security, they become more inclined to cooperate to improve security. (Choudhry et al., 2007).

In an attempt to understand how top management can influence information security compliance, Hu et al. (2012) develop a model that integrates the role of top management, organisational culture, and the theory of planned behaviour. They find that top management participation in information security initiatives has significant direct and indirect influences on employee perceptions of what others perceived to be important, think about their actions (subjective norms), and influences employee perceptions of management skill and control over the intended security outcomes, (perceived behavioural control). Several scholars (Cialdini et al., 1991, 1990; Conner & Armitage, 1998) argue that different types of norms, such as descriptive norms, injunctive norms, and moral norms should be added to the Theory of Planned Behaviour (TPB) to fully reflect the range of influence of social norms.

Kajava et al. (2006) believes that commitment is about getting personally involved with information security initiatives. Further, if management understands information security and can convey that understanding to employees, its influence will increase the success of information security culture and information security projects. (Puth & Ewing, 1998). According to Puth and Ewing (1998), managers enforce the culture of organisations through communication, and over time, the interaction affects the culture.

Figure 2-19: Relationship between Top Management Support and Information Security Culture in Omani Organisations. Source: Self

The influence of top management's actions regarding employee beliefs, attitudes, and behaviours has not attracted enough attention from scholars in the field. Von Solms and von Solms (2004) develop arguments based on their teaching and consulting experience, but they lack theoretical grounding. Alternatively, Puhakainen and Siponen (2010) provide circumstantial evidence of the importance of top management support in influencing employee behaviours towards information security compliance, and call for quantitative studies to complement their findings.

Finally, a successful security-aware culture depends on managers who can balance risk and rewards based on adequate information (Tipton & Krause, 2009; McFadzean et al., 2006), and who can assist with the improvement of security awareness by providing extensive training as well as enforcing and maintaining staff adherence to organisation security policy. This helps develop a positive staff attitude towards the organisation's security program, and ensure that staff members are accountable for their security actions and decisions.

Within these senior management activities, developing and implementing information security policy, and promoting information security awareness and training, are the most important components of security programs. (Soomro et al., 2015; Ma et al., 2009). They have a significant role in preventing organisational data from being breached. (Bulgurcu et al., 2010). Whitman (2004) argues that the effectiveness of information security relies on three key factors: information security policies, security mechanisms (controls), and information security awareness, all within the control of senior management.
The following three sections explore work in the field with regards to training, culture, and policy.

2.11.2. Information Security Policy

Information security policy (ISP) is fundamental to information security. It reflects the management expression of overall intentions and direction of the organisation. It contains all the guidelines, and rules that employees must comply with. It communicates the vision of the place of information security in the organisation, and assesses its information security needs to justify the deployment of appropriate security controls. (Peltier, 2013).
It is described by Olson et al. (2001, p.73) as the "...set of laws, rules and practices that regulate how an organisation manages, protects and distributes resources to achieve specified security policy objectives. To be meaningful, these laws, rules and practices must provide individuals (with a) reasonable ability to determine whether their actions violate or comply with the policy". Furthermore, Cheng et al. (2013, p.448) define an ISP as a "written statement that defines the requirements for organisational security management, the employees' responsibility and obligations, sanctions and countermeasures for non-compliance". Hedström et al. (2013) and Karlsson et al. (2015) confirm that definition. Ratner et al. (2013) define ISP as social, political, legal, economic, and technological stipulations about security enforcement in an organisation.

Wood (2003) explains that policies act as a clear statement of management intent and are central to virtually everything that happens in the information security field. Without a vital policy document, overall guidance will be lacking and managerial support called into question. Information security policies are sometimes framed in a life-cycle context with emphasis on development, enforcement, and maintenance, such as to be consistent with business objectives (Hare, 2002; Howard, 2003).

To meet the needs of an organisation, a good ISP should be easy to understand, of practical application, capable of implementation, enforceable, and proactive. It should avoid absolutes and meet business objectives. The policy should identify what is to be protected (the intent), who is responsible (responsibility), where it fits within the organisation (scope), how compliance will be monitored (compliance), when the policy takes effect, and why it was developed. Although every organisation's policy document is unique reflecting specific business objectives, international standards such as ISO 27002 offer a model structure for an organisation's policy document. (Danchev, 2003; Wood, 2005; Greene, 2014).

Much of the existing information security scholarly work is generally about information security policy and not specifically about information security practice. Some of this research focusses on information security policy planning and its role in establishing an appropriate organisational culture favourable to information technologies. (King & Zmud, 1981). Other study links the effect of organisational culture on information security policy and managerial effectiveness. (Beachboard, 2004). It is widely recognised that many security incidents are caused by human behaviour, rather than technical failures (Beautement et al., 2008; Schneier, 2000), which demonstrates negligence or ignorance of the information security policy within an organisation. David (2002) claims an information security policy needs to be enforced in order to make it effective. Enforcement helps secure the organisation's asset from any internal or external threat, because fear of sanctions and other consequences may deter positional abuse. (Parker, 1981). Rewarding good practice may also support enforcement. (Leach, 2003).

Knapp et al. (2009) in their research on the policy process model, establish organisational culture as a key internal influence on information security policy process. This organisational culture significantly determines the overall attitude of employees towards security. Thus, creating an information security policy is one of the early steps towards mitigating risks associated with the unacceptable use of organisational information assets

This study assumes that there is a strong influence of information security policy on employee behaviours and security discipline and the development of successful information security cultures in Omani public organisations.

Figure 2-20: Relationship between Information Security Policy (ISP) and Information Security Culture in Omani Organisations. Source: Self

Employee education regarding the importance of security awareness should be a priority of an organisation.

The next section sheds light on the third critically important factor, i.e. information security education, training and awareness.

2.11.3. Information Security Awareness and Training

Puhakainen and Siponen (2010) highlight the findings of the link between cognitive learning and information security communication. Cognitive learning is crucial to ensure a long-term attitude change in employee attitudes. Information security communication is about integrating information security within other communication in the organisation, so that it is not just a theme that is discussed once. The communication should also encourage all the appropriate stakeholders including management and users to share information proactively with one another. Simon (1957) classifies training as a key mechanism of organisational influence. Organisations train and instruct members to internalise knowledge and skill, enabling them to make decisions consistent with organisation objectives. As applied to security, the topic of training is linked with awareness. An organisational awareness program is often the initial phase of a broader security training program. Security awareness helps reinforce training materials through an ongoing cycle of security reminders and events. (Hansche, 2002). Training and awareness programs can be used to influence the culture of an organisation (Schein, 1995) by promoting favourable security practices and mind-sets.

Whitman and Mattord (2013) define information security awareness as a dynamic process, and any awareness program must be continually measured and managed to stay ahead of changes in risk profiles. It is about ensuring that all employees in an organisation are aware of their roles and responsibilities in securing the information they work with (Kritzinger & Smith, 2008; Schultz,2004; Siponen, 2001; Thomson &

Von Solms, 1998), such that they can be held accountable if this information is compromised. Knapp et al. (2009) reveal that awareness is often viewed as a tool to address and improve the overall behaviour and conduct of employees. It represents raised user consciousness and understanding of security issues and strategies to deal with them (Dinev & Hu, 2007), and it increases the adoption of ISPs and countermeasures. (Tsohou et al., 2008; Parker, 1981).

Training can help users to explore the required information and develop an effective understanding of how to implement policy. Security awareness and training can be delivered in a variety of ways, either alone or in conjunction with each other. The delivery media could include: classroom style training, a security-awareness website, helpful hints on computers when they start up and/or e-mailing helpful hints on a weekly or monthly basis, or utilising visual aids like posters, as well as regular reminders, ethical codes of conduct, and the declaration of an organisational policy that describes appropriate uses of system resources. (D'Arcy et al., 2009). Topics addressed by security awareness training should consist of existing organisational policies and procedures (how they tie in with each aspect of the business, if they do), physical security, desktop security, password security, phishing, hoaxes, malware, and copyright with regard to file sharing. These topics will help employees understand why security awareness is important and guide them in preventing and responding to security incidents.

Information security awareness can be understood as the general knowledge level of the personnel regarding risks. It informs training and awareness programmes coupled with management's commitment to facilitate the development of the appropriate security perceptions among employees. (Durgin, 2007; Fagerström, 2013). Researchers such as Nosworthy (2000), Thomson et al. (2006), Parsons et al. (2010), and Herold (2011) argue that training and awareness help to improve an information security culture and contribute to the protection of information from an employee perspective. (Kerko, 2001).

Some researchers have mistakenly simplified culture as synonymous with security awareness and training. For example, Rotvold (2008, p.32) argues that, "if management commitment is increased, and the security awareness goals are communicated and communicated often, progress and improvement can be made in creating a security culture". While security awareness and training may contribute to a favourable information security culture, researchers should be careful not to conflate security awareness, training and information security culture. Nevertheless, an ISP combined

with awareness can help to create a desirable information security culture. (Gaunt, 2000; Herath & Rao,2009).

Finally, the related fieldwork shows that security awareness is underfunded, under-represented, and generally applied in an ad-hoc process and in a reactive manner. Security awareness is highly unstructured in most Omani organisations and communication of security guidelines is generally at a basic level. Therefore, the current study argues that information security awareness should form an integral part of any organisations' overall information security management plan, as a critical factor contributing to information security compliance and the successful development of an information security culture. The findings from the interview and survey analysis conducted as part of the current study confirm this argument and prove to be highly pertinent to Omani organisations.

Figure 2-21: Relationship between Information Security Awareness, Training and Education and Information Security Culture in Omani Organisations. Source: Self

So far, the second part of this chapter has reviewed the related field research work linked to the critical socio-cultural and organisational factors, that are mentioned in figure 2-1 and ways in which management can promote information security effectiveness through policy, training and awareness. The following section sheds light upon the role of information security rewards and punishment. This element is not part of the hypotheses tested diagram in the findings chapter, but the researcher thinks it is important and has an influence on information security culture development.

2.11.4. Information Security Motivation

Some researchers argue that having a system in place to monitor information security behaviours can be challenging. (Herath & Rao, 2009). While proposing a model of the incentive effects of penalties and pressures, Willison (2006) argues that organisations should focus on the actual behaviours of offenders at various stages of their misuse to implement controls (safeguards) that will reduce the employees' ability to misuse information at any stage, as a way to effectively influence the decision-making processes of their employees.

One accepted principle is that rewards are more effective at changing behaviour than punishment (Schneier, 1974), though research into organisational behaviour suggests this is not always the case. For example, O'Reilly and Weitz (1980) examine the

supervisory behaviour of 141 employees and found that supervisors who were more likely to use sanctions had higher employee performance than those who avoided the use of sanctions. Previous research also yielded conflicting results regarding the effectiveness of sanctions and rewards for information security behaviours. Herath and Rao (2009) report that the certainty of detection (but not the severity of punishment) was a significant predictor of employee compliance with security policies, suggesting that the presence of penalties does motivate employees to comply with security rules, while enforcing more severe penalties does not in itself, deter information security abuse. Consequently, Chen et al. (2012) conclude that information about punishment should be conveyed through security policies and security education and training, emphasising the vital role of procedural security countermeasures in managing employee security behaviour. Furthermore, D'Arcy et al. (2014) emphasise the importance of user awareness of organisational security requirements and the consequences of breaking the rules, which can be achieved through clearly-written security policies and periodic security education and training.

This study claims that punishment has a positive effect on security behaviour intentions, and asserts that if public organisations in Oman punish employees who misuse organisational security assets as a technique, this will spread information about and compliance with the information security culture, and limit information security violation.

Figure 2-22: Relationship between Reward and Punishment and Information Security Culture in Omani Organisations. Source: Self

The researcher agrees with D'Arcy et al. (2009) and Straub (1990), who find that security behaviours improve when the penalties for noncompliance are explicitly stated. Furthermore, Li et al. (2010), and Guo and Yuan (2012), suggest that formal workgroup sanctions have a greater deterrent effect on information security violations. The study argues that, for effective motivation, rewards and punishment must be applied consistently, fairly, and evenly for a significant period. If nobody is ever sanctioned or rewarded, or if this occurs only sporadically, the motivational value is lost. Rumours of failure to take management action may travel faster than the news of effective actions. The next section sheds light on information security and business alignment.

2.12. Information Security and Business Alignment

Business-aligned security management is based on business objectives, values, and needs, rather than being technology-asset focused. (Spears & Barki, 2010; Herath et al., 2010). The relationship between business operations and information security has become increasingly important in enterprise systems. (Yaghubi & Modiri, 2014). According to Neubaueretal (2006), the integration of information security and business process methodologies is a step towards reducing the gap between information security and business. However, aligning information security with an organisation's goals and objectives is considered one of the greatest challenges in information security program. This challenge results from pressure to control security spending while risks, incidents, and losses continue escalating to unsustainable levels. The alignment component refers to the collaborative efforts between information security managers and business managers to align information security practices with business strategies. (Chang et al., 2011). Therefore, business management must lead it. (Kayworth & Whitten, 2010; Ma et al., 2009; Siponen & Oinas-Kukkonen, 2007; Smith & Jamieson, 2006; Van Niekerk & Von Solms, 2010; Von Solms, 1999).

Furthermore, clear alignment of information security controls with business processes is a crucial element for reducing the number and the severity of security breaches, confirming operational process as an important dimension. According to Williams (2001), information security governance is responsible for aligning information security requirements with a business. This alignment requires an organisational model to be established which, as noted by Britto (2011), should include people, processes, and technology.

Being business aligned means that it is the responsibility of the business and not the security function to determine acceptable levels of security risk. (Von Solms & Von Solms, 2004). Furthermore, when connecting information security to business processes, the business value of information security should be measured. (Scholz, 2004; Neubaueretal, 2005). According to Su et al. (2007), approaching information security from a business perspective is necessary because organisations have different business drivers that determine their different requirements for information security.

2.13. Chapter Summary

This chapter has reviewed earlier published work and studies relevant to the research topic and its related concepts and issues. Existing and previous fieldwork and studies were analysed to investigate different aspects and critical factors that may affect the successful implementation of an information security culture in public organisations in

Oman. The first part of this chapter considered information security in general, and discussed its definition, elements, sources of threat, components, risk assessment and management, and information security control and countermeasures. The publications selected for discussion were specifically included in the related work review for their major contributions and their unique approaches to information security. This was in the context of other works studying the relationship between aspects of national and organisational culture and information security culture.

This was explored in the second part of this chapter and focused on the following factors that are believed to have a direct effect on the development of organisational information security culture:

1. National culture factors and their effects on organisational information security culture, such as:
    - High Power Distance
    - High Uncertainty Avoidance
    - High Collectivism Values
    - High Level of Trust
2. Organisational factors and their effects on information security culture, such as:
    - Lack of Management Support and Commitment
    - Lack of Information Security Policy
    - Lack of Information Security Awareness and Training programs
    - Lack of Rewards and Punishment system
3. Alignment of information security with business strategies, plans, and goals.

The author of this study agrees with earlier research, which showed that non-technological issues are critical for organisational information security culture, and therefore, more attention should be given to these issues. Further, national and organisational culture can influence information security culture in many ways.

In the real world setting, an employee's behaviour is based on values, beliefs and knowledge about information security requirements. This is gained from both social dimensions (i.e. national and organisational culture values) and management activities (by enhancing employee information security knowledge through training, awareness and empowerment systems). Based on this, employees process the information and then make decisions affecting the security of the organisation’s information. Thus, the link between national culture and information security culture is primarily a link between

values and behaviours of an organisation's employees. However, existing research into information security culture is inadequate because most of it lacks empirical evidence. Research is often limited to a small number of factors in investigating a complex phenomenon.

The existing literature on Oman mostly provides a view of Oman ICT development, and very rare literature about information security in Oman. The analysis of related research work identifies no systematic descriptions of the behaviour of Omani managers and employees, particularly, in relation to information security and information security culture. This review of related fieldwork identifies an increasing need for comprehensive and specific approaches to information security to assist in developing and deploying information security culture in the context of developing countries, including Oman.

In general, the related work review demonstrated that there is still much to be developed in the field of information security culture concepts and practices, especially, in the case of developing countries, such as Oman. The gaps identified in the existing studies have not only informed but also motivated the present research, which aims to establish a foundation for future researches into information security culture development in public organisations in developing countries in general and in Oman specifically.

The next chapter is the methodology chapter, which describes the research design and methods that were followed to achieve the study objectives.

Chapter 3. Methodology

"Knowledge of the case faces hazardous passage from writer to reader. The writer needs ways of safeguarding the trip."
- (Stake, 1992, P.241)

3.1. Introduction

A research methodology is a systematic approach to studying a research problem; it includes the theoretical underpinning of the research as well as the collection, analysis, and interpretation of the data. (Kothari, 2004). According to Crotty (1998, p.3), it is "the strategy, plan of action, process or design lying behind the choice and use of particular methods and linking the choice and use of methods to the desired outcomes". (Crotty, 1998, p.3). Furthermore, it describes and develops the stages that are used to achieve the research objectives. (Creswell 2003; Johnson & Christensen 2004; Tashakkori & Teddie 1998). A research methodology is the overall approach to the research process, and it should not be confused with the research methods, which are the various means by which data can be collected and analysed. (Hussey & Hussey, 1997). The previous chapter reviewed related academic work in this field to build the theoretical foundation of this research. This chapter presents in detail the research methodology used in this study.

After introducing the research question and hypotheses, this chapter discusses issues related to the research methodology, such as outlining the philosophical paradigms, research strategy, as well as the research methods that include quantitative and qualitative (mixed-method) techniques. The sample of participants, and the tools used to collect the data are also explained. The last sections of the chapter discuss issues of validity, reliability, and ethics, and the chapter closes with a summary of the main topics.

Eldabi et al. (2002) maintain that to conduct any type of research, the researcher should follow a well-defined research methodology based on scientific principles. In this context, Hussey and Hussey (1997) argue that research can be classified as follows:

First, the reason for the research, (the purpose of the study); Second, the method used by the researcher to collect and analyse data, (the process of the research). Third, whether the researcher is moving from the general to the specific or vice versa (the logic of the research). And Fourth, whether the research is attempting to investigate a specific, problem, or make a general contribution to knowledge. The choice of any research

method depends on the research philosophy or paradigm that the researcher follows (Creswell, 2003). The next section explains research philosophy

3.2. Research Philosophical Paradigm

Research is considered an original investigation to gain knowledge and understanding. Burns (2002, p. 3) defines it as "a systematic investigation to find answers to a problem". The purpose of this research is to explore relationships to uncover meaning and facilitate the construction of explanations for the defects in the culture of information security within Omani public-sector organisations that lead to unsatisfactory information security practices in these organisations. This research purpose is achieved by investigating the current state of information security practices in Omani public organisations, and examining the critical socio-cultural, and organisational factors, that impact upon the adoption of information security culture in those organisations.

The related fieldwork review identified some of the interactions between these concepts. In addition, this relationship between information security culture and practice was developed further through a set of hypotheses that provide answers to the secondary research questions, and provided a guide to generating the evidence to answer the research questions. (Denzin & Lincoln, 2011). The research is not intended to discover an absolute truth or change a situation, because this is beyond the researcher's capacity as an employee at one of these organisations. Nevertheless, the researcher suggests some recommendations regarding the research subject, with decisions of follow up action being down to the organisations themselves.

Selecting the appropriate research methodology for a research project depends on the nature of the research and research problem. In this study, the researcher chose to investigate the research problem from the following different perspectives:

- A synthesized related work review to identify information security behaviours, critical success factors and develop knowledge and suitable techniques to facilitate discussion of the research problem.
- An integrated mixed-methods (e.g. qualitative and quantitative) approach: A qualitative approach based on the opinions and perceptions of senior security and IT managers in Omani organisations was used to assess the level of information security culture and practice in their organisations. In addition, a quantitative approach, justified by the need for a widespread survey questionnaire with hypothesis testing.

- The third perspective is the researcher's personal observation and work experiences.

It is critical for any research to be guided by a set of assumptions regarding its philosophical standing. An assumption from a scientific perspective, is that a hypothesis should be formulated and tested using specific measurement techniques. (Bryman, 2012). Another assumption is that there is a sensitive approach to addressing special qualities of people and social institutions. (Bryman, 2012; Creswell, 2012). These assumptions, concerning how a phenomenon is studied, are called epistemological assumptions or paradigms. The scientific perspective is known as a positivist approach as distinct from the interpretive approach. In addition to positivist and interpretive epistemological assumptions, Creswell (2003) suggests pragmatism as another paradigm. According to this paradigm, the researcher is not committed to a single set of assumptions or philosophy. Pragmatists argue that in social science research, researchers should stop asking questions about reality and laws of nature. The concern should be with applications and solutions to problems; the problem is more important than the methods. Therefore, researchers should use all available approaches to understand the problem and find solutions for it.

The philosophical paradigm (worldview) establishes the point of view from which research is conducted. (Creswell, 2014). Smith et al. (2002) argue that there are at least three reasons that an understanding of philosophical issues is useful. First, it can help to clarify research designs. Second, knowledge of philosophy can help identify which designs will work and which will not, and should indicate the limitations of different approaches. Third, knowledge of philosophy can help researchers identify and create designs that may be outside of their experience. It may also suggest how to adapt a research design according to the constraints of different subjects of knowledge structures.

According to Brennan et al. (2014); Saunders et al. (2012); Terre Blanche and Durrheim, (1999); Chua (1986); Guba and Lincoln (1994); Crotty (2003), the typology of social research processes revolves around four main elements: epistemology, theoretical perspective, methodology, and methods. Creswell (2009) confirms this, and suggests that four worldviews emerge with respect to the philosophical assumptions underpinning a research approach. These comprise post-positivism, constructivism, advocacy and participatory research, and pragmatism. Pragmatists believe that they can use all available methods, including quantitative, qualitative, or mixed methods. Researchers are primarily concerned with what and how to research in a way that best meets their needs and purposes, and should provide reasons for their choices. However,

Bryman & Bell (2015), argue that a paradigm can have more than the three sets of assumptions described above. Although those three are the core components of a research paradigm, studies might also consider issues of axiology and rhetoric.

Table 3-1 below, adapted from Salma Patel (2015), gives a detailed overview of each of these paradigms.

Table 3-1: Detailed Overview of Paradigm Types. Sources: Salma Salam Patel, 2015

Paradigm	Positivism	Constructivist /Interpretive	Pragmatism
Ontology What is reality?	There is a single reality or truth (more realist).	There is no single reality or truth. Reality is created by individuals in groups(less realist).	Reality is constantly renegotiated, debated, interpreted in light of its usefulness in new unpredictable situations
Epistemology How can I know reality?	Reality can be measured and hence the focus is on reliable and valid tools to obtain that.	Therefore, reality needs to be interpreted. It is used to discover the underlying meaning of events and activities.	The best method is one that solves problems. Finding out is the means, change is the underlying aim.
Theoretical Perspective Which approach do you use to know something?	Positivism Post-positivism	Interpretivism (reality needs to be interpreted) • Phenomenology • Symbolic interactionism • Hermeneutics Critical Inquiry Feminism	Deweyan pragmatism Research through design
Methodology How do you go about finding out?	Experimental research Survey research	Ethnography Grounded Theory Phenomenological research Heuristic inquiry Action Research Discourse Analysis Feminist Standpoint research etc	Mixed methods Design-based research Action research
Method What techniques do you use to find out?	Usually quantitative, could include: Sampling Measurement and scaling Statistical analysis Questionnaire Focus group Interview	Usually qualitative, could include: Qualitative interview Observation Participant Non participant Case study Narrative Theme identification ect.	Combination of any of the above and more, such as data mining expert review, usability testing, physical prototype

The readers of a thesis need to have insight into the philosophical paradigm in which the research is situated to eliminate any philosophical confusion. Burrell and Morgan (1979, p.24) explain that having a particular paradigm means, "to view the world in a particular way". This research adopts a mixed-methods approach with pragmatic worldview philosophical assumptions, as the researcher believes this to be the best way to meet the main aim and objectives of the study. Pragmatism, as Creswell (2009) explains, focuses on how to understand the research problem, and frees the researcher from being committed to one method or technique.

Mixed-methods, also known as deductive/inductive (Creswell, 2009), design with a pragmatic worldview was selected to provide a broad base for the investigation. Creswell (2009, p.7) supports such a choice by stating that, "for the mixed-methods researcher, pragmatism opens the door to multiple methods, different worldviews, and different assumptions, as well as different forms of data collection and analysis". This type of design was considered to provide a broad and holistic view of the status of information security within Omani public organisations, while at the same time

allowing issues identified to be explored in depth. In addition, using a mixed-methods design reinforces the results and findings to ensure the rigour of the research.

The next section addresses the main research question and sub questions and the related hypotheses.

3.3. Research Questions and Hypotheses

This study uses several hypotheses to address the research objectives, and to answer the following research question and sub-questions.

3.3.1. Research Questions

One of the essential techniques, in choosing a research method, is specifying appropriate research questions for the study. (Yin, 2014). Eisenhardt (1989) argues that determining the research question(s) for a study is an essential stage in building the research design. According to Yin (2003), determining the research questions is the most important task, and it requires specific preparation, such as reviewing the existing related work in the field of study. Arising from the preliminary related work review, and to address the research problem and achieve its aim, this study attempts to answer the following main research main (RM-Question) and sub questions (RS-Questions):

RM-Question: What is the current state of information security culture and practices in public and private organisations in the context of Oman? What are the critical socio-cultural and organisational factors that may affect the information security performance and hinder the development and maintenance of an effective information security culture in these organisations?

The main research question stated above was supplemented by the following sub-questions, which contain several hypotheses that are discussed in chapter six.

RS-Question#1: What is the current level of compliance with information security best practices in Omani organisations? What is the difference between public and private sector organisations in this regard?

RS-Question#2: What are employees' attitudes towards the role of rewards and punishment in motivating personnel to commit to good information security practices in Omani organisations?

RS-Question#3: How does the social factor "education" affect information security performance in Omani organisations?

RS-Question#4: What is the relationship between critical organisational factors and information security performance; and the development, and maintenance of an information security culture in Omani organisations?

RS-Question#5: What is the relationship between the development and maintenance of an information security culture, and information security disciplines and practices in Omani organisations?

RS-Question#6: What is the relationship between critical cultural factors and information security behaviours and practices; and the development, and maintenance of an information security culture in Omani organisations?

It is imperative that the culture of an organisation is reflected in attitudes towards information security throughout the entire organisation. (Vroom & von Solms, 2004).

The next section introduces the research hypotheses model to examine the interactions between critical socio-cultural and organisational factors, the effective adoption and maintenance of an information security culture (ISC), and employee behaviours around information security.

3.3.2. Research Hypotheses Testing Model

Following the literature review set out in the preceding chapter, a theoretical framework was developed to direct the methodology and further fieldwork of the current study. Figure 3.1 shows the hypotheses suggested by the researcher to examine the relationships between the critical socio-cultural and organisational factors, the organisational information security culture, and information security behaviours and practices.

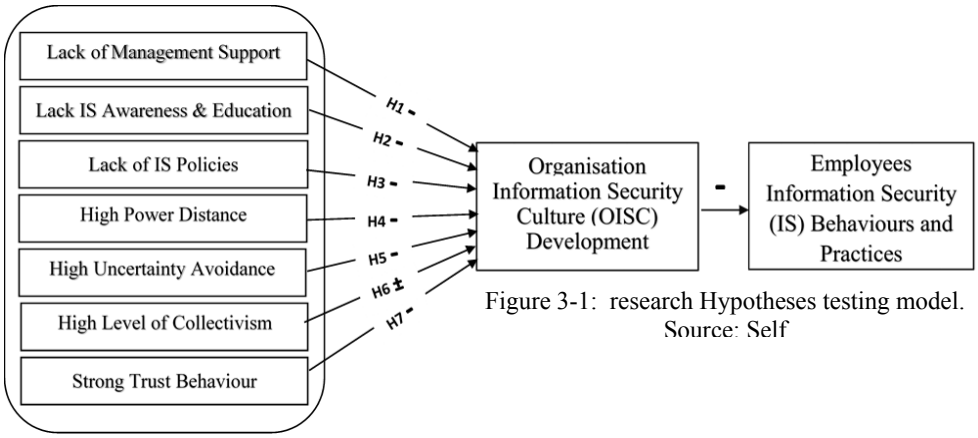

Figure 3-1: research Hypotheses testing model.
Source: Self

Research Hypotheses

Collis and Hussey (2003, p.10) define a hypothesis as "a proposition which can be retested for association or causality by deducing logical consequences which can be tested against empirical evidence". Therefore, after determining the main research question, several appropriately relevant hypotheses were formulated. These hypotheses were designed according to the findings revealed in the related work review (Chapters 2), and the context of the study. The study tested the following hypotheses that relate to the research question:

1- Hypotheses related to the organisation's education level factor:

H#1: Education level positively affects information security performance in Omani organisations.

The following sub-hypotheses are drawn from the previous (H#1) main hypothesis:

H#1.1: Education level is positively associated with information security policy in Omani organisations.

H#1.2: Education level is positively associated with information security training and awareness in Omani organisations.

H#1.3: Education level is positively associated with managerial support for information security in Omani organisations.

H#1.4: Education level is positively associated with employee commitment to information security disciplines in Omani organisations.

H#1.5: Education level is positively associated with an organisation's information security practices in Omani organisations.

2- Hypotheses related to the critical organisational factors:

H#2: Lack of management support and involvement negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#3: Lack of information security awareness and training negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#4: Lack of information security policy negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

3- Hypotheses related to information security disciplines and practices:

H#5: There is a positive correlation between the information security culture and employee commitment to information security disciplines in Omani organisations.

H#6: There is a positive correlation between the information security culture and information security practices in Omani organisations.

4. Hypotheses related to the critical cultural factors:

H#7: High power distance negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#8: A high propensity to avoid uncertainty negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#9: High Collectivism negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#10: High Trust negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

After identifying the research main and sub questions and hypotheses, it is essential to understand the philosophical issues of the research.

3.4. Research Design and Strategy

The purpose of the research design is to guide the researcher through the process of collecting, analysing data, and interpretation results. Robson (2002) argued that the research design is the process of turning a research question into a research project. Research designs are type of inquiry within qualitative, quantitative, and mixed-methods approaches that provide specific direction for procedures in a research strategy. They are also referred to as strategies of inquiry (Denzin & Lincoln, 2011). The related work review revealed different classifications used in the research design. For example, the research methodology model proposed by Saunders and Tosey (2013), classifies research strategies by reference to the techniques used to answer the research questions.

Bryman (2012) classifies the techniques presented by Saunders and Tosey (2013) as research strategy or research design. Other researchers such as Creswell (2009) use the terms strategies of inquiry, while research methodologies is the term used by Mertens. (1998). Furthermore, the related work review shows that research design may be determined by the nature of the research problem and the way in which it seeks answers. (Crotty, 1998). According to Kaplan and Duchon (1988), no single research methodology is inherently superior to any other methodology.

The reason for selecting the subject of this research is the ongoing concerns about the lack of information security culture in Omani public organisations, leading to ineffective information security practices and behaviours by employees, so that many of these organisations suffer leakage of sensitive data and documents. Therefore, the primary purpose of this research is to investigate the current state of information security practices and behaviours, and to examine the impact of the critical socio-cultural, and organisational factors on the adoption and maintenance of a culture of information security in Oman. This study objective and the research hypotheses guided the researcher's choice of method, as consistent with Trost (2005) who argues that a study's purpose and problem should determine the choice of method.

This chapter introduces the main methods that were used with the fieldwork instruments to achieve the main aim and objectives of this research.

3.4.1. Choice of Approach and Strategy

The rationale behind research methods and design is to utilise the most appropriate approach to answering the central research question. (Hayes et al., 2013; Yin, 2014). According to Yin (2002), three conditions distinguish different research approaches:

- The type of research question posed:
- The extent of control an investigator has over behavioural events:
- The degree of focus on contemporary as opposed to historical events.

The researcher adopted the pragmatic paradigm to satisfy the research objectives and selected a mixed-methods approach as the vehicle for data collection.

This research combines quantitative and qualitative techniques, to provide a rich contextual basis for interpreting and validating results. (Kaplan & Duchon, 1988). There are three broad benefits of linking qualitative and quantitative data. First, linking them can enable the confirmation and corroboration of research findings. Second, it can help elaborate or develop analysis and provide richer detail. Third, it can initiate new lines

of thinking and provide fresh insight into a given phenomenon. (Miles & Huberman, 1994; Rossman & Wilson, 1984).

3.4.2. Research Overall Process

The research process describes the flow of the research, and identifies and organises data collection methods and analysis techniques and reports the findings.

Figure 3.2 below sets out the research process and contents. The focus of the research was Omani public organisations, aiming to investigate the current state of information security practices and identify the level of information security culture in these organisations.

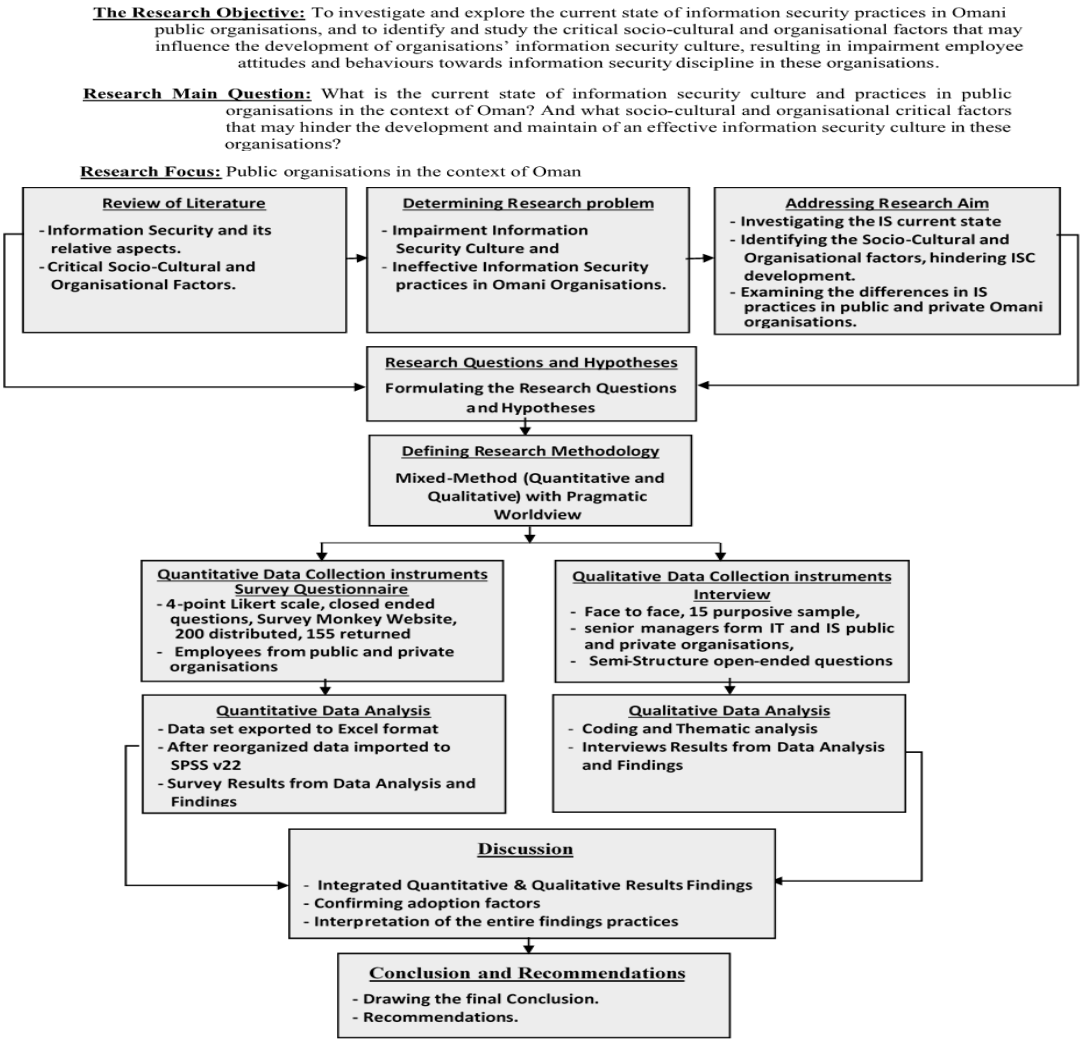

Figure 3-2: The overall Research Process : Source: Self

The diagram illustrates the research sequential mixed-methods design. In this design, quantitative and qualitative approaches were employed within the same research and both approaches have the same priority. (Creswell and Clark 2011).

3.4.3. The Mixed-Methods Approach

The decision to utilise quantitative and qualitative methods was taken after considerable reading and analysis to identify the ideal guide to the research approach, considering the nature of the research questions, the scope of the study, and bearing in mind the complicated and sensitive nature of the subject of investigation. The inclusion of surveys, observations, and interviews, results in a more comprehensive investigation, as quantitative and qualitative data are both utilised in collecting, analysing, interpreting and integrating data. (Creswell, 1998; Leech & Onwuegbuzie, 2007; Yin, 2003b; Johanson & Mattsson, 1987).

According to Creswell and Plano Clark (2006, p.5) mixed-methods is "a research design with philosophical assumptions as well as methods of inquiry. As a methodology, it involves philosophical assumptions that guide the direction of the collection and analysis of data and the mixture of qualitative and quantitative data in a single study or series of studies. The combination of quantitative and qualitative approaches provides a better understanding than one approach alone" (Clark, 2006, p.5).

In social science, according to Wendy Olson (2004), triangulation is defined as the mixing of data or methods, such that diverse viewpoints cast light upon the topic. Johnson and Onwuegbuzie (2004) argue that a methodological approach is mixed when the researcher combines quantitative and qualitative data and methods in a single study. According to Jacobsen (2002), this combination limits the disadvantages of each method. Creswell (2003, p.16) proposes: "Converge quantitative and qualitative data in order to provide a comprehensive analysis of the research problem".

It is useful to utilize mixed methods when the research questions cannot be fully addressed by quantitative or qualitative methods individually. (Ivankova, Creswell, & Stick, 2006). Partially mixed-methods allow quantitative and qualitative inquiry to be conducted concurrently and then mixed at the interpretation stage of data analysis. (Leech & Onwuegbuzie).

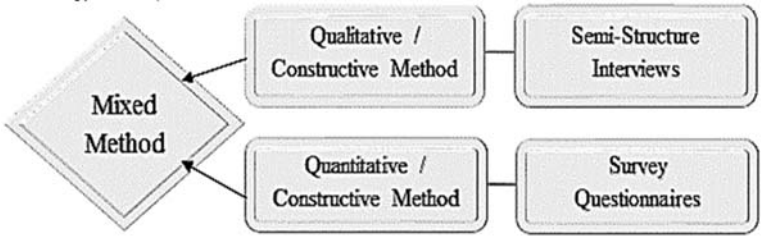

Figure 3-3: Mixed-Methods Components. Source: Self

In the current study, a mixed-methods design was adopted based upon a philosophical foundation of pragmatism to study how social, cultural and organisational issues affect attitudes toward information security culture in Omani public organisations. A mixed-

methods approach meant that quantitative analysis produces generalisability through mathematical comparisons of large amounts of data, and qualitative data provides richness through individual lived experiences. Greene, Caracelli, and Graham (1989) reference expansion as one of the purposes for mixed research which they define as seeking to extend the breadth and range of inquiry by using different methods for different inquiry components.

Multiple perspectives and a complete understanding of the problem can only be achieved by following a qualitative study with a quantitative study into the identified constructs and relationships. (Clark, 2010). This is in addition to further refining the hypotheses and research instrument development. (Morris & Venkatesh, 2000). Such a combination of methods to answer a research question is called a sequential mixed-methods design. (Narasimhan et al., 2009). The aim of mixed methods, as Johnson and Onwuegbuzie (2004) suggest, is not to replace either the quantitative or the qualitative approaches, but to benefit from the strengths and reduce the weaknesses of each of these techniques. A mixed-methods approach enables researchers to have a broader and complimentary view of the area being researched. (Collins & Hussey, 2003). In addition, research is becoming "increasingly interdisciplinary, complex, and dynamic" (Johnson & Onwuegbuzie, 2004, p.15). It is therefore necessary for researchers to complement one method with another.

Table 3-2: Mixed methods designs. Source: Creswell et. al., 2009

Design Type	Description
Sequential Explanatory	*A two phase design where the quantitative data is collected first followed by qualitative data collection. The purpose is to use the qualitative results to further explain and interpret the findings from the quantitative phase. For example, a survey may be used to collect quantitative data from a larger group. Members of that group may then later be selected for interviews where they can explain and offer insights into their survey answers.*
Sequential Exploratory	*a two phase design. The qualitative data is collected first, followed by collection and analysis of quantitative data. The purpose of this design is to develop an instrument (such as a survey), to develop a classification for testing, or to identify variables. Using the information from journals or diaries to develop an appropriate survey to administer to a larger sample would be an example of this design*
Sequential Transformative	*This type of design also has two phases, but allows the theoretical perspective of the researcher to guide the study and determine the order of data collection. The results from both methods are integrated together at the end of the study during the interpretation phase.*
Concurrent Triangulation	*In this design, qualitative and quantitative data are collected concurrently in one phase. The data is analysed separately and then compared and/or combined. An example would be if a researcher collected survey data and*

	interview data at the same time and compared the results. This method is used to confirm, cross-validate or corroborate findings. It is often used to overcome a weakness in one method with the strengths of another. It can also be useful in expanding quantitative data through collection of open-ended qualitative data.
Concurrent Nested	*This design includes one phase of data collection in which priority is given to one approach that guides the project, while the other approach is embedded or nested into the project and provides a supporting role. The embedded approach is often addressing a different question then the primary research question.*
Concurrent Transformative	*Iinvolves concurrent data collection of both quantitative and qualitative data. It is guided by a theoretical perspective in the purpose or research question of the study. This perspective guides all methodological choices and the purpose is to evaluate that perspective at different levels of analysis*

Table 3-2 above shows the mixed-methods approach design, which consists of three main design categories: exploratory design, explanatory design, and triangulation design. (Fraenkel & Wallen, 2008). These designs are further divided into the following six strategies (Creswell, 2009): sequential explanatory design; sequential exploratory design; sequential transformative design; concurrent design; concurrent embedded design; and concurrent transformative design. (Creswell, 2009).

Sequential Explanatory design (separate stages)

- Collect & analyse qualitative
- Collect & analyse quantitative
- Integrated during interpretation phase
- May or may not have theoretical perspective
- ***Purpose:*** use qualitative to assist in explaining and interpreting the quantitative
- Useful with unexpected quantitative results – qualitative examines in detail
- ***Strength:*** separate stages in design, description, reporting
- ***Weakness:*** length of time before the combining of two separate stages (especially if equal emphasis)

Sequential Exploratory design (2 stages)

- Priority in 1st stage
- Collect & analyse qualitative
- Collect & analyse quantitative
- Integrated during interpretation phase
- May or may not have theoretical perspective
- Quantitative assists interpretation of qualitative
- ***Purpose:*** explore a phenomenon (determine the distribution of a phenomenon within a chosen population); grounded theory (testing elements of an emergent theory so that it can be generalized); developing and testing new instrument (psychometrics)
- ***Strength:*** separate stages in design, description, reporting

- ***Weakness:*** length of time before the combining of two separate stages; can be difficult to build from the qualitative analysis to quantitative data collection

Sequential Transformative design (2 stages)

- Either method used first, either priority or equal emphasis
- Results integrated during interpretation phase
- Theoretical perspective drives research not just methods
- ***Purpose:*** employ the methods that will best serve the theoretical perspective (give voice to diverse perspectives, advocate for participants, better understand phenomenon or process that is changing as a result of being studied)
- ***Strength:*** separate stages in design, description, reporting
- ***Weakness:*** length of time before the combining of two separate stages (especially if equal emphasis)

Concurrent Triangulation design (one stage)

- Two methods in attempt to confirm, cross-validate, or corroborate findings within one study.
- Methods offset weaknesses of other method
- Ideally, priority is equal but not always practical
- Integrates results during interpretation phase: convergence strengthens knowledge claims or explains lack of convergence
- ***Strength:*** familiar; well-validated and substantiated findings; shorter data collection than two stage studies.
- ***Weakness:*** great effort and expertise to study phenomenon with two methods; difficulty comparing the results before the combining of different methods; unclear how to resolve discrepancies in findings between methods

Concurrent Nested design (one stage)

- Predominant method that guides project (lesser is embedded or nested, which can address a different question or seek information at a different level)
- Data mixed during analysis phase
- ***Purposes:*** broader perspective than one method (embedded quantitative can enrich description of the sample participants; embedded qualitative describe aspect of quantitative that can't be quantified); one within a framework of the other (e.g., conduct experiment as case study of different treatments)
- ***Strengths:*** shorter data collection; both quantitative and qualitative; gain multiple perspectives from different types of data or different levels within study
- ***Limitations:*** data must be transformed to be integrated within analysis phase; little written guidance; unclear how to resolve discrepancies in findings between methods; unequal evidence before combining of priority of one method makes it difficult to interpret results.

Concurrent Transformative design (one stage)

- Specific theoretical perspective drives research (critical theory; advocacy; participatory research; or a conceptual or theoretical framework)
- ***Purpose:*** theoretical perspective drives all methodological choices (problem definition, design and data source identification, analyse, interpreting, reporting results throughout process)
- Choice of model (triangulation or nested) facilitates theoretical perspective
- Equal or unequal priority during single collection stage
- Integration most often during analysis phase (but can be during interpretation phase)
- ***Strengths:*** transformative framework; shorter data collection; both quantitative and qualitative; gain multiple perspectives from different types of data or different levels within study
- ***Limitations:*** data must be transformed to be integrated within analysis phase; little written guidance; unclear how to resolve discrepancies in findings between methods; unequal evidence b/c of priority of one method makes it difficult to interpret results

It can be assumed that there is no best methodological approach, but there is an approach that is most appropriate for the investigation of a given research question. (Bryman et al., 2008; Denison, 1990; Gill et al., 2010; Jung et al., 2007; Niglas, 2009; Silverman, 2010). The choice of methods tends to be defined as a step between setting objectives and commencing fieldwork during the research process. (Buchanan & Bryman, 2007). It is usually a compromise between several philosophical assumptions, frequently influenced by the resources available and the ability to gain access to organisations and their members to conduct research. (Gill et al., 2010). Quantitative and qualitative research methods investigate and explore different concepts of knowledge, and both methods are designed to address a specific type of research question. While quantitative methods provide an objective measure of reality, qualitative methods allow the researcher to explore and better understand the complexity of a phenomenon.

The explanatory sequential mixed methods design was chosen as the best approach to investigate the current research problem. This approach allows different methods to complement each other. It uses the survey to identify significant issues from the general population of the study. It then uses the interviews to provide more understanding of those issues.

The following section explains the rationale for adopting mixed-methods in this study.

3.4.3.1. Rationale for Mixed-Method Adoption

Of the several reasons for selecting a mixed-methods (MM) approach, perhaps the main one is the researcher's aspiration to solve the problem comprehensively within a single piece of research. (Morse, 2003). Tashakkori & Teddlie (2003), argue that the reason for using a mixed methodology is to contextualise a particular theoretical approach by combining different methods of research, so as to validate the research results. As mentioned before, the choice of a mixed methodology approach is driven by the research question. Thus, when using mixed methodology research, more knowledge of the research subject is gained and the combined strengths of each method produces reliable and valid results. (Creswell & et al., 2004 and Driscoll & et al., 2007). In particular, some aspects of the current study, related to information security policies, management support, training and awareness, required detailed explanation to understand the results better. It was therefore deemed necessary to conduct semi-structured interviews with senior IT and IS managers, so that their rich experience could be used to inform and explain the survey findings and present a complete view of the phenomenon studied.

Notwithstanding the reservations of Creswell and Clark (2007), who claim that research is easier to implement with only one kind of data to collect and analyse at a time, the advantages of mixed-methods are felt to be:

i. Help improve the validity and reliability of the research findings and ensure scientific rigor.
ii. Have the opportunity to synergise the strengths of qualitative and quantitative methods. (Greene et al. 1989).
iii. In contrast with single method approach, mixed-methods research allows researchers to explore and investigate sophisticated issues more holistically and widely. (Fidel, 2008).
iv. Have the ability to address confirmatory and exploratory research questions simultaneously. (Teddlie and Tashakkori 2003, 2009; Venkatesh et al., 2013).
v. Mixed-methods research has the ability to provide stronger conclusions and implications than a single method (Venkatesh et al., 2013). This is because of the different ways each of these techniques works. For instance, qualitative methods are more concerned with the deeper structure of a phenomenon; while, quantitative methods are more interested in the high-level structure of a phenomenon.

vi. Mixed-methods research provides an opportunity for a greater variety of conclusions, which stimulates future research. (Venkatesh et al., 2013). Findings of qualitative and quantitative methods may not be the same and thus require more investigation of the topic to understand reasons for the differences.

Furthermore, in the current study, adopting the positivist quantitative approach was considered appropriate to studying a sample of the population of Omani employees using a survey questionnaire, to draw generalisation about the whole population of employees in Oman. However, positivist research has its limitations, as research findings in positivism studies are only descriptive, thus they lack insight into in-depth issues. (Dudovskiy, 2016). A constructionist qualitative approach was considered as well, as, according to Rubin and Rubin (2005), it is useful to understand experiences, to reconstruct events, to describe social and political processes and to elicit reasons behind particular actions.

Additionally, in this research, information security is not only comprised of technological components, but also has socio-cultural and organisational dimensions. Methods for collecting empirical data were chosen based on qualitative and quantitative approaches in an attempt to grasp this wider meaning in the Omani context, and given the exploratory nature of the study. The research design and the purpose of the study were the drivers to integrate quantitative and qualitative methods that complement each other to produce a precise analysis of the status of Omani information security status.

3.4.3.2. Pragmatic Approach

This research adopted mixed-methods with a pragmatic approach. This pragmatic approach emphasises the consequences of the research and is pluralistic in nature. (Onwuegbuzie & Leech, 2005). Pragmatists aim to develop a better understanding of the underlying structures and mechanisms of a phenomenon and pose questions that can be answered using positivist and interpretivist methods. (Creswell, 2012; Myers & Avison, 1997).

The pragmatic approach (Zakaria, 1994; Hausman, 1993; Senglaub et al., 2001) or pragmatic method is based on Pierce's theory of inquiry. (Pierce, 1878). According to Pierce, a method of inquiry is the best option for resolving doubt compared to methods of a priori, tenacity, and authority. Peirce's method of inquiry includes three cyclical processes of reasoning, including abduction, deduction, and induction. (Peirce, 1902; Peirce, 1903; Burk, 1946; Sowa, 2000; Aliseda, 2005). This approach is unique to Pierce's philosophy since it incorporates the three processes as a single unit of

methodological inference, which is comprehensive for resolving doubt (i.e. solving a problem). The pragmatic approach accepts the process of deduction as it derives the consequences of hypotheses and deduction tests and validates hypotheses (Zakaria, 1994; Pagnucco, 1995; Addis & Gooding, 2004; Berg-Cross, 2003).

Creswell (2009) suggests that a pragmatic research approach seems to be the most prominent paradigm with a strong philosophical relationship for a mixed-methods approach. Therefore, mixed-methods research usually employs pragmatism or a pragmatic approach as a system of philosophy. (Johnson & Onwuegbuzie, 2004). For instance, in mixed-methods studies, researchers normally build knowledge on pragmatic grounds. (Creswell, 2013; Maxcy, 2003). Pragmatism as a philosophical approach views knowledge as an indispensable reality or an intimate experience. (Johnson & Onwuegbuzie, 2004). Pragmatists believe that existing truth, implication, and the boundaries of knowledge are impermanent. Thus, knowledge can be changed, modified or altered with or without research over time. (Johnson & Onwuegbuzie, 2004).

It is obvious that a pragmatic approach provides a better grounding to explore complex phenomenon more fully than a single method approach. It is a better process to answer what, why, and how research questions (Saunders et al., 2009). Therefore, considering the unique features of this pragmatic perspective and critically deducing from above, a pragmatic approach is the approach best fitted for this research.

3.4.3.3. Rationale for the Adopted Paradigm

In a pragmatic research study, the researcher focuses first on the research problem, and then uses other approaches that might be helpful in understanding this problem. (Creswell, 2009). Researchers such as Holmes (1992), and Rossman and Wilson (1985) also note that a pragmatic approach focuses on the research problem rather than the methods, and uses a range of available approaches to understand the problem. Creswell (2009) outlines the key philosophical assumptions of pragmatic research, as used in this thesis:

a. Individual researchers are free to choose the methods, techniques, and procedures of research that best meet their needs and purposes.
b. Pragmatists do not see the world as an absolute unity.
c. The truth is what works at the time.
d. Pragmatist researchers look to the '*what* and *how*' of research, based on the intended consequences (i.e. where they want to go with it).
e. Pragmatists agree that research always occurs in social, historical, political, and other contexts.

f. Pragmatists believe in an external world independent of the mind as well as that lodged in the mind.
g. Pragmatism opens the door to multiple methods, different worldviews, and different assumptions, as well as different forms of data collection and analysis.

The above points, particularly with respect to uncertainty and subjectivity, validate the decision to use a pragmatic approach in the current research. The pragmatic research philosophy with mixed data collection methods, creates an opportunity to be both objective and subjective when analysing participants' perspectives. (Saunders et al., 2009).

The following sections shed light on the two research methods for data collection.

3.5. Data Collection Techniques

Data is defined as "the facts that are presented to the researcher from the research environment. Data is characterized by its abstractness, verifiability, elusiveness and closeness to the issues being studied". (Cooper and Schindler, 2003, p.183). For data collection, Waters (2001) recommends combining both quantitative and qualitative approaches in the same study in order to improve the decision-making process. Comprehensive decisions are made by assessing and analysing all the available information, from both qualitative and quantitative techniques. Bryman and Bell (2007) also argue that combining quantitative and qualitative data in the same study enables the utilisation of triangulation.

This research adopts survey questionnaires, as well as semi-structured interviews with open-ended questions as instruments for collecting data. The rationale of such an approach is to obtain a better understanding of the research problem, as it allows the researcher to present respondents with semi structured questions as well as unstructured questions, where the respondents are asked to provide answers in their own words. (Bhattacherjee, 2012).

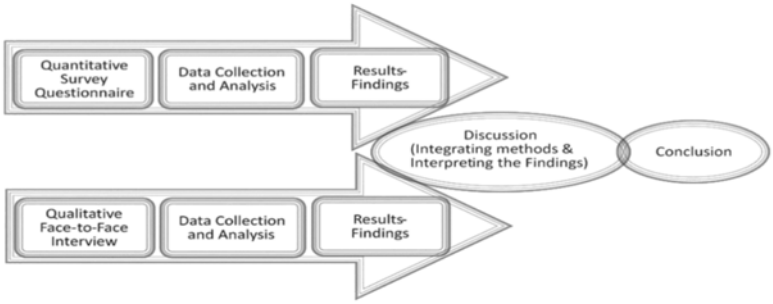

Figure 3-4: Mixed-Methods Data collection techniques ; quantitative and qualitative. Source: Self

As mentioned previously, the research question and purpose of the study are the drivers of the complementary quantitative and qualitative methods to produce an effective

analysis of Omani information security. According to Sampieri, (1991, p.285), "the instrument of data collection really represents the variables we have in mind. If it doesn't, our measure is deficient and therefore the research is not worthy to be taken into account". In this study, mixed-methods research approach that sits between the quantitative and qualitative approaches emerges as the most effective way of incorporating elements of both techniques in a single study. (Johnson & Onwuegbuzie, 2004), (Doyle et al., 2009).

The next section addresses the quantitative technique, which is one part of the data collection process.

3.6. Quantitative Technique

Quantitative research method varies according to the research objectives. It is a powerful tool for collecting data from multiple sources of analysis and diverse cases. It is widely accepted and utilised in the social sciences for studying cross-cultural and organisational issues. (Babbie, 1998; Bond, 1988; Cameron and Quinn, 1999; Hofstede, 1980; Schein, 1992; Straub *et al.*, 2001).

Survey research refers to the "collection of information from a sample of individuals through their responses to questions" (Schutt 2001, p. 209). The questionnaire is a popular technique and often used to discover peoples' attitudes and to enable the researcher to identify and describe the variability in phenomena as well as to examine and explain relationships between variables. (Saunders, Lewis & Thornhill 1997, p. 244). It is an "efficient method for systematically collecting data from a broad spectrum of individuals and in a variety of social settings". (Schutt 2001, p. 209). Moreover, Schutt (2001) and Saunders et al. (1997), state that survey research via questionnaire is often the only means available for developing a representative picture of the attitudes and characteristics of a large population. In quantitative research, data is gathered from a large group of people, and is then generalised, and conclusions are drawn from the results. Its primary objective is to illustrate a phenomenon and its occurrence in a population. Academic psychologists prefer quantitative methods (i.e. measuring key variables and analysing results with quantitative statistical methods) and connect this quantitative information with concepts and theory.

As mentioned earlier, positivists believe that there is a single reality, that can be measured and known, and they are more likely to use quantitative methods to measure this reality. (Salma Patel, 2015). A quantitative perspective is based on the positivist paradigm, and it is hypothetic and co-deductive, in that, it usually begins with a

hypothesis or research questions based on the analysis of the literature. Quantitative studies are conducted through surveys (questionnaires), experiments, and through mathematical modelling. (Myers & Avison, 2002). They use mathematical and statistical tools to identify facts and relationships between constructs within an area of study. (Fitzgerald & Howcroft, 1998).

According to Shuttleworth (2008), quantitative method is a great way to finalise results and prove or disprove a hypothesis, and it has not changed for centuries. After a statistical analysis of the results, a complete answer is reached and the results can legitimately be discussed and published. It tends to generate proven results with little uncertainty, leading to a definitive answer and a narrowing of the possible orientations for follow-up research.
Quantitative research investigates phenomena that are quantitative in nature using quantitative methods (i.e., methods that measure and examine the relationship between numbers, weights, quantities, volumes, and strengths to support specific questions or hypotheses, in contrast to qualitative research)

Quantitative research must first identify a specific hypothesis on a given topic, as a question to be answered by the research team. Creswell (2003) mentions that in quantitative studies, researchers use research issues and assumptions in order to define more accurately the purpose and objectives of the research study. (Creswell, 2003). Denzin (2000, p8) states that “Quantitative research focuses on the analysis of causal relationships between variables, and not between processes". Investigations and epidemiological studies (e.g. incidence, prevalence and risks studies) are included among quantitative research methods. (Peat, 2002; Creswell, 2003). Valid scientific answers are produced from quantitative methods, according to which, actions can be taken and changes can be made. (Carr, 1994).

There are three broad classifications of quantitative research: descriptive, experimental, and causal comparative. (Leedy & Ormrod, 2001). Descriptive research method examines the situation, as it exists in its current state. Descriptive research involves the identification of attributes of a phenomenon based on an observation or the exploration of correlations between two or more phenomena. Quantitative results do not provide many details about attitudes, behaviours, or motivational issues, though the results can be generalised because of the large sample sizes. (Scandura & Williams, 2000). Quantitative research often uses a narrow lens because the focus is on one or few causal factors. For this study, a questionnaire, which is a common instrument in quantitative

research, was used as a data collection method. The questionnaire survey was selected in this study to obtain data on topics to be covered in the research hypotheses model, as well as to test the relationships between the model's contents.

3.6.1. Quantitative Method Design

In the first stage of this research, a survey questionnaire was designed as the basic instrument for data collection. A questionnaire is an appropriate method for examining relationships between two or more variables, which are the result of assumptions derived from a positivist approach. (Saunders & et al., 2009). A survey questionnaire is commonly used in quantitative research for collecting data, and produces a numeric description of trends, attitudes, and opinions of the target population about a certain subject. Neuman (2006, p.272) states that a questionnaire is "the most widely used data gathering technique in the social sciences".

The survey data supported the thesis from different perspectives. It was used to explore the current status of information security culture and practices in the Omani organisations, by identifying employees' attitudes and behaviours regarding information security. It was also used to investigate the relationships between different critical socio-cultural and organisational factors and information security culture, together with the effect of these relationships on employee compliance behaviours and discipline

3.6.2. Survey Design

The survey for this study was designed to be as unobtrusive as possible, due to the sensitivity of information security topics within organisations. Some of the survey inquiries are based on questions from other studies that were previously validated, and the remaining inquiries are added by the researcher to ensure that the completeness of the survey. The questionnaire contained five pages, comprising three main sections and twelve parts with predominantly closed-ended questions, but with an open-ended note in the final part.

Section One contains parts 1- 4. It collected demographic data about participants. Section Two contains parts 5– 12, This section collected data about information security aspects in the organisation, as well as a number of information security independent variables, such as management support; information security policy; and information security training and awareness programs. The third and final section allowed respondents to record their own notes and suggestions, and any further details regarding information security in their organisations. This open-ended part is designed to allow the survey respondents to explore a concept further by not limiting their response to predetermined options or scales. (Cavana et al., 2001). The open-ended part was put at

the end as by then the respondents had a fair understanding of the kind of information sought in the survey. The questions for the availability construct were revised based on feedback from the author's supervisor.

The participants were asked to rank the items on a 3-point Likert scale with anchors 'Yes, No', and 'Not Sure'. This scale was designed to determine five specific values: Information security behaviour; training and awareness; management support; information security policies; culture and information security. The scale also identified the relevant national information security responsible parties (ITA) (See Appendix A). The questionnaire starts with a statement of consent to participate before proceeding with the survey, and indicates that participation is voluntary. The consent statement also explains the purpose of the study and the amount of time estimated for the completion of the survey. A statement of confidentiality is attached to assure individual and organisation anonymity. The survey is designed in an English and an Arabic version.

3.6.3. Survey Translation

The current study adopts the backward-forward translation method, which has been widely used in research to check the accuracy of instrument translations. (Douglas & Craig, 2007). (Bailey 2008) calls this the double (two-way) translation method. The process starts with translating items to the required language and then translating the words back to the original language, comparing the two translations, checking for discrepancies, and correcting them. (Triandis, 1972). This method helps in evaluating the accuracy of translations. However, the goal of the translation process was to produce an Arabic version equivalent in meaning to the original English version, and not an identical word-by-word translation of items. This would ensure that the items do not lose their core meaning in the translation process and that the language used in translated items has appropriate form and readability. (Brislin; 1970 and Lin, Chen, and Chiu, 2005).

The researcher initially developed the questionnaire in English. Two professional Omani English lecturers from Sultan Qaboos University, Oman, then independently translated it into the Arabic language. The questionnaire items were than compared to assess item-by-item similarity across the two translations. Where disagreements or discrepancies were found, the translators discussed and revised the items until consensus was reached and the Arabic translation was finalised.

Next, two people from our organisation who were participants in the pilot survey, one with an information security background, and one with a background in IT,

independently translated the questionnaire back from Arabic into English. Both translators speak and write English fluently, and followed the same comparison and revision process as the first transitions. Both Arabic and English versions were used as instruments for data collection. However, before the final version of the designed questionnaire was distributed to a larger group, both versions were tested through a pilot survey.

3.6.4. Survey Piloting

Conducting a pilot study is essential in assisting the researcher to identify potential issues with the research tool. Altman et al. (2006) say that good questionnaires require a pilot study. Johanson & Brooks (2009), and Al Arfaj (2001) point out that a pilot study is a great way to develop a good research tool and to test the reliability and validity of the research hypothesis. A pilot study followed the construction of Arabic and English versions of the questionnaire, prior to distribution. The researcher invited six respondents to take the pilot test, three of them from different departments within our organisation, one from the ministry of finance, and the remaining two from private-sector organisations. Both Arabic and English versions were placed online using survey monkey software. The researcher sent the participants a link via e-mail, and asked them to record the time taken to complete the questionnaire. The choice of language version was left to the participants. The researcher met the pilot respondents a week later, and listened and recorded all their comments about the questionnaire. Four of the respondents selected the Arabic version and two of them selected the English version. Changes to the questionnaire were made where necessary, based on their comments. This process was designed to avoid any misinterpretation by reference to gender or profession. In addition, the researcher wanted to make sure that the questions were easy to understand for all respondents.

3.6.5. Survey population

As suggested by Randall and Gibson, (1990), the data collected from employees of different Organisations and are of various sizes represented a good mix. In the current study, the target population for the survey was employees working in public and private sector organisations in Oman. 72% of the respondents were public sector employees and the remaining 28% from the private sector. The organisations represented a good mix of small (50-500 employees, 22%), medium (501-7,000 employees, 51%) and large organisations (> 8,000 employees, 27%). The largest four organisations were in the Financial, Education, Telecommunications and Health sectors.

3.6.6. Survey Sampling

A population is defined as all units of analysis with the characteristics that a researcher wishes to study. (Bhattacherjee, 2012). The unit of analysis may be a person, group, organisation, country, or any other unit that a researcher wishes to examine. According to Graziano and Raulin (1997) it is not possible to collect and gain data from all the available sources to solve research problems and find the solutions. Therefore, it is recommending that smaller units should be taken from the available population to gather data. These smaller units are referred to as samples.

Sampling techniques help to reduce the amount of data to be collected, by considering only data from a sub-group rather than all possible cases or elements. (Saunders & Thornhill, 2000). According to Neuman (2006), sampling is a process of systematically selecting cases for inclusion in a research project. A sample is a subgroup or subset of the population. (Sekaran, 2003). According to Easterby-Smith et al. (2002) when the population is small (less than 500) it is customary to use a 100% sample, called a census sample, in which the questionnaire is sent to all the members of the research population.

The participants in the current study were selected to explore the current status of information security discipline culture in their organisations. The targeted participants were all public and private sector employees, Omani and non-Omani, male and female, aged 20 to 60. No specific group was selected, as it was assumed that the general population would reflect the common information security discipline in Oman.

Table 3-4: Survey Questionnaire Sample for Omani organisations

Category (Respondents)	Number and Respondent %
Total Survey no	200
Total Respondent	155
% Respondent rate	77%
Public (Participants no.)	112 (72%)
Private (Participants No.)	43 (28%)
Male	110 (71%)
Female	45 (29%)
Public Organisations	92 (58%)
Private Organisations	68 (42%)
Nationality	95% Omani & 5% non-Omani
Age	=< 36 years = 67% & > 36 years= 33%
Education	=< BSc = 77% & > BSc= 23%

Table 3-4 above shows the sampling of the questionnaire instrument.

Since researcher did not have sufficient access to the whole population, and because of the research sensitivity, the researcher found it difficult to get enough participants to answer the survey questionnaire. For this reason, this study used a semi-random sampling technique to collect responses, (Patten, 2010; Trochim and Donnelly, 2008), assuming that the sample chosen is representative of the population as a whole (Patten, 2010), and expected to include respondents from different educational backgrounds, and work experience. The term semi-random used in this study because about 10% of the participants are known by the researcher either as friends or work colleagues. To achieve a higher response rate and obtain an effective and accurate outcome, the researcher appointed 15 key participants from different Omani public and private organisations. Such appointments were based on the strong relationships that the researcher had built up over a long time. These key participants were most helpful, and they showed an amazing capacity to participate in the study and to assist in attracting more employees to participate in the study by distributing the survey link.

The key participants were briefed about the research, its aims and importance in identifying the challenges that hinder the good information security in the Omani organisations. The survey link was then sent to them. This brief helped them convince colleagues within their organisations, employee friends and family members, to participate and complete the survey questionnaire. In this way the researcher managed to distribute the questionnaire link to 200 participants from both public and private organisations, hoping to receive back at least 170 completed questionnaires.

3.6.7. Survey Distribution

After sampling, the next stage was the distribution of the survey. The questionnaire was formatted using the 'Survey Monkey' online survey creation tool to gather data for the independent and dependent variables used in the hypotheses. Survey Monkey is an open source, data collection, software tool that allows researchers to create surveys and receive feedback from targeted samples. Survey Monkey uses encryption to secure data and ensure the confidentiality of information. The information is password protected and requires a security code to allow access by the survey owner. Collected data is stored in encrypted online files that can only be accessed by the researcher. All electronic research data is retained in an online survey tool through a secure internet connection. This data is deleted from all drives after an agreed period. All hard copy data will be shredded for data protection.

An email notification was sent to each participant to complete the survey, and after completion, Survey Monkey sent a thank you message to each participant. The

researcher received a notice from Survey Monkey, advising her of a new questionnaire completion. Survey Monkey provided speedy access at the same time to all participants in different geographical areas, and also reduced costs and resulted in high response rates. The online survey was made available for six weeks, after which data was collected and analysed. Fortunately, the researcher did not need to follow up with any of the participants as she received 155 completed survey questionnaires out of 200 in time, amounting to a 77.5% response rate, which was deemed as above average and therefore acceptable and reliable.

3.6.8. Survey Data Collection and Data Coding

All the data collected via Survey Monkey was coded into an Excel spreadsheet, involving conversion of the results into numeric data. (Groves et al., 2004). The researcher checked for missing data and cleaned it, before uploading the data to the Statistical Package for Social Sciences (SPSS v22) software. SPSS is a computer software statistical package that enables survey data to be coded, retrieved and stored flexibly and effectively. It provides tools for classifying, arranging and analysing information and data. In addition, to ensure the data was correctly entered on SPSS, the data was cleaned again through a manual process of error checking. The researcher checked the number of valid and missing cases and the labels for each variable before the analysis process, including running frequency tables for all the variables to check the accuracy of the entered data, as advised by Pallant. (2010).

Cleaning the data involved eliminating any questionnaire which skipped too many items or left them unanswered. Whereas questionnaires with a few unanswered items, the researcher filled these items with zeros to improve the reliability of the result. For the current study no questionnaire was eliminated as most data fields in the questionnaire were answered. However, there were very few answers missing, and these cases were filled with zeros during the cleaning process. Using SPSS reduced the analysis time and provided accurate automated results.

Finally, since all questions in the survey were answered using a 3-point Likert scale: “yes”, “No,” and “Not Sure”, response coding using reverse-scoring of the Likert scale of the relevant items was carried out before conducting statistical tests and analyses. For example, ‘Y=3’, ‘No=2’ and ‘Not Sure=1’. This process to improve the reliability of the research results and conforms to research best practice. (Field, 2012).

3.6.9. Survey Data Analysis

Data was analysed using the SPSS program. Descriptive statistics including frequencies, percentages, means, and standard deviations were computed for all the items in the questionnaire. Furthermore, multiple regression methods were used to analyse the relationship between a dependent variable and several independent variables. The correlation method was used to determine whether a relationship between variables existed. In addition, the concept of composite variables was used to make responses to enquiry items more manageable. In this regard, five composite variables were developed by combining items and computing a composite score for each variable. For example, the variable 'information security policy' had 6 items, the variable 'information security management support' had 4 items, the variable 'information security training and awareness' had 6 items, the variable 'employee security information compliance' had 10 items, the variable 'information security and organisational culture' had 6 items, and the variable 'information security national responsible body' had 4 items. Each item in the questionnaire was measured on a 3-point Likert-type scale. The composite score was computed as a mean for each variable. The techniques that were used in the analysis of the data consisted of: (1) t-test; (2) Pearson correlation coefficients; and (3) ANOVA. A 0.05 level of significance was used for the statistical tests. A reliability estimate was computed for each scale using Cronbach's ALPHA test.

3.6.10. Benefits and Limitations of the Quantitative Approach

Listed below some of the quantitative method benefits and limitations

***Benefits* of the Quantitative Approach**

- Enables gathering of information from a relatively large number of participants.
  The quantitative findings can be generalised to a whole population or a sub-population as a large sample, which is semi-randomly selected, is involved.
- Data analysis is less time consuming as it uses the statistical software such as SPSS.
- Analysis of several groups allows for comparison.
  Quantitative method is useful for conducting audience segmentation. By dividing the population into groups whose members are similar to each other and distinct from other groups, it is then possible to compare group responses to matters of research interest, and determine what influences that response. The use of standardised questions allows for easy comparability between respondents and groups of respondents.

- Greater objectivity and accuracy of results. Generally, quantitative methods provide summaries of data that support generalisations about the phenomenon under study. To accomplish this, quantitative research usually involves few variables and many cases, and employs prescribed procedures to ensure validity and reliability.
- Conducted remotely which reduces or prevents geographical limitations.
  Quantitative methods are convenient for data gathering, as surveys can be distributed to the participants through a variety of ways, such as e-mail or fax, or can be distributed through the Internet. Nowadays, the online survey method is the most popular way of gathering data from target participants. Researchers are able to collect data from people around the globe.
- Uses statistical techniques to determine relationships between variables.
  With quantitative methods, advanced statistical techniques can be utilised to analyse survey data, to determine validity, reliability, and statistical significance, including the ability to analyse multiple variables. It is often easier to find statistically significant results than other data gathering methods.
- Avoids personal bias or opinion. Quantitative methods provide all the participants with a standardised stimulus in that large groups of people are able to provide information, free from any knowledge of the surveyor. In other words, the researcher's own biases are eliminated.

Limitations of the Quantitative Approach

Beside the benefits that the quantitative method provides, there also some limitations as listed below:

- Difficulty recognising new and unexplored phenomena.
  The quantitative method overlooks respondents' experiences and perspectives in highly controlled settings. (Ary, Jacobs, Sorensen, & Walker, 2013). The lack of a direct connection between researchers and the participants when collecting data, results in a degree of objectivity in collecting data.
- Unrepresentative sample of the target population.
  Improper representation of the target population might hinder the researcher. Despite attempts at rigorous sampling, the representation of the subjects is dependent on the probability distribution of observed data. This may lead to miscalculation of probability distribution and lead to false propositions.
- Limited outcomes in a quantitative research.
  Quantitative research methods use structured questionnaires with close-ended questions. This can limit outcomes outlined in the research proposal. Results may not always represent the actuality in generalised terms. In addition, response options are limited to the question selection made by the researcher.

- Inability to control the environment.
  Sometimes researchers face problems controlling the environment in which respondents provide answers. (Baxter 2008). Responses often depend on particular time and the conditions occurring during that particular period.
- Possible Inappropriateness of Questions.
  Survey questions are always standardised before being put to respondents. The researcher is therefore obliged to create questions that are general enough to accommodate the general population. However, these general questions may not be equally appropriate for all respondents.

3.7. Qualitative Technique

The qualitative approach is one in which the researcher often draws conclusions based primarily on meanings, derived from individual experiences that are socially and historically constructed. Creswell (1998, p12), defines qualitative as "an inquiry process of understanding a social or human problem, based on building a complex, holistic picture, formed with words, reporting detailed views of informants, and conducted in a natural setting". The purpose is to develop a theory or pattern. By using research strategies, such as narratives, phenomenology, ethnographies, grounded theory, or case studies, the researcher collects open-ended emerging data with the primary intent of developing themes from the data to build a theory.

A qualitative approach may be appropriate for a concept that has not been extensively researched, or when there is a need to understand the concept or phenomenon and the factors surrounding it better. Furthermore, when researchers are not clear about which are the important variables to examine in such cases, exploratory qualitative research is ideal. (Morse 1991). Interviews are the most widely employed method in qualitative research. (Bryman, 2012).

Qualitative research methods are concerned with "the study of things in their natural environments, to try to understand or interpret [an event or experience] based on the sense that people give the study". (Denzin, 2000, pp. 256-265). They are characterised by their interpretive practices and their focus on meaning-making and building conceptualisations. Qualitative methods use participants' words rather than relying on numbers. (Saunders et al., 2007). According to Nardi (2014), qualitative research involves the settings of people's lives, such as participant observations and open-ended interviews.

This method is attractive in that it allows for the display of respondent's views and perspectives, which provide richness and fullness to the phenomenon or topic. The main

goal of using qualitative data is to allow participants to express their perspectives openly, such that they not only answer the research questions, but also provide additional information surrounding the issue. Qualitative methods are widely used in the social sciences to address human and organisational issues. Furthermore, the interpretive paradigm rests on the assumption that knowledge is gained through social constructions such as language, consciousness, and shared meaning. It operates on the basis that there is an intimate interaction between the researcher and the phenomenon being explored. (Rowlands, 2005). Patton (2005) explains that the interpretive paradigm accepts that reality only exists through a person's perceptions that emerge from the lens of prior experience, knowledge, and expectations, and that this lens will influence the interpretation of new information.

There are three main categories in Interviews; the structured interview, semi-structured interview and unstructured interview (Bryman, 2012; Creswell, 2012; Saunders et al., 2003). A structured interview also known as standardised interview consists of fixed questions and all respondent receive the same interview stimulus. Interviewees are often also offered a fixed range of answers. An unstructured interview is the opposite of the structured interview. An unstructured interview is guided only by a list of topics or issues to covered, prepared by the interviewer. There is no specific sequencing of questions therefore, the unstructured interview is usually informal (Saunders et al., 2003). Often the interviewee is given the opportunity to talk freely surrounding the issues to be discussed.
In a semi-structured interview, the interviewer will have a list of themes as well as some questions to be covered although these may vary from interview to interview. (Saunders et al., 2003).

Yin (2014) suggests that qualitative methods are appropriate for social science research, particularly when studying individual and group behaviour in an organisation. Cohen et al. (2007, p.461) argue that “qualitative data analysis involves organizing, accounting for and explaining the data; in short, making sense of data in terms of the participants’ definitions of the situation, noting patterns, themes, categories and regularities. The analysis will also be influenced by the number of datasets and people from whom data have been collected”.
Therefore, it is interpretive in nature and focuses on words, not numbers; it analyses the data to search for themes, patterns, and holistic features. Since it is dependent on the context, the same qualitative research could be conducted at a different time by someone else and produce different results. However, reliability, (i.e. generalisation and

replication by applying results to new settings) (Yin, 2003, p. 37; Creswell, 2003, p. 195) is limited since this is a single case study.

In addition, qualitative studies do not have large samples, data analysis is inductive, researchers build qualitative research from an individual theme, and qualitative researchers are open to adjusting questions based on previous responses. (Patten, 2012). In qualitative methods, the researcher uses instruments that are less structured to collect data, and the researcher is often the primary instrument for data collection and analysis. (Miles & Huberman, 1994). Data analysis contains a series of fluctuations that are constantly pushing and pulling the research questions and guiding theoretical frameworks. (Creswell, 2003).

Qualitative results offer insight into the social, emotional and experimental phenomenon, and can allow one to grasp the hidden nature of behaviour, attitudes, and motivation. Glesne and Peshkin (2010) note that multiple methods need to be used by researchers in qualitative studies to understand, describe, and make sense of the research. They highlight the importance of considering how open the qualitative inquiry should be to encompass the complexity of participant experiences.
The semi-structured interview guide approach, with Open-ended questions is considered to be the most appropriate to this study.

3.7.1. Rational for Using Semi Structure Interview with Open Ended Questions

The major advantage of the qualitative method is to fill the gaps in the questionnaire method and to enhance the validity and reliability of the research. (Tashakkori & Teddlie, 2003; Creswell & Clark, 2007). Further, according to Brenner, Brown, and Canter (1985), the main benefit of interviews as a data collection method is that they provide both parties with a chance to explore the meaning of the questions posed and the answers given. In addition, the interactive quality and immediacy of face-to-face interviewing provide substantial flexibility to the data collection process, in terms of the direction of the discussion and the areas explored. (Darlington & Scott, 2002). According to Gorman and Clayton (1997), interviews allow the researcher to receive immediate responses to questions. They can yield rich and extensive data, as well as insights related to issues that the researcher never considered.
Because the study uses a mixed-methods approach, the researcher had certain pre-considered themes to discuss with participants, as well as prompting in-depth answers to specific questions via the questionnaires. Further, the researcher could guide the interviews by means of an investigative framework or interview guide. (Appendix B),

as with several other information security researchers e.g. (Doherty et al., 2012; Hu et al., 2007). While the open-ended questions have the advantage of allowing the respondent to answer in a relatively unconstrained way. This type of question allows the respondent the satisfaction of including finer details that can be more motivating for this reason. (Kidder & Judd, 1986).

3.7.2. Interview Guide Design

According to Lee and Fielding (1991), the interview is one of the most important sources in qualitative data collection. Interviewing is a method of collecting data in which selected participants are asked questions to find out what they do, think or feel. (Collins and Hussey, 2009). According to Denzin and Lincoln (2011), interviews are seen as the primary tool for the data collection process within qualitative research. An interview guide for this study was developed during the data collection process, based on the related work review, and the researcher's knowledge of the subject and her work experience. It provided some degree of structure during the semi-structured participant interviews and provide the link between interview questions and their corresponding research question.

The interview guide had 29 questions in total grouped into six themes. Each set of questions focused on a particular theme title. Most of the questions were designed to understand the state of information security as experienced by participants in their organisations, together with the various socio-cultural and organisational factors that influenced the development of a culture of information security in those organisations, and the extent of employee compliance with information security best practice. The questions also tied to elicit the reasons behind specific information security behaviours. However, as is common in such flexible semi-structured interviews, the themes were only the starting point and participants were encouraged to express themselves freely.

The interview guide was composed of detailed and organised semi-structured open-ended questions that engaged the participants in providing comprehensive responses. Semi-structured interviews can be defined as "a qualitative data collection strategy in which the researcher asks informants a series of predetermined but open-ended questions". (Ayres, 2008, p. 811). A key feature of semi-structured interviews is that questions can be added and changed and supplementary prompts included, depending on the evolving themes. In addition, this type of interview can be easily managed to obtain the required information from interviewees within a given time slot.

The interview guide covered questions about the current state of the organisation's information security; organisational culture; national culture; management support; information security awareness and training; information security policy; and motivation and punishment. At the beginning of each interview, the research information page, which provided information about the research in general and the interview in detail, was given to the participant. The participant was also given a consent form to sign confirming that he/she had read and understood the information page and agreed to participate. With the participant's permission, the interviews were then carried out and recorded for later analysis.

3.7.3. Interview Guide Translation

The interview guide questions, the information page, and the consent form, were developed in the English language and then translated to Arabic and verse versa, following the backward-forward technique to ensure accuracy and conformity and that the translation was as close to the original as possible. (The backward-forward technique was explained earlier in this chapter at section 3.6.3). The interview guide was first reviewed and evaluated by an Omani expert in information security from ITA, who pointed out some issues for adjustment, which were adopted. The researcher's supervisor carried out a final review, and recommended some further changes to improve the contents.

3.7.4. Interview Guide Piloting

Two of the researcher's work colleagues, one of them heading the HR department and the other one heading the communication department, piloted the interview guide. Van Teijlingen and Hundley (2001) report that a pilot study enables a researcher to identify difficult questions and to assess the interpretation of the answers. The pilot interviews used both the Arabic and the English versions. The participants were asked to provide comments about the clarity of instructions and the questions addressed. The participants reported no difficulty in understanding the interview questions but suggested some comments on reformulating a couple of questions to aid understanding.

3.7.5. Interview Choice of Organisations

The researcher should carefully consider interviewee selection and not depend on chance or opportunity. (Benbasat et al., 1987). Looking at the research, certain aspects had to be in place in order to complete the project successfully. Getting answers to the research questions, which was the goal of the study, meant obtaining data that would

provide valuable findings and outcomes. The nature of the topic under study, (the implementation of an information security culture in public-sector organisations in Oman), was the key aspect to be considered while selecting interviewees. The emphasis is on the human aspects of the adoption of information security culture, rather than on technology issues.

The major concern of this research is to study how employees in an organisation practice information security in the workplace. This requires exploring the culture of the organisation to understand the employees in their work surroundings while collecting the data required for the study. However, it is important to keep in mind that the research also compares public and private organisations, which means the interviewees should be selected from both sectors.

The criteria for selecting interviewees were:

- To identify representatives from organisations that have recently introduced electronic links for sharing information rather than manually through post or mail.
- To include representatives from organisations with a large number of employees, to discover how culture affects employee behaviour in these organisations.
- To identify representatives from organisations that are engaged providing government services to the public.

These different types of organisations helped to identify the key socio-cultural and organisational drivers and barriers to information security culture adoption, and also they were found to be appropriate for exploring the problems of the lack of information security culture in organisations.

3.7.6. Interview Sampling

The selection of appropriate interviewees is an important and complex issue in qualitative research. Rubin and Rubin (2011) argue that participants should be selected based on their knowledge and experience. Therefore, the researcher purposely selected senior managers at the organisational level within the targeted organisations, to deepen the understanding of the current state of information security and the effect of socio-cultural and organisational factors on information security in Oman. It was planned to solicit their views using semi-structured qualitative interviews with open-ended questions.

Purposive sampling is appropriate for this study, as it is necessary to obtain information from specific target groups. (Sekaran, 2003). Smith, Colombi, and Wirthlin (2013) explain that researchers use purposive sampling to identify participants with business

knowledge who are therefore likely to provide the data needed to answer the research question. Ishak and Bakar (2014) state that purposive sampling is appropriate for case study research, while Guetterman (2015) uses purposive sampling to select information-rich case studies. Sangestani and Khatiban (2013) explain that researchers use purposive sampling to deliberately select research participants that meet established criteria, which the researcher assumes to be representative of the study population. There are two types of purposive sampling, judgment sampling and quota sampling. Judgment sampling is when the participants are specifically selected because they are the best people to provide information on the research topic.

The purposeful sampling for the interviews in this study were selected under the three levels of screening mentioned in section 3.7.5 above, after consulting the Information Technology Authority (ITA). From the total number of public and private organisations in Oman, those that had a security and IT function in their organisational structure were identified before conducting the interviews. Several organisations were thus excluded. An initial selection was made and 22 senior managers were identified from the shortlisted public and private organisations to participate in the interviews. However, only fifteen information security and IT senior managers responded to the request; nine of them from public organisations and six from private organisations.

Table 3-5 shows the interview sample for Omani public and private organisations.

Table 3-5: Interviews Sample for Omani organisations

Category (Respondents)	**Number and Respondent %**
Total No	22
Respondent no.	15
% Respondent rate	63%
Public	9
Private	6
Specialisation	IT & IS Managers
Nationality	9 Omani and 3 non-Omani
Experiences	Between 06 -18 years

The selected interviewees were information security and IT managers who possessed experience and knowledge in their fields. The researcher was aware before conducting interviews of the possibility that few Information Security and IT managers would be willing to discuss information security-related issues in their organisations despite the researcher's non-disclosure commitment.

Table 3-6 below shows the profiles of the study interviewees.

Table 3-6: Participants Profile

S	Participants	Sector	Job	Years of Experience	Education Level	Gender	Nationality	Age	Population %
Public Sector Organisations									
1	GINT1	Public	IS Manager	16	PhD	M	Omani	44	9 60%
2	GINT2	Public	IT Manager	18	MSc	M	Omani	42	
3	GINT3	Public	IS Manager	18	MSc	M	Omani	44	
4	GINT4	Public	IS Manager	12	BSc	M	Omani	36	
5	GINT5	Public	IS Manager	8	BSC	M	Omani	36	
6	GINT6	Public	IT Manager	8	MSc	F	Omani	34	
7	GINT7	Public	IS Manager	6	BSc	M	Omani	36	
8	GINT8	Public	IS Manager	12	BSc	M	Omani	32	
9	GINT9	Public	IS Manager	9	BSc	M	Omani	34	
Private Sector Organisations									
10	PINT1	Private	IS Manager	18	PhD	M	Indian	48	6 40%
11	PINT2	Private	IS Manager	16	MSc	M	Jordanian	41	
12	PINT3	Private	IT Manager	16	MSc	M	Omani	39	
13	PINT4	Private	IT Manager	7	BSc	M	Indian	34	
14	PINT5	Private	IS Manager	15	MSc	M	Omani	42	
15	PINT6	Private	IS Manager	8	BSc	M	Omani	35	

3.7.7. Interview Data Collection

A face-to-face, semi structured, open-ended, interview was conducted with each participant. The researcher was able to interact with respondents, allowing them to expand their replies to obtain further useful insights into the research questions. (O'Keeffe, Buytaert, Mijic, Brozovic, & Sinha, 2015; S. Pandey & Chawla, 2016.). The respondents could also discourse on the topic in their own terms. (P. Jones et al., 2014; S. Pandey & Chawla, 2016). They were each expected to answer the interview guide questions freely. The semi-structured interview was selected to understand the world from the interviewees' points of view and to complement the picture from the quantitative analysis conducted earlier. The semi-structured interview also enabled the participants to provide an in-depth understanding of the topic. (Cao et al., 2013).

The interviewees were mainly IT and information security senior managers from Omani public and private organisations. They were interviewed to elicit their perceptions of the status of information security in their organisations and to explore the factors that affect the implementation of a culture of effective information culture in these organisations. Respondents were asked for facts as well as their opinions about events. In the circumstances of the study, an interviewee's role can shift between that of

respondent, and that of informant. Rubin and Rubin (2005, p.4) state that "in qualitative interviews, each conversation is unique, as researchers match their questions to what each interviewee knows and is willing to share" (Rubin & Rubin, 2005, p.4). Notably, this research is not only interested in the attitudes of participants towards the given subject, but also in the organisational reality within which these participants operate.

The researcher's primary strategy was to use open-ended questions to develop credibility and trust with participants, as an important element in qualitative data collection. (Fjellström & Guttormsen, 2016; S. Gibson et al., 2013; Siu et al., 2013). All fifteen senior IT and information security managers were contacted to agree a suitable interview time and venue. All interviews were conducted at the interviewee's office. According to Owen (2008, p548), "conducting research in participants' natural environments is essential . . . because the complexity of human interaction is available only in the settings of everyday life". The interviews were conducted over a period of six weeks, and each interview session took between 90 to 120 minutes to complete. Nine interviews were conducted in Arabic with public-sector participants. The remaining six interviews were conducted in English with participants from private-sector organisations. The recorded Arabic conversations were manually transcribed into English while listening to the recorded voice. During the interview, the researcher first informed the participants about the interview purpose, research topic, and duration of the interview. The researcher obtained permission to take notes and to voice record each interview, before commencing. The researcher also informed the participants that they could stop the interview whenever they wished. Participants were then asked to sign the consent form guaranteeing confidentiality.

All participants, except one, agreed to have their interview digitally recorded to ensure low inference reception, and this facilitated the transcription process at a later stage. In the one exceptional case, the researcher documented the interview through detailed note-taking focused on capturing the meaning conveyed by the participant rather than a word by word transcription. (Stake, 1995). According to Britten (1995) and Gill et al. (2008), the voice recording of interviews is regarded as more reliable and accurate than written records. Writing notes can interfere with the process of interviewing, and notes written afterwards are likely to omit some details.

In addition to audio recording, field notes were used to record key themes, significant points, researcher's views and ideas for inclusion in later interviews. Immediately after each interview, the researcher filled in the interview guide with a summary of key points on each question that was asked and noting questions skipped or any overlap. During

interviews all participant were presented with a list of the same pre-prepared set of questions (interview guide), and the researcher asked the same set of questions to each participant to stay on track during the interview. (Doody & Noonan, 2013). The inquiry topics that guided the interviews are later used as theme headings in the analysis section, although the topics often overlap.

During the interviews, the researcher successfully used different approaches and techniques during the introduction and follow up, using probing, direct, and interpretive questions, to guarantee reaching deep into the interviewees' experiences. These interview techniques generated rich and detailed information, and encouraged participants to interact more and provide better quality information. (Kvale 1996). To maximise the outcome value of the interviews, the researcher used a neutral tone of voice, and let the interviewees use their own vocabulary and phrasing when answering questions. She avoided altering interviewees' responses by not showing any visible emotional reactions to replies. The researcher phrased questions to maintain an open-ended interviewee response, and asked related questions that prompted further replies, to ensure a more reliable link to the research themes. (P. Jones et al., 2014). She tried to be unbiased during the interviews by avoiding leading questions. (Onwuegbuzie & Hwang, 2014).

The researcher would summarise the interview experience as follows:

- With most of the participants, the interview was a friendly method of data gathering and an easy means to draw constructs from answers. (Seale, 2011; Talmy, et.al., 2010).
- The researcher also found that the data gathered from interviews were detailed, there were some obvious similarities in experiences and interpretations among all participants, as well as uniqueness.
- Although the interpretation of their own experiences or thoughts about the concept or phenomenon was subjective, there were common themes that suggested that many participants shared the same experiences and interpretations.

Following the interviews, the researcher added the data to the existing literature about the information security status and culture in Omani organisations

3.7.8. Interview Data analysis

Data analysis is important as it brings together the researcher's interpretation of her observations, along with what the participants perceive and describe. The researcher

analysed the data to identify relationships, patterns, concepts, themes and meanings. Initially, the researcher focused on the data as a whole, and then looked in detail at the different parts, and attempted a more meaningful restructuring. Grouping the data in this way helped the researcher to compare and contrast patterns, and reflect deeply on particular patterns to make complete sense of them.

Denscombe (2014) states that there are different methods of undertaking qualitative data analysis based on interpretations such as content analysis, grounded theory, discourse analysis, conversation analysis and narrative analysis. Yin (2014) adds that thematic analysis as another approach. He recommends that in order to obtain solid evidence from in-depth interviews, the researcher should consider three elements of interview analysis:

1. Categorise interview data into several headings and subheadings according to the interview objectives.
2. Coding each interview with a specific code for referencing and
3. Summarise and accumulate each category.

This procedure of qualitative data analysis allows for the creation of a substantial body of evidence relating to the phenomenon studied (Information security behaviour and ISC).

3.7.8.1. Thematic Interview Data analysis

The analysis in this study aims to develop a detailed and systematic recording of the themes and issues identified during the interviews. A thematic analysis technique (an approach widely accepted and used in information security research), was applied to the semi-structured, open-ended, interview data, in order to identify commonalities in the participants' experiences and perceptions. Thematic analysis is suitable for small samples (Joffe & Yardley, 2004), so the researcher considered whether the technique is appropriate for the sample size and the data set (Wilkinson, Joffe & Yardley, 2004). According to Braun and Clarke (2006), thematic analysis is a method that allows researchers to identify, analyse and report themes within data. It minimally organises and describes the data set in rich detail (Braun and Clarke, 2006). Moreover, the developed data set in the study isn't so large as to require the use of qualitative data analysis software (Patton, 2002).

Krippendorf (1980, p.21) defines thematic analysis as "a research technique for making replicable and valid inferences from data to their context" (Krippendorf, 1980, p.21). Berelson (1952, p.20) defines content analysis as "a research technique for the

objective, systematic and quantitative description of the manifest content of communication" (Berelson, 1952, p.20). The thematic analysis approach identifies patterns within data, and interprets and clusters them in a meaningful way (Braun & Clarke, 2006).

This study adopts a theory-driven thematic analysis technique, because the researcher approached the data with specific questions in mind, based on the dimensions of the themes referred to earlier in the thesis, that she wished to codify. According to Clark & Braun (2016) 'theoretical' thematic analysis tends to be driven by the researcher's theoretical or analytic interest in the area, and as a result of that it is more explicitly analyst-driven (Clark & Braun, 2016). Tashakkori & Teddlie (2003) consider this type of thematic analysis more realistic in reading, annotating, and linking the collected data based on defined theoretical dimensions (Tashakkori & Teddlie 2003). This confers accuracy and complexity to the research findings, while enhancing the interpretation of the collected data in the study (Creswell 2009).

The researcher carried out a manual analysis of the fifteen interview data concerning different attitudes to the Omani culture of information security.

According to Miles and Huberman, (1994, p10) there are three recommended stages for data analysis: data reduction, data display and conclusion. Data reduction is the process of "selecting, focusing, simplifying, abstracting and transforming the data that appears in written-up field notes or transcriptions" (Miles and Huberman, 1994, p10). Accordingly, all electronic audio-recorded interviews were transcribed into text and then coded and saved in Microsoft Word documents (Lichtman, 2013). The researcher accompanied these with her impressions and observations, recorded in a logbook during the interviews sessions, in order to complement the interview data. The researcher read and reread each transcript carefully while listening to its accompanying audio file. As the process of interpretive analysis of data rests with the researcher, she repeated this process many times, thereby ensuring immersion in the data as the researcher gradually became familiar with each interview.

The researcher examined each individual script and looking for differences as well as similarities (Huxley et al., 2011, p.86). Braun and Clarke explain in their 2006 paper that "…thematic analysis involves searching across a data set – be that a number of interviews or focus groups, or a range of texts – to find repeated patterns of meaning". Huxley et al. (2011, p.419) also highlight this, stating "…the primary emphasis is on themes/commonalities across the data set, rather than detail of individual experience…". The elements of interview text data were first highlighted, and then

placed in the categories that they belonged to, based on the thematic categorisation of the interview guide. According to Creswell (2009b, p. 187), the researcher can either (a) develop codes based on the emerging information collected from participants, (b) use predetermined categories and then fit the data to them, or (c) use some combination of predetermined and emerging codes. Thematic data can be identified more easily following predetermined categorisation.

The formulated interview guide used in this study contains questions that tried to identify the interviewees' thoughts and the way that they understood the "reality" behind adopting an information security culture in their organisations. Interviewee responses were examined independently of the category of the question in the interview guide. Each interviewee was given a code number in order to help the researcher to distribute the identified data from the answers of the interviewees. However, new themes, that were especially useful in analysing the strength of various factors influencing information security culture in Omani organisations, emerged as analysis progressed. The emerging themes and sub-themes were then highlighted and grouped together to form additional major themes with their related research objectives.

During the analysis, keywords, or key phrases, in the transcription, related to every predefined theme were identified, systematically organised and introduced in tables, with their related excerpts. Quotations have been selected in order to give the reader a better understanding. The researcher hopes that the selected quotes make the reader gets a sense of "being present". Links between quotes and participants' codes were also included to indicate the strength of an opinion on a dominant concept. (Cavana et al., 2001; Grbic, 2007). The thematic content analysis allowed for contextualisation and development of theoretical interpretations that could support and elucidate the survey results.
The resulting findings of this thematic analysis of the qualitative data are presented in Chapter Five.

3.7.9. Benefits and Limitations of the Qualitative Approach

Qualitative research is optimal for collecting data on individuals, personal histories, perspectives and experiences, particularly when sensitive topics are being explored. Interviews in qualitative research are usually wide ranging, probing issues in detail. The researcher encourages subjects to express their views at length. These are typical benefits of Qualitative research. However, it also associated with some limitations.

Benefits of Qualitative Methods

- Designed to elicit detailed information, and are useful to a study of social processes. Further, qualitative methods are often face-to-face, allowing researchers to make observations beyond respondents' oral responses. A respondent's body language, and even her or his choice of time and location for the interview, might provide a researcher with useful data.
- Can provide a deeper understanding of mechanisms. In-depth interviews provide very rich information and offer the opportunity to ask follow-up questions, probe additional information, justify previous answers, and establish a connection between several topics. They also offer a relaxed atmosphere in which to establish a conversation.
- Offer one-on-one and anecdotal information. Qualitative research can be thought of as anecdotal, when pooled across a number of participants it provides a conceptual understanding and evidence that certain phenomena are occurring within particular groups or individuals.
- Provide verbal information that may be converted to numerical form. Quantitative research may use numbers in analysing, interpreting, and re-presenting qualitative data. Statistical measures can be used to extract more meaning from a qualitative data set, as certain of these data sets will lend themselves to transformation or translation into quantitative data sets.
- May reveal information that would not be identified through pre-determined survey questions.

A researcher employing this method can explore a topic in much more depth than with quantitative method. It gives participants the opportunity to elaborate in a way that is not possible with survey research, and they are able to share information with researchers in their own words and from their own perspectives rather than being asked to fit those perspectives into limited response options provided by the researcher.

Limitations of Qualitative Methods

- Cannot generalise to the general population. The data collected cannot be used to make assumptions beyond the current group of participants. This is because the data collected is specific to how the current group of participants feel, think and behave.
- Silverman (2010) argues that qualitative research approaches sometimes leave out contextual sensitivities, and focus more on meanings and experiences. A phenomenological approach, for instance, attempts to uncover, interpret and understand the participants 'experience. (Wilson, 2014; Tuohy et al., 2013).

- The quality of research is heavily dependent on the skills of the researcher and can be easily influenced by personal idiosyncrasies and biases of researchers.
- A smaller sample size raises the issue of generalisability to the whole population of the research. A researcher faces the issue of applicability to the population as a whole when working with a small number of participants. Data interpretation and analysis may be more difficult/complex. (Richards & Richards, 1994).

3.8. Research Validity and Reliability

According to Daymon and Hallway (2002), the researcher's background, culture, and characteristics can influence results and their interpretation. Yin (1994) describes the four parts of validity and reliability as: constructs validity, internal validity, external validity, and reliability.

The construct validity of this research was ensured through a triangulation technique, which means using more than one method to collect data on the same topic and involves different types of samples. Since this study applied mixed-methods (qualitative and qualitative), it follows that the data collected results complement each other, therefore enhancing overall reliability. Triangulation is one of the most widely used methods for increasing the validity of qualitative research. (Gibbert et al., 2008; Johnson, 1997; Jonsen & Jehn, 2009; Kirk & Miller, 1986; LeCompte & Preissle, 1993; Lincoln & Guba, 1985). According to Wendy Olson (2004), the mixing of data types, known as data triangulation, helps to validate the claims that arise from an initial pilot study. Likewise, Jonsen and Jehn (2009) state that the overall validity of a research design is gauged by its use of triangulation to contribute to trustworthiness and defensibility.

The researcher conducted a pilot survey, pre-tested, and then improved the questionnaire and interview guide, all of which added extra validation by reference to participants' feedback. At the same time, the researcher stressed to participants from the beginning how the results would be helpful for their organisations when handling issues related to information security.

Furthermore, in the quantitative research 'reliability' involves the accuracy or dependability of the method employed to ensure consistent results. (Creswell & Clark, 2007; Wrench et al., 2008). Reasonable measures have been taken to ensure that the quantitative data collected is reliable. The three Likert scale related questions in the survey include items that all face the same direction to avoid any confusion in answering. Additionally, to ensure consistency, the results obtained from the coded data analysis on SPSS were crosschecked with those obtained from the 'Survey Monkey' online survey data collection tool.

There are greater limitations to validating the qualitative portion of this research than there are to the quantitative component in respect to stability, consistency, or generalisability of responses. (Creswell, 2003). However, to ensure the reliability and validity of interviews, interview questions were asked to expert colleagues prior to the planned interviews to determine their clarity and become confident that these questions "measure what is intended to be measured". (Stukat, 2005, p.125). This is consistent with Pietersen and Maree's (2007) argument that to guarantee the content validity of an instrument, the researcher usually presents an interim version to specialists in the field of research for their comments before finalising the instrument.
The default themes often emerged spontaneously in interviews and conversations (i.e. without any influence from the researcher) which increases the reliability since the experiences of interviewees were highly relevant to the discussions. After conducting interviews, the researcher listened to the recordings and read the notes several times to ensure that there were no misinterpretations or misunderstandings. The data was analysed several times with the same results, to ensure the reliability of the study. However, the reliability of the qualitative portion of the study is limited since the interviewees belong to a limited group of organisations. The results could not be generalised and replicated in a different context. (Yin 2003; Creswell, 2003).

Besides reliability and validity, reflectivity is an important component of qualitative research, which is highly significant to the present study. In qualitative research, the collaboration of the subjective views of the respondent and the researcher is the means to arrive at an interpretation. Since the researcher here views the subject through the particular lens of her work experience, the possibility of bias cannot be ignored. The researcher's past experiences and emotions might affect the interpretations. (Denzin & Lincoln, 2005; Grbich, 2007; Tashakkori & Teddlie, 2008). The researcher therefore must be critically reflective and identify possible biases. (Tashakkori & Teddlie, 2008).

To attain reflectivity, the researcher must first concede that her work background might influence her interpretations. The researcher had a prior understanding of the subject under study, especially in regards to public organisations, because of her work experience as an employee working in an Omani public sector. There is a business link between the researcher's department and the information security department in the organisation. This placed researcher between the information security specialists and other employees at different levels in the organisation. The researcher also had previous exposure to, and knowledge of, the culture of the organisation and the behaviours of other employees regarding information security. The researcher attempted to position

herself as if an outsider to provide an objective view of information security in Oman. It is therefore suggested that her involvement with the public organisation in Oman served to position her closer to the subjects of this study and to minimise the risk that her interpretations are unduly influenced by her work experience.

3.10. Ethical Considerations

The goal of ethical research is to ensure that no one is harmed or suffers negative consequences from research activities. (Cooper & Shindler, 2011). Prior to the commencement of this research, ethical approval was obtained, and measures were implemented to ensure that the research was conducted in an ethical manner. Sekaran (2003, p.17) defines ethics in business research as "a code of conduct or expected societal norm of behaviour" (Sekaran, 2003, p.17).

Ethical issues for this research involve a number of entities. First, approvals were sought and granted for this study, from the ethics committee at the University of Strathclyde. The committee was contacted through e-mail, and a pro-forma sent, setting out a description of the study and information about the data collection procedure. The ethics committee at the University of Strathclyde sent its approval by an e-mail to the researcher. Another ethics approval was requested and granted, at the time the e-mails all potential questionnaire respondents were sent. The researcher provided potential respondents with an introduction to the context of the research and the objective of the questionnaire. Those who agreed to participate were clearly informed before starting to respond to the questionnaire inquiries. They gave their informed consent to use their answers for the context of this study by completing and submitting the questionnaire.

For the interviews, the interview guide's first page included all the details of the study and a consent form was signed by participant interviewees before commencing the interviews. The consent form embodied details about the purpose of the study, benefits of the research, how the interview would proceed, and how the results would be presented. In addition, it ensured participants that they could, at any time, withdraw their participation. Moreover, all participants were informed that anonymity was assured by not using their real names and their organisations name unless they agreed to that, and that their identities, personal data, and signed consent forms would not be disclosed under any circumstances either verbally or in documents.

The anonymity of respondents was ensured by using numbers on the questionnaires and interviews, rather than their real names. This was essential to respect their privacy and

to protect them from any potential risk or harm. In addition, the researcher was the only one who had access to the completed questionnaires and interviews. The data collected was used only for the purpose of the current research, which was advised to respondents before completing the questionnaires. During the research process, no financial or other compensation was requested or submitted to the researcher or the participants involved. The researcher took great care to ensure that all questionnaire participants, interviewees, and managers had a positive perception of the research.

3.11. Chapter Summary

This chapter presented and justified the methodological framework and approach of the research. Given the nature of the research questions and the scope of the study, it is appropriate that more than one method was chosen. The researcher chose a mixed paradigm with a philosophical foundation of pragmatism to study how social and cultural issues affect attitudes towards information security in Omani organisations. The research methods included a questionnaire as a quantitative method, as well as semi-structured interviews with open-ended questions.

This chapter describes the implementation of the data collection process using the adopted data collection tools. It addresses issues of validity, reliability, and research ethics in the context of the adopted mixed paradigm. The researcher recognises the importance of providing a clear account of the methods used in this research to evaluate the validity of the findings in chapters five and six.

Chapter 4. Findings – Survey Analysis

"What gets measured, gets managed"
-(Peter Drucker, 1954, p.71)

4.1. Introduction

The researcher sought to understand existing security practices in organisations as the first stage in addressing wider issues of information security. Some elements of the questionnaire were aimed at tracking the state of security practices in organisations, in particular, the current state of information security culture and practices in public and private organisations in Oman, and any differences between public and private organisations in regards to information security practices and behaviour. Results from this survey were meant to complement other findings gathered from interviews, as the basis for an effectively developing organisational information security culture.

The quantitative research method is one of the most powerful commonly used tools for collecting data from multiple units of analysis, and it is a widely accepted research method in the social sciences for studying organisational issues. (Babbie, 1998; Bond, 1988; Cameron & Quinn, 1999; Hofstede, 1980; Schein, 1992; Straub et al., 2001). Researchers define survey research according to their individual objectives and disciplines. For example, Fink (1995) defines a survey as a system of collecting information to describe, compare, or explain knowledge, attitudes, and behaviour.
There are three different characteristics of the survey method:

- It is designed to generate quantitative explanations of certain features of a population.
- It gathers information by asking people structured, predefined questions.
- The data it collects is generally gathered from a portion of the study population such that the findings can be generalised to a larger population.

This chapter presents the results of the analysis of the data collected by a questionnaire survey instrument. The survey consists of three sections:

- Demographic information,
- Information security aspects,
- The respondent's notes and suggestions.

The questionnaire items were rated on a Likert scale with three points ('yes', 'no', and 'not sure'). According to Sampieri (1991, p.285), "the instrument of data collection

really represents the variables we have in mind. If it doesn't, our measure is deficient and therefore, the research is not worthy to be taken into account". (Sampieri, 1991, p.285).

In this research, the survey inquiries were based on questions drawn from other studies that were previously validated. The survey was anonymous, and respondents were selected semi-randomly from different Omani public and private organisations as agreed with the Information Technology Authority. Participants received an e-mailed link to Arabic and English versions of the survey.

The next section explains briefly the statistical methods used in the survey data analysis.

4.2. Statistical Methods

A number of statistical analyses were conducted in this study on the survey data. The IBM Statistical Package for the Social Sciences (SPSS version 22) was used as a tool to investigate the association between socio-cultural and organisational factors and information security culture. In addition, the correlation between organisational cultural characteristics and information security was investigated. Scholars consider SPSS to be one of the most preferred statistical tools that researchers can use to resolve and analyse complex research problems. Its ability to provide analytical results with enhanced validity makes it an extremely practical tool for analysing research data. (Foster, 2001). Further, SPSS is a self-competent computer program; the user needs only to insert the data from the research into the program, which can then produce accurate as well as reliable and organised formatted result outcomes, that significantly reduces the amount of time needed by the researcher to accomplish the task. It is an extremely effective and efficient tool for complex analyses. (Bryman and Cramer, 2000).

The rationale for using SPSS in this study mainly focused its ability provide an overall analysis of the data, as well as a comparative analysis of the current state of information security in public and private organisation in regards. SPSS Correlation and Regression analyses were conducted to determine the most important focuses. ANOVA and t-tests were used to determine significant differences between the results of the public and private organisations participants' statements. The t-test compares the results of the two groups to determine whether the differences were significant. ANOVA tests were used to compare the results of more than two groups to determine whether the differences were significant.

Different tests were conducted through the IBM Statistical Package for the Social Sciences (SPSS version 22), to determine and compare differences in survey analysis results between public and private organisations. These tests were:

Simple and averaged percentage

The analysis uses percentages rather than frequency to represent the proportion of the population sample in relation to the relevant information-security-related elements. According to Ellen (1989), this is a good way to show relationships and comparisons between categories of respondents or between categories of responses. Moreover, some participants did not respond to some questions or marked some questions as 'NA' (i.e. not all participants answered all questions). Only participants who answered a question were used to calculate percentages. Average percentages were used to compare different information security aspects and to compare public and private sectors with regard to each information security aspect. The average percentage was calculated for every scale item in each dimension by dividing the total number of responses of every scale item in the dimension by the total number of responses to all questions in that dimension.

T- test

The t-test is a procedure used to compare two independent variables. (Frude, 1990). The t-test was applied in this study to examine whether the answers provided by private organisations participants were substantially different from the answers provided by public organisations participants. A "significant difference" between the two groups, means that the observed results are most likely to reflect the characteristics of the population in Omani public and private organisations rather than just a sampling error or chance.

Multiple Regression

Multiple regression is used in the study to analyse the relationship between a dependent variable and several independent variables. Multiple regression analysis makes it possible to calculate, for each independent variable, a regression coefficient, which indicates how much the value of a dependent variable varies with the change in the value of the independent variable.

Correlation

Correlation is a statistical method used to determine whether a relationship between variables exists. The study uses this method to measure how strong the relationship is between an Omani organisation's information security culture and information security aspects. The strength of the link is expressed by means of the correlation coefficient

(Pearson, r), a number always lying between -1 (perfect linear relation with negative slope) and +1 (perfect linear relation with positive slope).

Concepts and Tools

The concept of composite variables, are those that have been defined and calculated based upon a number of criteria or scores of different answers. These composite variables are multiple item measures, which are calculated and not directly observed. However, they are considered to be measured variables. In the current study, composite variables were applied to make responses to inquiry items more manageable. They were created using the transform and compute functions in SPSS software version 22, each composite variable indicator takes a turn as the Dependent Variable (DV) and all other composite indicators are treated as Independent Variables (IVs). Each composite variable is determined by combining the responses to a group of questions that, together, reflect the associated information security aspect. Each composite variable was calculated by summing the individual composite item scores and dividing that sum by the number of items in a particular scale. The MEAN function and the scores were used to calculate the average per latent variable. It is also a usual practice to treat composite variables as continuous variables. (Newsom, 2013).

Description of quantitative Measures (Likert scale)

In the current study, scaled responses were used in the questionnaire, to measure the perceptions of Omani employees regarding the status of information security in their organisations. Scaled-response questions are designed to use a certain scale to measure the quality of a construct. They are commonly used to measure respondents' attitudes towards particular issues. (Frazer and Lawley, 2000, p.28). The study uses the Likert scale, often used for analysing people's attitudes, by measuring the extent to which a person agrees or disagrees with a given question. The Likert scale scores were calculated in order to compare respondents' answers. According to Neuman (2006, p.207), Likert scales refer to “a scale often used in survey research in which people express attitudes or other responses in terms of ordinal-level categories (e.g., agree, disagree) that are ranked along a continuum”. In this study Likert scale measures were used as a quantitative approach to employees’ perceptions about information security.

The questionnaire items were rated on a three point Likert scale (yes, no, not sure) as a "discrete" scale of measurement, where the respondent indicates the extent to which they agree or disagree with a statement. To prevent the respondents from becoming confused and replicating their answers, only one choice was provided for each question.

Questions were formulated in a way that facilitates the collection of best practice. So "yes" denotes most preferred practices while "no" denotes least preferred, to give respondents a variety of choices that were most appropriate for them. If a respondent chose a "yes" value, it signified that the individual felt a more powerful associative connection with the statement. If a respondent chose a "no" value, it signified that the individual felt a weak associative connection with the statement.

For every scale item, the number of participants who marked "yes" were collected and the percentages were calculated, to represent the perspective of the population sample towards positive information security aspects. The formatting of the survey questions in the typical Likert scale has the advantage of providing information that is useful for data analysis. (Bryman and Bell, 2007). Further, the use of a three-point Likert scale throughout in the questionnaire, allows the researcher to obtain more statistically valid responses.

4.3. Calculating Statistical Significance

This study calculates statistical significance using a standard 95% confidence level, which simply means the "probability of the observed difference arising by chance was sufficiently small". (Norman & Streiner, 2003, p.32), When an answer option is shown as statistically significant, it means that the difference between the two groups has less than a 5% probability of occurring by chance or sampling error alone, which is often displayed as $p < 0.05$.

Table 4-1: Formulas used to calculate the statistical significance between public and private Organisations' groups

Statistic	Description	Formula
a1	The proportion of the first group answering a question a certain way multiplied by the sample size of that group.	$a_1 = p_1 * n_1$
b1	The proportion of the second group answering a question a certain way multiplied by the sample size of that group.	$b_1 = p_2 * n_2$
Pooled Sample Proportion (p)	The combination of the two proportions for both groups.	$p = \frac{a_1 + b_1}{n_1 + n_2}$
Standard Error (SE)	A measure of how far your proportion is from the true proportion. A smaller number means the proportion is close to the true proportion, a larger number means the proportion is far away from the true proportion.	$SE = \sqrt{(p*(1-p)) * (\frac{1}{n_1} + \frac{1}{n_2})}$
Test Statistic (t)	A t-statistic, is the number of standard deviations a number is away from the mean	$t = \frac{p_1 - p_2}{SE}$
Statistical Significance	If the absolute value of the test statistic is greater than 1.96* standard deviations of the mean, then it's considered a statistically significant difference	$\|t\| > 1.96$

*1.96 is a number used for the 95% confidence level since 95% of the area under the study, t-distribution function lies within 1.96 standard deviations of the mean.

Table 4-1 above, shows formulas that were used to calculate the statistical significance as between public and private sector groups. Applying these formulas to the results

obtained from the SPSS statistical tool, produces the final results for the study dependent variables as shown in the next page in table 4-2.

Table 4-2: Final results for the study dependent variables using statistical significant differences (Calculating |t|) – Absolute t

Variables	p1	n1	a1	p2	n2	b1	p	SE	1/n1	1/n2	t	|t| Absolute t
IS POLICY	0.31	83	25.73	0.6	36	21.6	0.3977	0.0977	0.0121	0.0278	-2.969	2.9691
IS Training and awareness	0.39	97	37.83	0.65	47	30.55	0.4749	0.0887	0.0103	0.0213	-2.929	2.9296
IS Management support	0.26	70	18.2	0.52	33	17.16	0.3433	0.1003	0.0143	0.0303	-2.593	2.5932
IS Culture	0.38	46	17.48	0.65	32	20.8	0.4908	0.1151	0.0217	0.0312	-2.346	2.3463
IS Best practices	0.45	68	30.6	0.56	31	17.36	0.4844	0.1083	0.0147	0.0323	-1.0157	1.0157
IS Responsible Bodies	0.5	66	33	0.37	31	11.47	0.4585	0.1085	0.0152	0.0323	1.1982	1.1982
Average	0.38	72	27.36	0.59	36	21.24	0.45	0.1016	0.0139	0.0278	-2.0679	2.0688

(ISP)Information Security Policy- (ISTA)Information Security training & awareness.
(ISMSC) Information Security management support – (ISC) Information Security Culture.
(ISBP) Information Security best practice- (ISNRB) Information Security national responsible body.

4.4. Survey Sample

The target participants of this study were employees working in public and private sector organisations in Oman. The researcher extrapolated the conclusions drawn from the individuals in the sample to the total population. Thus, the sample was representative of the total population (see table 3-4 in chapter three section 3.6.5, page 105). The questionnaires were distributed semi-randomly to 200 employees from public and private organisations in Oman. There were 155 (77%) responses in total; 71% were male and 29% were female from both sector organisations, with a rate of 72% for public organisations and 28% for private organisations. Stratified semi-random sampling (Snowball sampling) where the population area was divided into two strata (public and private) was used, and a simple semi-random sample was selected from each stratum. This created reliable estimates for each stratum and for the entire population.

4.5. Descriptive Statistics

4.5.1. Demographic Analysis

The descriptive information about the people who were surveyed included age, gender, education level, job experience, type of organisation (public or private), organisation size, organisation specification.

The details of that information as processed through SPSS in the study are:

Type of Organisation (Public/ private)

Both public and private sectors were represented in the sample; 72% of the individuals who participated in the survey were from the public sector.

Gender

Gender is important when studying organisational information security, since the behaviours and norms when dealing with information security differ between men and women. 29% of the respondents were females. This reflects the actual labour force participation rate of females in Oman, which is 28.3% according to the UN human development report of 2013.

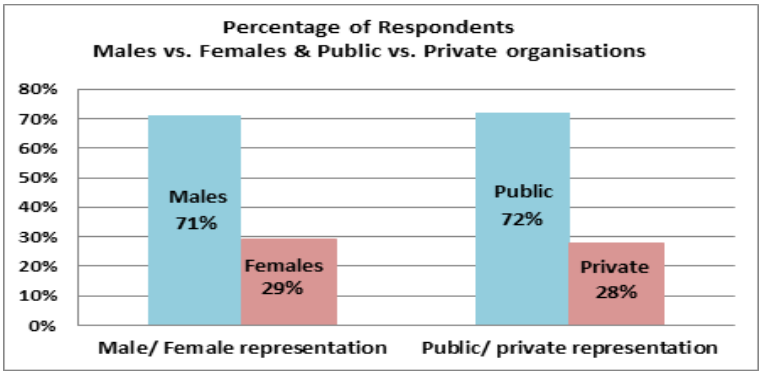

Chart 4-1: Respondents according to gender in Public and Private Organisations in Oman

Chart 4-1 above shows the percentages of respondents from public and private organisations as well as the percentages of male and female respondents.

Age

Chart 4-2 below shows that of the 155 participants, 61% were in the range of 25 to 36 years old, 33% were in the range of 36 to 55 years old, and 6% were in the range of 20 to 25 years old. This indicates the general pattern of working age distribution in Omani organisations.

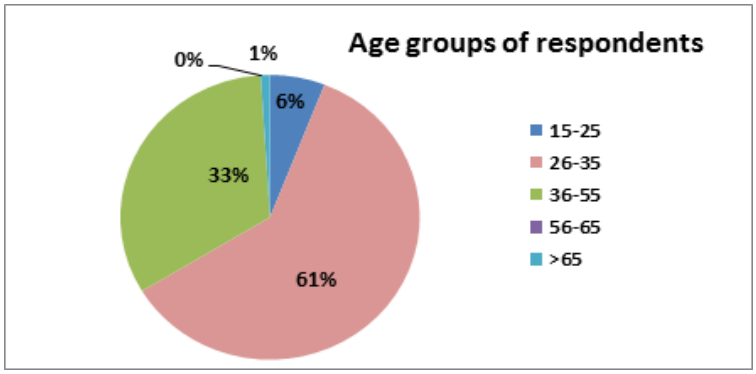

Chart 4-2 Respondents according to Age groups in Omani Public and Private organisations

Nationality

95% of the sample participants were Omani citizens and 5% were non-Omani. This information proves that employees in public sector organisations in Oman are mostly Omani, and a small percentage are not, as depicted in chart 4-3 in the next page.

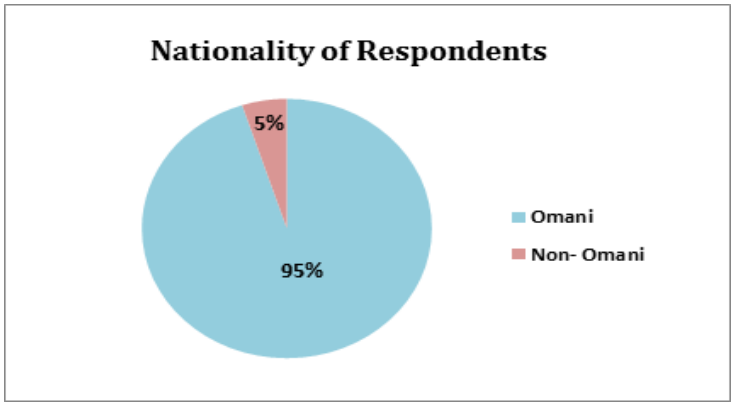

Chart 4-3 Respondents according to Nationaliy in Omani Public and Private organisation

4.5.2. Specialization of the Organisations

Different types of organisations are represented in the sample, including banking and insurance, consultancy, IT, manufacturing, medical care, retail, and education and training. Of the 155 participants, approximately 58% were from public organisations, as depicted in chart 4-4 below.

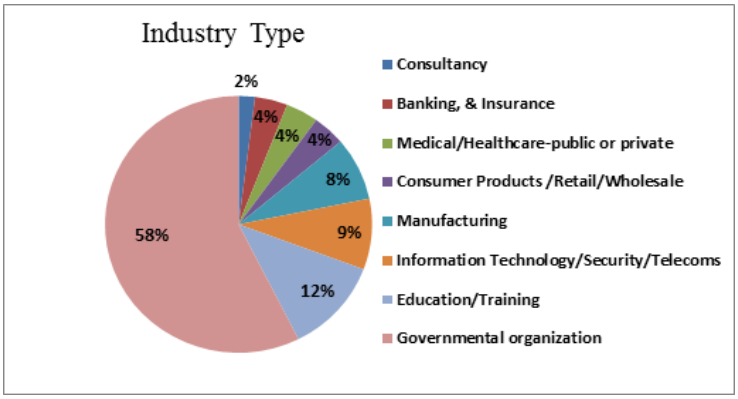

Chart 4-4 Respondents according to specialisation of Omani Public and Private organisation

4.5.3. Organisation Size

The participants were from organisations of different sizes, including small organisations with 500 employees or less mainly from the private sector, while the large organisations with more than 15,000 employees were mainly public sector. Chart 4-5 in the previous page details the distribution.

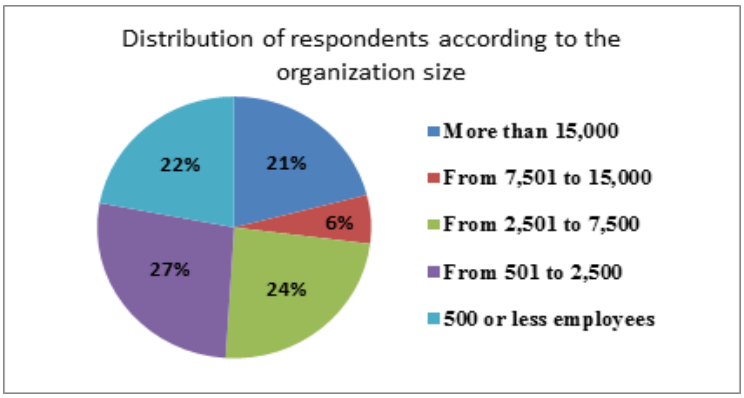

Chart 4-5 Respondents according to organizational size in Omani public and private organisations

4.5.4. Education Level

Chart 4-6 below shows that the sample included all levels of education from high school to PhD. 77% of the respondents had university degrees, (47% BSc; 26% MSc; 4% PhD). The remaining 23% was distributed between high school and higher diploma levels.

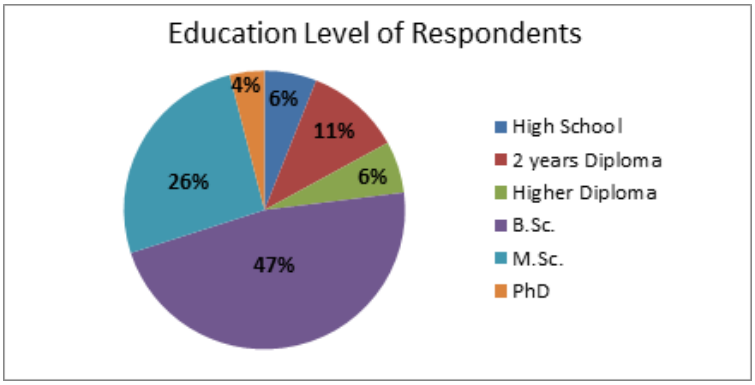

Chart 4-6 Respondents according to Education Level in Omani public and private organisations

The fact that most workers in Omani organisations are educated theoretically enhances the environment for the development of a culture of information security in their organisations. However, other factors such as lack of management support, lack of training and awareness, power distance, lack of an information security policy, and the collectivist nature of Omani culture all work to reduce the impact of education levels.

4.5.5. Work Experience

Chart 4-7 below shows that 41% of respondents had ten years or more work experience, while 31% had between six and ten years, 25% had between one and five years, and only 3% had less than one year. These percentages may explain the slow development of information security in Omani organisations, because younger and less experienced

employees are more likely to accept and follow change, in contrast with the more experienced older employees who show greater hesitation towards change and stronger adherence to the existing norms of an organisation. (Hambrick, 2007).

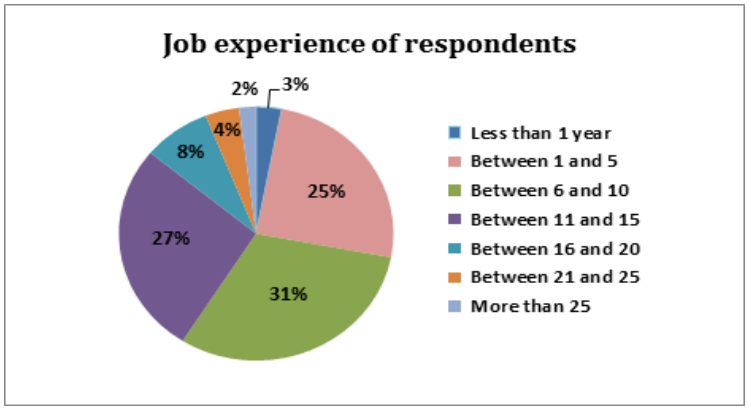

Chart 4-7 Respondents according to Job years of experiences in Omani public and private organisations

4.6. Organisational Critical Factors and Information Security in Oman

This research aimed to identify the status of information security in Oman by investigating the level of compliance with information security best practice along with any differences between public and private sector organisations.

Appendix D outlines the questions that represent activities associated with information security and shows the data that represents participant perceptions of information security. These questions, which comprise the measurement instrument used in this study, are categorised into the following six security aspects or dimensions of information security status in Oman:

1. An Organisation's Information Security Policy
2. Information Security Training and Awareness
3. Managerial Support of Information Security
4. Employee Commitment to Information Security Disciplines
5. An Organisation's Information Security Procedures
6. Omani National Information Security Bodies' Duties

Analysed data are presented below under these categories.

The statistical test applied

Simple and average percentages are used to represent the perspective of the population sample towards the relevant information security related elements.

Results

4.6.1. Information Security Policy

Chart 4-8 shows the answers of the survey respondents to questions about their organisations' information security policies in Oman. It measures responses to the following seven questions that expose the extent to which these organisations are concerned with information security policies and the degree of compliance with any related best practices:

1. Does the organisation have a detailed and documented information security policy?
2. If the answer for the above question is YES, do employees follow it?
3. Are employees educated about any updates in the security policy?
4. Are employees obligated to commit to the information security policy?
5. Is the information security policy reviewed and updated periodically?
6. Does the organisation periodically monitor information security policy violations?
7. Are employees forced to commit to the information security policy? In addition, do they know where to access it?

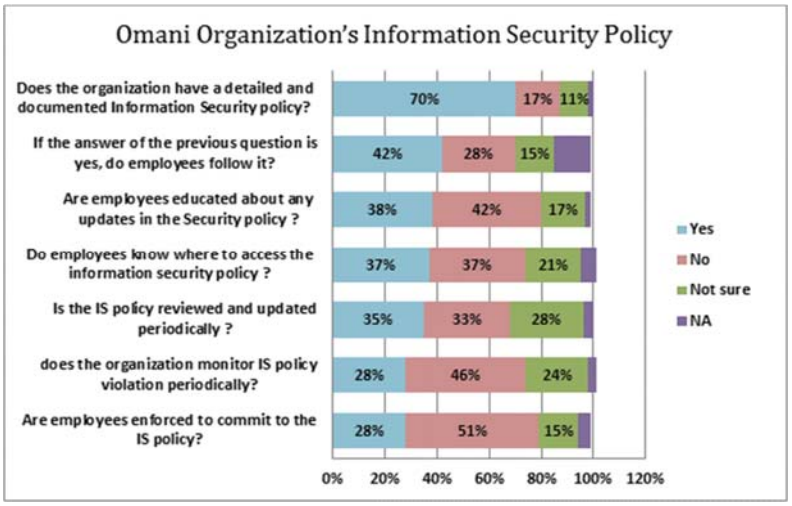

Chart 4-8 Survey Result of the Availability of Information Security Policy (ISP) in Public and Private Organisations in Oman

A high percentage of 'yes' answers (higher than 50%) indicates a positive status with regard to information-security-policy-related best practices within the targeted organisations. It also indicates that the respondent is likely to work in an organisation that is highly concerned with information security. As depicted in the chart, less than 50% of the respondents marked 'yes' to all questions related to information security policies except for one question (Does the organisation have a detailed and documented information security policy?) which was marked 'yes' by 70% of the respondents.

All other central features of a good information security policy received less than 50% from the respondents. These features, prioritised in descending order, are as follows:

- Whether employees follow the information security policy if it exists in the organisation (42%),
- Whether employees are educated about any updates in the security policy (38%),
- Whether employees are obligated to commit to the security policy (37%),
- Whether the security policy is reviewed and updated periodically (35%),
- Whether the security policy is monitored periodically against violation (28%),
- Whether employees are forced to commit to the information security policy (28%).

The average percentage of positive participant perceptions of information security policy was 40%.

These results show that most Omani organisations have an information security policy regardless of how seriously it is implemented and monitored, and regardless of the level of employee compliance. However, the results for public sector and private sector organisations are different. The comparison is summarised in chart 4-9 below.

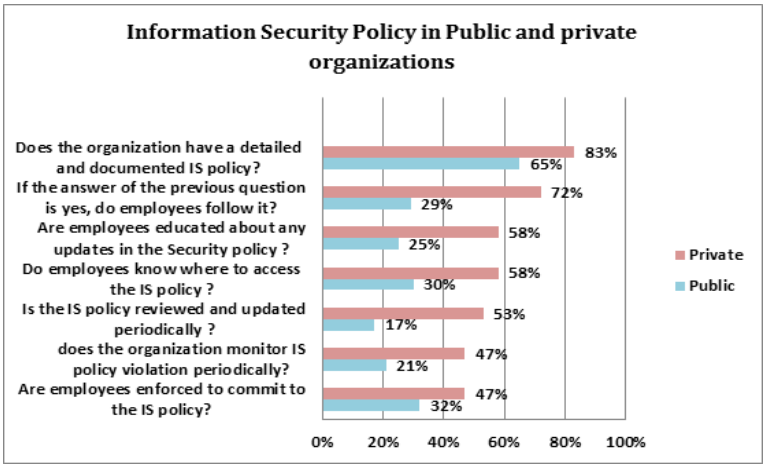

Chart 4-9: Comparison between Public Vs Private Organisations in Oman Regarding Information Security Policy (ISP)

Most information security policy aspects received more than 50% of 'yes' marks in the private sector, as shown in chart 4-9 above. The chart shows that from the respondents' perspectives, the private sector in Oman is more advanced than the public sector with regard to information security policy implementation. More than 50% marked 'yes' to five questions related to information security policy, and 47% chose 'yes' to two questions about monitoring the information security policy violation periodically and about enforcing employees to commit to the information.

In the public sector, less than 50% of the respondents marked 'yes' to all questions related to information security policies, except for one question (Does the organisation

have a detailed and documented information security policy?), which was marked 'yes' by 65% of respondents.

The average percentage of positive participant perceptions of information security policies was 31% in public sector organisations and 60% in private sector organisations, as illustrated in chart 4-10 below.

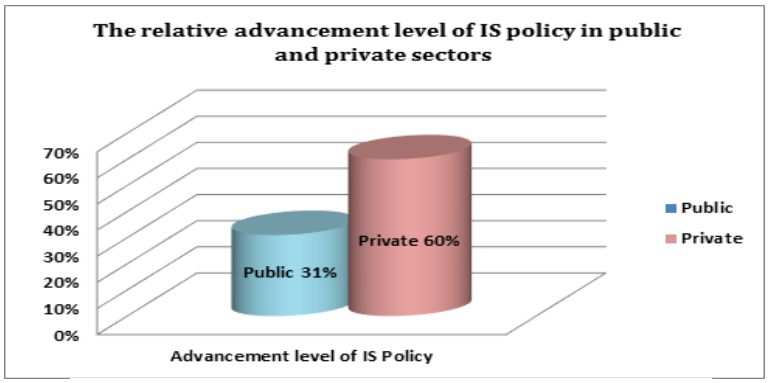

Chart 4-10 Comparison of Information Security Policy in public and private organisations in Oman

These comparative results demonstrate that private sector organisation compliance with information security best practices is high and nearly double that of the public sector organisations in the perception of the respondents.

Moreover, when the statistical significance between public sector and private sector groups was tested, the statistical significance (| t |) found to be 2.9691. The absolute value of the test statistic is greater than 1.96, so that the difference between public and private organisations in Oman, regarding compliance with information security policy is statistically significant. (i.e. Private organisations are more likely to comply with information security policy than public organisations).

4.6.2. Information Security Awareness and Training

The measurement scale for Omani organisations' attitudes towards information security training and awareness contains the following six questions that expose the level of compliance with information security training and awareness best practices:

1. Does the organisational structure include a department or section (or skilled security officer) that is concerned with information security in the organisation?
2. Are there regular knowledge updates for the information security staff?
3. Does the organisation conduct adequate training and awareness programs on information security for all employees in the organisation?
4. Does the organisation conduct refresher awareness programs on information security for employees?
5. Are security officers exercising their roles to the fullest?

6. Is there mutual coordination between human resource (HR) and the information security officers?

Chart 4-11 below shows responses to the questions in section 5.4.2. Less than 50% of the respondents marked 'yes' to all questions related to information security training and awareness, except for one question which 77% marked 'yes'. (Does the organisation's structure include a department, section, or skilled security officer that is concerned with information security in the organisation?).

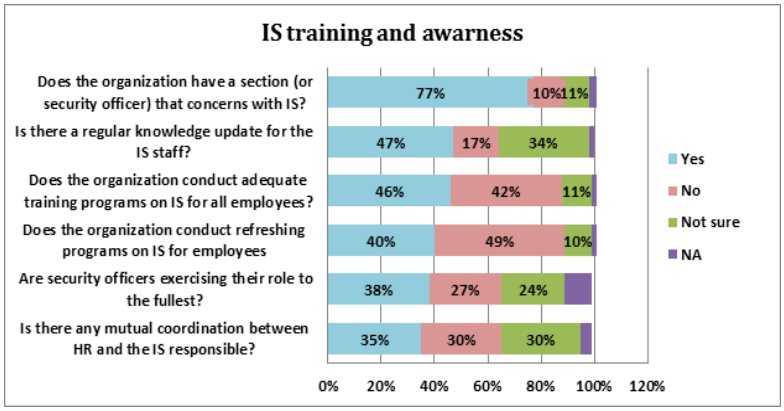

Chart **4-11** Survey Result of Information Security Training & Awareness in Public Vs Private Organisations in Oman

All other factors about training and awareness best practice scored less than 50%. These factors are, prioritized in descending order:

- Are there regular knowledge updates for the information security staff (47%)?
- Are there adequate training programs on information security for all employees (46%)?
- Are there refresher programs on information security for employees (40%)?
- Re the existing security officers exercising the position's full role (38%)?
- Is there mutual coordination between HR and the information security employees (35%)?

The average percentage of positive participant perceptions of information security training and awareness in Omani organisations, indicated by the responses that were marked with 'yes', is 47%.

The analysis in this section shows that most Omani organisations are keen to assign responsible personnel to oversee and implement their information security arrangements, but the overall compliance with best practice training activities is less than 50%. More than 50% private sector responses were positive, (i.e. percentage 'yes' responses), but less than 50 % positives in public sector organisations, with one

exception, (Does the organisation have a section or security officer that is concerned with information security? which was marked 'yes' by 75% of the respondents from the public sector).

Chart 4-12, which shows that private sector organisations in Oman are more advanced with regard to information security training and awareness.

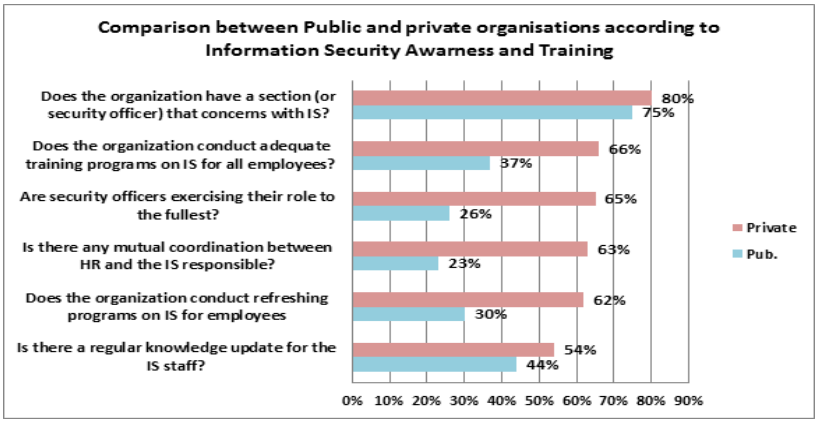

Chart 4-12 Level of Information Security Training & Awareness in Public Vs Private Organisations in Oman

The average percentage of positive participant perceptions of information security training and awareness was 39% in the public sector organisations and 65% in the private sector organisations, as depicted in Chart 4-13 below.

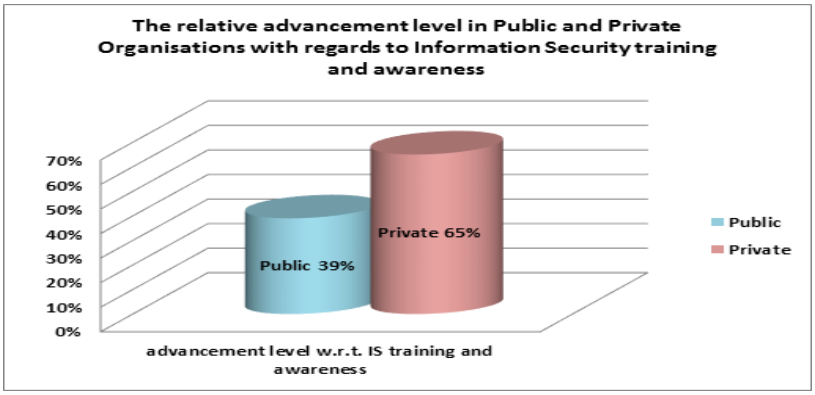

Chart 4-13 Comparison of Information Security Training and Awareness in Public and Private Organisations in Omani

Moreover, when the statistical significance between public sector and private sector organisations groups was tested, and (| t |) found to be 2.929588. The absolute value of the test statistic is greater than 1.96 so the difference between public and private organisations in Oman, regarding information security awareness and training is statistically significant. (i.e. Private organisations are more likely to comply with information security policy than public organisations).

4.6.3. Information Security Management Support and Commitment

The results of respondents' perceptions which reflect the attitudes of Omani organisations' managers towards supporting information security shown in appendix D. The measurement scale contained the following six questions:

1. Is there an assigned annual budget to develop information security?
2. Do managers at all levels support information security policies?
3. Do senior managers follow the organisation's information security policies?
4. Is the organisation interested in consulting internal or external information security auditors to ensure compliance with information security policies?
5. Do you think managers only care about information security when there is a breach of security in the organisation?
6. Does the information security policy applied to all organisation' members including managers in different levels?

Chart 4-14 below shows respondents' answers to these questions.

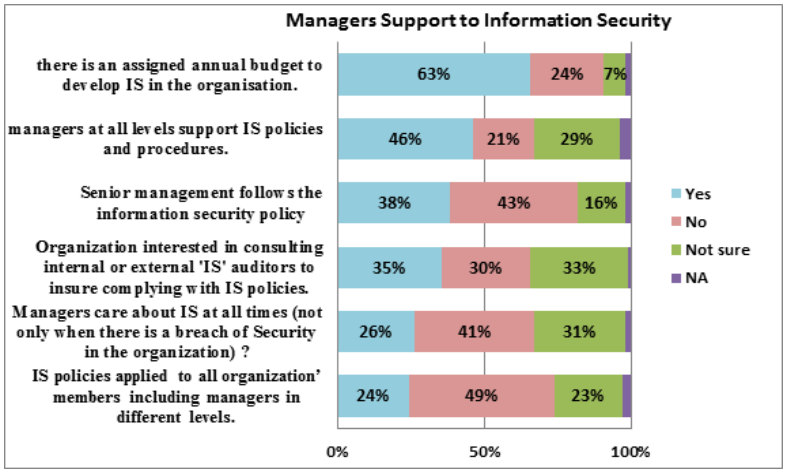

Chart 4-14 Survey result of Information Security Management Support in Public Vs Private Organisations in Oman

The above chart shows that more than 50% of the respondents marked 'yes' to the question denoting that there is an annual budget assigned to information security. The five other factors received less than 50%, and they are prioritised in descending order as follows:

- Manager support of information security policies at all levels (46%).
- Adequate management interest in information security (38%).
- Organisational interest in consulting internal or external information security auditors to ensure compliance with information security policies (35%).
- Managerial concern for information security at all times, and not only when there is a security breach. (26%).

- Application of information security policies to all organisational members including managers at different levels (24%).

The average percentage of positive participant perceptions (i.e. represented by responses that were marked with 'yes') of managers support for information security in Omani organisations was 34%.

This analysis shows that there is a considerable lack of management support for information security in Omani organisations and that the level of management support is below average. However, a higher level of managerial support was shown in private sector organisations than in the public sector.

Chart 4-15 below shows that the private sector in Oman is more advanced with regard to managerial support of information security with more than 50% of the private sector respondents replying 'yes' with regard to management support of information security.

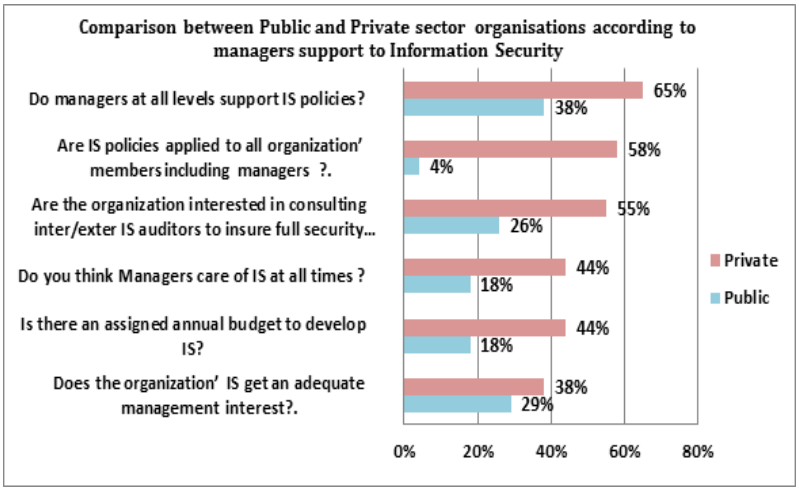

Chart 4-15 Level of Information Security Management Support in Public Vs Private Organisations in Oman

- 65% of private sector respondents marked 'yes' with regard to management support of information security at all levels;
- 58% gave positive responses to the application of information security policies to all organisational members including managers at different levels;
- 55% gave a positive response to managers' interest in consulting internal or external information security auditors to ensure that full security is provided to projects and systems.

However, the following three items were marked 'yes' by less than 50% of the respondents:

- Managers' care about information security at all times and not only when there is a breach of security in the organisation (44% of 'yes' marks).
- An annual budget is assigned to develop information security (44% of 'yes' marks).
- Managers provide adequate interest in information security (38% of 'yes' marks).

In the public sector, all items were marked 'yes' by less than 50% of the respondents. The major deficiency identified in the public sector is in the application of information security policy to all members including managers, to which only four percent of the respondents marked 'yes'. The average percentage of positive participant perceptions of management support for information security in Omani organisations was 26% in the public sector and 52% in the private sector, as depicted in the next chart 4-16.

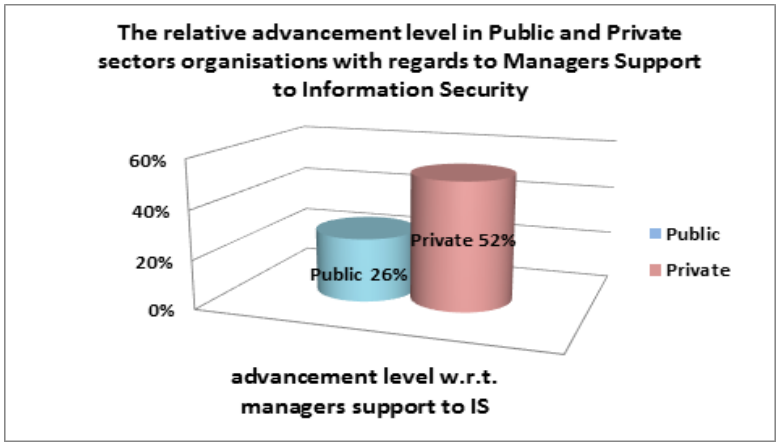

Chart 4-16 Comparison of Information Security Management Support in public and private organisations in Oman

This analysis generally denotes that information security lacks adequate managerial support in public sector organisations and that managerial support of information security in the private sector organisations is higher than in the public sector. Moreover, the difference between private and public sector responses has a statistical significance of (t|) 2.593224. The absolute value of the test statistic is greater than 1.96, so that the difference between public and private organisations in Oman, regarding management support and compliance is statistically significant. i.e. Private organisations are more likely to comply with information security policy than public organisations.

4.7. Information Security Culture in Omani Organisations

4.7.1. Employees' Attitudes Toward Information Security Culture

The measurement scale for the employees' attitudes towards a positive information security culture in Omani organisations contains the following eight questions:

1. Have you contributed any suggestions to improving the information security policies and procedures?
2. Do you think that the weakness of the culture of employee information security leads to higher information security risks?
3. Do you think the work environment limits employees' actions towards information security?
4. Is cooperation between the organisation's departments and information security staff important?
5. Is practicing good information security part of the shared beliefs of the organisation's members?
6. Are employees familiar with the importance of information security to the organisation?
7. Is it a condemned practice in the organisation for employees to exchange passwords with each other?
8. Are the organisation's employees often satisfied with information security procedures?

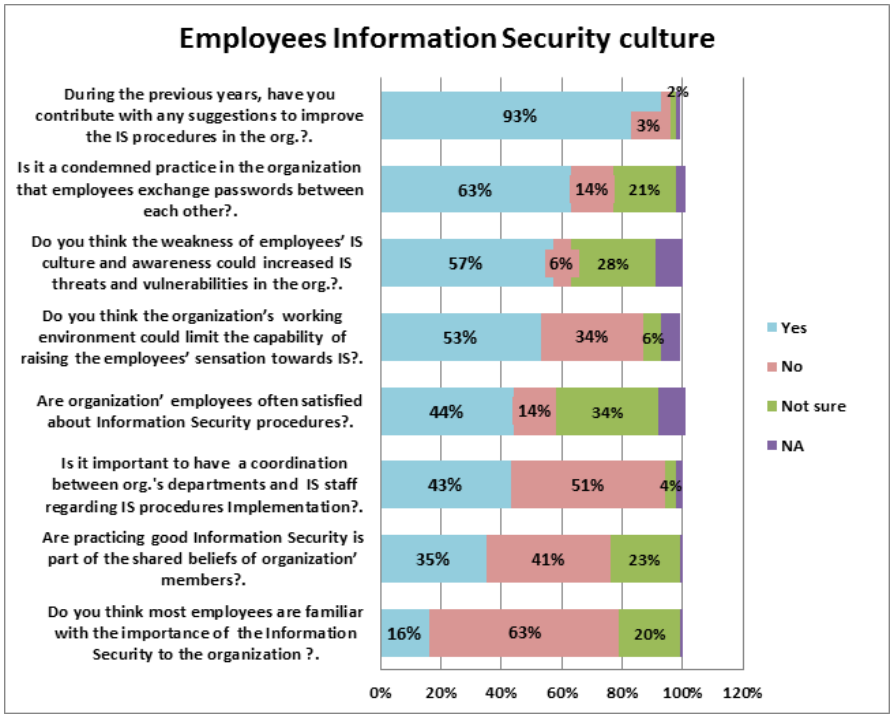

Chart **4-17**: Survey result of Employees Information Security Culture in Public Vs Private Organisations in Oman

Chart 4-17 shows the survey responses concerning the employee information security culture in Omani organisations. The chart demonstrates the respondents' level of positive perspectives on the information security culture in their organisations as represented by their 'yes' marks. A high average percentage of 'yes' (higher than 50%) indicates a positive perception of information security culture attributes.

The responses show that 93% of the respondents have contributed suggestions to improve information security policies and procedures. In addition, 63% of the respondents confirmed that the practice of employees exchanging passwords is condemned. 57% believed that a weak employee information security culture leads to higher information security risks, and 53% thought that the work environment limits employee actions supporting information security.

By contrast, the responses also show some less positive aspects of the information security culture:

- Satisfaction with the information security policy (44% of 'yes' marks).
- The importance of cooperation between the organisation's departments and information security staff regarding information security (43% of 'yes' marks).
- The belief that information security best practice is part of the shared beliefs of an organisation's members (35% of 'yes' marks).
- Familiarity with the importance of information security to the organisation (16% of 'yes' marks).

The average percentage of positive participant perceptions of the information security culture was 49%. However, there were twice as many positive responses from private sector respondents (i.e. responses that were marked with 'yes') than from public sector respondents, as shown in Chart 4-18 below.

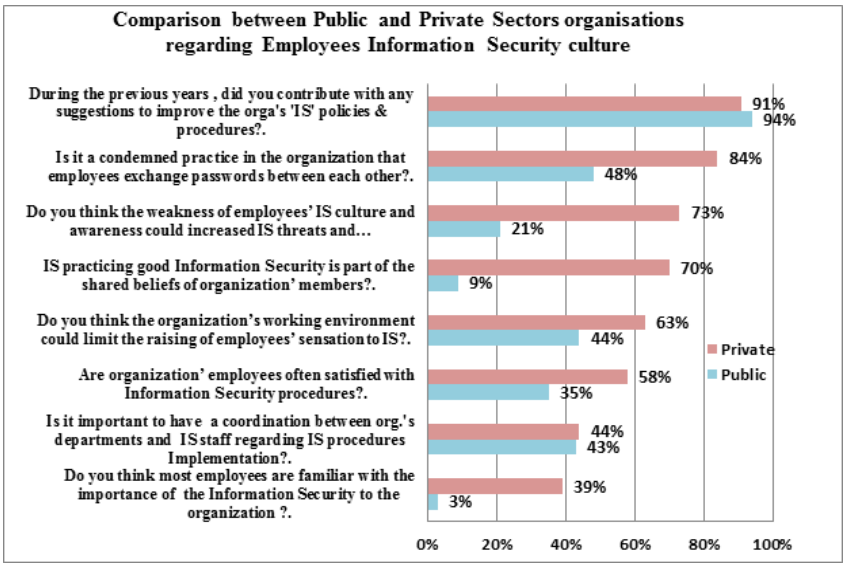

Chart 4-18: Level of Employees Information Security Culture (ISC). in Public Vs Private Organisations in Oman

Only one attribute of information security culture (employees' contribution of suggestions to improve information security policies and procedures - private 91% and public 94%), achieved 'yes' marks in both the private sector and public sector.

84% of private sector participants marked 'yes' to the condemnation of exchanging passwords between employees. 73% believe that the weakness of the employee information security culture leads to higher information security risks. 70% consider good information security practice is part of the shared beliefs of an organisation. 63% believe that the work environment limits employee actions regarding information security, and 58% are satisfied with information security procedures.

The rest of the information security culture attributes achieved less than 50% of 'yes' marks from respondents in the private sector. However, except for the contribution of suggestions to improve information security policies, all items were marked 'yes' by less than 50% of the respondents from the public sector.

There is a substantial difference between the two sectors with regard to considering information security as part of the shared beliefs within an organisation. For this item, 70% of the private sector respondents marked 'yes', while only 9% of public sector respondents marked 'yes'.

Likewise, for familiarity with the importance of information security to organisations, 39% of the private sector respondents marked 'yes' while 3% in the public sector marked 'yes'. These findings denote that information security has a lower profile among public sector employees compared to the private sector.

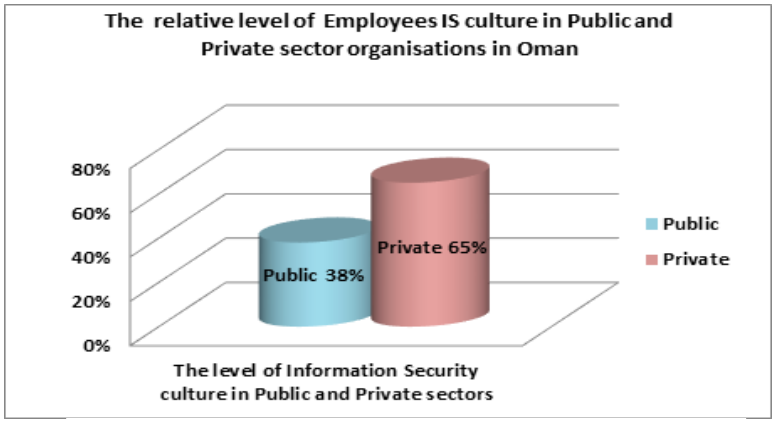

Chart 4-19 Comparison of Employee Information Security Culture in Public and Private Organisations in Oman

The average percentages of 'yes' responses, reflecting positive employee perception of information security culture in Omani organisations, were 38% in the public sector and 65% in private sector organisations. The statistical significance between public sector and private sector groups was (| t |) 2.346251. Since the absolute value of the test statistic is greater than 1.96, this means the difference between public and private organisations, in Oman, regarding employees′ perception towards positive information security

culture attributes is statistically significant. (i.e. Employees in private organisations are more likely to have better information security culture than those in public organisations)

4.7.2. Information Security Practice in Omani Organisations

The following 19 questions from the measurement scale included in Appendix D reflect Omani employees' attitudes towards information security practices:

1. Should every employee have a unique username and password for network authentication?
2. Does the information security policy require changing passwords at least every 90 days?
3. Are there network security measures, such as firewalls and ids/ips?
4. Are there any preventive measures to protect the organisation's information from sabotage?
5. Are all access rights and network accounts removed on employment termination?
6. Does the organisation use access control to manage the separation of duties?
7. Are certain security measures followed by the organisation to secure classified documents?
8. Is the security background of new recruits investigated?
9. Are there certain procedures to secure laptop usage in meetings and businesses?
10. Are suppliers prohibited from accessing the organisation's network?
11. Are short-term contract employees prohibited from accessing the organisation's network?
12. Are network firewall logs and server logs monitored regularly for intrusion attempts?
13. Is there a physical separation between the organisation's network and the Internet network?
14. Is a disciplinary process applied when an information security violation is repeated?
15. Is a 'need-to-know' policy used among the organisation's employees when exchanging information?
16. Is there a disaster recovery plan in the organisation?
17. Is copying documents and data into external storage devices restricted?
18. Does the organisation motivate employees by notifying superiors in the event of an information security violation?
19. Is the use of mobile phones restricted within the organisation's premises?

Chart 4-20 in the next page summarises respondents' answers to questions about information security best practices in Omani organisations. A high average percentage of 'yes' answers (higher than 50%) indicates a positive attitude towards core information security best practice procedures. Furthermore, the chart explores the level of compliance with those core information security best practice procedures.

Chart 4-20 Survey Results of Information Security Best Practice in Omani Organisations

The results show that three of the core information security best practices achieved more than 75% of 'yes' responses, which indicates that there is a high level of compliance with these practices. These practices include:

- The existence of a policy requiring every employee to have a unique username and password for network authentication (87%);
- The existence of a policy requiring passwords to be changed at least every 90 days (74%); and
- Security measures such as firewalls and ids/ips (70%).

Seven practices achieved 50% to 66% of 'yes' marks from respondents, which indicates a moderate level of compliance with these practices. These practices include:

- The existence of preventive measures to protect the organisation's information from sabotage (66%);

- The removal of all access rights and network accounts during employment termination (59%);
- The use of access control to manage the separation of duties (58%);
- The existence of certain security measures to secure classified documents (53%);
- The investigation of security background when recruiting new employees (52%),
- The existence of certain procedures to secure laptop usage in meetings and businesses (51%), and
- The prohibition of suppliers and outsourcing workers from accessing the organisation's network (51%).

The average percentage of positive participant perceptions of compliance with the of information security core best practice procedures was 48%. Chart 4-21 below compares responses to elements of information security best practice and procedures in public and private sector organisations.

Chart **4-21:** Level of Information Security compliance in public and private organisations in Oman

Chart 4-21 shows that there are many information security practices that attain a similar number of 'yes' marks in both sectors, whether they were on the high compliance side of the chart (the upper part) or the low compliance side.

The practices that show high compliance levels in both public and private sectors are:

- Assigning every employee, a unique username and password for network authentication (84% public and 89% private),
- The existence of network security measures such as firewalls and ids/ips (69% pub and 74% private) and
- Prohibiting suppliers from accessing the organisation's network (50% public and 55% private).

The public and private sectors are also similar in the following practices that are on the low compliance side of the chart (the lower part):

- The existence of a physical separation between the organisation's network and the Internet network (41% public and 48% private).
- Prohibiting short-term contract employees from accessing the organisation's network (13% public and 7% private).
- Restricting the use of mobile phones within the organisation's premises (19% public and 26% private).

On the other hand, there are considerable differences between private and public sectors in regard to other practices that have high compliance (i.e. more than 50% of 'yes' marks) and those that have low compliance (i.e. less than 50% of 'yes' marks).

.

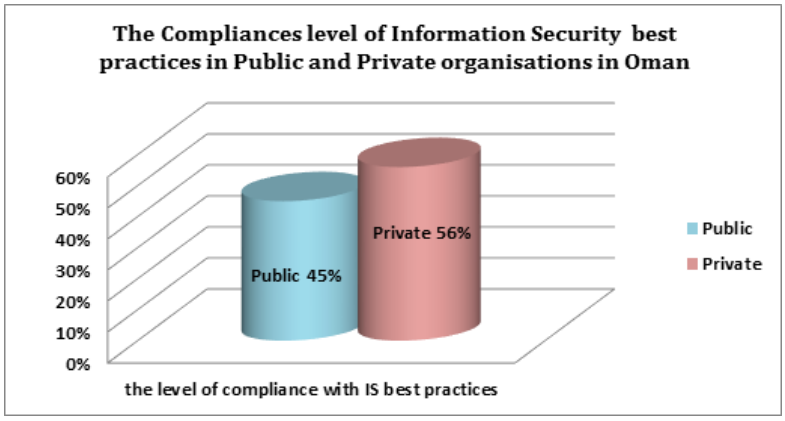

Chart 4-22 Comparison of Information Security Best Practices in public and private organisations in Oman

The average percentages of compliance with information security best practices from the perspective of the public sector respondents is 45%, and 56% in the private sector. The private sector has more positive as shown in the chart 4-22 above. However, the tested statistical significance between public sector and private sector groups is (| t |) 1.015665. Since the absolute value of the test statistic is less than 1.96, this means there is no statistically significant difference between Omani public and private organisations with regard to this aspect of good information security best practice. i.e. the study

indicates no statistical difference between public and private organisations in this regard.

Upon examining the participants' answers, the researcher suggests the reason for this result could be due to the extreme variability in the responses of participants from public organisations, and the resulting different frequencies of response. In contrast, the answers from private organisations' participants are more consistent. Large variability within a group decreases the 't' value, and makes it difficult to find significance. The study suggests that the magnitude of difference was not enough to be statistically significant because of the high variability in the public organisations group. Therefore, in this instance the statistical significance test missed the apparent differences between public and private organisations and the researcher relied more on the interviews for this aspect of information security best practice.

4.7.3. Duties of Information Security Responsible Bodies in Oman

The results that reflect how well the Omani national information security responsible bodies support Omani organisations with regard to information security are shown in appendix (D). The measurement scale contains the following three questions:

1. Do information security bodies in Oman, such as ITA and CERT, guide the public sector and private sector to apply the best information security practices in their organisations?
2. Did the organisation previously receive any invitations from these bodies to attend information security conferences and workshops?
3. Does the organisation receive any periodic alerts from these bodies regarding detection of new information security vulnerabilities and threats?

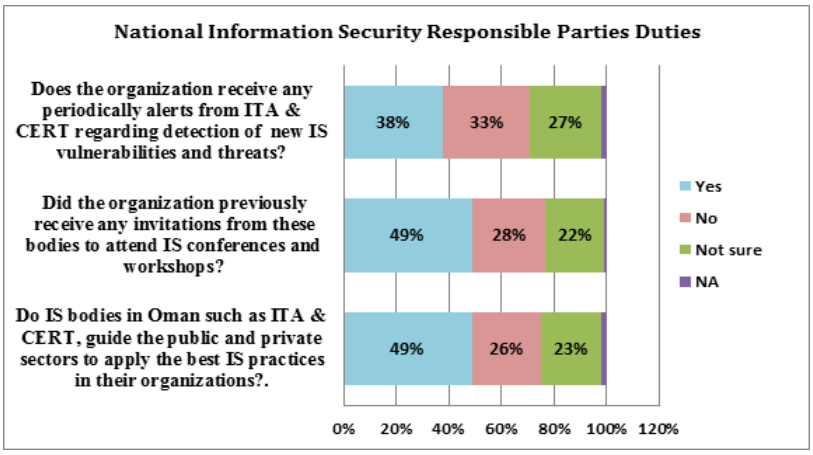

Chart 4-23: Survey Result of National Concerned Bodies Support to Omani Organisations

Chart 4-23 above shows the responses to questions about how well Omani organisations consider the information security bodies are in performing their duties. A high

percentage of 'yes' answers (higher than 50%) indicates a positive attitude towards the performance of information security bodies in Oman. The chart exposes the respondents' perspectives of the level of support provided by national information security parties, and it also shows that all three items related to information security support received a below average 'yes' mark of less than (50%). However, chart 4-23shows that approximately 25% (22%- 27%) of respondents answered 'not sure' to these three questions. This finding suggests that a considerable number of employees in Omani organisations. Are unaware or vague about the support provided by the national information security bodies. The average percentage of positive participant perceptions of information security bodies' duties was 46%.

A comparison of the public private sector positive responses to these three factors (i.e. responses that were marked with 'yes') are shown in the chart below.

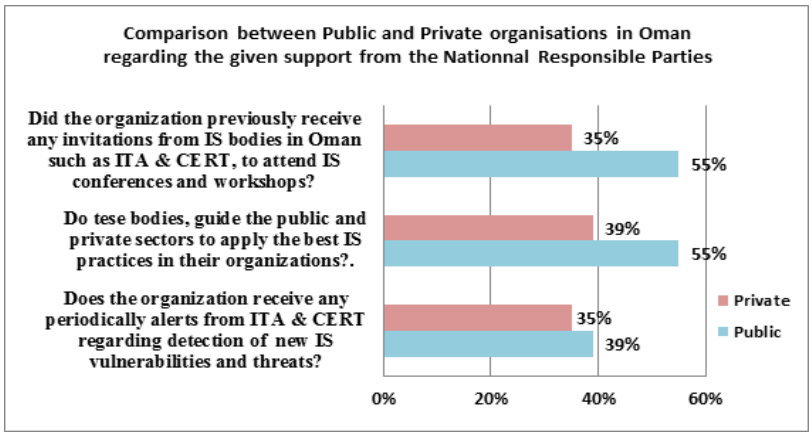

Chart 4-24 Level of National Security Concerned Bodies Support to the Omani Public and Private Organisations

Chart 4-24 above shows that according to the survey respondents' perceptions, the public sector receives more invitations to attend information security conferences and workshops and more guidance about applying the best information security practices from the national bodies, as 55% of respondents marked 'yes' for both items. By comparison, the private sector marked 35% and 39%, respectively, with regard to these two items. With regards to receiving periodic alerts about the detection of new information security vulnerabilities and threats, both sectors achieved results below average (i.e. less than 50% of respondents answered 'yes'). The private sector scored 35%, while the public sector scored 39%. The average percentage score for support provided by the national information security bodies was 50% for the public sector and 37% for the private sector. These findings suggest that national information security bodies give more attention to public sector organisations than to private sector organisations, as indicated in chart 4-25 in the next page.

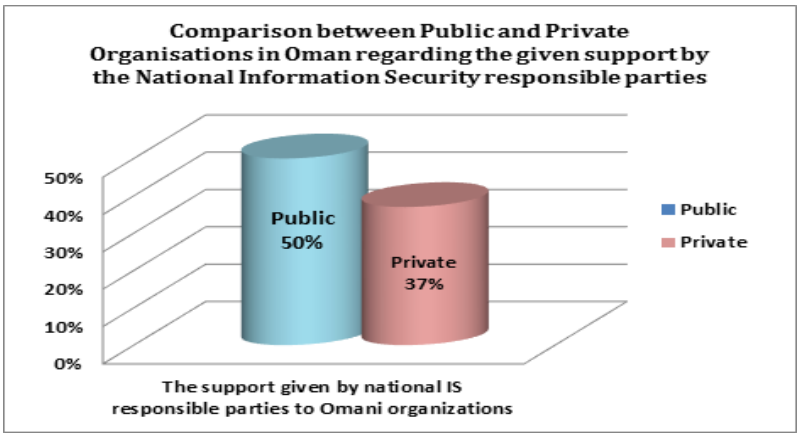

Chart 4-25 Comparison of the national Concerned Bodies support to the public and private Omani organisations

The tested statistical significance between public sector and private sector groups was (| t |) 1.198243. Since the absolute value of the test statistic is less than 1.96, this means there is no statistically significant difference between public and private organisations regarding their perception of information security support provided by national bodies to their organisations. i.e. the study shows the statistically there is no difference between public and private organisations in this regard.

The researcher believes that the reason behind this result may be due to participants lack of information about the support provide to their organisations by the national body, as this only known at managerial level. It appears that their answers are based on personal perception rather than the real situation. Therefore, in this part the researcher suggests the statistical significance test missed the apparent differences between public and private organisations in showing the level of information security support provided by national bodies to Omani public and private organisations.

4.8. The Relationship Between Social Factor "Education" and Information Security Culture in Omani Organisations

The study aimed to identify any relationships between social factors and the characteristics of organisational culture, and information security, in Omani organisations. The researcher therefore investigated the correlation between a number of ***Dependent variables,*** (these included aspects of ***information security*** such as: information security policies; information security training and awareness; management support; employee information security culture; and information security procedures), and ***Independent variables,*** (which included "education" as a social factor).

The dependent variables are composite variables that represent all the relevant information security aspects. Each variable was built by combining the responses to a group of questions that reflect one aspect.

Example of creating composite variables:

Composite variables were created and calculated based upon a number of scores of responses to particular answers, to enable them to be managed easily. For instance, to assess information security policy, seven items defined in the survey were used to measure this aspect. These items are:

1. Foundation of a detailed and documented information security policy.
2. Employee compliance with information security policy.
3. Employee education about information security policy updates.
4. Employee obligation to commit to information security policy.
5. Periodically reviewing and updating information security policy.
6. Periodically monitoring violations of information security policy.
7. Enforcement of employee commitment to information security policy.

The responses for these 7 variables/items were combined into one composite variable (OrgISP), by using the transform and compute function in SPSS software. Each composite variable was calculated by summing the individual composite item scores and dividing that sum by the number of items in the particular scale, which is 7 in this case. This created composite variable, was used in testing the research hypotheses.

4.8.1. Testing the Effect of "Education" on Information Security aspects in Omani Organisations

"Education" is the independent variable that represents a social factor, while the dependent variables include the following composite information security aspects:

- An Organisation's Information Security Policy OrgISP
- Information Security Training and Awareness OrgIST
- Management Support of Information Security OrgISMS
- Employees' Commitment to Information Security Disciplines OrgEISC
- An Organisation's Information Security Practices OrgISPR

The information security aspects set out above were tested against the effect of "education", as a social factor, on information security, though the following hypotheses:

H#1: Education level positively affects information security performance in Omani organisations.

The following sub-hypotheses are drawn from the previous (H#1) main hypothesis:

H#1.1: Education level is positively associated with information security policy in Omani organisations.

H#1.2: Education level is positively associated with information security training and awareness in Omani organisations.

H#1.3: Education level is positively associated with managerial support for information security in Omani organisations.

H#1.4: Education level is positively associated with employee commitment to information security disciplines in Omani organisations.

H#1.5: Education level is positively associated with an organisation's information security practices in Omani organisations.

Statistical method used:

Multiple regression analysis was used to test the above hypotheses.

Reason for using regression analysis

The researcher used regression analysis to find out if the employees' education level could affect their attitudes towards practicing good information security and developing a good culture of information security in Omani organisations. In other words, could "education" be a predictor variable with regards to information security aspects, i.e. could the study indicate that, the higher the employee level of education, the higher the level of information security. Alternatively, the researcher wished to know if education is not significant for predicting any of the above mentioned information security aspects.

Results

The outputs of the multiple regression analysis in SPSS are discussed below:

1- The effect of "Education" on Information Security policy in Omani organisations (OrgISP vs. education).

The following sub-hypothesis were tested:

H1.1: *Education level is positively associated with information security policy in Omani organisations.*

The relationship of the composite variable "OrgISP" Vs. education was investigated, through regression analysis and the result shown in table 4-3 in the next page.

Table 4-3: OrgISP Vs Education variables

1. OrgISP Vs Education Variable								
Coefficients[a]								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	1.009	.321		3.145	.002	.374	1.645
	Education	-.051	.044	-.087	-1.170	.244	-.138	.036
a. Dependent Variable: OrgISP								

Table 4-3 shows the significance level is >0.05 for the independent variable education. Therefore, β, which expresses the relative importance of the education variable, is not a significant predictor (i.e. this independent variable is not significant for predicting OrgISP). This finding suggests that there is no association between the socio-cultural factor education and the composite information security policy.

2- The effect of "Education" on training and awareness in Omani Organisations (OrgIST vs. education)

The following sub- hypothesis was tested:

> ***H#1.2:*** Education level is positively associated with information security training and awareness in Omani organisations.

The relationship of the composite variable "OrgIST" Vs. education was investigated, through regression analysis and the result shown in table 4-4 below.

Table 4-4: OrgISTA Vs Education variables

2. OrgISTA Vs Education Variable								
Coefficients[a]								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	.864	.540		1.599	.113	-.207	1.934
	Education	-.162	.075	-.157	-2.169	.032	-.311	-.014
a. Dependent Variable: OrgISTA								

Table 4-4 shows that the significance level is < 0.05 for the education variable, which means the independent variable education significantly predicted the OrgISTA variable. Since the β value is 0.157, there is a relationship between the socio-cultural factor education and the composite variable denoting information security training and awareness.

3- The effect of "Education" on Management Support to Information Security in Omani Organisations (OrgISMS vs. education

The following sub- hypothesis was tested:

> ***H#1.3:*** Education level is positively associated with management support for information security in Omani organisations

The relationship of the composite variable "OrgISMS" Vs. education, was investigated, through the regression analysis and the result shown in table 4-5 below.

Table 4-5: OrgISMS Vs Education variables

3. OrgISMS Vs Education Variable								
Coefficients[a]								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	.142	.347		.409	.683	-.546	.830
	Education	.008	.049	.012	.169	.866	-.088	.105
a. Dependent Variable: OrgISMS								

Table 4-5 above illustrates that the significance level is > 0.05 for the education variable. Therefore, the β, which expresses the relative importance education, is not a significant predictor (i.e. independent variable education is not significant for predicting OrgISMS). This finding indicates that there is no association between the socio-cultural factor education and the composite variable denoting management support for information security.

4- The effect of "Education" on Employee Commitment to Information Security Disciplines in Omani Organisations. (OrgEISC vs. education).

The following sub- hypothesis was tested:

> ***H#1.4:*** Education level is positively associated with employee commitment to information security disciplines in Omani organisations

The relationship of the composite variable "OrgISMS" Vs. education, was investigated, through regression analysis and the result shown in table 4-6 in the next page.

Table 4-6: OrgEISC Vs Education variables

4. OrgEISC Vs Education Variable								
Coefficients[a]								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	2.189	.317		6.908	.000	1.561	2.817
	Education	.017	.043	.038	.392	.696	-.068	.101
a. Dependent Variable: OrgEISC								

Table 4-6 above indicates that the significance level is > 0.05 for the independent variable education. Therefore, the β, which expresses the relative importance of education variable is not a significant predictor (i.e. the independent variable education is not significant for predicting OrgEISC). This finding shows that there is no relationship between the socio-cultural factor education and the composite variable denoting employee compliance to information security.

5- The effect of "Education" on Organisation's Information Security Practices in Omani Organisations (OrgISPR Vs. education)

The following sub- hypothesis was tested:

H#1.5: Education level is positively associated with an organisation's information security practices in Omani organisations

The relationship of the composite variable "OrgISPR" Vs. education, was investigated, through the regression analysis and the result shown in table 4-7 below.

Table 4-7: OrgISPR Vs Education variables

5. OrgISPR Vs Education Variable								
Coefficients[a]								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	1.762	.278		6.337	.000	1.210	2.313
	Education	-.007	.038	-.016	-.184	.854	-.082	.068
a. Dependent Variable: OrgISPR								

Table 4-7 shows that the significance level is > 0.05 for the independent variable education. Therefore, the β, which expresses the relative importance of the education variable is not a significant predictor (i.e. the independent variable education is not significant to predict OrgISPR). This finding demonstrates that there is no relationship

between the socio-cultural factor education and the composite variable denoting information security best practices.

Based on the results of the above regression analysis, the hypothesis H#1.2, related to the effect of "Education" on information security training and awareness, was accepted, whereas the hypotheses: H#1.1, H#1.3, H#1.4 and H#1.5, were rejected.
The results of this analysis are summarised in the table 4-8 below.

Table 4-8: Hypotheses Result of " Education" effect on Information Security

IS Dependent Variables	Result
Organization's Information Security Policy	Rejected
Information Security Training & Awareness	Accepted
Managers Support to Information Security	Rejected
Employees commitment to Information Security disciplines	Rejected
Organization's Information Security practices	Rejected

The low impact of the education factor on many aspects of information security occurred because most of the respondents were highly educated, (83% had a B.Sc. or above), as shown in the following table.

Table 4-9: Survey respondent's Education level

Education Level of Respondents	Percentage
High School	6%
Two-year Diploma	11%
Higher Diploma	6%
B.Sc.	47%
M.Sc.	26%
PhD	4%

4.9. The Relationship Between Critical Organisational Factors and Information Security Performance and the Development, and Maintenance of an Information Security Culture.

The way that an organisation handles information security issues is governed by its organisational culture. Some characteristics of organisational security culture directly reflect the wider culture of the organisation as a whole. The researcher constructed a new dimension to represent this organisational culture in order to examine its impact on other information security aspects. The characteristics of organisational culture were themselves abstracted from the aspects of information security described above:

1. A strong and enforced information security policy.
2. Adequate awareness and training programs on information security for all employees before they receive a network account and regularly thereafter.
3. Regular refresher security programs and awareness activities to raise the security awareness levels among employees at all levels of an organisation.
4. An annual budget for the development of information security in an organisation.
5. Information security policies and procedures applied to all of an organisation's members including managers at different levels.
6. Motivation for employees to notify superiors in the event of an information security violation.
7. Managerial concern for information security at all times, not only when there is a security breach in the organisation.
8. Good information security as part of the shared beliefs of an organisation's members.

The independent variable OrgISC is a composite variable which reflects the above characteristics of organisational security culture. The dependent variables include the following composite information security aspects:

- Management Support of Information Security. OrgISMS
- Information Security Training and Awareness. OrgIST
- An Organisation's Information Security Policy. OrgISP

To test the relationship between critical organisational factors and information security culture, the following hypotheses were formulated:

H#2: Lack of management support and involvement negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#3: Lack of information security awareness and training negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#4: Lack of information security policy negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

The statistical method applied

The researcher applied the correlation statistical method through SPSS software analysis, to determine whether a linear relationship between critical organisational factors and information security culture exists. The researcher wished to examine the effect of each of the three critical organisational factors mentioned above on the development of an organisation's information security culture; and whether information security performance was influenced by these three factors. She also wished to determine, for each critical organisational factor, whether the effect is positive or negative.

The findings from this method could help managers in Omani organisations to understand better the critical areas that they can most readily influence, in order to protect organisational information assets more effectively.

Results

The Pearson correlation analysis in SPSS, as set out in table 4-10 below, depicts the correlation between the composite aspect denoting organisational information security culture, OrgISCF, and the above mentioned information security composite aspects in Omani organisations. The significance level is < 0.01 for all variables. The Pearson correlation factor (r) has the following respective values: 0.550, 0.636, and 0.672.

Table4-10: Correlation between Organisation Critical Factors and Information Security in Omani organisations

Information Security Critical Success Factors (OrgCSF)		
OrgISP	Pearson Correlation	.550**
	Sig. (2-tailed)	.000
	N	129
OrgISTA	Pearson Correlation	.636**
	Sig. (2-tailed)	.000
	N	116
OrgISMS	Pearson Correlation	.672**
	Sig. (2-tailed)	.000
	N	113

There is a strong relationship between an organisation's information security culture, which is represented by the composite variables of OrgISCF and the three information security aspects of the composite variables OrgISP, OrgISTA, and OrgISMS, which represent an organisation's information security policy; information security training and awareness; and management support for information security, respectively. Consequently, hypotheses H#2, H#3 and H#4, have been accepted based on the correlation analysis as summarised in in table 4: 11 in the next page.:

Table 4-11: Hypotheses test results between Orga
ISCF Vs Organisational ISC in Omani organisations

IS Dependent Variables	Result
Organization's Information Security Policy	Accepted
Information Security Training & Awareness	Accepted
Managers Support to Information Security	Accepted

4.10. The Relationship Between the development and maintenance of an information security culture, and information security disciplines and practices in Omani organisations.

The following hypotheses were tested to examine the relationship between information security disciplines and practices, and information security culture in Omani organisations.

H#5: There is a positive correlation between the information security culture and employee commitment to information security disciplines in Omani organisations.

H#6: There is a positive correlation between the information security culture and information security practices in Omani organisations.

The Statistical Method Applied

The correlation statistical method in SPSS was applied to determine if a linear relationship between information security disciplines and practices, and information security culture exists in Omani organisations. The researcher was interested in the potential to improve the employee attitudes towards information security, and so provide better protection for information assets. In addition, it is important to know if a change in the level of commitment to information security best practice will result in a real change in information security performance.

Results

The Pearson's correlation analysis in SPSS, set out in table 4-12 depicts the correlation between the composite aspect denoting organisational information security culture, OrgISCF, and the information security composite variables denoting employee commitment to information security disciplines OrgEISC, and information security practices OrgISPR, in Omani organisations:

Table 4-12: Correlation between Information Security Culture and Information Security Disciplines and Practices

OrgEISC	Pearson Correlation	.160
	Sig. (2-tailed)	.094
	N	110
OrgISPR	Pearson Correlation	.477**
	Sig. (2-tailed)	.000
	N	103

Table 4-12, shows that the significance level is > 0.05 for the composite variable OrgEISC, and that the coefficient of correlation is not significant, and it cannot be interpreted regardless of its value. This finding indicates that there is no relationship between an organisation's information security culture, which is represented by the composite variable OrgISC, and employee commitment to information security disciplines that is represented by the composite variable OrgEISC.

However, the correlation table 4-12 also shows that the significance level is < 0.01 for the variable OrgISPR, and the Pearson correlation factor (r), for this variable, has a value of 0.477. Therefore, there is a strong correlation between an organisation's information security culture, which is represented by the composite variable OrgISC, and information security practice which is represented by the composite variable OrgISPR.

Accordingly, hypothesis H#4 has been rejected and hypothesis H#5 has been accepted as summarised in as shown in table 4-13 below.

Table 4-13: Hypotheses Results between OrgaISC and Information Security disciplines and practices in Omani Organisations

IS Dependent Variables	Result
Employees commitment to Information Security disciplines	Rejected
Organization's Information Security practices	Accepted

4.11. Survey Data Analysis Conclusion

4.11.1. Information Security Best Practices in Omani Organisations

Information security in Oman was examined from the perspective of the following six dimensions:

1. Organisation Information Security Policy.
2. Information Security Training and Awareness.
3. Managerial Support and Information Security.

4. Employee Commitment to Information Security Disciplines.
5. Organisation Information Security Procedures.
6. National Information Security Bodies Input.

The above analysis shows that:

1. Most Omani organisations have an information security policy that is implemented and monitored. Nevertheless, the level of Omani organisations' compliance with information-security-policy-related best practices is below average (40%).
2. Most Omani organisations are keen to assign responsible personnel to oversee and implement their information security training and awareness arrangements. However, the overall compliance with the best practices in this regard is slightly below average (47%).
3. There is a considerable lack of managerial support for information security in Omani organisations. This analysis demonstrates that managerial support is well below average (34%).
4. The level of Omani employee perceptions of positive information security culture attributes is average (49%).
5. The level of compliance of Omani organisations with the central best practices of information security procedures is average (48%).
6. The efficiency of national information security bodies with regard to performing their duties is slightly below average (46%).

The following chart depicts the status of the six dimensions of information security aspects in Oman, as concluded from the previous analysis:

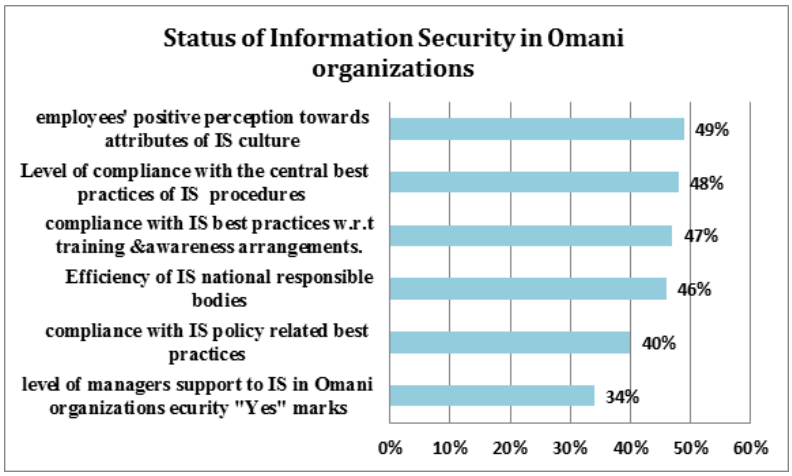

Chart 4-26 The status of Information Security in Omani organisations

Generally, all information security aspects in Omani organisations are below the average. ***The global level of compliance with information security best practices in Omani organisations is 45%.***

The results above were obtained by dividing the total number of 'yes' responses to all items in the five dimensions (1-5) by the total number of responses to all questions for these five dimensions. Dimension six was excluded because it is related to the efficiency of the national supporting bodies, rather than the compliance of Omani organisations with information security aspects.

4.11.2. Differences Between Public and Private Organisations in Oman Regarding Compliance with Information Security Best Practices

The above analysis shows significant differences in compliance best practice between public and private sectors across all aspects of information security aspects.

1. Omani private sector Compliance with information security policy best practice is almost twice as high in the Omani private sector than in the public sector. (31% in the public sector and 60% in the private sector).
2. The development of information security training and awareness in the Omani private sector is above average (65%), and it is much better than in the public-sector (39%).
3. Information security lacks adequate managerial support in both sectors. Nevertheless, the private sector receives twice as much support as the public sector (26% in public sector and 52% in the private sector).
4. There is a lack of concern about information security among public sector employees compared to private sector employees. The percentage of positive perceptions of information security culture attributes in the private sector is approximately two times higher than in the public sector (31% in the public sector and 60% in the private sector).
5. The private sector and public sector are similar regarding compliance with information security best practices, with the private sector slightly better. (45% in the public sector and 56% in the private sector).
6. The national information security bodies give more attention to public sector organisations than to private sector organisations (50% for the public sector and 37% for the private sector).

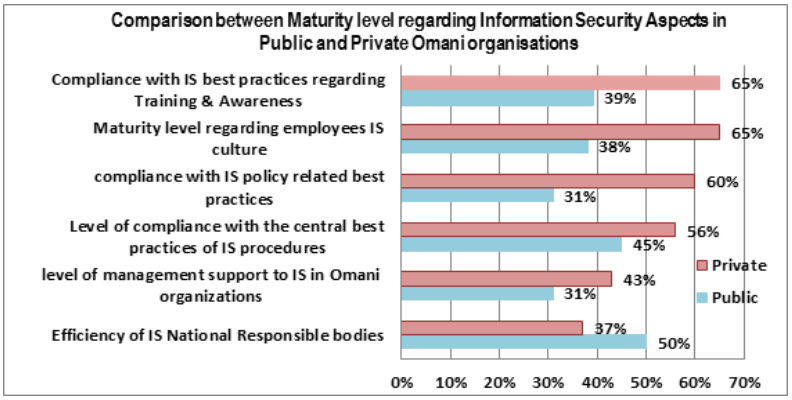

Chart **4-27**: Public Vs Private Organizations according to Information Security Current Status in Oman organisation

Chart 4-27 above, depicts the status of the six dimensions of information security in public and private sectors in Oman, as concluded from the foregoing analysis. Despite the stronger support from the national information security bodies for Omani public organisations compared to private organisations, the following conclusion was reached:

> *The global level of compliance with information security best practices in Omani organisations is 59% in the private sector and 38% in the public- sector.*

The global level of compliance with information security best practices was calculated for both sectors by dividing the total number of 'yes' responses to all items in dimensions one to five by the total number of responses to all questions in these five dimensions. Dimension six was excluded because it is it is related to the efficiency of the national supporting bodies rather than the compliance of Omani organisations.

The average statistical significance between public and private groups was $(|\ t\ |) = 2.067937$. Since the absolute value of the test statistic is greater than 1.96, it means the average difference between public organisations and private ones, in Oman, regarding the level of compliance with information security best practices, is significant. (i.e. private organisations are more likely to have better compliance with information security best practices than public organisations.

4.11.3. The Impact of "Education" on Information Security in Omani Organisations

The following conclusion was drawn from the above analysis:

> *There is no relationship between education and the information security aspects in Oman, except for information security training and awareness aspects.*

Although education usually affects other information security aspects, the analysis did not show this. The reason for the low impact of education on information security is that most of the survey questionnaire respondents were already highly educated (83% had a B.Sc. or higher). For this reason, it is assumed that the actual impact of education impact could not be measured in this study.

4.11.4. The Relationship Between Critical Organisational Factors and Information Security performance and Information Security culture development in Omani Organisations.

The analysis described previously in section 4.9, concludes that there is a positive correlation between information security culture development and performance, and the three organisational factors, that include information security policy, information security training and awareness, and managerial support and involvement.

4.11.5. The Relationship between Organisational Information Security disciplines and practices, and Information Security culture development in Omani Organisations.

The analysis described in section 4.10 above, leads to the following conclusions:

- There is no correlation between organisational security culture development and employee commitment to information security disciplines in Omani organisation.
- There is a positive correlation between the development of a culture of organisational security and organisational information security practice in Omani organisations.

4.12. Chapter Summary

This chapter presents the analysis and results of the quantitative stage of this study. The analysis used SPSS software version 22. The results reveal some social and organisational factors that affect the adoption of a culture of information security in Omani organisation, and that tend to enhance information security performance.

The effect of these factors was examined by analysing answers to the following research sub-questions:

> **RS-Question#1:** *What is the current level of compliance with information security best practices in Omani organisations? What is the difference between public and private sector organisations in this regard?*

The results show that the status of information security in Omani organisations needs to be enhanced. This could be achieved by improving those elements of information

security practice that received less than 50% of 'yes' answers from the survey respondents.

Additionally, research sub question 3 was resolved by answers to hypothesis (H#1),

RS-Question#3: *How does the social factor "education" affect information security performance in Omani organisations?*

Hypothesis (H#1): *Education level positively affects information security performance in Omani organisations. was tested to* confirm if there is an effect of the social factor "education" on information security performance and information security culture development. However, based on the conducted regression analysis carried out, the sub-hypotheses related to hypothesis (H#1) above, were rejected except for the one that was used to test the effect of education on training and awareness, which was accepted.

Although education usually affects other aspects of information security, the analysis did not show this. The reason for the low impact of education on information security is that most of the survey respondents were highly educated (83% had a B.Sc. or higher). Besides that, respondents' answers related to dependent variables were binary coded scale yes/no rather than being scaled on Likert's scale. Which, indicate that, regression analysis was not the appropriate statistical test tool to be use in this case. Therefore, it is assumed that the actual impact of educational levels may not be measured accurately in this study.

The relationship between critical organisational factors and information security performance and the development and maintenance of an information security culture, was explored by research sub-question four:

RS-Question#4: *What is the relationship between critical organisational factors and information security performance; and the development, and maintenance of an information security culture in Omani organisations?*

The response was based upon testing several hypotheses that were accepted:

H#2: *Lack of management support and involvement negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

H#3: *Lack of information security awareness and training negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

H#4: *Lack of information security policy negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

The above hypotheses test shows a positive correlation between information security performance, and the three critical organisational factors, which are: managerial support and involvement, information security training and awareness and information security policy.

In addition, the fifth research sub-question: (RS-Question#5. What is the relationship between the development and maintenance of an information security culture, and information security disciplines and practices in Omani organisations?), has been answered, by testing the following hypotheses:

H#5: *There is a positive correlation between organisational information security culture and employee commitment to information security disciplines in Omani organisations.*

H#6: *There is a positive correlation between organisational information security culture and an organisation's information security practices in Omani organisations*.

The results confirm the two hypotheses above and confirm that employee good information security best practice and commitment affects the development of a culture of information security, which in turn enhances information security performance in Omani organisations.

All of the issues found in the analysis of the survey results could have a huge effect on the information security culture in Omani organisations. The survey findings were verified by a series of interviews. Chapter 5 describes the interview findings in detail.

Chapter 5. Findings – Interview Analysis

"The explorer who will not come back or send back his ships to tell his tale is not an explorer, only an adventurer; and his sons are born in exile."
- (Ursula K. Le Guin, The Dispossessed, 1974, p.127)

5.1. Introduction

Stemming from an interest in understanding human behaviour, social scientists tend to use qualitative research to accumulate a detailed account of human behaviour and beliefs within the contexts in which they occur (Rubin & Rubin, 2005). According to Kvale (1996, p.174), an interview is "a conversation, whose purpose is to gather descriptions of the [life-world] of the interviewee with respect to interpreting the meanings of the described phenomena". Likewise, Schostak (2006) states that an interview is an extendable conversation between partners that aims to obtain in-depth information about a topic or subject, through which a phenomenon can be interpreted in terms of the meanings that interviewees bring to it. Researchers can accumulate meanings in several ways, including one-on-one interviews, which are the most common. In addition to one-on-one interviews, focus-group interviewing is also popular (Marshall & Rossman, 2006).

To obtain a richer understanding of the effect of culture on information security, this chapter presents the analysis of the data that was collected through semi-structured, open-ended, face-to-face interviews with fifteen experienced managers from Omani public and private organisations, who had worked regularly with information security and information technology (IT) for 6 to 18 years. The interviewees differed in age and work specialism as either IT or information security managers and experts. Since they were all deeply involved with IT and information security aspects, it was easy for them to reflect on the information-security-related issues in their organisations.
Nine of the fifteen interviewees were from the public sector and the remaining six were from private sector organisations. Four of the six private sector interviewees were information security managers and two were IT managers. Among the nine public sector interviewees, two were IT managers and seven were information security managers. The interviews lasted between 90 and 120 minutes and were audio-recorded. The general purpose was to determine the status of information security in Omani organisations from different perspectives. Semi-Structured interviews were used to understand the world from the interviewees' point of view. The interviews were to

complement the results of the quantitative analysis conducted earlier and described in chapter four of this thesis.

During the interviews, each interviewee was presented with an identical set of questions in the same format and sequence. However, a number of additional questions were asked based on the different participants' responses. The research topics guided the interviews and are used later in this chapter as sub-headings, although the topics often overlap. In addition, semi-structured interviews provided the ability to compare individual responses with different perspectives on the same topic and to conduct analysis in a textual format. All interviews were recorded, and then written out in full. The names of individuals were replaced with codes for transcript and data analysis purposes, to ensure participant anonymity. The assignment of numbers to names was kept in a separate document so that participants could be identified and contacted by the researcher at a later date, if more clarification were needed, and also for transcript review. Individuals were then referred to with pseudo names in the final report.

The interviewees were questioned about the basis of information security best practices in their organisations, by reference to particular elements of information security. Their answers were then analysed to determine the extent to which information security best practices were implemented. Interviewee perceptions of key elements of information security as elicited from their answers formed the basis of the comparison between public and private sectors.
This chapter includes the results of all the interviews, presented by reference to eleven themes covering the different aspects of the research study. The themes are:

1. The main drivers of information security.
2. The current state of information security in Omani organisations.
3. Organisational culture and information security.
4. Information security management support and commitment.
5. Information security policy.
6. Information security education, training, and awareness.
7. Information security rewards and punishment.
8. Information security and power distance.
9. Information security and uncertainty avoidance.
10. Information security and collectivism
11. Information security and trust

Interviewee statements were grouped by reference to the appropriate theme, along with sub-themes or categories, as identified in the interview guide. A theme example is

shown in table 5-1. Some textual data, recording verbatim examples from the interview, are included to highlight and clarify the key common responses and concepts.

Table 5-1: Example of interview data analysis themes process

Main theme	Sub- Theme/ Category	Participants' Responses
The current state of Information Security	1. Current status of IS incidents 2. The biggest threat to IS 3. Top barriers to improve IS 4. The biggest challenge to IS 5. Foundation of a disaster recovery plan 6. Management convincement 7. A qualified IS department 8. Implementation of a network security measures, such as firewalls, ids/ips, etc 9. Monitor log files	"It is a mandate from the minister's cabinet that all ministries should have a security unit, but I think in most, if not all organizations, there is no proper information security team available in these units"GINT9. "recently we established a unit for information security and added to the main organization structure, and we are in the process of formalizing its roles and responsibilities and developing the skills of the security team. Unfortunately, earlier, we used to have a small section under the computer department, which sorry to say wasn't functioning as it should be"GINT5. "I can say the information security in our organization is very new and still needs a lot of consideration at the national level. Also, the organization security culture needs a lot of improvement, because until now, employees didn't realize the differences between normal information and classified information. Sometimes they share critical information without recognizing that this shared information could be a guide or a step to hack the organization systems. Also, because of the lack of information security culture, most of the employees are easy targets for social engineering"GINT1. " there is no proper information security team available"GINT6. " I will say it is at a very low level because of the different employees' culture and their low security knowledge and awareness, which make them very easy target for social engineers" GINT4. lack of experience; we don't have skilled and trained security staff who are able to monitor those security systems, and our total dependence on the support of the suppliers of these services. Additionally, nobody ever asks for regular reports regarding the security situation"GINT6. "The current information in the organization I can say is not high and not low but in the middle level. We have some security policies in place, such as a policy to prevent data leakage. Nevertheless, these policies are not enough especially when dealing with insiders. PINT11. "because of the nature of the organization's business, I can say we are in a good position regarding information security"PIN14 . "Without management support it is very difficult to improve the business security"PIN12.

The data analysis themes enabled inferences to be drawn about the status of information security in Omani organisations and the impact of critical socio-cultural and organisational factors on the development of the information security culture.

5.2. Interview Findings and Themes

5.2.1. The Main Drivers of Information Security in Omani Organisations

All interviewees from both sectors understood that information security is a continuous process where the speed of progress is limited by many issues. Thus, organisations must always be up to date with relevant best practice and technological solutions. The interviewees were asked to identify some of the drivers of information security implementation in their organisations. Although there is not a full consensus on the appropriate drivers of information security, many interviewees from both sectors stated

that management support, information security training and awareness, and effective information security policy, would continue to form the foundation of information security. Most of them believe that management is less supportive of information security, and that controls tend to be insufficiently observed or adhered to.

Public Sector

The interviewees cited many different drivers behind information security. From their perspectives, these drivers were anything that could affect the business, including all information security issues and matters (e.g. a lack of management commitment, the bad behaviour of users, a lack of information security policies, a lack of information security training and awareness, organisational visions and strategies, business needs, organisational culture, and limiting social engineering vulnerabilities). For example, one interviewee commented on management support and commitment, saying:

> ***GINT9***: *"it is a lack of management commitment because they have the visions and decisions for all directions in the organisation and not only security".*

Another interviewee considered business sensitivity as an important driver for implementing information security. He stated that:

> ***GINT6****: "information security is essential for the organisations because its save business data and document leaks, and by implementation information security will contribute to limiting this problem".*

Other drivers of information security included managing Business risk, Preserving business continuity, and business strategic alignment.

> ***GINT3****: "information security is essential for the organisation's strategy and will contribute to better risk management".*

Many private sector interviewees highlighted issues of security awareness programs, management involvement in information security, as well as understanding the benefits of compliance with information security disciplines to the organisation's business.

Private Sector

interviewees focused on issues such as information security policies, management support and business needs, business opportunities, compliance with standards and laws, and the protection of an organisation's reputation and customer information. Management commitment to direction and governance of security policy was seen as an important and necessary driver.

> ***PINT15**: "Well, the power who is pushing the information security is the management, who I consider to be the most important part in security, and they can improve it in many ways. Nevertheless, the other driver of security for our organisation is the business protection from security breaches and also the protection of our customers' data from any leakage".*

Another interviewee expressed awareness of the significance of information security policy as follows:

> ***PINT11:** "The information security policies are very important, and it should be enforced and followed by the top management ".*

Another driver for the implementation of information security is business strategy:

> ***PINT14:** "Information security is important for the need to protect information to support business and strategy ".*

Many of interviewees' answers indicate that they consider information security fundamentally indispensable for business continuity.

5.2.2. The Current State of Information Security in Omani Organisations

According to the interviewees, a commitment from senior management is necessary to define roles and responsibilities related to information security matters and to assign the required resources. Many medium and small enterprises (MSE) have few information security specialists solely responsible for this issue. Senior management is also responsible for staff awareness and competence, in addition to reviewing the effectiveness and efficiency of implemented policies and procedures. Interviewees from both sectors directly or indirectly highlighted the need for organisations to invest in security teams. Technology itself is limited by the capabilities of the people who use it, and they usually do not take advantage of more than 50% of its functionality.

Interviewees from both sectors cited concerns about the current state of particular aspects of information security:

- Information security incidents.
- The greatest threat to information security.
- The top barriers to improving information security.
- The greatest challenge to information security.
- The foundation of a disaster recovery plan.
- The foundation of a qualified information security department.
- The implementation of network security measures such as firewalls.

- The monitoring of log files.
- The absence of roles and responsibilities.

Public Sector

Their answers demonstrate that, although there are security units and security teams in all of the interviewees' organisations, the status of information security is inadequate. Organisations need to enhance their information security. One interviewee made the following comment regarding the availability of the information security units in the Omani organisations:

> ***GINT9:*** *"It is a mandate from the minister's cabinet that all ministries should have a security unit, but I think in most, if not all organisations, there is no proper information security team available in these units".*

While another interviewee commented on information security unit performance:

> ***GINT5****: "yes, recently we established a unit for information security and added to the main organisation structure, and we are in the process of formalising its roles and responsibilities and developing the skills of the security team. Unfortunately, earlier, we used to have a small section under the computer department, which sorry to say wasn't functioning as it should be".*

The interviewees believed that the main reason for this was lack of managerial awareness and support. They believed the human factor plays a significant role. Six out of nine interviewees consider insider behaviour the greatest threat to information security.

The interviewees defined and prioritized the greatest information security challenges to their organisations as follows:

- Educating management about security.
- Defining a vision and objectives.
- Creating policies, and.
- Educating employees.

The top barriers to improving information security included:

- Lack of management support.
- Absence of an information security policy.
- Inadequate information security budget.
- Lack of awareness and training.
- Unclear responsibilities and duties.

- Lack of an information security culture.
- Lack of information security skills.
- Lack of a national security strategy.
- Lack of a regulatory body.

For example, one of the interviewees described the state of information security where he worked:

> ***GINT1****: "I can say the information security in our organisation is very new and still needs a lot of consideration at the national level. Also, the organisation security culture needs a lot of improvement, because until now, employees didn't realise the differences between normal information and classified information. Sometimes they share critical information without recognizing that this shared information could be a guide or a step to hack the organisation systems. Also, because of the lack of information security culture, most of the employees are easy targets for social engineering".*

Some other issues were identified as indicators of suboptimal information security. Six out of nine interviewees stated that there is no physical separation between the organisation's network and the Internet network. In addition, seven interviewees stated that they do not have a disaster recovery plan in their organisations. For instance, one comment on disaster management was:

> ***GINT2***: *"unfortunately we don't have a location for disaster recovery, and even there isn't a plan to follow in case of a disaster. Nevertheless, if our data and systems get hacked or damaged, we act at that moment and try to solve the problem, and that could take us days or weeks".*

Furthermore, six interviewees stated that they do not monitor firewall logs and server logs for security intrusion. For instance, GINT6 stated:

> ***GINT6*****:** *"Yes, there are several active security devices on the organisation's network, but unfortunately the logs are not regularly monitored for intrusion attempts, because of the lack of experience; we don't have skilled and trained security staff who are able to monitor those security systems, and our total dependence on the support of the suppliers of these services. Additionally, nobody ever asks for regular reports regarding the security situation".*

Another interviewee, who was annoyed about the lack of specialised information security personnel commented that:

> ***GINT3:*** *"shortages of information security personnel are a big issue and we as an information security department have to deal with this limitation by rely on outsource from private organisations".*

GINT1 agreed with this comment and added:

> ***GINT1:*** *"shortages of information security personnel will continue to be an issue in public organisations and information security department have to live with this limitation, unless the top management deal seriously with this issue.*

According to many interviewees, because government organisations do not have enough specialised resources to handle information security issues and listen to employee concerns, they address issues only 'as they arise'. They also believe that the overall status of information security in governmental organisations ranges from 'very weak' to 'good'. In this regard, one interviewee stated:

> ***GINT4:*** *"The current state of information security in our organisation: On one hand we have applied many technical devices to protect the organisation's network and users' PCs. On the other hand, if we talk about the insiders and the information security culture, I will say it is at a very low level because of the different employees' culture and their low security knowledge and awareness. This makes them very easy target for social engineers who can easily penetrate the organisation's information, because most of the employees are naive and deal with all people as they are all trusted people. We as a security team do our best to educate them to increase their security culture, but sometimes national culture has a big impact on people and that is difficult to change".*

Private Sector

Compared to the public sector, the state of information security in private sector organisations is better, as most of these organisations have active security departments and adequate security specialist personnel, according to the interviewees. In addition, none of them had suffered from information security incidents in the past two years. For example, one interviewee noted that:

> ***PINT11:*** *"The current information in the organisation I can say is not high and not low but in the middle level. We have some security policies in place, such as a policy to prevent data leakage. Nevertheless, these policies are not enough especially when dealing with insiders. There are some critical issues that organisations follow, which in my opinion could*

harm the business security, such as hosting all business emails and financial reports and applications in the cloud, another critical issue is the use of flash memories and CDs by the organisation' employees".

Although most of interviewees' organisations have a disaster recovery plan, as with public organisations, they suffered from a lack of adequate management support and a lack of adequate employee awareness and training programs. PINT14 referred to the difficulty in obtaining information security training in his organisation.

> ***PINT14:*** *"because of the nature of the organisation's business, I can say we are in a good position regarding information security. This is due to the presence of very clear information security policies and procedures as well as security technology such as firewalls and intrusion prevention systems. However, our challenge is the employees' behaviours and the lack of security training. Even if we try to train them, they are very difficult to control and give us a hard time, especially if they are all from one city and have the same culture".*

Most interviewees in this sector recognised that, a proactive stance must be taken by management for information security to become more involved an organisation's strategies. For example, PIN15 commented on management attitudes with regard to information security as:

> ***PINT15*****:** *"I found that management in the organisation supports the security policies and they work hard to make sure all employees are following it, but not themselves".*

The interviewees cited a number of barriers to improving information security:

- lack of awareness and training.
- Lack of management support.
- Inadequate information security budget.
- Unclear responsibilities and duties.
- Lack of knowledge transfer.
- Lack of an information security policy.
- Lack of an information security culture.
- Lack of a national security strategy.
- Lack of a regulatory body support.

The greatest challenges their organisations faced were outside threats, bad insider behaviour, and the rapid development of technology.

One interviewee said that funding information security is a big issue in his organisation:

> ***PINT11:*** *"It really comes back to priorities and funding. We need to have the time and funding to investigate appropriate security solutions".*

Another interviewee described the lack of management support as a barrier to information security:

> ***PINT12:*** *"Without management support it is very difficult to improve the business security".*

Other issues indicated a positive information security culture. For example, they all stated that they monitor firewall logs and server logs for intrusion attempts, and many of them stated that, they forward monitoring reports to higher levels of their organisations. These are indicators that the information security situation in the private sector is better than that in the public sector organisations. Three of the interviewees mentioned that the greatest threat to organisations is the insider behaviour:

> ***PINT10*****:** *"the organisation's staff, vendors, contractors, and auditors, are all threats to the business security if they don't follow the security policy".*

Four out of six interviewees stated that they have a disaster recovery plan in their organisation that was tested regularly. One of them mentioned the necessity of a disaster recovery plan in an organisation and remarked that:

> ***PINT14***: *"If a disaster happens, the company will lose a lot of money, not to mention the company reputation".*

The interviews indicate that the overall information security status in Omani private sector organisations, ranges from 'moderate' to 'very good'.

5.2.3. Organisational Culture and Information Security

Organisational culture affects information security. In this context, culture is that collection of meanings, actions, beliefs, and behaviours, associated with information security, which defines how employees care for and protect assets that are valuable to them and their organisation. According to Richards et al. (2005), information security is a subset of the overall security in organisations. The development of an internal information security culture depends on organisational culture. Furthermore, Lim et al. (2009) argue that the concepts of information security culture and organisational culture may be interrelated.

All interviewees from both sectors agreed that it is necessary to incorporate information security as a fundamental part of an organisation's strategy. They highlighted the importance of management commitment to promoting a culture of information security within an organisation. They considered this commitment a business driver that maintains continuity of information security. In addition, they all believed that there should be a shared understanding of information security practice. If there is insufficient communication between information security officers and the other members of an organisation, those members will construct their own perceptions of the value of information security, and of possible threats, often based upon inadequate knowledge.

Public Sector

All nine interviewees had the same view that shortcomings in an organisation's culture are a result of inadequate management. They believed that employees lack a shared understanding of information security and its main goals. In this regard, one interviewee commented on the lack of a successful information security culture in the organisation he belongs to, stating that:

> ***GINT9:*** *"security culture doesn't mean only following instructions, but believing and valuing these instructions, and valuing to secure the organisation's business is very important".*

Whereas, GINT2 commented on employee behaviour regarding information security in his organisation as:

> ***GINT2*****:** *"They see that performance is more important than security".* He continued, *"Security is not part of the organisation's strategy and there is no written or thought security instructions to be followed from any level in the organisation, so how can we create a security culture in this situation".*

Regarding the effect of organisational culture on information security, five interviewees responded positively, two said that it depends on employees, and three stated that there is no effect. For example, one interviewee stated that:

> ***GINT6:*** *"Unfortunately, organisational culture is not helping at all in creating an information security culture. There is a very small percentage of the employees who appreciate the importance of information security, and they are trying to spread this culture through the organisation. But for how long they can stand against this if the organisation' management themselves are not familiar with the importance and the culture of information security".*

Further, five interviewees admitted that their organisations have no successful information security culture; others stated that information security culture could be valid, but mainly at a personal level. In this regards GINT4 stated that:

> ***GINT4:*** mentioned the foundation of the information security culture in organisations*: "Individually I can say that some organisations' members have a very good and successful information security culture, but in total, the organisation requires quite some time to have a successful information security culture".*

On the other hand, many of the interviewees thought that most employees do not recognise the value of information security. Moreover, employees who do recognise the value of information security, still do not practice optimal information security discipline as part of the shared organisational beliefs. For instance, one interviewee, asked to discuss the lack of a shared understanding of information security noted:

> ***GINT8****: "Information security will never succeed in the organisation, unless employees at all levels understand and believe in the importance of the information security and embrace its shared values".*

Private Sector

Regarding information security in private sector organisations, five out of six interviewees stated that their organisation's culture originated from both management and employees. PINT10 stated that:

> **PINT10:** *"If one of them is weak, the whole organisation culture will be weak".*

All of interviewees perceived their organisations as having successful information security cultures and practice. For instance, one of them commented that:

> **PINT14:** *" when employees have good information security culture it helps to implement information security successfully in the organisation"*

Most interviewees recognised the value and importance of information security. For example, one commented on the extent to which members of his organisation recognise the value and importance of information security, and stated that:

> ***PINT13*****:** *"they value information security and accept its importance, which makes it easy for the security team to implement the security policy".*

Regarding the effects of an organisation's culture on information security, all interviewees responded positively with statements including 'positive effect' and 'big effect'. For example, one stated that:

> ***PINT11:*** *"The nature of the work forces new employees, when they join the organisation, to change their culture and respect the importance of maintaining information security".*

5.2.4. Management Support and Commitment

Information security should be addressed strategically; it is no longer only 'bits' and 'bytes'. Establishing an information security strategy is important because it clearly defines the direction and objectives of information security activities, and aligns them with the business objectives. The chief executive officer (CEO) or general manager (GM) must dictate the strategic direction of information security in the organisation.

From the interviewees' perspectives, the level of management involvement in, and support of, information security tends to be low. Managers are not adequately involved in the implementation of information security policies and procedures. All interviewees considered continuous managerial commitment as paramount for successful ongoing information security programs. Likewise, a key management responsibility is the provision of specialised resources as a fundamental requirement for any successful information security initiative. It will be difficult to implement an information security program and to conduct activities associated with its maintenance and improvement without the necessary dedicated resources.

Many interviewees from both sectors are concerned whether managers have the necessary knowledge and tools to manage and resolve the various complex types of information security risks that can occur. Furthermore, they believe that the adequate involvement of management in information security will set the 'tone at the top' by reinforcing effective policy and enhancing behavioural change. Several interviewees in both sectors thought that the level of funding for information security, either for human resources or for training and equipment expenditure, was a direct measure of management support. Managerial financial support for ongoing recurrent funding for maintenance and enhancement is a practical reflection of management attitudes to information security.

The answers of many interviewees indicate that individuals within an organisation need to be clear about what they should do to help deliver the objectives of information security policy. Many employees working in information security are not clear as to

what they should do to help achieve the goals of the organisation. Management is responsible for preventing this situation. Each organisation should have a document that defines information security responsibilities throughout the organisation. However, there is usually no such document in governmental organisations. According to interviewees, many employees believe that information security is a specific area that has its own officials, and they do not understand that information security is the responsibility of everyone in the organisation. Management is also responsible for spreading a wider understanding of everyone's role.

Public Sector

Several aspects were cited as measures of management support for information security, such as showing interest in any reported security-related issues, supporting information security polices, and quickly reviewing progress reports on policy implementation.

Managers are occasionally inundated with various reports on information security, which include a large amount of data that is difficult to analyse. There are indications that they do not always know how to respond. For instance, GINT1 stated that:

> ***GINT1:*** *"Management are not aware about the information security and they are not educated enough in this regard".* He continued, *"Information security is not a priority to them".*

As such, managers do not pay attention to progress reports or feedback on the implementation of information security policies and procedures, and they do not care about issues that arise from these reports. In this regard, one interviewee mentioned that:

> ***GINT8:*** *"Management on all levels in the organisation doesn't pay much attention to information security, and the most important thing for them is to finish the work fast no matter if it is secured or not".*
>
> ***GINT2:*** added *"Management sees it as a pain that gets in the way of doing the job. There is a perceived tension between being secure and meeting mission objectives".*

On the other hand, information security officers feel pressure to issue monthly information security reports and complete data sheets, and they wonder if anyone in the organisation (especially managers) will read them. Therefore, it is imperative to establish a proactive management approach to information security to avoid generating a negative cycle. Regarding their support of information security polices, many

interviewees commented that they do not have such policies. In this regard, one interviewee commented that:

> ***GINT4:*** *"In our organisation, it is very rare to notice management's involvement in or support of information security culture, and they've never asked if an information security policy exists and is implemented or not".*

Most of the managers in the interviewees' organisations do not support information security adequately. One interviewee noted that:

> ***GINT5:*** *"It is not enough at all and we need more support and involvement from the organisation's managers… They never asked about security reports, which is why we don't send them any reports".*

Further, some of the interviewees mentioned that, managers only address information security when serious security threats that might affect the business occur. Many of them, according to several interviewees, are not even aware that information security threats exist. Those who are aware, operate under the notion that all information security threats will be addressed by installing anti-virus software. Many interviewees thought that governmental managers do not know how to implement information security measures properly, or how to help reduce information security risks in their work. For example,

> ***GINT1: "****It is interesting; managers are only aware of security when there is a security breach".*

As an exception, one of the nine interviewees disagreed with the others and stated:

> ***GINT7:*** *"Yes, in our organisation, management are part of the information security improvement in the organisation, and they are involved in organisation security's vision improvement. Furthermore, their involvement increases if any information security incident occurs and then they will be part of finding the solution for that incident".*

Private Sector

All interviewees perceived managers as supportive of information security policies, because of their high awareness about information security. For example, PINT15, commented that:

> ***PINT15:*** *"our centralized management cares a lot about information security due to their high information security awareness".*

Furthermore, there is evidence that links exist between consistent reporting to management and their support of information security functions. In this regard, one interviewee commented on managers' interest in reviewing information security progress reports and said:

> ***PINT12***: *"They do so with the help of the security team who sends the report and keeps following it up to make sure the management takes action."*

Most interviewees see that, management is adequately involved in the implementation of information security policies and procedures in the organisations to which they belong. For instance, PINT10 noted that there were:

> ***PINT10*****:** *"Few who do not realise the importance of the security".*

Another interviewee commented on managerial support:

> ***PINT13:*** *"Their support is increased if any security breach occurs".*

According to several private organisation interviewees, most managers perform quick reviews of issues arising from information security progress reports. In this regard, PINT14 stated that:

> ***PINT14:*** *"most of them do it and that is due to the good security culture they have and their awareness of different types of risks".*

5.2.5. Information Security Policy

Information security is one of the greatest challenges facing organisations. Many organisations have information security policies and plans documented on hundreds of pages, but they forget the most important component, which is keeping their critical assets secure. Several interviewees from both sectors expressed the view that setting up information security policies was different from implementing those rules, controls, and procedures. Without management sponsorship and support, any information security policy will fail. All interviewees directly or indirectly stressed the importance of the enforcement of information security policies. Some highlighted its importance for creating an information security culture, while others considered policies and procedures the drivers of awareness, education, and training programs in their organisations.

Interviewees from both sectors expressed concerns about optimising communication, which they believe makes the staff active participants rather than passive observers of

information security activities. Regular communication among all members of the organisation ensures a comprehensive understanding of all information security issues.

All interviewees identified in different ways the following common concerns:

- The information security policy should be firmly established in an organisation.
- All employees should know and understand the policy.
- All employees should sign the information security policy.
- Information security roles should be clearly defined and communicated.
- Information security incidents should be handled effectively.
- Information security policy should have a regular review and update process.

Public Sector

The status of information security policies vary considerably between organisations. Most interviewees spoke negatively in setting out the above concerns. Interviewees thought that information security policies had no real effect because of the lack of a standard policy document, the lack of resources, and a delay in approving information security policy. GINT9 explained the situation of information security policy in his organisation, and stated that:

> ***GINT9*****:** *"No, there isn't any written security policy, but there are some rules and general procedures and instructions, and they are not known by all employees because of the lack of awareness programs. There is nothing".*

Similarly, GINT6 noted that:

> ***GINT6: "****We don't have any policy; we follow some organisational procedures and our superiors' instructions or command. So it is up to the person who gave us the direction, it may also change".*

Many interviewees explained that their organisations either have no information security policy, or have a minimal or outdated information security policy. For example, GINT8 made the following pessimistic statement:

> ***GINT8*****:** *"If we assume it exists, it will be then on the shelf and not implemented or shared with employees ".*

Other interviewees such as GINT3 pointed out that even where there are procedures in the organisation, these need to be updated and employees kept aware of the changes through e-mail.

> ***GINT3*****:** "*Update, and make sure all members of the organisation should adhere to the procedures regardless of job and not only the end users"*.

Some described the existing information security policies as adequate but described a lack of policy enforcement across their organisations. For example, GINT1 stated:

> ***GINT1:*** *"One thing that we need to be clear about is enforcing the policies, it is all very well to have policies but if they are not prepared to enforce them when necessary, the whole process is pointless really"*.

Generally, from this set of interviews, the researcher found that, most public organisations do not educate employees about new and updated security measures because there is no information security policy to build on. However, a lack of policy does not prevent some organisations from keeping employees aware of procedural changes through e-mail.

Private Sector

There are information security policies in all of the interviewees' organisations. One interviewee commented on maintaining a regular review process to consider new changes to the information security policy and said:

> ***PINT15*****:** *"We have to have best practices on information security"*.

Further, all interviewees except PINT10, expressed positive views of the information security concerns mentioned previously. His view was:

> ***PINT10:*** *"policy is very complicated and has very deep details which could not apply to all members"*.

However, many interviewees described policies without enforcement and lack of compliance with policies due to the lack of an information security culture. Several interviewees also referred to the need for communication to promote awareness of information security policies, and to ensure monitoring and compliance with those policies. One interviewee commented on the necessity of clear definitions of, and communication about information security:

> ***PINT13*****:** *"It is one of the security policy's main points that, it should be identified and communicated with the organisation's employees, but in this organisation the people that are found information security they ignore it. He added "Also enforcing information security policy is critical, otherwise employees won't refer to it"*.

5.2.6. Awareness, Training and Education Programs

Raising awareness ensures that employees in an organisation will become aware of the risks and threats facing the protection of information and understand the impacts and benefits of their role in this regard. In addition, many interviewees consider education, training, and awareness key elements of information security culture. Incident occurrence was cited by many of them as a vehicle for raising awareness rather than formal training sessions.

The following concerns are indicative of the importance placed on these three elements by all interviewees:

- Conducting training programs on information security for new employees
- Conducting refresher awareness programs on information security
- Management obligating employees to attend regular training programs
- Designing training programs for all employees, and not only for selected categories of staff.
- Educating employees about new and updated security policies.
- Conducting regular checks to ensure that employees are not breaching information security policy.

The lack of training in information security management contributes to information security problems in both sectors.

Public Sector

The absence of information security education, training, and awareness was repeated many times during the interviews. According to interviewees, most organisations do not consider raising awareness about information security as part of the organisations' training functions. In this regard, GINT6 said:

> ***GINT6:*** *"I am afraid no awareness program is available in the organisation. Having said that, there is only one time, they set up a workshop for one day for all employees in different organisation levels including new and old employees, which I don't think it's enough. Also, in my opinion, it would be better if the new employees were subjected to an awareness and training program before being granted permission to use the organisation's systems".*

However, ad-hoc training sessions are held occasionally to address issues or incidents, and they vary from one organisation to another according to management attitudes. One interviewee highlighted these informal practices for new employees and commented:

> ***GINT4:*** *"There are some optional security awareness sessions such as talking to the employee face to face in case of problems.* This interviewee thought that the reason for not conducting training programs was that *"managers don't value the importance of information security due to their low information security culture".*

The most common type of awareness activity is e-mail communication, particularly in relation to virus activity. In this regard, one interviewee noted that:

> ***GINT1:*** *"The organisation doesn't have a clear information security policy".* He also discussed making employees aware of information security issues, stating, *"Sometimes we send them an email about any new adjustment done to the security procedures we apply".*

Despite their opinions that information security training and awareness is an important priority, seven out of nine interviewees stated that their organisations do not conduct awareness and training programs on information security for new employees. Their organisations recognise its importance but are not sufficiently interested.
However, GINT8 believed that there are mixed motives around management interest in conducting training sessions:

> ***GINT8:*** *"It depends on who is conducting this training. If it is the IT authority, then the management will push their employees to attend these programs, so that they can improve their images, but if these programs are conducted by non-governmental organisations, they are ignored ".*

Most interviewees said there are no obligatory training or awareness programs in their organisations. For instance, GINT9 stated that:

> ***GINT9*** *"No, there isn't any awareness sessions or programs because awareness should be regular, systematic, based on risk, and tested as well. Furthermore, there are not any mandatory security training programs that exist in the organisation. Nevertheless, information technology authority conducted some basic awareness programs and invited the organisation's manager to send some of the organisation's employees to attend".*

Private Sector

The attitude towards information security awareness, education, and training is positive compared to the governmental sector. Interviewees stated that most organisations have awareness activities as part of their organisations' training functions. They often have

formal training sessions in addition to the ad-hoc information security processes. Moreover, mistakes are often learning opportunities to raise awareness levels. Many interviewees considered existing activities as adequate to raise information security awareness to a proper level. However, several of them described security incidents and breaches as playing a major role in raising awareness rather than formal training sessions.

Most interviewees stated that organisations conduct training programs on information security for new employees and refresher awareness programs for old ones. In most of the organisations, management obliges employees to attend regular programs. For example, PINT12 said*:*

> ***PINT12:*** *"Each of them has a different view about security depending on their duties"*.

Some interviewees noted that management espouse the value of information to the end users and staff:

> ***PINT15:*** *"We used e-mail and our intranet portal to inform our organisation's staff on issues of the information security"*.

Many organisations have different information security programs for different categories, and they all educate their employees about new and updated security policies. For instance, PINT11 commented on educating employees about new and updated security policies and said:

> ***PINT11:*** *"This is a top priority for us"*. He added, *"Regarding the foundation of a regular check to assure that employees are not breaching information security policy, some checks are conducted randomly, together with feedback from direct managers and auditing systems"*.

Further, most interviewees from private organisations mentioned that there are regular checks to ensure that employees are not breaching information security policies, and most of the time these checks are conducted randomly rather than regularly.

5.2.7. Rewards and Punishment System

The researcher used a qualitative rather than a quantitative method to explore the status of reward and punishment systems related to information security in Omani organisations. Qualitative methods produce expressive information conveyed through the language and perceptions identified during cognitive debriefing interviews.

The following research question was investigated to find out the status of rewards and punishment in Omani organisations:

> *RS-Question#2: What are employees' attitudes towards the role of rewards and punishment in motivating personnel to commit good information security practices?*

Interviewees thought that managers misunderstood the impact of continuously motivating employee behaviour regarding information security, and the significant difference this can make to reaching information security goals. Furthermore, they were all concerned that employees should understand the rationale behind information security behaviours, as this increases their motivation to comply with information security disciplines and to use its tools. Thus, information security is enhance by understanding employee motivation. Interviewees also described how a limited culture of information security contributes to poor compliance.

The problem is that motivation varies from day to day and week to week. The challenge is to maintain motivation, as this is the foundation of high-level information security compliance. Interviewees expressed the following concerns:

- The extent to which organisations have motivated employees
- The inadequacy of disciplinary actions when there are repeated information security violations.

Public Sector

Most interviewees stated that there are no disciplinary actions for breaches of information security, even if such actions are required by their organisation's security procedures. GINT1 commented that:

> ***GINT1:*** *"We have punishment if we discover a security violation, but most of the time the emotion of the managers overwhelms and they don't execute the disciplinary action, and that goes back to the culture".*

On the same lines, GINT2 added that:

> ***GINT2:*** *"often the emotion overwhelmed".*

While, GINT4 related lack of effective management of discipline to the predominant culture, and he noted that:

> ***GINT4:*** *"Regarding disciplinary action, we don't follow any system, and when information security is repeatedly violated by any of the employees, no action is applied, even if a report about that employee is discussed with the related department, and it all goes back to culture".*

Further, interviewees mentioned that there is some verbal encouragement to report information security violations, but this is not common. Moreover, some interviewees perceive encouragement as useless. For instance, GINT5 noted that:

> ***GINT5*****:** *"We don't think motivation will be successful due to the employees' culture"*

On the same lines GINT8 added that:

> ***GINT8*****:** *"I think it is acknowledged it is important but the actions are just not there yet".*

Accordingly, most interviewees thought that disciplinary actions are useless, and that overall disciplinary actions regarding information security in Omani public sector organisations are weak, even if such actions are set out in organisational procedures.

Private Sector

Most of the interviewees recommended disciplinary action for repeated security violation. However, some of them believed more in the value of education and awareness to improve information security in an organisation.

> ***PINT14*****:** *"Improving security awareness in the organisation is more efficient than applying disciplinary action".*

According to this view, developing a "compliance culture" depends on the extent to which each member of an organisation is motivated to be information security compliant. However, once this was done, disciplinary action for repeated violation was preferable according to most interviewees. Most Omani private sector organisations take some moderate disciplinary actions to preserve information security.

5.3. The Effects of critical cultural factors and information security behaviours and practices; and the development, and maintenance of an information security culture in Omani organisations.

In developing countries such as Oman, national culture might have a significant impact on information security culture. This section briefly discusses the influence of national

cultural attributes that seem to have impact on information security practices and performance in Omani organisations.

The results for this section were derived from the perspectives expressed during the interviews with participants from public and private organisations. The following national culture attributes were analysed by combining the public organisation interviewee responses and the author's personal observations and work experience based on Hofstede's national cultural dimensions. (Hofstede, 1984):

- Power distance
- Uncertainty avoidance
- Individualism vs. collectivism
- Trust

Trust was added to the other three values, which are from Hofstede's national cultural dimension, because trust is seen as an important value that characterises Omanis in their daily activities. Below is a brief discussion about each value, which includes interviewee feedback and a hypothesis that links these values to the information security culture.

5.3.1. The Power Distance

The power distance dimension depicts the level of acceptance by the less powerful individuals in an organisation where there is an unequal distribution of power. Subordinates do not seek involvement in the decision-making process nor is this encouraged by superiors. Indeed, the involvement of subordinates in decision-making processes may be viewed as a sign of poor leadership, resulting in greater anxiety and confusion for both parties in high-power distance cultures. (Child, 1981). Similar to other Arab countries, the power distance value in Oman is high, indicating that Omani employees are more likely to accept a hierarchical structure and the power of executives with higher rankings. (Hofstede,1994).

Power distance can have implications for how an organisation approaches information security issues. In Oman, which has a high power distance culture, employees usually count on managers to solve complications in the workplace, since managers often assume the role of father- figures and problem solvers.

The researcher formulated the following hypothesis to be qualitatively tested through cognitive debriefing interviews, in order to investigate the effect of high power distance on information security culture and performance in Omani organisations,

> ***H#7:*** *High power distance negatively affects the development and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

Most of the interviewees observed that employees in their organisations accept a hierarchical order in which everyone finds his place without any justification required. For example, GINT3 pointed out that:

> ***GINT3:*** "*The simplest thing is if we think there is a need for awareness programs for the employees, we have to write a request, which is then raised to upper management to approve it".*

Even when there is a need to take action regarding a security risk, employees should wait until the manager give instructions. In this regard, GINT5 noted that:

> ***GINT5:*** "*If there is a security issue, we investigate it, prepare a report, and send it to the upper management to approve it and state the next actions".*

On the same lines, GINT8 highlighted that this is normal in all public organisation and he commented that:

> ***GINT8:*** "*Like other public organisations in Oman, if we need to process any request, we follow the organisation's procedures by getting the decision from high management".*

Nearly all interviewee responses provided evidence that power distance seems to influence the decision-making processes associated with information security issues. Furthermore, all interviewees strongly agreed that the power of the immediate managers seems to play an important role in individual information security behaviours. Thus, the high power distance as noticed by most interviewees has a negative effect on information security in Omani organisation because, as mentioned earlier in section 5.2.4, the current level of managerial involvement and support for information security tends to be low. Accordingly, employees are not as proactive as they should be. When there is a need to take action regarding security risks, they usually wait for instructions from their superiors, who are not concerned with information security issues.

This analysis shows a positive association between high power distance, where employees usually count on 'father-figure' and 'problem-solver' managers to solve

complications in the workplace, and weak development of information security culture and performance. The qualitative analysis set out above, based on interviews with IT and information security managers and specialists, confirms the hypothesis (H#7)) which is therefore accepted.

5.3.2. Uncertainty Avoidance

High uncertainty avoidance has a negative influence on employee compliance with information security in Omani organisations. Uncertainty avoidance is defined as "the extent to which the members of a culture feel threatened by uncertain or unknown situations". (Hofstede, 1997, p. 113). People in cultures with high uncertainty avoidance are more emotional; they tend to avoid unusual circumstances and prefer to follow clear rules. Alternatively, low uncertainty avoidance societies attempt to cope with changes in an organisation by acquiring more knowledge and education and becoming trained in technological innovations and their effect on information systems. Knowledge serves as a means of controlling and avoiding risks of information security violations.

Organisations in strong uncertainty avoidance cultures are characterised by a strong need for rules and regulations; enhanced structuring of organisational activities; an employee preference for clear unambiguous instructions from management; less risk-taking; an intolerance toward deviant ideas and behaviours; and less individual initiative and responsibility. (Hofstede, 1980). Oman has high uncertainty avoidance, especially regarding information security, and organisations resist change to avoid risk.

This value is closely related to information security policies and information security awareness. Therefore, the researcher formulated the following hypothesis to investigate the effect of high uncertainty avoidance on information security performance in Omani organisations. It was qualitatively tested via the cognitive debriefing interviews.

> ***H#8:*** *A high propensity to avoid uncertainty distance negatively affects the development and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

Omani organisations are known for their high value of uncertainty avoidance, managers do not have confidence that employees will behave properly and thus control everything by themselves. The cultural message conveyed to employees is that knowing things, outside of instructions from managers, is dangerous. That is why everything is passed

up to managers, even from specialised personnel, as mentioned by many interviewees, such as the security specialist GINT1, who noted that:

> ***GINT1:*** *"We as security specialists, in case of any unaccepted security issue discovered, we try to deal with it, with management's guidance if needed, but most of the time we do ask".*

High uncertainty avoidance is sometimes considered the reason behind sub-contracting the provision of information security services to third-party vendors. This was highlighted by GINT6 who commented:

> ***GINT6:*** *"All our systems are from third-party vendors, and we have maintenance contracts with them, so we don't have to worry about anything, we just call them when needed".*

On the same lines GINT2 agreed with the above comment and he also commented on management attitudes towards sub- contract third party vendors:

> ***GINT2:*** *"If any data migrations are required, the organisation contacts a third-party to do that. We tried to explain to them this data is important and shouldn't be expose to a third-party. But unfortunately, they didn't listen to us. I don't know, maybe they are uncertain about our capability to deal with such issues".*

Another concern is unclear instructions leading to poor information security. When employees are rule-oriented they are not allowed to use their own judgement and knowledge if these rules are not clear, giving rise to poor information security handling. The security manager GINT3 raised and confirmed this issue.

> ***GINT3:*** *"As a security manager, when I try to advise an employee in the organisation after noticing him trying to commit wrong action such as violating his systems authentication or his PC, his answer is I read the security procedure but nothing was mentioned about this". Which really makes me so embarrassed because I know it's there, but the security instructions are not clear".*

All interview participants seemed to believe that employees were fearful of the risk of breaching information security rules and procedures, both at management and lower levels. However, the influence of uncertainty avoidance appears to have a low influence on the security related behaviour of employees when there is an available information security policy and effective information security awareness in the organisation. When uncertainty avoidance exists without an information security policy and a lack of

information security awareness, its effect is harmful to the security of an organisation's assets. One feature of uncertainty avoidance is resistance to change, but this was not an issue of concern for most interviewees. However, reports of managerial reliance on third party vendors because of uncertainty about their own security specialists' capabilities, or specialised information security personnel passing issues to managers, are indicators of low information security culture and performance.

Accordingly, the analysis has shown that there is a negative association between high uncertainty avoidance, where employees tend to avoid unusual circumstances and prefer to follow clear rules on the one hand, and information security culture development and performance on the other. Therefore, the qualitative analysis set out above, based on interviews with IT and information security managers and specialists, confirms the hypothesis (H#8)) which is therefore accepted.

5.3.3. The Collectivism Value

Individualism is defined as follows: "The interest of the individual prevails over the interest of the group". (Hofstede, 1997, p. 50). In collectivist societies as in collectivist organisations, societal or group achievements and organisational rights are more important. Collectivist societies are more trusting since they are focused on group work and synergy. Therefore, they are more likely to commit to an overarching information security policy.

Oman scores high on collectivism and low on individualism, indicating that colleagues within the same organisation or the same unit may view each other as members of an extended family. (Hofstede, 2001). Neal et al. (2007: 295) described Oman as "highly tribal, firmly rooted". Furthermore, Landen (1993) postulates that tribalism in Oman is a state requirement; the major role of the tribe is to serve society and its values. Thus, the official system and social structure have played a significant role in serving tribalism. Supporting such a view, Rabi (1997) asserts that tribal practice provides a critical counterweight to economic and technological change.

The researcher formulated the following hypothesis to discuss the above argument and to investigate the effect of high collectivism value on information security culture development and information security performance in Omani organisations. It was qualitatively tested via the cognitive debriefing interviews:

H#9: *High Collectivism negatively affects the development and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

A high collectivism value is noticeable in Omani organisations, and it strongly affects the development of information security culture and practice, leading to a weak information security performance in many organisations. Many interviewees pointed to the problem of sharing passwords, which is common among colleagues, who are considered as members of one big family. Conversely, they do not expect to hide passwords from each other. Additionally, employees disclose passwords at the workplace because there is a tendency not to prohibit privacy sharing among family members. This was referred to by GINT4, who explained that:

GINT4: *"Employees share passwords because they trust each other. For example, if two people are preparing a report and the one who saved it on his PC happened to be on vacation, the other one will just call him, and he will dictate him the username and password over the phone".*

GINT6 also agreed with this comment and he added:

GINT6: *"Employees sometimes go too far. For example, one has permission for the HR system and his friend is in a different department, he just goes to visit him and receive all information he wants*".

However, information security specialists, like GINT3, who is an information security manager, didn't accept this behaviour:

GINT3: *"I can assure you that we, as security specialists, don't share any information with other departments or personnel, unless the top management ask for it, and I think it is the same with the IT department. Employees sometimes go too far, like one has permission for the HR system and his friend in a different department, he just goes to visit him and receives all information he wants*".

A strong collectivism value seems to play a key role in Omani organisations, producing a culture of information sharing in whatever format, indicating a weakness in information security culture and performance. Accordingly, the analysis shows that there is a negative association between collectivism value, leading employees to view each other as members of an extended family, and information security. Therefore, the

previous qualitative analysis above based on the perspectives of interviewees, who are IT and information security managers, confirms the hypothesis (H#9) under scrutiny.

5.3.4. The Trust Value

Trust is defined in this context as the level of faith that an employee might have in his or her co-workers to the extent of sharing or granting access to work-related information. Trust builds up over time in a work environment, and it is essential to accomplishing tasks. However, according to Ikonen and Savolainen (2013), time alone is not sufficient to create trust, which also requires continuous interaction for trust to be earned. Most Arabic societies, including Oman, are trusting societies, as the people in these countries easily trust each other. This often promotes risky habits (e.g. close workers may share their account passwords). This practice can expose organisations to a myriad of serious information security risks, including data loss, unavailable systems, and malicious system use.

Trust is similar to collectivism in action and nature. The following hypothesis was formulated to discuss and investigate the effect of high trust levels on information security performance in Omani organisations. The hypothesis was qualitatively tested via the cognitive debriefing interviews:

> ***H#10:*** *High Trust negatively affects the development and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

Trust was a significant predictor of information security violations. All interviewees strongly agreed that a high level of trust is dangerous and negatively influences information security in Omani organisations.
GINT2 gave an example:

> ***GINT2:*** *"Some employees are very naïve. If one received a phone call from a person telling I am from minister office and we need this information, he gives him the information*".

Further, when employees feel an attachment or emotional bond to someone, they are more likely to feel committed to divulge sensitive information. That is why one of the techniques used by social engineers is to build an emotional bond with victims. GINT9 pointed this out and commented:

GINT9: *"Actually, trust is causing big problems in Oman, that's why social engineering is very much effecting many organisations*".

In this regard, it is worth mentioning that employees must be educated on how to handle trust since collectivism is a strong value in Oman. This is important given the lack of awareness programs. Factors that reduce implementation or compliance with information security practices in the work environment have a significant impact on establishing an information security culture and good information performance in Omani organisations.

This is in line with (McIlwraith, 2006), who notes that group norms can affect an individuals' password behaviour. For instance, password sharing can be considered a sign of trust in a group or a family, and therefore, refusing to share a password could be seen as a sign that a person does not trust his family.

Thus, the analysis has shown that there is a negative association between employee trust behaviours, and the people who contact them either as friends or foes, and the development of information security culture and performance. Therefore, the qualitative analysis above, based on the perspectives of interviewees, who were IT and information security managers, confirms the hypothesis under scrutiny. Accordingly, hypothesis (H10) is accepted.

5.4. Discussion and Conclusion of the Interview Findings

This chapter sets out the findings of the qualitative data, based on fifteen interviewees who were questioned about different information security issues, to corroborate the quantitative survey findings. The objective was to conduct the interviews in a manner that allowed the participants to provide insight into data security within their organisations, and to confirm that the fundamentals derived from the study of related academic fieldwork were relevant to the specific context of this research.

Research on the use of interviews is a mature and expanding area of study, and helps to consider several conceptual problems.

5.4.1. The Main Drivers of Information Security in Omani Organisations

The interviewees from the public sector identified many different drivers of information security. Although there is no complete consensus on the basic drivers of information security, many of the interviewees believe that management support, policies, and training and awareness will continue to be the foundation of information security and

the basis for future improvements. Many other interviewees highlighted the importance of management awareness and involvement in information security. Managers also needed to understand the benefits of compliance with information security disciplines.

The main drivers of information security from the perspective of the private sector interviewees focus on three issues: information security policies; management; and business needs. Many of their answers indicate that they consider information security a fundamental and indispensable requirement for business continuity. Furthermore, all interviewees from both sectors expressed an understanding that information security is an endless process, but that many issues slow down progress and improvement. Therefore, organisations must always keep up to date with best practice and technological solutions.

5.4.2. The Current State of Information Security in Omani organisations

In public sector organisations, it is evident that there is no work on the prevention or mitigation of information security risks due to a lack of managerial interest and knowledge. These organisations do not fulfil or meet the minimum information security requirements, and information security is not given the importance it deserves. By contrast, most private sector organisations in Oman have at least given thought to information security. However, they seem to be implementing technological measures only, which has only helped in part helped to neutralise or minimize some negative impacts. There is a lack of managerial interest in other important issues such as sufficient management support and enhancing the knowledge and awareness of employees.

5.4.3. Organisational Information Security Culture in Omani Organisations

Interviewees reached a consensus that management support is a significant predictor of information security culture and the level of policy enforcement. They identified organisational culture and the need to change it as a critical factor for the implementation and on-going improvement of information security programs. In addition, they highlighted organisational culture from a managerial and a tactical perspective, including employee behaviour and awareness.

In the private sector, all of the interviewees perceived their organisations as having a successful information security culture, while most public sector interviewees admitted that their organisations had no successful culture, although some stated that it could be valid at a personal level.

5.4.4. Lack of Management Support and Commitment

Information security not only consists of technology, but also includes organisational issues, processes, and people. Thus, managers must be more involved. This study indicates that the proactive, intelligent management of information security in organisations using a holistic approach is critical to ensuring information security. Kolkowska and Dhillon (2012) argue that management's visible participation in and ongoing communication about information security stimulates employees' intentions to comply with information security policies.

Many interviewees believe that information security is a problem that is primarily affected by how managers address it. All interviewees from both sectors believe that the current organisational culture derives primarily from the management's vision. Due to the lack of management support, governmental organisations do not have successful information security cultures. Interviewees from the private sector who stated that they have a successful information security culture expressed mainly positive views about information security. Conversely, public sector interviewees who stated that their organisations do not have a successful information security culture expressed mainly negative views.

The above discussion confirms the following hypothesis:

> ***H#2:*** *Lack of management support and involvement negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

5.4.5. Lack of Information Security Awareness, Training and Education

Information security education, training and, awareness, and are some of the most effective countermeasures against human behavioural threats to information security. The availability of education, training, and awareness programs can increase the knowledge and understanding of employees with respect to information security in organisations. (Bulgurcu et al. 2010; Puhakainen & Siponen 2010; Tsohou et al. 2008). However, a lack of knowledge was still the most worrisome factor for interviewees, especially those from government-sector organisations. Governmental organisations have neither training programs in information security awareness, for new employees, nor refresher awareness programs for existing employees. On the other hand, the private sector is much better in this regard. All interviewees stated that they have these programs for new and existing employees or that they have new employees sign a policy

document before giving them network accounts, and that organisations conduct refresher programs for selected individuals in different departments. Tsohou et al. (2008) show that the use of information security awareness and training programs can reduce the misuse of information security policies and procedures, and it can minimise information security risks and threats:

> ***H#3:*** *Lack of information security awareness and training negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

5.4.6. Lack of Information Security Policy

Governmental organisations either, have no, or at best, a small or outdated information security policy. Moreover, some governmental organisations that have well documented information security policies pay insufficient attention to enforcing them. The document simply to comply with a requirement or regulation.

This finding contrasts with private sector, where interviewees stated that their organisations have information security policies that are documented and applied. Furthermore, most of the interviewees from the governmental sector expressed negative views about information security policy, whereas all of the private sector interviewees expressed positive views. Martins and Veiga (2015) define an information security policy's effectiveness as the appraisal of whether it is understandable, practical, and successfully communicated.

The above argument and discussion confirms the following hypothesis:

> ***H#4:*** *Lack of information security policy negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

5.4.7. Lack of Information Security Rewards and Punishment

Employees must be motivated to adopt secure behaviour and practices, and management must identify factors that motivate their staff. Most interviewees from governmental organisations stated that there are no disciplinary actions with regard to information security in their organisations, in contrast with interviewees from private organisations. Moreover, even if an organisation's information security policy addresses this point, the subjective personal responses of managers usually overrides

sanctions in both public and private organisations. Consequently, most interviewees from both sectors, recommended disciplinary actions for repeated information security violations. Bulgurcu et al. (2010) and Siponen et al. (2010) indicate that applying stipulated sanctions for information security breaches in organisations encourages individuals to comply with policies and standards.

This argument answers the following research sub- question:

> ***RS-Question#2:*** What are employees' attitudes towards the role of rewards and punishment in motivating personnel to commit to good information security practices in Omani organisations?

According to interviewees, disciplinary actions for information security breaches, are weak and ineffective in Omani public organisations, even if such actions are specified in organisational procedures. However, there are some moderate disciplinary actions for breaches in Omani private organisations, usually when a security violation is repeated.

It is clear that the private sector organisations of the interviewees are in a better situation than the public sector organisations with regard to their information security status. The following chart shows a comparative view of the main barriers between public and private organisations in Oman.

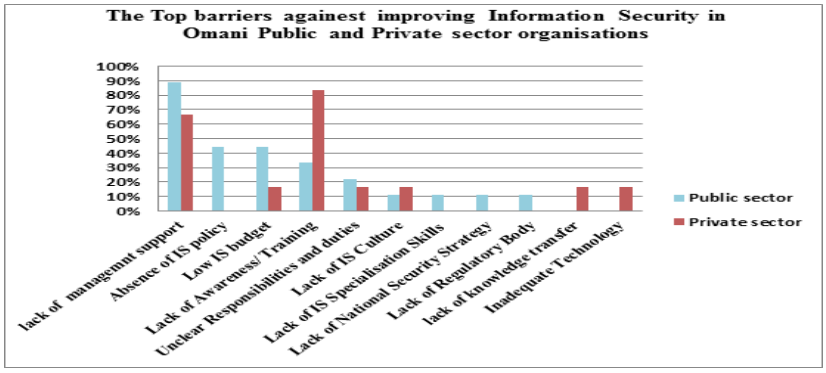

Chart 5-1: Information Security (IS) Top barriers in Oman Public sector and Private sector

Chart (5-1) illustrates the following common findings:

- Management support and awareness of information security can serve as great drivers of information security in both public sector and private sector organisations in the view of the interviewees.
- Information security policies and procedures are also drivers for public organisations.

- The level of information security is affected by the organisational culture, which originates from management priorities and vision and from the information security environment in an organisation.
- These factors interact and can result in behaviours that often have a high impact on information security

5.4.8. The Effects of National Cultural Values on Omani organisations

This analysis, based on the perspectives of interviewees, who were IT and information security managers, highlights the impact of the three national culture values (power distance, uncertainty avoidance, and individualism vs. collectivism) and trust, on behaviour related to information security performance and information security culture development in Omani organisations.

The main conclusions are:

- High power distance negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.
- A high propensity to avoid uncertainty negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.
- High Collectivism negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.
- High Trust negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

Overall, the analysis reveals that some specific national cultural values may have stronger effects on the broad approaches that these organisations have adopted towards information security management. These values shape the processes and decisions related to information security, to some degree.

This study also found that the three national cultural values and trust were relevant because they seemed to play a role in shaping managerial and individual information security behaviours and actions. Furthermore, the findings reveal that involved management support and an effective information security policy, together with training and awareness programs, all serve to moderate the impact of national culture values and trust, upon the quality of the information security culture in Omani work settings.

5.5. Chapter Summary

This chapter presents the findings of the interviews data analysis, which is the second approach within mixed-method research. The results identify eleven themes believed to affect the readiness to adopt a culture of information security in Omani organisations, particularly the public organisations. The presentation of the interview finding also provides many useful insights into the various factors that managers identified within their organisation that have the potential to enhance their organisations' information security culture.

By the end of this chapter, the researcher concludes that the following research sub-questions have been answered:

- ***RS-Question#1:*** What is the current level of compliance with information security best practices in Omani organisations? What is the difference between public and private sector organisations in this regard?
- ***RS-Question#2:*** What are employees' attitudes towards the role of rewards and punishment in motivating personnel to commit to good information security practices in Omani organisations?
- ***RS-Question#6:*** What is the relationship between critical cultural factors and information security behaviours and practices; and the development, and maintenance of an information security culture in Omani organisations?

Accordingly, the qualitative data analysis has played a considerable role in achieving the research objective reflected by the following research main question;

RM-Question: What is the current state of information security culture and practices in public and private organisations in the context of Oman? What are the critical socio-cultural and organisational factors that may affect the information security performance and hinder the development and maintenance of an effective information security culture in these organisations?

Chapter 6. Discussion

"What gets measured, gets managed."
- (Ursula K. Le Guin, 1954)

6.1. Introduction

Related academic work in this field suggests that the problems with improving security within an organisation were made more complex by the speed of evolving technologies. The related work also identified other issues such as organisation culture and organisational capability, which have an influence on information security management within organisations. Further, the related work revealed that although much has been written about factors that challenge the implementation of information security and information security culture in organisations in different countries around the globe, there is very little has been published about socio-cultural and organisational factors that influence the implementation of information security and information security culture in developing countries among which is Oman. Most published information security work about these countries, is either related to the e-government security or cyber security.

The prevailing message from peer-reviewed work is that information security is a business issue not an IT issue and implementing information security culture requires senior management support and participation, good information security policies and information security training and awareness, if it is going to be successful and effective. Zakaria's (2004) research study stated that organisations need to emphasize an information security culture by making security a part of their employees' everyday work routine. Freeman (2007) discussed a holistic approach to information security that should be incorporated into every aspect of a business environment. Other current studies develop a framework and demonstrate the importance of understanding factors that affect information security culture. Yet, there is no mutual agreement on factors that have to be considered for creating or assessing an information security culture. Nonetheless, a few studies, such as Alnatheer's (2012), which specifies factors that constitute information security culture. Minimal studies such as Alnatheer et al. (2012), as well as Da Veiga and Eloff (2010) provide an approach that uses the same framework to create and assess information security culture. The two studies provide a statistically sound assessment instrument based on the defined framework to perform a security culture assessment.

The research problem stated in chapter one, section 1.3 is "The ongoing concerns about the lack of information security culture in Omani public organisations, which has led to ineffective information security practices in these organisations". The current study investigates the research problem by applying a mixed-methods approach using both quantitative and qualitative methods. Existing academic literature was reviewed to identify key factors that would have an impact on information security performance and information security culture development within Omani organisations. During the research, data was gathered via semi-structured interviews with senior managers, specialising in IT (Information Technology), and IS (Information Security), working in public and private organisations in Oman, together with a web based on-line survey of employees from those organisations.

The researcher posed the following questions to address the research problem, and achieve its aim. (RM= Research Main Question, RS= Research Sub-Question):

RM-Question: What is the current state of information security culture and practices in public and private organisations in the context of Oman? What are the critical socio-cultural and organisational factors that may affect the information security performance and hinder the development and maintenance of an effective information security culture in these organisations?

The research main question was approached via the following sub-questions, and hypotheses.

RS-Question#1: What is the current level of compliance with information security best practices in Omani organisations? What is the difference between public and private sector organisations in this regard?

RS-Question#2: What are employees' attitudes towards the role of rewards and punishment in motivating personnel to commit to good information security practices in Omani organisations?

RS-Question#3: How does the social factor "education" affect information security performance in Omani organisations?

This sub-question was resolved through the examination of the following hypothesises:

4. Hypotheses related to the organisation's education level factor:

H#1: Education level positively affects the information security performance in the Omani organisations.

The following sub- hypotheses derive from the main one:

H#1.1: Education level is positively associated with information security policy in Omani organisations.

H#1.2: Education level is positively associated with information security training and awareness in Omani organisations.

H#1.3: Education level is positively associated with managerial support for information security in Omani organisations.

H#1.4: Education level is positively associated with employee commitment to information security disciplines in Omani organisations.

H#1.5: Education level is positively associated with an organisation's information security practices in Omani organisations.

RS-Question#4*:* What is the relationship between critical organisational factors and information security performance; and the development, and maintenance of an information security culture in Omani organisations?

This sub-question was resolved through the examination of the following hypotheses:

2. Hypotheses related to critical organisational factors:

H#2: Lack of management support and involvement negatively affects the information security performance; and the development, and maintenance of an information security culture (resulting in impaired employee information security behaviours and practices) in Omani organisations.

H#3: Lack of information security awareness and training negatively affects the information security performance; and the development and maintenance of an information security culture (resulting in impaired employee information security behaviours and practices) in Omani organisations.

H#4: Lack of information security policy negatively affects the information security performance; and the development and maintenance of an information security culture (resulting in impaired employee information security behaviours and practices) in Omani organisations.

RS-Question#5*:* What is the relationship between the development and maintenance of an information security culture, and information security disciplines and practices in Omani organisations?

This sub-question was resolved through an examination of the following hypotheses:

3. Hypotheses related to information security disciplines and practices:

H#5: There is a positive correlation between the information security culture and employee commitment to information security disciplines in Omani organisations.

H#6: There is a positive correlation between the information security culture and information security practices in Omani organisations.

RS-Question#6*:* What is the relationship between critical cultural factors and information security behaviours and practices; and the development, and maintenance of an information security culture in Omani organisations?

4. Hypotheses related to critical cultural factors:

H#7: High power distance negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#8: A high propensity to avoid uncertainty negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#9: High Collectivism, negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

H#10: High Trust, negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.

This chapter summarises, interprets, and discusses the findings from chapters four and five in relation to the research problem and objective presented in chapter one, as well as the research questions and hypotheses described above. The chapter is divided into five sections. Following the introduction, the researcher discusses the research findings on the level of compliance with information security best practices in Omani organisations and the difference between public and private sector organisations. The third and the fourth sections discuss the research findings regarding effects of socio-cultural and organisational factors on information security performance and information

security culture in organisations in Oman. The discussion in all sections are headed with the relevant research questions. Finally, this chapter concludes with a summary section.

6.2. What is the current level of compliance with information security best practices in Omani organisations? What is the difference between public and private sector organisations in this regard?

The above two sub-questions are discussed together because they are integral to each other. The researcher collected information about the following five information security elements in Oman to investigate the level of compliance with information security best practice:

1. Organisational Information Security Policy (ISP).
2. Information Security Training and Awareness.
3. Managerial Support for and Commitment to Information Security.
4. Organisational Information Security Best Practice.
5. The Responsibilities of Omani National Information Security Bodies.

6.2.1. Information Security Policy in Omani Organisations

The results of this study show that 40% of respondents believe that the organisations they belong to are following an information security policy. Compliance with these policies is nearly twice as high private than in public organisations. (60% private and 31% public). Survey answers clearly denote that a number of Omani organisations have information security policies and procedures, regardless of how seriously they are implemented and monitored, and regardless of the level of employee compliance. However, many public sector interviewees are pessimistic about information security policies. They believe that employees follow the individual subjective wishes of IT and IS managers rather than the policies of the organisation. Furthermore, they said that even where policies exist, they remain on the shelf, and are not implemented or shared with employees. Many of them thought one of the reasons for inadequate information security culture and compliance in these organisations is the lack of information security policies.

Furthermore, the interviewee answers imply that in most cases employees are not aware about the existence of the information security policies in their organisations. This is consistent with the finding of Parsons *et al.* (2014) who examine the relationship between an employee's knowledge of policies and procedures and their behaviour. Their findings suggest that employee knowledge of policies and procedures has a significant influence on reported attitudes and behaviour. When employees are aware

of information security threats and dangers the organisation faces, they are more effective in preventing such events (Parsons *et al.*, 2014). Whereas, leaving employees out of the communication loop creates significant weak points exposed to security threats.

Additionally, the current study shows that many interviewees see that failure to fully implement information security policy is one of the major barriers to improving the information security practices in their organisations. They consider that greater management engagement in information security will set the "tone at the top", reinforce policy more effectively, and improve behavioural change. This aligns with the work of Talbot and Woodward (2009) who argue that even when security policies exist, there is a challenging history of employees in an organisation ignoring these policies. Canavan (2003) also stresses that when an organisation implements an information security policy, employees who are required to follow the rules should also be made aware of their rights and responsibilities.

One possible reason that information security policies are lacking, according to Samar & Usha (2014), is the allocation of responsibility. For instance, a study in Tanzania shows that information security policies are viewed as the responsibility of the IT department or as a technical issue (Bakari, 2005), while other research highlights situations in which responsibility for information security stops at technological controls without any policy enforcement. (Tarimo, 2006).
Thus, this research study demonstrates two challenges facing the ISP in Omani organisations:

I. Implementing a realistic information security policy, that is carefully translated into procedures, training, and education at all levels of the organisation, helping to achieve information security objectives.

II. Ensuring that the organisations' employees comply with these policies.

According to Whitman and Mattord (2003), the objective of a policy is to influence the decisions, actions and behaviour of employees. Moreover, it specifies what behaviour is acceptable and what is not. An effective security policy is the foundation for the other components of successful information security. It has a number of functions including setting standards and ensuring a minimum level of uniformity in implementation; providing a framework for action and for dealing with potentially sensitive security issues; and promoting transparency and accountability among departments and employees.

The researcher believes that, in Omani organisations the lack of information security policy creates other information security issues such as an inadequate assessment of the level of the risk posed to the organisation's assets and the level of security protection to protect those assets. In the absence of effective information security policies, security practices without clear demarcation of objectives and responsibilities among work units will be developed. Effective information security policies would help to define users' rights and responsibilities in relation to information and help establish acceptable and responsible behaviour concerning information resources.

6.2.2. Information Security Awareness and Training in Omani Organisations

Awareness is one key to protecting an organisation's information assets. (Johansson & Riley, 2005). Information security awareness is a process that requires a series of steps to convince and educate the employees, so that their behaviour supports organisational security measures. This issue is highlighted in previous research work as a major determinant of information security performance and development of information security culture. Khalfan (2004), in his research into information system outsourcing in private and public organisations in Kuwait, claims that the employee lack of security awareness was one of the important drivers, notwithstanding managerial consciousness of the risks involved in outsourcing itself.

In addition, Bean (2008) argues that most currently identified information security breaches occur because of human errors arising from lack of appropriate knowledge and training; ignorance of and failure to follow procedures. Moreover, Al-Omari et al. (2011) and Bulgurcu et al. (2009) suggest that awareness plays a considerable role in establishing prior intention to behave in ways that comply with information security. Siponen (2000) suggests occurrences of human error in information security need to be mitigated by a security awareness programme based on or reflecting a framework similar to the one proposed by NIST (1998). The NIST guidelines recommend identifying programme scope, goals and objectives; identifying and targeting staff training needs; motivating management and employees; administering, maintaining and evaluating the programme.

Da Veiga and Martins (2015) also suggest that information security training and awareness is a significant factor in positively influencing the culture of information security within an organisation. Safa et al. (2015) also demonstrate that awareness can significantly affect the attitudes of users and promote positive information security behaviour. Information security awareness and security monitoring has significant influence on security culture. (Chen et al., 2015). Bélanger et al. (2017) highlight the

importance of information security awareness in influencing positive changes in security behaviours amongst employees. Boss et al. (2015) demonstrate that organisations need to present employees with strong arguments for adhering to security policies, and not just set out the information security policy. Tsohou et al. (2015) explain that leaders in organisations use information security awareness to exercise positive influence over user intentions to comply. Chen et al. (2015) indicate that SETA programs have significant influence on information security culture.

In the current study, data analysis shows that many Omani organisations are keen to assign responsible personnel to oversee and implement information security training. However, the results indicate that awareness-raising activities in Omani organisations fall far below requirements. Consequently, overall compliance with information security training best practice is less than 50%. Moreover, information security training and awareness at an advanced level in public organisations is below average (39%), although the situation is better in private organisations, with 65% of the respondents having a positive perception. Many of the interviewees stated that their organisations do not conduct awareness and training programs on information security for new employees or refreshment programs for existing employees. However, this lack of training does not prevent some organisations from making employees aware of procedural changes.

The interviewees cited poor training, of and by, security officers especially in Omani public organisations, regardless of their size, as the most pressing aspect of the current information security environment. In general, these organisations do not have sufficient training programmes. The interviewees thought that information security risks for Omani public organisations have increased because of the greater use of IT. The level of information security awareness in these organisations has not kept pace and remains low.

To explain this phenomenon, interviewees suggested that many managers in Omani public organisations do not yet recognise the existence of an information security problem, and are thus unwilling to allocate a budget to this area. Indeed, interviewees think that organisational managers generally do not believe that information security is a priority. Furthermore, managers in most Omani organisations do not consider the human resource factor in information security, and do not understand how to address the human resource element effectively. This tendency to ignore, instead of tackling training programs, was evident in several other studies such as (Katz, 2005; Tarimo, 2006; Rezgui et. al, 2008).

The current study results suggest that information security awareness has an important role in promoting security-conscious behaviour. The research clearly exposes the lack of employee training in Omani organisations, not only regarding the technological aspects of information security, but also with regard to the cultural aspect of employee behaviour. This is consistent the findings of Alfawaz (2008), who indicates the need to educate people in both technical abilities and non-technical behaviours to secure sensitive national or organisational information. That is why organisations need a program with three pillars: training, education and awareness, and funding for implementation.

The researcher believes that the purpose of security training is to educate employees on how to protect vital organisational assets and why a certain set of rules have to be in place. The 'why' is particularly important. If employees do not understand the significance of a certain rule, they may not undertake the extra effort to follow the rule, and, consequently, breach organisational information security requirements. In addition, the researcher also believes that, when employees do not understand the reasons behind security rules, they may interpret those rules inaccurately. Furthermore, the researcher believes that management should explain the reasoning behind policies and regulations, so that employees are able to understand why these should be followed. Workshops, where the employees can communicate with the information security team, express concerns and ask questions, are much preferred to the usual lecture-like education.

6.2.3. Management Support and Commitment in Omani Organisations

The results in this study show that there is some managerial interest in information security, but not to a sufficient the extent to have a positive impact on employee behaviour. The analysis records the perception of a low level of support in Omani organisations at only 34%. The level of support in private-sector organisations is 62%, but only 26% in public-sector organisations. Many interviewees identified a lack of managerial awareness and knowledge of information security. Managers tend to consider finishing work more important than securing it. Additionally, managers in Omani public organisations have a multitude of competing tasks, and information security may occupy a less important position among many other concerns. As such, one manager may prioritise information security, while another manager may consider it a low priority because it is not a key aspect of his business, which competes with other concerns in the organisation.

Interviewees pointed out that it is difficult to persuade Omani public sector managers of the importance of information security culture because there is no immediate visible value. They also observed that managers do not pay attention to security progress reports or feedback on implementation because of the low priority given to information security. Some managers only care about this topic when serious security issues or threats to the business arise. Wright (2001) supports this finding and suggests that when senior management has a focus on security that is merely reactive to crisis and the perceived threat level, then lower level management will adopt a similarly reactive approach to information security. Wright (2003) highlights the significant role of managerial support, especially among top-level management. He suggests that a limited, reactive culture of information security contributes to poor motivation, resulting in half-hearted compliance activities.

The current study compares public and private organisations, and shows that managerial support in private organisations is better. Many interviewees from private organisations confirmed that some managers do support information security policies, and that their support increases if a security breach occurs. These interviewees believe that managers are aware of different types of information security risks, and that they sometimes encourage those who report information security violations. Other interviewees suggested that managers in public organisations should be more focused on information security, and ready to invest and proceed systematically to bring about the necessary technological, cultural and educational improvements. Furthermore, these interviewees thought that public sector managers should incorporate a culture of information security into their organisations, and understand that investing in information security is equally important to the search for more efficient employees.

In line with this vision, Al Izki and Weir (2015) set out the way in which perceptions of managerial information security governance and practice can affect compliance with information security procedures in Omani public sector organisations. They identify a considerable lack of management interest in information security in Omani public organisations and conclude that the information security environment in Omani public organisations is not optimal. They also refer to related academic research into managerial influence in shaping organisational culture and commitment to good governance. They echo the arguments of other scholars that management commitment is a prerequisite to improvements in security, since this commitment increases levels of motivation and security concerns throughout the organisation.

Many researchers comment on the involvement of top management as an essential element in the creation of a culture of information security awareness. (Chia et al., 2002; Schlienger & Teufel, 2002, 2003). Others consider that the degree of senior management understanding of the importance of the information security function is the factor which identifies the level of their support for information security. (Armstrong & Sambamurthy, 1999; Ragu-Nathan, et al. 2004).

6.2.4. Organisations Information Security Best Practices in Oman

This section covers a diverse range of areas related to information security. In the first place, risks to information security are often intangible, and so its value to the organisation is not always recognised. The reactive approach to information security is reflected in the number of incidents due to a lack of established baselines in both public and private organisations. This current study shows that notwithstanding a slight better performance in the private sector, both types of organisations are broadly similar. There is an average percentage of compliance with best practice at 45% in public organisations, and 56% in private organisations.

However, the results also show high levels of compliance with some best practice in both sectors. For example, both types of organisation assign every employee a unique username and password for network authentication (84% public, 89% private); the existence of network security measures such as firewalls (69% public, 74% private); and prohibiting suppliers from accessing the organisation's network (50% public, 55% private).

It is also the case however that both public and private-sector are similar regarding best practices with low compliance levels, for example, prohibiting short-term contract employees from accessing the organisation's network (19% public, 26% private), and restricting the use of mobile phones on the organisation's premises (13% public, 7% private).

Interviewees cite a poor 'culture of compliance' as the number one barrier to improving overall compliance with security, particularly in public organisations, followed by funding issues, resourcing, management support, awareness and training and information security policy. Notwithstanding the establishment of security units in all organisations, the interviewees consider the overall information security status in Omani organisations inadequate. However, some interviewees noted higher levels of compliance where individual information technology and information security managers were particularly proactive.

The researcher considers that achieving improved compliance with information security in public organisations in Oman faces a number of challenges. In many cases, Omani public organisations believe that because it has not happened to them it never will. This type of mind-set, unless proven otherwise, makes committing to information security seem an unnecessary expense as evidenced in the interviewees' answers. Often, information security is associated with IT itself and not connected to business information flows and the budgetary allocation process. Therefore, there is a reluctance to release resources, which in turn restricts the level of awareness provided, further exacerbating the situation. Often, there is no direct funding, or inadequate funding, for information security, reflecting a lack of prioritisation. Achieving a culture of compliance requires a change at the individual, group and organisational level. The researcher therefore sees compliance with information security best practices as a challenge for Omani managers, as failure to comply with them always leads to risks and security breaches.

Knapp, et al (2006), state that low levels of top management support for information security produces an organisational culture that is less tolerant to good information security practices. That is why, according to Ammann and Sowa (2013), internal and external information technology auditors consider security policies when evaluating the compliance of the internal regulatory framework with information security. When auditing the effectiveness of security measures, auditors usually account for the consistency of the implemented measures with the security policy requirements.

6.2.5. Responsibilities of Omani National Information Security Bodies

Approximately 25% of respondents answered 'not sure' to the three questions related to the support received from the Omani national information security bodies. A considerable number of employees in Omani organisations are unaware that such support exists. Moreover, the analysis of these answers shows that the amount of support from national information security bodies is in general below average (46%); (50% for public-sector organisations and 37% for private-sector organisations). Public-sector organisations receive more invitations to attend information security conferences and workshops than those in the private sector, and they receive more guidance and support when applying the best information security practices. Both sectors are also below average (35% private, 39% public) at detecting new information security vulnerabilities and threats. It is obvious that the level of support provided to Omani organisations by national bodies is low.

From the researcher's perspective, there is a need to ensure that the policies of the national bodies are implemented in writing and practice, backed up by regular visits to ensure that information security policies exist and are being followed. The greater amount of support for public sector organisations could be because national bodies are governmental authorities that exist to support public organisations. However, they also offer many services to the private sector. The predisposition towards public sector organisations is because they need more support.

In summary, the current study suggests that information security is not optimal in most Omani organisations, which means that there is an information security divide between Oman as a developing country and the developed world. Moreover, the information security situation in public-sector organisations is far worse than it is in the private-sector organisations, which means that there is an internal information security divide between these sectors within Oman.

The research suggests that managerial support, and training and awareness of information security can greatly improve information security in both public and private organisations. Improving information security policies and procedures is also important, especially for public organisations. Furthermore, an organisation's information security level is affected by the organisational culture, which originates from the vision and objectives held by management and the environment within the organisation. These factors interact with each other and can result in behaviours that have a high impact on information security.

This finding aligns with UNESCAP's (2008) statement that for developing countries, attempts to reduce the digital divide through investment in infrastructure alone, without taking into account the need for security and control of information technology risks, will result in the creation of a security divide as prejudicial for developing countries as the digital divide. This relevance of the security divide has been highlighted by many scholars, such as Norris (2001), who describes the urgent needs of society to purchase increasingly complex computer equipment to avoid being 'off-line', while ignoring the implications, responsibilities, and learning processes imposed by this technology. It is possible that the rapid growth of information technology has left nascent information societies, including Oman, unaware of the social and technological implications of being an information society, further widening the information security divide.

This section clearly shows that appropriate recognition of security must be acknowledged and acted upon. Information security is a multi-faceted problem that

requires a comprehensive solution to encompass physical, procedural and logistical forms of protection. As a result, a range of expertise is required to progress appropriate solutions (Furnell et al., 2000). The expertise often resides in the person responsible for the progression of information security. A succinct understanding is needed of how to conceptualise the way forward to improved information security implementation.

6.3. What are employees' attitudes towards the role of rewards and punishment in motivating personnel to commit to good information security practices in Omani Organisations?

The answer to this question was obtained from the qualitative method, using the expressive information that is conveyed through language and perceptions.

Motivating employees to commit to information security good practice involves the principle of rewards and sanctions; a way of adhering to information security rules and guidelines in Omani public organisations by punishing those who violating the information security, and encouraging those who follow security guidelines. Most interviewees see action to motivate and punishment as very important because they help to discipline employees for any wrong doing regarding business and information security, as well as motivation employees in that concern. Most of them believe that there is little or no substantial evidence of appropriate sanctions being imposed upon those who breach information security.

From the researcher's perspective, the principle of rewards and punishment is one of the methods that should be used to achieve compliance with information security. This includes rewarding employees who report information security violations. However, the researcher believes that the principle of rewards is less effective than punishment.
This is consistent with the finding of O'Reilly and Puffer, (1989), who suggest that punishment policies and rules may help in creating group norms by distinguishing between acceptable and unacceptable behaviours in an environment perceived as fair. (O'Reilly and Puffer, 1989). It is known that people learn by observing others' attitudes and behaviours. (Bandura and Simon, 1977). For this reason, employees who are aware that sanctions exist against security violations, adjust their behaviours by imitating those who have never been punished before. (Atwater et al., 2001; Bandura, 1971). When the probability of punishment is high and the sanction is severe, potential violators will be deterred from committing undesirable acts. (Blumstein, 1978; Hoffer and Straub, 1989).

The interviewees in this study have the perception that current disciplinary actions regarding information security violation in Omani public sector organisations are useless. Even where such actions are specified in organisational procedures. However, some moderate disciplinary actions regarding information security violation do take place in private sector organisations.

6.4. How does the social factor "education" affect information security performance in Omani organisations?

The current study shows no clear correlation between the level of education and compliant/non-compliant behaviour with regard to information security behaviour, notwithstanding a general belief that education usually affects information security, through more compliant behaviour, and increased information security awareness.
This finding does not align with the suggestion of (Al Izki and Weir, 2015), that there is a direct relationship between human development, the digital divide and skills-based information security risks. They highlight the ITU report of 2013, that skills sub-index indicators (adult literacy, gross secondary education enrolment and gross tertiary enrolment), provide a clear measure for the overall level of human capacity in a country. This is important because, in addition to ICT infrastructure, education and skills are necessary for making effective use of ICTs and building a competitive and inclusive information society (ITU, 2013). They go on to explain that education is an expression of a cultural and technical level of the population and a parameter for interpreting the possibility to assimilate new concepts and behaviours in relation to ICTs. Therefore, populations with limited reading and writing capabilities will have difficulty in achieving access to ICTs on their own.

Many other researchers highlight the importance of education for information security. Johnson (2006) emphasises that a full education helps in changing people's mind-sets and behaviours regarding information security. (Da Veiga & Eloff, 2007, p.149), state that organisations need to ensure that "an information security culture is inculcated through training, education and awareness raising, in order to minimise risks to information assets". (Tarimo, 2006) points out an effective information security culture is necessary for effective information security management, and how such culture cannot be achieved unless there is an interest in security awareness, training and education for ICT users.

The current study shows that "education" has a low effect on information security performance in Omani organisations. This may related to the survey sample, which was

not statistically distributed to reflect different education levels in Omani society. Most respondents to the survey questionnaire are highly educated (83% with B.Sc. and above). Accordingly, the researcher assumes that the real influence of education on information security is not measured accurately in the current study. However, the study does generate some insights into such an influence.

The researcher believes that education about information security is one of the most important issues that should be addressed at the individual, organisational and national level. Awareness and education programs must be ongoing and include information security updates. If employees are aware of the different aspects of information security, the organisations have fewer security problems. The researcher also identifies a recurring problem of insufficient time allocated to employee education. Online education, for example virtual lectures or video-conferencing can solve the logistical problems in providing employee education in larger organisations.

6.5. What is the relationship between critical organisational factors and information security Performance and the development and maintenance of an information security culture in Omani organisations?

The hypotheses related to this question are:

> ***H2:*** *Lack of management support and involvement* negatively affects the *information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*
>
> ***H3:*** *Lack of information security awareness and education* negatively affects the *information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*
>
> ***H4:*** *Lack of information security policy* negatively affects the *information security performance; and the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

There has been much discussion about organisational culture, (defined as a set of beliefs and values that are important for an organisation), in the international context. Such a culture is the foundation of an organisation's internal environment because it determines

employees' collective understanding of daily operations. It thus translates into two conjoined elements: what people believe and what people do. These two elements shape employee behaviour with regard to organisational regulations including those relating to information security. These critical organisational factors shape the organisational culture, govern the organisation's response to security issues, and influence employee behaviours. The cultural characteristics of effective information security in an organisation are:

1. The organisation has a strong and enforced information security policy.
2. The organisation conducts adequate awareness and training programs on information security for all employees before they receive a network account and regularly thereafter.
3. The organisation conducts regular refresher security programs and awareness activities to raise security awareness among its employees at all levels.
4. The organisation assigns an annual budget to the development of information security in the organisation.
5. The organisation applies information security policies and procedures to its members and managers at all levels.
6. The organisation encourages employees notify superiors of information security violations.
7. Managers are permanently concerned with information security, and not simply when there is a security breach.
8. Organisation members share a belief in information security best practice.

This relationship between culture and information security performance in an organisation agrees with the published ideas of many scholars such as (Richards et al. 2005) who argue that information security is a subset of an organisation's overall security. Similarly, the development of an internal culture of information security culture depends upon the overall culture in the organisation. Lim et al. (2009) see an interrelationship between the concepts of information security culture and organisational culture. They argue that information security culture is still not embedded in many organisations. They identify the following key challenges to embedding information security culture in organisations:

- Having an information security culture as an integral part of an organisational culture.
- Obtaining a sufficient budget for security activities.
- Locus of responsibility.
- Organisational motivation towards implementing security measures.
- Different perceptions towards security risk.

The current study identifies a strong relationship between the organisational culture characteristics above, and the following three critical organisational factors that come together to develop information security culture and performance.

- Manager support and involvement.
- Information security awareness and training.
- Information security policy.

The researcher believes that, these critical organisational factors, are highly influential with regard to information security performance, especially when organisations succeed in integrating, implementing, and maintaining a successful information security culture. The contribution that each of these factors makes to a successful information security culture varies. However, combining these factors can multiply their impact on information security culture and performance.

6.6. What is the relationship between the development and maintenance of an information security culture, and information security disciplines and practices in Omani organisations?

The current research finds that:

> ***H5:*** *There is a positive correlation between the information security culture and employee commitment to information security disciplines in Omani organisations.*
>
> ***H6:*** *There is a positive correlation between the information security culture and information security practices in Omani organisations.*

Lim et al. (2009) argue that understanding organisational culture may be useful when investigating the impact of employee behaviour on security practices. They echo the argument that organisational culture is a powerful, underlying and often unconscious force that establishes employee behaviours. Thus, this relationship between organisational culture and employee behaviour should be considered when implementing security practices. On the same lines, Stan (2007) argues that real security culture lies in the security related beliefs, and values, which manifests itself in employee actions and behaviours. Therefore, organisations need to think carefully about generating the desired level of information security culture that will influence their employee behaviour to protect organisational information.

The researcher believes that establishing an information security culture in Omani organisations requires a transformation and sustainability plan at organisational

level. There are many key aspects to this. The most important one is that employees have behaviours, learned since childhood that affect their perceptions of information security. In particular, employees may consider that complying with information security discipline is simply a matter of observing regulations, without understanding the deeper need to acquire sufficient information security knowledge to protect themselves from any threats.

6.7. What is the relationship between critical cultural factors and information security behaviours and practices; and the development, and maintenance of an information security culture in Omani organisations?

The interviews confirm Hofstede's claim that there is a relation between organisational culture and national culture, because individuals take the social values and norms they receive from birth to the organisations they work in. managers enforce these values through training, monitoring, and other processes of socialisation.

The current study interviews tested and confirmed the following hypotheses related to this question:

H#7: *High power distance negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

H#8: *High propensity to avoid uncertainty negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations*.

H#9: *High Collectivism negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations*.

H#10: *High Trust negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

Moreover, the analysis based on the perspectives of interviewees, who were IT and information security managers and specialists, highlights the impact of four national culture values on information security performance, security culture development and maintenance, in Omani organisations:

- Power distance
- Uncertainty avoidance

- Individualism vs. Collectivism
- Trust

Overall, the analysis of interviewee responses reveals that these national cultural values shape processes and decisions related to information security, to some degree.

The impact of the four critical cultural factors on information security culture in Omani organisations is explained as follows.

6.7.1. High Power Distance

Power distance as a factor in information security becomes clear in discussions of actions taken in response to security issues and problems. This research confirms the hypothesis above that the high power distance in Omani organisations clearly influences the activities and practices related to information security practices and culture. Specifically, power distance seems to influence the decision-making processes associated with information security issues. Employees in Omani organisations rely on managers to solve work issues.

Interviewees provided evidence that Omani employees are more likely to accept the power of executives with a higher ranking in the hierarchical structure. This behaviour affects the way by which Omani organisations tackle information security risks. When an information security problem occurs, employees wait higher authority to provide guidance and directives to the IT department. This finding is in the line with the view of Ali, 1993; Bjerke and Al-Meer, (1993), that there is little participation in decision making in Arab organisations. Users are strictly limited in their freedom to take decisions related to information security, and decision-making is the role of organisation managers. They suggest that this low level of employee participation could be due to the rigidly hierarchical structure style of organisation, where middle managers and employees have to comply strictly with orders from higher-level managers.

> Thus, the current study confirms: *High power distance negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

The researcher believes that it is important for decision makers in Omani organisations to rely more on the role of middle managers in handling information security issues and thus promote information security performance and culture among employees. The

researcher also believes that employees should be included in the decision making process when security rules are established. If this is not the case, employees may feel forced to follow certain rules without understanding or agreeing with them.

6.7.2. High Uncertainty Avoidance

According to Al-Shanfari (2010), Omani national culture is characterised by high uncertainty avoidance, and this suggests limited societal support for risk takers. Hofstede (2001) argues that people in such cultures are anxious in uncertain situations and rely on experts to deal with the uncertainty. Such cultures need rules and procedures to make people feel safe and secure. Specifically, they are averse to taking risks when handling information security issues.

> The current study confirms that: *High propensity to avoid uncertainty negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

The research finds that employees in Omani organisations exhibit a high level of uncertainty avoidance. This has a consequent negative impact on information security performance and the development of information security culture, because information security problems often require actions to minimize risks while they wait for instructions. A high level of uncertainty avoidance limits proactive behaviour in dealing with information security risks.

This study also shows that the majority of interviewees are unaware of the existence of their organisations' information security policies. If those policies exist, employees have no idea how to access them. Moreover, the study shows that only those who work in the information security unit are likely to be aware of management security planning and policies. There is a gap between management efforts in planning security rules, and what the employees know and do, indicating a need for more awareness-raising efforts.

This finding agrees with Zakaria et al. (2003), who point out that a high uncertainty avoidance value seems to play a role in determining how information is transmitted, who receives it and the allowable circumstances under which different types of communication are applied. They argue that, information security policies and guidelines should be convenient and accessible to all employees, as cultures with a high uncertainty avoidance level, are less willing to take risks and to accept organisational change.

The researcher believes that information security needs more rules and procedures that can be used as guidelines and permanent reminders for employees, to maintain proactive security-aware behaviour.

6.7.3. High Collectivism Level

Oman is a highly collectivist society. According to Pinillos and Reyes (2009), collectivism implies subordinating personal interests to the interests of the group and is based on cooperation and harmony, and a concern for the well-being of the group.

> The current study confirms that: *High Collectivism negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

Employees in Omani public organisations value group achievements above individual ones, and colleagues view each other as members of an extended family. The influence of collectivist values are particularly apparent with regards to the dominant culture of sharing passwords and confidential information.

The influence of group behaviour over personal behaviour has both good and bad implications. The inadequacy of awareness and training programs may contribute to the phenomenon of sharing passwords and confidential information. Nevertheless, the negative impact of the sharing culture is obvious in Omani public organisations, where rules and regulations are often overridden by higher values of loyalty to the group, friends or family. Password sharing is common because of this close-knit society. Wrongdoing or breaches are seldom reported to save face.
These findings are consistent with the insights of Elashmawi (1993) concerning Arab culture. Elashmawi points out that Arab culture is neither collectivist as in Asian society nor individualistic as in western culture, yet remains strongly oriented towards maintaining family security.

The researcher believes that sharing password in Omani public organisations often happens for a perceived good reason, such as to get the job done. Managers can utilise collectivist attributes to encourage employees to cooperate with each other in recognising information security risk, and to proactively comply with the set rules.

6.7.4. High Level of Trust

Trust is believing in the reliability and honesty of another person. Martins (2002) defines trust as "the process in which a principal relies on a trustee (a person or group of people) to act according to specific expectations that are important to the principal without taking advantage of the principal's vulnerability". Trust is dynamic and changeable in different circumstances of vulnerability. (Corritore et al., 2003). Paine (2003), states that trust is only one component of the strength of relationships in business management and organisational communications. Trust is perhaps one of the most important factors influencing the development of organisational knowledge. This confidence is the result of structural and behavioural processes in the field of information security. (Haman, 2013). Purser (2004) argues that many issues, including trust, have grown dramatically in importance because of the increased use of networked applications. Kaplan (2007), argues that trust can be linked to culture since it, too, is influenced by norms, values and beliefs, and plays an important role in the effectiveness of information security mechanisms. Behaviours that imply social and personal risk exhibit the attributes of trust.

> The current study confirms: *High Trust negatively affects the development, and maintenance of an information security culture (resulting in impairment of employee information security behaviours and practices) in Omani organisations.*

The interviewees stated that one of the reasons for the high trust level among employees and between employees and outsiders, is organisational trust culture, where employees trust each other in sharing passwords and sensitive information. This finding is consistent with the findings of Al-Mukahal & Alshare, (2015), who argue that in a collectivist society (such as Oman), employees in organisations are more trusting towards each other and are therefore more likely to commit information security violations such as sharing passwords, work sensitive information and copyrighted material. On the same lines, McIlwraith (2006), argues that password sharing can be considered as a sign of trust with colleagues, and therefore, refusing to share a password could be seen as a sign that people do not trust their colleagues. A great deal of education about information security will be necessary to change these behavioural norms.

The current study also finds that information security in Omani organisations suffers from employees who are very easily targeted by social engineering, because they trust others easily. This is consistent with Workman (2008), who argues that susceptibility is greatly associated with an individual's likeability and trust. People who are more

trusting are more likely to succumb to social engineering approaches. The good nature of these employees make them see the request for information as reasonable. Further, this is also consistent with Mitnick and Simon (2002), who explain that it is human nature to trust people, particularly when their requests seem reasonable, and when they do not have any reason to be suspicious. Hence, social engineers can use this knowledge to exploit people, and they will often attempt to build a friendly rapport, knowing that victims are more likely to comply with any requests if they like or trust the attacker.

The researcher believes that trust gives privileged access to insiders in Omani organisations that enables them to do serious damage far more easily than anyone attacking from outside. Nonetheless, for the most part, the access that enables them to cause so much potential damage is also essential to enable them to do their jobs. Therefore, there is an urgent need to limit such privileged access to highly trusted employees and to set strict rules to control such access.

6.8. Chapter Summary

This chapter discusses in detail the research findings in relation to the research questions and the review of related academic work. Furthermore, the critical socio-cultural and organisational factors have been highlighted based on their impact on the employee information security practices and the successful implementation of information security culture in Omani organisations in general and public organisations specifically.

The chapter identifies eight key socio- cultural and organisational factors, including trust and reward/punishment mechanisms that have the potential to influence the implementation and integration of a successful information security culture in Omani organisations. The factors are:

- Organisational factors:
    1. Information Security Policy
    2. Information Security Training and Awareness
    3. Manager Support and Commitment of Information Security
    4. Rewards (Motivation) and Punishment (Sanctions)
- Socio-Cultural factors:
    5. Power Distance
    6. Uncertainty Avoidance
    7. Collectivism Values
    8. Trust Level

This research study proposes that these key critical factors have an impact on an organisation's information security culture development and information security practices. It follows that identifying these factors will enable organisations to focus time, effort, and financial resources in areas that will produce positive results in terms of developing, integrating, and maintaining a successful information security culture and positive information security practices.

The current study also identifies a number of challenges facing Omani organisations in relation to the development of information security culture, and the great need to improve the level of information security culture and practice. The majority of information security incidents are caused either by the absence of effective information security policies, or lack of compliance on the part of employees. However, an information security culture that adopts values of knowledge, awareness and secure behaviour can minimise these incidents.

The study also identifies the role of four Omani national cultural values, (high power distance, high uncertainty avoidance and high collectivism level, and trust), in shaping information security. Accordingly, these effects of national culture on employee information security behaviours culture cannot be ignored in formulating information security policy. The study shows the importance of having effective information security policies, management support for, and involvement in, those policies, backed by information security training and awareness programs. Taken together these elements serve to moderate the influence of Omani national culture values on information security within the work environment, and the quality of information security performance and culture.

The next chapter concludes this thesis sets out the key finding in relation to the initial research objectives. The chapter will highlight the contributions of this study to the research field, as well as outlining the research limitations together with opportunities for further research in the future. The chapter will also present recommendations based on the findings and analysis.

Chapter 7. Conclusion

"Progress is impossible without change; and those who cannot change their minds cannot change anything."
— (George Bernard Shaw, 1944, p.330)

7.1. Introduction

Information has become a necessary resource in business transactions, and needs protection from unauthorised disclosure, modification, or destruction. The increased business use of information and communications technology (ICT), and its integration into nearly all areas of business have increased the potential risks to businesses of data breach (Al-Ahmad, 2013; Casey, 2012). Failure to protect business-critical information properly brings serious risk to business, and hence inadequate information security cannot be tolerated.

In recent years more and more organisations have realised that a significant proportion of threats to information security comes from within the organisation. It is hard to counter this problem with hardware or software alone, as it requires a more delicate and holistic approach bringing together people, processes and technology. Whilst technology itself is relatively objective in nature, the operating environment influences people and processes. Human behaviour has a substantial influence on information security culture and practice. Many academics argue that the human dimension in information security forms its weakest link. (Chia et al., 2003; Da Veiga & Eloff, 2009; Da Veiga. et al., 2007; Martins & Eloff, 2002; Maynard & Ruighaver, 2002; Schlienger & Teufel, 2003, 2005; van Niekerk & von Solms, 2005, 2006). Therefore, it is essential and inevitable for organisations to create a culture that enhances the effectiveness of information security.

A security culture needs to be established and maintained, with a focus on individual knowledge and understanding of information security, to ensure the safety of an organisation's data. That information security culture should be based on management commitment, support and endorsement of the organisations security policies, procedures, awareness and training programs. It may be a fact that no organisation can ever have one hundred percent information security. However, there are specific practices and rules that organisations can follow to maximize the protection of their critical information resources. Both management and employees should be educated

regularly, about the basics of an organisation's policies and any changes made. Management should also be kept up to date on the progress of both external and internal information security issues. This education should be practical, non-technical, and based on real life scenarios and examples to improve learning and understanding. When compliance problems arise, they should be investigated and resolved. The level of information security should also be measured, and any problem areas and issues pin-pointed, investigated and corrected in line with the organisation's information security policy.

This chapter, starts by reiterating the research problem, aim and questions, followed by general summaries of the key outcomes regarding the current state of information security culture and behaviour in Omani public organisations and the differences between public and private organisations. The chapter then summarises specific key outcomes related to the impact of critical socio-cultural and organisational factors on the development of information security culture in Omani organisations are summarised. The chapter includes recommendations to enhance information security culture and practices in Omani organisations. This is followed by highlighting both the contribution and limitations of this research. Finally, the last section of this chapter recommends future research areas arising from the analysis and outcomes of the thesis. There is a chapter summary.

7.2. Research Problem

The research problem addressed in the current study addresses ongoing concerns about the lack of information security culture in public organisations, leading to ineffective information security practices. To address the research problem, a survey questionnaire and open ended, semi-structured interviews were conducted in order to identify the critical socio-cultural and organisational success factors that influence the development and maintenance of information security culture in Omani organisations.

7.3. Research Aim and Questions

The aim of this research was to study and explore the current state of information security practices and behaviour in Omani public and private organisations and to investigate and identify the critical socio-cultural and organisational factors that may influence the development and maintenance of an information security culture, resulting in impaired employee attitudes and behaviours. The study also aimed to examine the difference between public and private organisations in Oman regarding information security practices and behaviour.

The following questions and sub questions were posed to address the research problem and achieve it's objectives.

RM-Question: What is the current state of information security culture and practices in public and private organisations in the context of Oman? What are the critical socio-cultural and organisational factors that may affect the information security performance and hinder the development and maintenance of an effective information security culture in these organisations?

The main research question was supplemented by the following sub-questions:

RS-Question#1: What is the current level of compliance with information security best practices in Omani organisations? What is the difference between public and private sector organisations in this regard?

RS-Question#2: What are employees' attitudes towards the role of rewards and punishment in motivating personnel to commit to good information security practices in Omani organisations?

RS-Question#3: How does the social factor "education" affect information security performance in Omani organisations?

RS-Question#4*:* What is the relationship between critical organisational factors and information security performance; and the development, and maintenance of an information security culture in Omani organisations?

RS-Question#5*:* What is the relationship between the development and maintenance of an information security culture, and information security disciplines and practices in Omani organisations?

RS-Question#6*:* What is the relationship between critical cultural factors and information security behaviours and practices; and the development, and maintenance of an information security culture in Omani organisations?

To achieve the objectives within the study, the second chapter details related academic work regarding aspects of information security in general and socio-cultural and organisational issues specifically. The detailed related fieldwork review enabled the researcher to clarify the critical socio-cultural and organisational factors influencing the successful development and maintenance of information security culture and practices in Omani public organisations.

The researcher adopted a mixed-method approach using a survey questionnaire and open-ended semi-structured interviews. The research findings identified from the qualitative and quantitative data analysis are consistent with the findings obtained from the related work reviewed in chapter two.

The results from this study suggest that six main socio-cultural and organisational factors have an impact on the successful implementation of information security culture in Omani public organisations.
These factors are:

- High power distance.
- High uncertainty avoidance.
- High Level of Collectivism.
- Lack of management support and commitment.
- Lack of information security policy.
- Lack of information security awareness and training.

There were another two factors, found influence the success of organisational information security culture:

- High Level of Trust.
- Failure to apply a rewards/punishment system.

The study has thus identified eight factors that have an impact on the success of organisational information security culture, as illustrated in the diagram below and in agreement with the findings in chapter two.

Figure 7-1: Research Interest Critical Socio-Cultural and Organisational factors that influenced the successful development of ISC in Omani public organisations.
Source: Self

7.4. Research Outcomes

The researcher believes that this study identifies the lack of an information security culture as the main issue challenging improvement in the information security behaviour and practices of Omani public organisations. Furthermore, the investigations show that managing the security related behaviour of employees is critical and highly complex. The results show that Omani public organisations need to conduct various levels of information security awareness and training programs for all staff to emphasise the importance of information security to their organisations. The results also indicate that the managers need to pay more attention to the information security officers in their organisations and provide them with support and authority as a means to improve the development of an information security culture.

The current study is one of the earliest to investigate the relationships between critical socio-cultural and organisational factors and information security culture, in the context of Oman. In addition, the study offers a set of best practice guidelines in information security management, which can be followed as a blueprint when implementing an effective information security management system. The study identifies the standing of information security in Omani public-sector organisations. It adds new scientific insight to studies of information security in Arab countries, particularly in Oman that will, hopefully, concentrate more attention on information security and change the way it is considered in public-sector organisations.

A synthesis bringing together the results derived from the in depth qualitative and qualitative analysis, the perspectives illustrated in the interviews and the related work review is set out below:

- ***Information Security Results in General:***
    - The analysis of the survey responses and the interviewees' answers indicate that, although there is a security department/security section in every organisation in Oman, the information security culture is inadequate for protecting the organisations information. Furthermore, the status of information security behaviour ranges between 'very weak' and 'good' in the public sector, and it ranges between 'weak' and 'very good' in the private sector.
    - Many Omani organisations have an information security policy, though how serious it is considered and the level of employee compliance with it varies. The analysis results show the level of Omani organisational compliance with

information security policy best practices is below average (40%); it is 31% in public-sector organisations and 60% in private-sector organisations.

- Managerial support of information security is lacking in Omani organisations. The analysis shows managerial support is below average (34%); it is 26% in public-sector organisations and 52% in private-sector organisations.
- The level of compliance of Omani organisations with the core best practice for information security procedures is average (48%); it is 45% in public-sector organisations and 56% in private-sector organisations.
- The efficiency of national bodies that are responsible for information security when performing their duties is slightly below average (46%); it is 50% in public-sector organisations and 37% in private-sector organisations.
- There is no relationship between employees' educational level and overall information security behaviour in Omani organisations.

- ***Information Security Results link to Related Work Review:***
  - The research identifies personnel behaviour in Oman as one of the main threats to information security and one of the main challenges to Omani public organisations. This means that Omani public organisations need to take the human element into account alongside technological solutions, as part of their strategy to protect the information.
  - There is a strong relationship between critical organisational factors. Top management support and involvement is considered an essential element for creating a security culture. (Chia et al., 2002; Schlienger & Teufel, 2002, 2003). Policy enforcement is also an essential factor in creating a security culture, (von Solms & S. von Solms, 2004; Vroom & von Solms, 2004), along with information security training and awareness. These three factors are strongly related to the successful development and maintenance of a culture of information security in Omani public organisations, because of their strong impact on employee behaviours.
  - The culture dimension, as conceptualised by Hofstede's three values of national culture (2001) (high power distance, high uncertainty avoidance and collectivism), has a strong impact on employee behaviour in Omani public organisations. These dimensions were investigated through qualitative interviews as part of the data collection process described in chapter five.

- The study also shows that most employees have high expectations and trust of each other, which can affect the security of information. For example, many users share passwords, or dictate their network passwords and office safe combinations during phone conversations.
- Because employees are committed to the prevailing culture of their society, their information security level is determined by regional culture factors, such as hierarchical management, friendship grouping, and fear of losing face. These all have strong impacts on their information security behaviour. Overall, the analysis shows that cultural dimensions have a fundamental influence on the employee security behaviours.
- There is a clear lack of information security awareness of roles and responsibilities, especially on how to detect and report threat and risk, and to whom the threats should be reported.

These points indicate that the situation of information security in Omani organisations, especially public-sector organisations, is unsatisfactory and that improvement requires hard work. This research suggests that there are the beginnings of a culture of information security in Omani organisations, albeit not very well understood or considered. Organisations only become aware of information security risks once they have been victims of attacks. Moreover, the situation in public-sector organisations is far worse than in the private sector. The level of information security ranges from 'very weak' to 'good' in the public sector, and between 'weak' and 'very good' in the private sector. This indication of a general information security divide between the two sectors, can be interpreted as one or all of: an awareness divide, an information security policy divide, a security culture divide, or a management commitment divide.

7.5. Research Final Remarks

This research suggests that a culture of information security does exist in Omani organisations, but either it is in the early stages of development, or it exists within a defective framework. Establishing an information security culture requires transformation and sustainability plans at organisational level, within which employees are the key element.

The key challenges to information security in Omani organisations, highlighted by this research are:

- Organisation managers must recognise and take account of the implications of digital transformation in raising the importance of information security. They

should recognise that compliance with information security is not simply a matter of regulations. A culture of security is required, which managers should generate or promote right across their organisations. They should also recognise that establishing an information security culture is not a short-term task, but a long-term challenge; two to five years is required to create information security habits and culture. Thus, patience and persistence are necessary.

- Organisations managers should recognise that information security culture is an organisational aspect and establishing an information security culture requires enforcement of instructions, employee training, education, awareness, time, money, and the joint participation of everyone in the organisation. In addition, Managers should be persistent in pursuit of information security policies regardless of the number of repetitions.
- Managers must work to convince employees engaging with the culture of information security in the organisation is useful. To accomplish this, managers must be willing to follow information security disciplines strictly, be patient when educating staff and raising awareness, and be committed to processes and not outcomes until knowledge is assimilated.
- Organisations must have a program with three pillars (training, education, and awareness) and have associated plans to establish an information security culture. This process requires a series of steps to convince and educate employees, such that their behaviour supports organisational security measures. In this regard, creating an environment in which employees can ask questions and receive answers about information security will promote the spread of an information security culture.
- Information security training should integrate consideration and understanding of ethical issues, to develop employee abilities to resolve moral conflicts in information security situations. This will help create an environment where employees can make personal choices that are consistent with information security best practice.
- Managers must ensure that information security officers receive adequate coaching to enable them to design appropriate communication strategies to deliver effective information security messages at all levels in an organisation as well as the competency to manage any information security issues that arise.
- Managers should design information security strategies that recognise the characteristics of social norms in Oman. For example, the high power distance value in Omani organisations might make it easy for managers to change

employee behaviours and habits in support of positive information security practice.

- Prevention, rather than reaction, is the most successful way to address information security threats. Therefore, employees must be empowered with the necessary skills and tools to make appropriate preventive decisions, and implement measures that support information security. This ability should be an indispensable organisational component.
- Finally, managers must be information-security oriented, and ready to invest time and resources into a planned, systematic program to carry out the necessary technological, cultural, and educational changes.

The next section presents a set of recommendations for Omani organisations based on the broad literature review, the results of the mixed-methods analysis and the researcher's own work experience. These recommendations target organisation executives, security officers and regulatory bodies in Oman. The recommendations reflect the current information security situation in Omani organisations. And they aim to help and guide the implementation of a culture of information security in those organisations. Furthermore, they will help organisations to assess their own current information security situation and decide whether it is satisfactory, or whether it needs improvement to enhance business performance.

An organisation must be clear about the security behaviours that it wishes to encourage among its employees before adopting any of the recommendations, by considering the following questions:

- What assets require protection?
- What security threats are currently facing the organisation?
- What level of exposure to security risk does the organisation face?
- What is the level of security risk is the organisation prepared to accept and/or challenge?
- What level of protective security is proportionate?

Once an organisation has considered these questions, managers will be in a more informed position to decide on the additional security behaviours required of its employees to complement existing physical and personnel measures.

7.6. Research Recommendations

The proposed recommendation framework set out below, provides a comprehensive foundation for organisations to develop effective information security and protection

for information assets. Adopting this framework in an organisation will have a positive impact on employee interaction with information assets, and help to guard against many of the information security threats that insiders pose.

Filkins (2014, p.6) defines an information security framework as "a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment". There are different types of information security frameworks, depending on the situation to which the framework is applied. However, most frameworks must cover a wide set of issues related to both technology and human behaviour to create a secure environment for information assets.

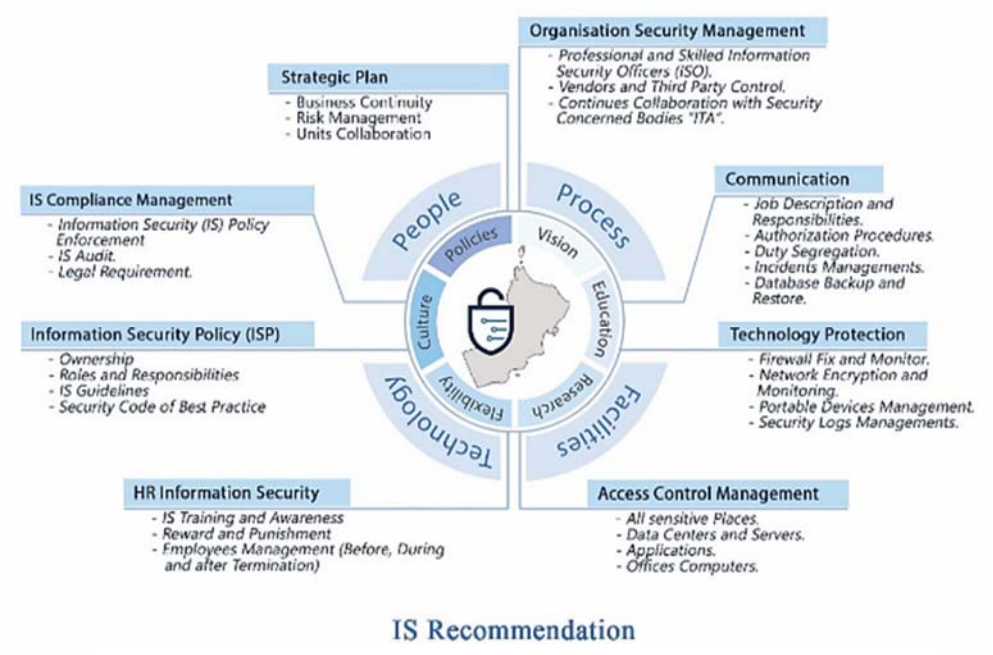

Figure 7-2: Research Information Security recommendations framework. Source: Self

The proposed framework can be used as a guide to improve employee behaviours, values, assumptions, and knowledge. The framework provides Omani public organisations with an objective mechanism to minimise data loss arising from internal security threats. The framework could also be used to assess the state of information security within an organisation. The author observed during the interviews that most Omani public and some private organisations contextualise information security as a technological problem. They lack a clear management methodology and a structured information security framework to help them reduce information security risks.

This model is for use by an organisation as the basis for its own more detailed and customised framework when it needs to enhance its information security situation. It provides Omani organisations with a road map for improvement by developing effective sustainable information security programs with defined policies and procedures, and

standardised management of information security. The framework also helps to define the accountability of managers and executives for organisation-wide information security. The framework reflects the perspectives of Omani public and private sector employees derived from their responses to the survey questionnaires and the interviews with information security and IT managers. It also complies with ISO / IEC 27002, which is a widely used, internationally recognised standard of best practice for information security.

7.6.1. Information Security Recommendations Framework Description

The proposed framework is comprised of the following seven elements that address key areas of information security management:

1. Information Security Strategy.
2. Information Security Management Compliance.
3. Information Security Policy.
4. Information Security and Organisational Control.
5. Information Security and Human Resources.
6. Information Security, Communications, and Operations Management.
7. Physical Aspects of Information Security.
8. Information Security and Access Control.

Each element is set out from the perspective of organisational infrastructure, referencing the four "pillars" of process, people, technology, and facilities. Each relationship in the framework is viewed from both managerial and operational perspectives. The term managerial refers to how work is organised (i.e. who performs which tasks), and how interpersonal interaction, such as management action, coordination, planning or motivation, will proceed. The term operational refers to how tasks are completed. Although there is some overlap between "managerial" and "operational", information security policy, organisational security management, and policy compliance are largely managerial, while the rest of the domains are operational.

An effective system of information security management requires an up-to-date information security policy; relevant documentation, regular risk management of current activities, and risk evaluation of planned changes. This can then form the basis of information security strategy and planning, so that the organisation can implement solutions to meet current information security requirements. Management systems regularly measure and assess the effectiveness and appropriateness of information security actions.

The essential components for successful implementation of information security programs in Omani organisations are described below.

A Clear Vision of Security in the Present and Future

A strategic plan is an essential part of defining clear organisation-wide security goals and explaining how to achieve them. A clear and concise strategic security plan allows executives, management, and employees to understand what they are trying to achieve, focus their efforts in the right direction, and recognize when they have accomplished their goals. Many organisations lack an up to date strategic security plan, and some claim to have a strategy when they do not. As a result, there is a lack of focus, and inconsistency of actions across the organisation. If organisations continue to view strategic planning as impractical or unnecessary, then they are less likely to manage information risk effectively.

A holistic approach to information security strategic planning is most effective. This requires the integration of the people, processes, and technology dimensions of information security, while ensuring that the plan is risk balanced and business based. Furthermore, it requires a clear alignment between business and IT strategies. Greater alignment and integration of strategic decisions makes it easier to meet expectations and perform tasks in a prioritised order. Organisations can reach their goals through having a clear vision desired outcomes, and clear analysis of the challenges to be overcome.

The plan must be comprehensive in scope, and integrate units inside the organisation and across different organisations. It should be divided into phases and the time period for each phase must be specified. Furthermore, the plan should include a definition of the techniques and procedures proposed to enhance the security culture of the organisation. Education and awareness programs should also be included in the plan. In summary, the strategic information security vision should include the following components:

- Clearly specified goals to achieve.
- Consistent and integrated methodologies for design, development, and implementation.
- Planned and dated implementation phases to achieve the specified goals.
- A dedicated mission delivery team with assigned timeframes for each phase.
- A dedicated team to monitor progress and to detect and resolve problems.
- Assigned roles and responsibilities for all team members and any other personnel brought in to help.

- Reduced delivery time from the solution concept through to implementation.
- The provision of flexible and adaptable architectures.
- Proactive decisions for efficient delivery of results.
- No redundant actions, so that objectives are more readily achieved.
- The planning and management of human resources (by relying on external expertise to augment internal staff when required).
- Employee education and awareness programs.
- Evolution into an organisation where security is integrated as seamlessly as possible with applications.
- Data, processes, and workflows in a unified environment.

Finally, the plan should be flexible where needed to remove obstacles to implementation. Organisations should put the elements of the plan into operation as soon as possible during the implementation process.

Compliance Management

Once organisations have established the parameters of information security in strategic planning, the next step is to devise appropriate security methods to ensure the full implementation of security standards. (Jose, 2005). Organisations usually apply audit and enforcement techniques to ensure compliance with security standards. As a result, the cost in time and money of security procedures should be justified as an internal business activity. The security compliance process should review technological, physical, and administrative practices. It should specify the security policies and procedures that are to be implemented. Security compliance should be integrated within existing security and business activities. It should identify how well business departments work together to ensure consistent harmonisation of information security practice. (Elephant, 2008).

The information security program must ensure that all system users understand and follow information security practices. Before any new security procedures are put in place, there should be a full risk assessment/risk analysis exercise. Compliance with information security requires a team effort that reaches from the highest levels of a hierarchy (usually the CEO or Board) to the lowest level (employees as end users). Making successful adjustments to a security framework relies heavily on the skill of organisational management and transparent operations.

To reduce compliance costs while strengthening security, organisations should automate much of their security processes, while maintaining continuous human monitoring. (Liberti, 2008). Compliance controls are a mixture of software-

programmed processes and human procedures. Integrating business process with information security compliance will reduce the cost of the compliance program.

Information Security Policy

Information security policy is primarily to provide employees with a clear understanding of the direction of management support for information security. In addition, information security policy safeguards the confidentiality, integrity, and availability of an organisation's assets; the privacy of employees; and protects the organisation as a whole from various threats and hazards. (Da Veiga et al., 2007).

The main reasons for an organisation to establish a security policy are to ensure a firm foundation for information security, to describe staff roles and responsibilities in protecting information assets, and to demonstrate the importance of securing the organisation's communications. It also provides a regulatory framework for acceptable and unacceptable behaviour, and it outlines what staff are and are not, allowed to do when using the organisation's resources. In other words, the authorised use policy helps to identify the behaviours that the organisation wants to reinforce as part of a security culture program, and it helps identify undesirable behaviours that the organisation wants to mitigate through the security culture program.

Information security policy will have direct consequences on the organisation's risk control budgets, including budgets for security culture and awareness campaigns. Consequently, information security policies are usually set out as living documents, which are revised and expanded over time. This type of document is particularly suited to information security policy in an environment of rapid technological, procedural, and business change. (Von Solms & Von Solms, 2004). It is the duty of the board to develop information security policy. They must ensure that security policies are aligned with the organisation's objectives. Successful information security policy is dependent on how appropriate it is to the business of the organisation. Equally, an effective security policy depends on the board's level of understanding of information security. The organisation's specific needs for, and importance of, information security are determined by its overall business objectives.

Establishing a security policy fully engages staff participation in the organisation's efforts to protect its information resources, and decreases the risk of a security breach caused by human error. According to Liang and Xue (2010), it is critical to understand the impact that an individual working in a socio-technical environment can have on the security of an information system. Socio-technical theory recognises two distinct yet

interrelated subsystems that operate in most organisations: a technical subsystem composed of equipment, techniques, and processes and a social system composed of employees and their skills, expertise, viewpoints, and principles (Bostrom et al., 2009).

The greatest barrier to the success of an information security policy is inadequate communication with employees, leaving users unaware of the policy, because it is too long or technical, or there is a disconnect between the policy and daily tasks. Therefore, an organisation's information security policy must be contained in a well-written document and communicated to all personnel concerned. Although every organisation's policy document is unique to its own business objectives, there are international standards, such as the ISO 27002, which offer a structural model of an organisation's policy document (Danchev, 2003; Wood, 2005).
Some general guidelines for ISP.

1. The organisation should have a strong and enforced information security policy.
2. The information security policy should be reviewed and updated periodically.
3. Employees should be educated about any updates in the security policy.
4. All employees should sign a hard copy of the information security policy.
5. Information security policies should apply to all members of the organisation, including managers at different levels.

Human Resources and Information Security

This domain aims to integrate information security into the HR processes for engaging and dismissing personnel. Evidence of the information security related background of potential employees should be included in HR recruitment processes. HR should also educate employees about the priority of preserving the confidentiality of information and set clear sanctions for security breaches. HR should be responsible for managing termination of employment where necessary. The features of this domain are as follows:

- ***Prior to employment*** organisations should conduct appropriate investigations into individuals' backgrounds to determine whether they have prior security related issues. Terms and conditions are included in the labour contract, and the responsibilities of employees regarding information security are established, acknowledged, and accepted.
- ***During employment*** employees should receive training and awareness programs and obtain reference materials on their security responsibilities, the acceptable use of information assets, and the sanctions imposed in the case of a policy breach. They should also be encouraged to respond proactively to

incidents and security flaws, and to provide clear and timely reports to management about failures or malfunctions.

- ***Contractors and third-party users*** should be made aware of their responsibilities to protect the confidentiality and security of the information and the system.
- ***Employment termination*** should involve the timely elimination of access rights and employees should return assigned assets before they leave or change their roles in an organisation.

Some further guidelines regarding human resources and information security are:

1. Security backgrounds should be investigated when recruiting new employees.
2. The organisation should conduct refresher programs on information security for employees.
3. The organisation should conduct adequate training programs on information security for all employees.
4. Employees should have training courses to become familiar with the importance of information security to the organisation.
5. Employees should be taught to become aware of information security as part of the shared beliefs of the organisation's members.
6. Employees should be taught the importance of coordination between the various departments in the organisation and cooperation with information security staff.
7. All access rights and network accounts should be removed on termination of employment.

Organisation Security Management

Information security must be included as part of organisational operating processes to ensure that its implementation. This requires cooperation between information security management, personnel responsible for information security, information system owners, and service providers. Furthermore, information security measures should be incorporated into business process planning from the outset.

This dimension includes elements in the business that promote the effective management of information security in an organisation. It sets out how to structure the information security office by reference to regulatory requirements. The components in this category relate specifically to the processes and structures of the information security function.

Below are some guidelines:

Features of an organisational information security Programme:

- Formal design of organisational information security, including its composition and reporting structures. (e.g. centralised or decentralised management of security)
- The roles, responsibilities, skills, experience, and resource levels committed to an organisation's security architecture. (McCarthy & Campbell 2001)
- Information security responsibilities within an organisation that should be allocated by reference to its information security policy.
- Clear and formal definition of the roles (i) of the information security officer, responsible for managing the information security and (ii) the network specialist who will ensure that the network is configured in a secure manner. The formal definition of these security roles will a clear statement of departmental hierarchy and authorities.
- A clear segregation of duties in order to prevent the unauthorised, unintentional use or intentional misuse of assets.
- Security process to prevent the risks associated with third-party access to an organisation's information system, and the appropriate controls to implement it. Trusted third parties are expected to protect the organisation's information to the same degree as internal employees.

- ***Legal and regulatory components involving compliance with legislation*:**
  - Different aspects of national and international legislation must inform information security policy.
  - Update the organisations knowledge of information security through contact with national information security bodies to receive guidance on implementing information security best practice and receiving periodic alerts regarding detection of new information security vulnerabilities and threats.

Communications and Operations Management

This domain links information security with the whole area of communications, which an organisation needs to plan carefully. The organisation should establish formal procedures and operational documents to define responsibilities and segregate mutually conflicting tasks. These procedures must consider incident management; network management; the use of external services; protection against malware; backup information; access to the system by external parties (e.g. suppliers, customers, public); the security of e-government; e-mail security; and desktop systems. Security

instructions should specify internal and external responsibilities, rights, and obligations regarding all of the above.

For internal communications and instructions, employees should be informed of the rules that apply to the use of private e-mail; any permitted activities that are not work related, and the consequences of unauthorised use. Successfully surviving a crisis is determined by how well an organisation has prepared for communications in a crisis. Successful communication is ensured by pre planning, establishing clearly specified communication channels, and holding crisis communication exercises in advance. There should be a clear division of roles between those responsible for communications and other contact personnel.
Some guidelines regarding communications and operations management:

- ***Responsibilities and operational procedures:*** The roles, responsibilities, and job descriptions of all staff across the organisation should be identified and clearly explained to the entire organisation. In addition, operational procedures, instructions for business processes and handling of errors, and restrictions on the system's use should be documented.
- ***Change management:*** Users should request changes to information security procedures. These should then be evaluated and approved by the department or area manager. A change log should be maintained. Back-up of essential information should be carried out before implementing any changes.
- ***Incident management:*** The process and related roles, responsibilities, and procedures for incident handling should be clearly defined. Procedures to notify any event or suspicious weakness that may affect the normal operation of information systems should also be defined. In addition, security events should be assessed according to their origin, destination, and time of occurrence, and specific actions taken according to their severity. Technological error log and operational problem logs should be maintained, including the personnel involved.
- ***Protection against malicious codes:*** Employees must know that they are prohibited from using personally owned desktops, laptops, flash drives, and other devices at work. Employees must also understand that installing or using software that is not authorised by the responsible information security officer is prohibited. In addition, anti-virus software should be installed and automatically update.
- ***Information and data backup:*** Back-up and restoration of data, operating systems, and utilities must be performed effectively and systematically in conformity with best practice procedures. Critical data and system back-ups guarantee their continuity, restoration, and recovery. Back-ups should be kept in different locations.

- ***Network management:*** All internal networks, for the sole use of the organisation's staff, together with any external networks that link the organisation with other organisations for data and document exchange, must be managed and monitored. Organisations must continuously ensure that the transmitted information is free from unauthorised access. In addition, only authorised personnel should have access to locations that house network equipment. Networks should be functionally subdivided, such that each department has access to a dedicated network segment. No employee can use more than one segment unless granted authorisation from the responsible security unit.
- ***Exchange information with third parties:*** The means used to transfer information should be defined, and information must be encrypted during transmission. Management should monitor and documents and data that are exchanged internally between units and externally between organisations.

Information Security and Access Control

This domain aims to control access to information systems, services, databases, and processing facilities by means of access restrictions and exceptions. This helps to secure information against unauthorised access and improper handling.

Below are some guidelines to implement this element:

- ***Business requirements and access control:*** Security requirements for each application and system in an organisation should be defined. Organisations must ensure compliance with laws and regulations, and access levels that are consistent with defined responsibilities. Furthermore, there should be simple business wide procedures to authorise access, and scheduled reviews and audits of access rights.
- ***Access Management:*** Each employee must have a unique ID. User access rights should be regularly reviewed to ensure that only optimally necessary access to information. In addition, organisations must verify that information and data networks are authorised by the responsible security manager. The number of employees with elevated privileges must be minimised to ensure appropriate service levels. Employees should modify sensitive data through an approved and controlled process.
- ***Network access control:*** Access to network resources should be limited to authorised users. Users should use external connections only if approved or carried out by responsible security managers. Moreover, all external connections to internal networks should only be allowed after being passed through an access

control point. There should be encrypted authentication mechanisms for both users and devices.

- ***Access control of mobile computing:*** The use of the organisation's equipment and connectivity to its networks must be limited to authorised employees only. Information created by employees on behalf of the organisation is the property of the organisation and must be stored on media that it owns. The organisation may examine equipment used by its employees regardless of ownership if circumstances merit an investigation. The responsible security manager must approve devices that are not owned by the organisation, but are connected to the organisation network. Devices should have virus protection software and the necessary operating security patches.
- ***Application and information access control:*** Applications should only permit access to authorised users and prohibit access to stored information unless via approved methods. A security event log and user activity should be maintained and monitored. Finally, responsible security managers must audit applications regularly to prevent security risks.

7.7. The Contribution of this Research

1. The findings of this study constitute a basis for Omani organisations to reform their information security programs, in the context of serious contemporary threats to information security. The study identifies the socio-cultural and organisational factors that are most critical to the development and maintenance of a culture of information security, and effective best practice.

2. Omani organisations can use this study to structure their assessment of information security and then to identify and mitigate major gaps in their current performance. In addition, the research findings can help managers to understand their critical areas of influence in order to protect information assets better.

3. To the best of my knowledge, this is the only study that investigates the current state of ISC in Omani organisations and identifies the critical socio-cultural and organisational factors that influence ISC. This mean the study also contributes to filling the gap caused by scarcity of research into information security behaviour in Oman.

4. The study provides practical recommendations for security specialists in Omani public organisations to structure information security processes more effectively. These recommendations are also suitable for other organisations in countries with similar environments to mitigate the effects of compromised information security.

5. Finally, researchers in Oman can utilize this study as a starting point for further research projects that approach different aspects of this subject that have not been addressed by other researchers. As the research unfolds, it is expected that the findings will help organisations everywhere to better understand and determine the steps that are needed to improve an organisation's information security.

7.8. Research Limitation

Research projects can often face restrictions which might limit their scope, conclusions and recommendations. The researcher sought, wherever possible, to minimise, if not eradicate, any such limitations which arose during the course of her research. However, as well as the significant contributions which the thesis makes to the field of study, it is necessary and appropriate to identify the research limitations, not least because these may form a fruitful basis for future research.

Limitations in the Research Background

1. An immediate obstacle was the lack of prior academic research into Omani organisations in general, and the critical socio-cultural influences on information security culture in particular. The researcher addressed this by a wide ranging review of the research literature, looking at issues around information security in different societies, as the basis for her initial research framework.
2. The analysis, within the thesis, of critical cultural influences relies primarily on the extensive work of Hofstede (2001), covering both national and organisational cultural values. The research therefore applies this general analysis to the specific case of Omani organisations, with the expectation that the values identified by Hofstede will have an influence on the culture of information security in the Omani context.
3. The researcher has practical experience of working in environments similar to the ones studied in the thesis. Although this has the advantage of giving the researcher a closer and deeper view of the subject, there is a risk to the total detachment and objectivity, which is essential in positivist research, as pointed out for example by Susman and Evered (1978).

Limitations arising from the Omani Context:

4. Research work in the public-sector is sensitive because it involves government services, especially when dealing with confidential issues of information security.

As a result some interviewees were not very open in their responses to some of the research questions. Notwithstanding the assurances given regarding the anonymity/confidentiality of respondents, their organisations and the data from questionnaires and interviews, some respondents remained concerned and/or sceptical. As a result, the researcher felt that in some cases, the respondents showed less willingness to disclose information which they perceived as sensitive. In some other cases the respondents were worried about potential consequences of replying, and so limited their answers to "Yes we do" or "I don't know" and skipped details. Where interviewees had to be coaxed into providing answers, the researcher some time used leading questions to elicit replies.

5. The interview stage was limited to senior managers. The researcher wished to use their extensive experience to explore the existing culture of information security in their organisations. However, it is possible that middle or entry level managers would have had different views on the same topics. To that extent those views are outside the scope of this research and therefore not accounted for.

6. The researcher attempted to obtain interview data mainly from managers with responsibility for information technology in general or information security in particular. However, this proved difficult to achieve in all cases and a number of managers apologised for their unavailability for different reasons. The interview stage was limited to fifteen interviewees from both public and private organisations in Oman.

7. Participants from public sector organisations outnumbered participants from private sector organisations, this reflect the size of the public sector in Oman.

Limitations within the Research Tools:

8. The questionnaire was lengthy, extending to 56 questions. Some participants may have lost interest, which might reduce the reliability of their answers.

9. The sample size of both interviews and questionnaires was relatively small: the interviews had 15 participants and there were 114 completed survey questionnaires.

10. The number of female participants is low in both interview and questionnaire research exercises.

11. Each individual response both in interviews and to questionnaires was directly influenced by a variety of specific circumstances including educational level,

regional origins, industry sector, and type of organisation. The impact of these limitations is heightened by the small sample number.

12. As explained in the methodology chapter, the number of participants is sufficient for the immediate purposes of this thesis. However, any future research should involve a larger sample in order to make the results more widely applicable and to give a more reliable overview of information security culture.

Limitations on the effectiveness of recommendations

13. The various factors that were critical in promoting or hindering the development of a culture of information security within organisations, were examined singly and separately from each other. No attempt was made to determine whether particular combinations of specific factors would be more effective in the success of an organization's information security culture.

14. The research concentrated on organisations within Oman. The conclusions are therefore limited to the experience within that one country. The results and the findings may be rather different in the context of the prevalent culture, traditions and types of government found in other countries. This could be tested by duplicating the research in other contexts, including both developing and developed nations.

15. In this study it was not possible to precisely measure the actual impact of the educational levels factor on the information security performance in Omani organisations. This was because the replies of respondents to questions relating to dependent variables were recorded in binary code (i.e. a simple yes/no). The variations in education level were more complex than yes/no.

    The impact of education level could be investigated in greater detail in future through the use of Likert's scale, with responses ranging from "strongly disagree" to "strongly agree". This would provide a more accurate regression analysis and accordingly improve the quality and accuracy of the results.

16. The study focused very much on issues and influencing factors, and therefore an examination of the technical side of security was outside the scope of this research. It is the firm belief of the researcher nonetheless, that technology must ultimately be accompanied by an appropriate behavioural response towards security to facilitate effective security management across the enterprise.

7.9. Future Research

The recommended future research areas that emerge from the analysis of the research outcomes are provided below:

1. Future research is required to benchmark the maturity of information security in different Omani organisations, to form conclusions about the impact of organisation type on information security.

2. The opinions provided by survey and interview participants may not reflect the opinions of their colleagues in the same organisations. In addition, the questionnaire was based on supposed information security best practices according to other studies. Thus, there may be other best practices from other studies that were not considered in the questionnaire. Similar studies with different personnel, and which consider other aspects of information, might provide a clearer view of information security in Oman.

3. Further research on the impact of other demographic characteristics apart from education, gender, and nationality should be conducted to gain better insight into information security in Oman.

4. Further research is required for a full understanding of the influence of rewards and punishment on information security culture and compliance, including the types of rewards and punishment that will influence different individuals.

5. Finally, it is advised that, given the lack of research in this field, the relationships between other organisational factors and the successful implementation of information security culture and employee information security behaviours requires greater study.

7. 10. Chapter Summary

Information security threats and the technologies used to combat them become more complex over time. Actions that can change attitudes towards information security should be addressed. Managers have the power to bring information security to the attention of all in an organisation. They should be held accountable for establishing a concrete information security strategy. This is an essential step toward setting attainable goals. A focus solely on technology is not a sufficient basis for strategy. A culture of information security should be the basis of strategy. This research focus is on the reasons for increased breaches in data security in Omani organisations generally public organisation specifically. These organisations hold a large amount of data, much of it

sensitive. As technology evolves, stored data becomes easier for most employees to access, which means that public sector organisations must take information security issues seriously to protect data and save their business.

To this effect, developing an information security culture is crucial to protecting the organisation from potential information security threats and breaches. The outcomes of this research indicate that Omani organisations are facing many challenges regarding the implementation of information security controls. This study shows that the aspects of information security best practice received less than 60% of 'yes' answers from the survey respondents, and must be improved.

No organisation can be 100% compliant with best practices or 100% risk free. Improving information security is a journey rather than a destination. Positive employee behaviours cannot be guaranteed in security situations, but it is possible to increase the chance of positive employee behaviour in potentially threatening information security situations, through adequate education and training strategies and by modelling good behaviour.

Organisations must have a triple programme of training, education, and awareness, linked to plans to establish a culture of information security. This process requires a series of steps to educate employees and convince them of the merits and necessity of organisational security measures. In this regard, creating an environment in which employees can ask questions, and receive answers, about information security, is helpful when spreading an information security culture. Above all mangers must show commitment to preserving the organisation from any security breaches, and protecting valuable information assets. Managers should promote a culture of valuing and protecting information through:

- Strong management leadership and commitment.
- Responsibility of everyone for protecting information.
- Extensive awareness, training, and education programs.

Furthermore, organisations must believe that:

- Information security is a business enabler that is crucial for the success of a business and its digital transformation.
- Information security should operate as a business process that is aligned with an organisation's business objectives.

- The emergence of information security threats cannot always be controlled, but whether organisations are prepared for them can be controlled, and the impact of most attacks can be mitigated in this way.
- Organisations should focus on the human aspects and emphasise education, awareness, and training programs.
- Organisations should focus on their information security officers.
- Organisations should address cyber security holistically using a risk-based approach.
- Organisations should ensure that spending on cyber security is strategically aligned with the overall business strategy.
- Organisations should improve visibility and focus on incident detection and response.
- Organisations must share threat intelligence with other organisations within the same sector (e.g., health, finance, and telecoms) and with other national organisations.
- Organisations should adhere to the policies, standards, and guidelines published by regulators (e.g. ITA and TRA) and other entities.

References

Addis, T. R., & Gooding, D. C. (2004). Simulation methods for an abductive system in science, In Magnani, L. (Eds.). MBR'04: Proceedings of the Fourth International Conference on Model- Based Reasoning, Pavia, Italy.

Afyouni, H. A. (2006). Database security and Auditing. Protecting Data Integrity and Accessibility, Thomson Course, Canada.

Ajzen, I. (1991). The theory of planned behavior. Organisational behavior and human decision processes, 50(2), 179-211.

Al-Arfaj, A. (2001). The perception of college students in Saudi Arabia towards distance web-based instruction. (Doctoral dissertation, Ohio University), Available from UMI. (3032949).

Alas, R. (2006). Ethics in countries with different cultural dimensions. Journal of Business Ethics, 69(3), 237-247.

Al-Ahmad, W., (2013). Addressing information security risks by adopting standards. International Journal of Information Security Science, 2(2), 28-43.

Alarifi, A., Tootell, H., & Hyland, P. (2012, June). A study of information security awareness and practices in Saudi Arabia. In Communications and Information Technology (ICCIT), 2012 International Conference on (pp. 6-12). IEEE.

Alavi, R., Islam, S. and Mouratidis, H. (2014), "A conceptual framework to analyze human factors of information security management system (ISMS) in Organisations", in Tryfonas, T. aAlbrechtsen, E. (2007). A qualitative study of users' view on information security. Computers & security, 26(4), 276-289.

AL-Azazi, S. (2008). Multi-layer model for e-government information security assessment, Cranfield University.

Al-Busaidy, M., & Weerakkody, V. (2009). E-government diffusion in Oman: a public sector employees' perspective. Transforming Government: People, Process and Policy, 3(4), 375-393.

AlFawaz, S., May, L. J., & Mohannak, K. (2008). E-government security in developing countries: A managerial conceptual framework.

AlFawaz, S., Nelson, K., & Mohannak, K. (2010). Information security culture: a behaviour compliance conceptual framework. In Proceedings of the Eighth Australasian Conference on Information Security-Volume 105 (pp. 47-55). Australian Computer Society, Inc.

AlGarni, K. (2015). Information Security Policy for E-government in Saudi Arabia: Effectiveness, Vulnerabilities and Threats. Rochester Institute of Technology.

Alhogail, A. (2015). Design and Validation of Information Security Culture Framework, Computers in Human Behavior, (49), 567-575.

Al-Hamadi, A. B., Budhwar, P. S., & Shipton, H. (2007). Management of human resource in Oman. International Journal of Human Resource Management, 18(1), 100-113.

AlHogail, A., & Mirza, A. (2014). Information security culture: a definition and a literature review. In proceedings of IEEE World Congress On Computer Applications and Information Systems. Hammamet, Tunisia.

Ali, A. J. (1996). Organisational development in the Arab world. Journal of Management Development, 15(5), 4-21.

Ali, A. J. (1993). Decision-making style, individualism, and attitudes toward risk of Arab executives. International Studies of Management & Organisation, 23(3), 53-73.

Ali, A. J., Taqi, A. A., & Krishnan, K. (1997). Individualism, collectivism, and decision styles of managers in Kuwait. The Journal of Social Psychology, 137(5), 629-637.

Ali, M., and Brooks, L. (2008). Culture and IS: National Cultural Dimensions within IS Discipline. In Proceedings of the 13th Annual Conference of the UK Academy for Information Systems. Bournemouth. UK. pp. 1-14.

Al-Izki, F., & Weir, G. R. (2016). Management attitudes toward information security in Omani public sector organisations. In Cybersecurity and Cyberforensics Conference (CCC), 2016 (pp. 107-112). IEEE.

Al Izki, F., & Weir, G. R. (2015). Gender Impact on Information Security in the Arab World. In International Conference on Global Security, Safety, and Sustainability (pp. 200-207). Springer, Cham.

Aliseda, A. (2005). The logic of abduction in the light of Peirce's pragmatism. Semiotica, 2005(153-1/4), 363-374.

Alkaabi, A., & Maple, C. (2012). Cultural impact on user authentication systems. International Journal of Business Continuity and Risk Management, 4(4), 323-343.

Alkahtani, A. (2018). Raising the Information Security Awareness Level in Saudi Arabian Organizations Through an Effective Culturally Aware Information Security Framework, Loughborough University Institutional Repository.

Al-Kalbani, A. (2017). A Compliance Based Framework for Information Security in E-Government in Oman. Australia.

Alkalbani, A., Deng, H., & Kam, B. (2014). A Conceptual Framework for Information Security in Public Organisations for E-Government Development. ACIS.

Allison, G.T. (2012). Public and Private Management: Are They Fundamentally Alike in All Unimportant Respects. In J. M. Shafritz & A. C. Hyde (eds.), Classics of Public Administration (17th edt). Boston: Wadsworth.

Al-Mukahal, H. M., & Alshare, K. (2015). An examination of factors that influence the number of information security policy violations in Qatari organisations. Information and Computer Security, 23(1), 102-118.

Alnatheer, M., Chan, T. & Nelson, K (2012). Understanding and Measuring Information Security Culture, Pacific Asia Conference on Information Systems, pp144.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2011). Information Security Policy Compliance: A User Acceptance Perspective.

Al-Ruzaiqi, S. S., & Baghdadi, Y. (2016). Government Approach to Integration in Oman. IT Professional, 18(4), 10-13.

Al-Shanfari, D.A. (2010). National Environment and High Potential New Ventures in Developing Countries, Unpublished PhD thesis, Deakin University, Australia.

Al-Tameem, A., Zairi, M., & Kamala, M. (2009). Critical factors of information security implementation. In Networked Digital Technologies, 2009. NDT'09. First International Conference on (pp. 379-385). IEEE.

Al-Thakhri, R. & REES, C. (2008). Organisational change strategies in the Arab region: A review of critical factors. Journal of Business Economics and Management, 9(2), 123-132.

Altman, Burton, N., Cuthill, I., Festing, M., Hutton, J., & Playle, L. (2006) . Why do a pilot study? National centre for the Replacement, Refinement and Reduction of Animals in Research. . Consulted 2.2.2011 http://www.nc3rs.org.uk/downloaddoc.asp?id=400

Atwater, L. E., Waldman, D. A., Carey, J. A., and Cartier, P. (2001). Recipient and observer reactions to discipline: Are managers experiencing wishful thinking? Journal of Organisational Behavior, 22(3):249–270.

Al-Yahya, K., Lubatkin, M., & Vengroff, R. (2009). The impact of culture on management and development: A comparative review. Dubai School of Government Working Paper, (09-01).

Alves, J. C., Lovelace, K. J., Manz, C. C., Matsypura, D., Toyasaki, F., & Ke, K. (2006). A cross-cultural perspective of self-leadership. Journal of Managerial Psychology, 21(4), 338-359.

Alvesson, M. (2013). Understanding Organisational Culture, 2nd ed. London: SAGE Publications.

Alvesson, M. (2002). Understanding Organisational Culture. London: SAGE Publications.

Ammann, F., & Sowa, A. (2013). Readability as lever for employees' compliance with information security policies. ISACA-J, 4, 39-42.

Amos, E. A., & Weathington, B. L. (2008). An analysis of the relation between employee-Organisation value congruence and employee attitudes. The journal of psychology, 142(6), 615-632.

Andress, J. (2014). Chapter 1 - What is Information Security? In J. Andress (Ed.), The Basics of Information Security (Second Edition) (pp. 1-22). Boston: Syngress.

Anderson, J. M. (2003). Why we need a new definition of information security. Computers & Security, 22(4), 308-313.

Anderson, R. (2001). Why information security is hard-an economic perspective. In Computer security applications conference, 2001. ACSAC 2001. proceedings 17th annual (pp. 358-365). IEEE.

Armstrong, C. P., & Sambamurthy, V. (1999). Information Technology Assimilation in Firms: The Influence of Senior Leadership and IT Infrastructures. Information Systems Research, 10(4), 304-327

Ary, D., Jacobs, L. C., Sorensen, C., & Walker, D. (2013). Introduction to research in education: Cengage Learning.

Ashkanasy, N., Wilderom, C. & Peterson, M. (2011). The Handbook of Organizational Culture and Climate, SAGE Publications, p650

At-Twaijri, M. I., & Al-Muhaiza, I. A. (1996). Hofstede's cultural dimensions in the GCC countries: An empirical investigation. International Journal of Value-Based Management, 9(2), 121-131.

Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. IEEE transactions on dependable and secure computing, 1(1), 11-33.

Aytes, K. & Connolly, T. (2004). Computer Security and Risky Computing Practices: A Rational Choice Perspective. Journal of Organisational and End User Computing (JOEUQ, Computing (JOEUC), 16(3), 22-40.

Babbie, E.R., Halley, F.S., & Zaino, J.S. (2007). Adventures in Social Research: Data Analysis Using SPSS 14.0 and 15.0 for Windows, 6th edn, International Student Edition, Sage Publications, Thousand Oaks, CA.

Babbie, E. R. (1998). Survey Research Methods (2nd ed.). Belmont, CA: Wadsworth Publishing Company.

Bakari, J. K. (2005). Towards A Holistic Approach for Managing ICT Security in Developing Countries: A Case Study Of Tanzania (Doctoral dissertation).

Bakari, J. K., Tarimo, C. N., Yngstrom, L., & Magnusson, C. (2005, July). State of ICT security management in the institutions of higher learning in developing countries: Tanzania case study. In Advanced Learning Technologies, 2005. ICALT 2005. Fifth IEEE International Conference On (pp. 1007-1011). IEEE.

Bandura, A. K. (1971). Social learning theory. Stanford University Press, Palo Alto, California.

Bandura, A. and Simon, K. M. (1977). The role of proximal intentions in self–regulation of refractory behavior. Cognitive Therapy and Research, 1(3):177–193.

Banks, E.(1999). Creating a knowledge culture . Work Study, 48(1), 18-20.

Barber, K. (2007). Tribal Ties Among Zanzabaris in Oman. Macalester Abroad: Research and Writing from Off-campus Study, 1(1), 4.

Barton, K.A., Tejay, G., Lane, M. & Terrell, S. 2016. Information system security commitment: A study of external influences on senior management. Computers & Security, 59, pp.9–25.

Barton, K. A. (2014). Information System Security Commitment: A Study of External Influences on Senior Management (Doctoral dissertation, Nova Southeastern University).

Bean, M. (2008). Human Error at the Center of IT Security Breaches. Available at: http://www.newhorizons.com/elevate/network%20defense%20contributed%20article.pdf.

Beck, B. E. F., & Moore, L. F. (1985). Linking the host culture to organisational variables. In Frost (Ed.), Organisational culture (pp. 335-354). Beverly Hills, Calif: Sage.

Becker, G. S. (1968). Crime and Punishment: An Economic Approach. Journal Of Political Economy, 76(2), 169-217.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. Information & Management. Advanced Online Publication. doi:10.1016/j.im.2017.01.003

Bell, E., Bryman, A., & Harley, B. (2018). Business research methods. Oxford university press.

Bess, D. (2009). Understanding information security culture for strategic use: a case study. AMCIS 2009 Proceedings, 219.

Bess, D., and Tejay, G. (2010). "Aligning Information Security Program Objectives and Deployment with Organisational Culture for Increased Success. " Proceedings

of the 41st Annual Meeting of the Decision Sciences Institute, San Diego, California, USA, November 20-23, 2010.

Bennett, T. M. (2009). A study of the management leadership style preferred by IT subordinates. Journal of Organisational Culture, Communication, and Conflict, 13(2), 1-25.

Benson, C. (2000a). Security Threats. Microsoft Corporation . Available Online at: http://www.microsoft.com/technet .

Berelson, B. (1952). Content Analysis in Communication Research. Glencoe, Ill.:Free Press.

Berg, B. L. (2004). Methods for the social sciences. Qualitative Research Methods for the Social Sciences. Boston: Pearson Education.

Berg-Cross, G. (2003). A pragmatic approach to discussing intelligence in systems. In Performance Metrics for Intelligent Systems Workshop (PerMIS) NIST in Gaithersburg, MD (pp. 16-18).

Bernard, H. Russell, ed. 1998 Handbook of Methods in Cultural Anthropology. Walnut Creek: AltaMira Press.

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. Computers & Security, 23(3), 253-264.

Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. Paper presented at the workshop on New security paradigms (pp. 47-58). ACM.

Bhattacherjee, A. (2012). Social science research: Principles, methods, and practices.

Bik, O. P. G. (2010). The behavior of assurance professionals: A cross-cultural perspective. Eburon Uitgeverij BV.

Bjerke, B., & Al-Meer, A. (1993). Culture′ s consequences: Management in Saudi Arabia. Leadership & Organisation Development Journal, 14(2), 30-35.

Blumstein, A. (1978). Introduction, A. Blumstein, J. Cohen, D. Nagin, Editors, Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates. National Academy of Sciences, Washington, DC

Bond, M. H. (1988). Finding universal dimensions of individual variation in multicultural studies of values: The Rokeach and Chinese value surveys. Journal of personality and social psychology, 55(6), 1009.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Quarterly, 39, 837-864. Retrieved from http://www.misq.org/

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. European Journal of Information Systems, 18(2), 151–164.

Boss, S., & Kirsch, L. (2007). The last line of defense: motivating employees to follow corporate security guidelines. Paper presented at the Proceedings of the 28th International Conference on Information Systems.

Bostrom, R. P., Gupta, S., & Thomas, D. (2009). A meta-theory for understanding information systems within sociotechnical systems. Journal of Management Information Systems. Journal of Management Information Systems, 26(1), 17-48.

Boyne, G. A. (2002). Public Private Management: What is the Difference? Journal of Management Studies, 39 (1), 97-122.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.

Brennan, L., Voros, J., & Brady, E. (2011). Paradigms at play and implications for validity in social marketing research. Journal of Social Marketing, 1(2), 100-119.

Brindley, C.S., & Ritchie, R.L. (2001). The information-risk conundrum. Marketing Intelligence and Planning, 19(1), 29-37.

Brislin, R. W. (1970). Back translation for cross-cultural research, Cross-Cultural Psychology, 1, 185–216

Britten, N. (1995). Qualitative research: qualitative interviews in medical research. Bmj, 311(6999), 251-253. Available Online at: http://www.bmj.com/content/311/6999/251.

Britto, T. D. (2011). Levantamento e diagnóstico de maturidade da governança da segurança da informação na administração direta federal brasileira.

Bruce, G. & Dempsey, R. (1997). Security in distributed computing – did you lock the door? Upper Saddle River, New Jersey : Prentice Hall.

Bryman, A. (2012). Social research methods. 4th Edn. Oxford university press.

Bryman, A. (2007). Barriers to integrating quantitative and qualitative research. Journal of mixed methods research, 1(1), 8-22.

Bryman, A., Becker, S., & Sempik, J. (2008). Quality criteria for quantitative,qualitative and mixed methods research: a view from social policy. InternationalJournal of Social Research Methodology, 11(4), 261-276.

Buchanan, D. A., & Bryman, A. (2007). Contextualizing methods choice inorganisational research. Organisational Research Methods, 10(3), 483-501.

Buchanan, D. & Huczynski, A. (2004). Organisational behaviour: An introductory text. Harlow, FT: Prentice-Hall.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), 523-548.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of information security awareness and perceived fairness in information security policy compliance. AMCIS 2009 Proceedings, 419.

Burns, R. (2002). Introduction to Research Methods. London: Sage

Burrell, G., & Morgan, G. (1979). Two dimensions: Four paradigms. Sociological paradigms and organisational analysis, 21-37.

Calder, A., & Watkins, S. (2008). IT governance: A manager's guide to data security and ISO 27001/ISO 27002. Kogan Page Ltd.

Cameron, K. S., & Quinn, R. E. (2005). Diagnosing and changing organisational culture: Based on the competing values framework. John Wiley & Sons.

Cameron, K. S., & Quinn, R. E. (1999). Diagnosing and changing organisational culture. Reading: Addison-Wesley.

Canavan, S. (2003). An information security policy development guide for large companies. SANS Institute.

Carr, L. T. (1994).The strengths and weaknesses of quantitative and qualitative research: what method for nursing?.Journal of Advanced Nursing, 20(4), 716-721.

Casey BM. Linking psychological attributes to smartphone addiction, face-to-face communication, present absence and social capital. Unpublished Master's thesis. The Chinese University of Hong Kong, Hong Kong, China, 2012.

Caudle, S. L., Gorr, W. L., & Newcomer, K. E. (1991). Key information systems management issues for the public sector. MIS quarterly, 15 (2), 171-188.

Chadwick, A. (2002). Socio-economic impacts: are they still the poor relations in UK environmental statements?. Journal of Environmental Planning and Management, 45(1), 3-24.

Chatman, J. A., Polzer, J. T., Barsade, S. G., & Neale, M. A. (1998). Being Different Yet Feeling Similar: The Influence of Demographic Composition and Organisational Culture on Work Processes and Outcomes. Administrative Science Quarterly, 43(4), 749-780.

Chang, S. E., Chen, S. Y., & Chen, C. Y. (2011). Exploring the relationships between IT capabilities and information security management. International Journal of Technology Management, 54(2/3), 147-166.

Chang, S. E., & Ho, C. B. (2006). Organisational factors to the effectiveness of implementing information security management. Industrial Management & Data Systems, 106 (3), 345-361.

Chen, Y., Ramamurthy, K., & Wen, K. (2015). Impacts of comprehensive information security programs on information security culture. The Journal of Computer Information Systems, 55(3), 11-19. doi:10.1080/08874417.2015.11645767

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organisations' information security policy compliance: Stick or carrot approach?. Journal of Management Information Systems, 29(3), 157-188.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organisations: An integrated model based on social control and deterrence theory. computers & security, 39, 447–459.

Cherdantseva Y. & Hilton J. (2012). A Reference Model of Information Assurance & Security. Proc. IEEE ARES 2013 SecOnt workshop, 2-6 September, 2013, Regensburg, at HYPERLINK "http://users.cs.cf.ac.uk/Y.V.Cherdantseva/RMIAS.pdf"

Chia, P. A., Maynard, S. B., & Ruighaver, A. B. (2002). Understanding organisational security culture. Proceedings of PACIS2002. Japan.

Choi, Y.S. (2001). An empirical study of factors affecting successful implementation of knowledge management. Unpublished academic dissertation. University of Nebraska.

Child, J. (1981). Culture, contingency, and capitalism in the cross national study of organisations. In LL, Cummings, & BM, Staw, (Eds.), Research in organisational behavior (Vol. 3), pp. 303-356.

Choudhry, R. M., Fang, D., & Mohamed, S. (2007). The nature of safety culture: A survey of the state-of-the-art. Safety science, 45(10), 993-1012.

Cialdini, R. B. (1984). How and why people agree to things. New York: Morrow

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: compliance and conformity. Annual Review of Psychology, 55(1), 591–621

Cialdini, R. B., Kallgren, C. A., & Reno, R. R. (1991). A focus theory of normative conduct: A theoretical refinement and reevaluation of the role of norms in human behavior. In Advances in experimental social psychology (Vol. 24, pp. 201-234). Academic Press.

Cialdini, R. B., Reno, R. R., & Kallgren, C. A. (1990). A Focus Theory of Normative Conduct: Recycling the Concept of Norms to Reduce Littering in Public Places. Journal of Personality and Social Psychology 58(6), 1015-1026.

Cohen, L., Manion, L., & Morrison, K. (2007). Research Methods in Education(6th ed.). New York: Routledge.

Conner, M., & Armitage, C. J. (1998). Extending the theory of planned behavior: A review and avenues for further research. Journal of applied social psychology, 28(15), 1429-1464.

Collins, J., Hussey, R., 2009. Business Research: a Practical Guide for Undergraduate and Postgraduate Students, 3rd ed. Palgrave Macmillan, Houndmills.

Collis, J. and Hussey, R. (2003). Business Research: A Practical Guide for Undergraduate and Postgraduate Students, Palgrave Macmillan, Houndmills, Basingstoke, Hampshire.

Cooper, C. R., & Schindler, P. S. (2011). Business Research Methods (11thed.). NewYork: McGraw-Hill.

Corriss, L. (2010). Information security governance: Integrating security into the organisational culture. In Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies (pp. 35-41). ACM.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. International journal of human-computer studies, 58(6), 737-758.

Creswell, J. W. (2014). Research Design. Qualitataive, Quantiative and Mixed Methods Approaches. (4th ed.). Lincoln: Sage Publications Ltd.

Creswell, J. W. (2013). Qualitative inquiry and research design: Choosing among five approaches (3rd ed.). Thousand Oaks, CA: Sage.

Creswell, J. W. (2012). Qualitative inquiry and research design: Choosing among five approaches: Thousand Oaks, CA: Sage Publications.

Creswell, J. W. (2009). Research design: Qualitative, quantitative, and mixed methodsapproaches (3rd ed.). Thousand Oaks, CA: Sage.

Creswell, J. W. (2003). Research Design: Qualitative, Quantitative and Mixed Methods Approaches (2nd ed.). London: Sage Publications Ltd.

Creswell, J.W., & Plano Clark, V.L. (2011). *Designing and conducting mixed methods research* (2nd ed.). Los Angeles, CA: Sage.

Creswell, J. W., & Plano Clark, V. L. (2007). Designing and conducting mixed methodsresearch. Thousand Oaks: CA, Sage.

Crotty, M. (2003). The foundations of social research: Meaning and perspective in theresearch process. London, UK: Sage.

Crotty, M. (1998). The foundations of social research: Meaning and perspective in the research process. Sage.

Daft, R. L. (2001). Essentials of Organisation Theory and Design (2nd ed). Cincinnati: South-Western.

Dahl, S. (2004). Intercultural Research: The Current State of Knowledge. Middlesex University Discussion Paper, 26, 1-22.

Dahl R.A. and Lindblom C. E., (1953). Politics, Economics, and Welfare, New York.

Danchev, D. (2003). Building and implementing a successful information security policy. Available online at: www. windowsecurity. com.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. Information Management & Comp Security, 22(5), 474–489.

D'Arcy, J., and Hovav, A. 2007. "Deterring internal information systems misuse," Communications of the ACM (50:10), pp. 113-117.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses tostressful information security requirements: A coping perspective. Journal of Management Information Systems, 31(2), 285-318.

D'Arcy, J., Havav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79–98.

Da Veiga, A. & Martins, N. (2015). Improving the Information Security Culture through Monitoring and Implementation Actions Illustrated through a Case Study, Computers & Security, vol. 49, p. 16

Da Veiga, A., & Martins, N. (2015b). Information security culture and information protection culture: A validated assessment instrument. Computer Law & Security Review, 31(2), 243-256.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196-207.

Da Veiga, A., Martins, N., & Eloff, J. H. (2007). Information security culture: Validation of an assessment instrument. Southern African Business Review, 11(1), 147-166.

David, J. (2002). Policy enforcement in the workplace. Computers & Security, 21(6), 506-513.

Daymon, C., & Holloway, I. (2002). Qualitative Research Methods in Public Relationsand Marketing Communications. New York: Routledge.

Deal, T. E., & Kennedy, A. A. (1982). Corporate cultures: The rites and rituals of organisational life. Reading/T. Deal, A. Kennedy.–Mass: Addison-Wesley, 2, 98-103.

Dedoussis, E. (2004). A cross-cultural comparison of organisational culture: evidence from universities in the Arab world and Japan. Cross Cultural Management: An International Journal, 11(1), 15-34.

Delone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: a ten-year update. Journal of management information systems, 19(4), 9-30.

Denison, D. R. (1996). What is the difference between organisational culture and organisational climate? A native's point of view on a decade of paradigm wars. Academy of management review, 21(3), 619-654.

Denison, D. R. (1990). Corporate culture and organisational effectiveness. Oxford:John Wiley & Sons.

Denscombe, M. (2014) The Good Research Guide Open University Press, Chapter 13 &15

Denzin, N. K. (2000). Aesthetics and the practices of qualitative inquiry. Qualitative inquiry, 6(2), 256-265.

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2005a). The Sage handbook of qualitative research (3rd ed.). Thousand Oaks, CA: Sage.

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2011). The SAGE handbook of qualitative research (4th ed.). London, England: SAGE

Deshpande, R., & Webster, F. E. (1989). Organisational Culture and Marketing: Defining the Research Agenda. Journal of Marketing, 53(1), 3-15.

De Villiers, M. R. (2005). Interpretive research models for Informatics: action research, grounded theory, and the family of design-and development research. Alternation, 12(2), 10-52.

Dhillon, G. (1995). Interpreting the Management of Information Systems Security. London, London School of Economics and Political Science.

Dhillon, G. (1997). Managing Information Systems Security. Macmillan Press. London.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organisations. Information Systems Journal, 16(3), 293-314.

DiMaggio, P., Hargittai, E., Celeste, C., & Shafer, S. (2004). From unequal access to differentiated use: A literature review and agenda for research on digital inequality. Social inequality, 355-400.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. Journal of the Association for Information Systems, 8(7), 386.

Doherty, N.F. & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan, Computers & Security, 25(1): 55-63.

Doherty, N. F., Ashurst, C., & Peppard, J. (2012). Factors affecting the successful realisation of benefits from systems development projects: findings from three case studies. Journal of Information Technology, 27(1), 1-16.

Doyle, L., Brady, A. M., & Byrne, G. (2009). An overview of mixed methods research. Journal of Research in Nursing, 14(2), 175-185.

Drennan, D. (1992). Transforming company culture. Berkshire, England: MacGraw-Hill.

Drucker, P. F. (1954). The Practice of Management. New York: Harper & Row Inc.

Dudovskiy, J. (2016). The Ultimate Guide to Writing a Dissertation in Business Studies: A Step-by-Step Assistance. Pittsburgh, USA.

Dunkerley, K. D., & Tejay, G. (2011). A confirmatory analysis of information systems security success factors. In System Sciences (HICSS), 2011 44th Hawaii International Conference on (pp. 1-10). IEEE.

Durgin, M. (2007). Understanding the importance of and implementing internal security measures. SANS Institute Reading Room (https://www2. sans. org/reading_room/whitepapers/policyissues/1901. php).

Dutta, A., & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. California Management Review, 45(1), 67-87.

Dutta, A. & Roy, R. (2008). Dynamics of organisational information Security. In: System Dynamics Review, 24(3), 349-375.

Easterby-Smith, M., Thorpe, R., & Lowe, A. (2002). Management Research: An introduction. London: Sage

Eisenhardt, K. M. (1989). Building theories from case study research. Academy of Management Review, 14(4), 532-550.

Elashmawi, F. (1993), Multicultural Management. New Skills for Global Success, Gulf Publishing Company, Houston, TX.

Eldabi, T., Irani, Z., Paul, R. J., & Love, P. E. (2002). Quantitative and Qualitative Decision-Making methods in simulation modelling. Management Decision, 40(1), 64-73.

Elephant, P. (2008). IT service management tools: compatibility considerations. January Whitepaper, 1-11.

Ellen Taylor- Powell (1989), Analyzing quantitative data. Available at: HYPERLINK "http://learningstore.uwex.edu/assets/pdfs/g3658-6.pdf"

Eloff, J. H. P., & Eloff, M. M. (2005). Information security architecture. Computer Fraud & Security, 2005(11), 10-16.

Eloff, M. M., & Von Solms, S. H. (2000). Information security management: an approach to combine process certification and product evaluation. Computers & Security, 19(8), 698-709.

Ernest Chang, S., & Lin, C. S. (2007). Exploring organisational culture for information security management. Industrial Management & Data Systems, 107(3), 438-458.

Esposito, J., (1991). Islam: the strait path. Oxford: Oxford University Press.

Fagerström, A. (2013). Creating, maintaining and managing an information security culture. Arcada University of Applied Sciences.

Fang, T. (2003). A critique of Hofstede's fifth national culture dimension. Cross Cultural Management. 3(3). 347-68.

Ferrari, E. & Thuraisingham, B. (2006). Web and Information Security, IRM Press, United States of America.

Filkins, B. (2014, December). New Threats Drive Improved Practices: State of Cybersecurity in Health Care Organisations. Retrieved January 14, 2015, from https://www.sans.org/reading-room/whitepapers/analyst/threats-drive-improvedpractices-state-cybersecurity-health-care-Organisations-35652.

Fink, A. (1995). The Survey Handbook (Vol. 1). Thousand Oaks, CA: SAGE Publications.

Fitzgerald, T. (2007). Building management commitment through security councils, or security council critical success factors. Information Security Management Handbook, 105-121.

Fitzgerald, B., & Howcroft, D. (1998). Towards dissolution of the IS research debate: from polarization to polarity. Journal of Information Technology, 13(4), 313-326.

Fraenkel, J. R., & Wallen, N. E. (2008). Introduction to qualitative research. How to Design and Evaluate Research in Education, 7th ed. Boston, MA: McGraw-Hill International Edition.

Freeman, E. H. (2007). Holistic information security: Iso 27001 and due care. Information Systems Security(16), 291-294.

Fryer, K. J., Antony, J., & Douglas, A. (2007). Critical success factors of continuous improvement in the public sector: a literature review and some key findings. The TQM Magazine, 19(5), 497-517.

Fumudoh, S., & Viswanathan, U. (2014). Exploring the Relationship between Online Privacy on Cyber Security.

Furnell, S. M., Dowland, P. S., Illingworth, H. M., & Reynolds, P. L. (2000). Authentication and supervision: A survey of user attitudes. Computers & Security, 19(6), 529-539.

Furnell, S., & Thomson, K. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. Computer Fraud & Security, 2009(2), 5–10.

Gagné, M., & Deci, E. L. (2005). Self-determination theory and work motivation. Journal of Organisational behavior, 26(4), 331-362.

Garrison, C. P., & Ncube, M. (2011). A longitudinal analysis of data breaches. Information Management & Computer Security, 19(4), 216-230.

Gaunt, N. (2000). Practical approaches to creating a security culture. International Journal of Medical Informatics, 60(2), 151-157.

Geertz, C. (1973). The interpretation of cultures (Vol. 5019). Basic books.

Geertz, C. (1966). Person, Time, and Conduct in Bali: An Essay in Cultural Analysis. Cultural Report Series No. 14. Southeast Asia Studies, Yale University.

Gerber, M., & von Solms, R. (2005). Management of risk in the information age. Computers & Security 24, 16-30.

Gerber, M., & von Solms, R. (2001). From Risk Analysis to Security Requirements. Computers & Security, 20 (7), 577-584.

Ghernaouti-Helie, S. (2008). From risk management to information security policies and practices. Amulti perspective framework for ICT Security Effectiveness, ITU-T, at http://www.itu.int/dms_pub/itu-t/oth/15/05/T15050000030001PDFE.pdf

Gibbert, M., Ruigrok, W., & Wicki, B. (2008). What passes as a rigorous case study?. Strategic Management Journal, 29(13), 1465-1474.

Gill, J., Johnson, P., & Clark, M. (2010). Research methods for managers (4th ed.). London: Sage Publications Ltd.

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. British dental journal, 204(6), 291-295.

Glesne, C., & Peshkin, A. (1992). Becoming qualitative researchers: An introduction. White Plains, NY: Longman.

Granneman, J. (2013). IT security frameworks and standards: Choosing the right one. TechTarget.

Gragg, D. (2002). A multi-level defense against social engineering. White paper, SANS Institute, Retrieved on June

Graziano, A.M., & Raulin, M. L. (1997). Research Methods. A process of Inquiry. 3rd ed. Addison-Wesley.

Greene, S. S. (2014). Security Program and Policies: Principles and Practices. Pearson Education.

Gregory, K. L. (1983). Native-view paradigms: Multiple cultures and culture conflicts in organisations. Administrative science quarterly, 359-376.

Groves, R. M., Fowler Jr, F. J., Couper, M. P., Lepkowski, J. M., Singer, E., & Tourangeau, R. (2004). Survey methodology (Vol. 561). John Wiley & Sons.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. Handbook of qualitative research, 2(163-194), 105.

Guo, K. H., & Yuan, Y. (2012). The effects of multilevel sanctions on information security violations: A mediating model. Information & Management, 49(6), 320-326.

Gustave Flaubert Quotes. (n.d.). BrainyQuote.com. Retrieved July 22, 2018, from BrainyQuote.com Web site: https://www.brainyquote.com/quotes/gustave_flaube

Haddad, Y. Y. & Esposito, J. L. (1998). Islam, gender and social change, Oxford University Press, USA.

Hadnagy, C. (2010). Social engineering: The art of human hacking. John Wiley & Sons.

Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organisational information security measures. Information Management & Computer Security, 16(4), 377-397.

Hall, E. (1990). Understanding Cultural Difference, Intercultural Press, Yarmouth, Maine.

Hall, E.T. (1959). The Silent Language. Garden City. NY .Anchor Books,.

Hall, J. H., Sarkani, S., & Mazzuchi, T. A. (2011). Impacts of organisational capabilities in information security. Information management & computer security, 19(3), 155-176.

Hambrick, D. C. (2007). Upper echelons theory: An update. Academy of management review, 32(2), 334-343.

Haneef, S. (1979). What everyone should know about Islam and Muslims. Chicago: Kazi Publication.

Hare, C. (2002). Policy Development. In H. F. Tipton & M. Krause (Eds.), Information Security Management Handbook. New York. Auerbach Publications. 4(3), 353-383.

Harl. (1997), People Hacking the Psychology of Social Engineering, Text of Harl's Ta lk at http://www.noblit.com/docs/peoplehacking.pdf .

Harris, S. (2013). Access Control. In CISSP Exam Guide (6th ed., pp. 97, 98, 157- 277). USA McGraw-Hill;

Harris, P. R., & Moran, R. T. (1996). Managing Cultural Differences, 4th ed, Gulf Publishing Company. Texas.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. Management Information Systems Quarterly, 20(3), 257–278.

Hausman, C. R. (1993) Charles S. Pierce's Evolutionary Philosophy, USA: Cambridge University Press.

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. Information Management & Computer Security, 21(4), 266-287.

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. The Journal of Strategic Information Systems, 20(4), 373-384.

Heiser, J. G. (2004). The regulation of information security. Intermedia, 32(2), 29-30.

Herath, T., Herath, H., & Bremser, W. G. (2010). Balanced scorecard implementation of security strategies: a framework for IT security performance management. Information Systems Management, 27(1), 72-81.

Herath, T. & Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations, European Journal of Information Systems, 18 (2), 106-125

Herath, T., & Rao, H. R. (2009b). Encouraging information security behaviors in organisations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165.

Herold, R. (2011). Managing an information security and privacy awareness and training program. 2nd ed. Boca Rotan. CRC press.

Hoffer, J. and Straub, D. W. (1989). The 9 to 5 underground: Are you policing computer crimes? Sloan Management Review, 30(4):35–43.

Hofstede, G. (2005). Cultures and organisations: Software of the mind. McGraw-Hill Publishing Co.

Hofstede, G. (2001). Culture's consequences: comparing values, behaviours, institutions, and organisations across nations. London: Sage Publications.

Hofstede, G. (1997), Cultures and Organisations: Software o f the Mind. New York: McGraw-Hill.

Hofstede, G. (1994). Value Survey Model (VSM). Available at: http://stuwww.uvt.nl/~csmeets/~1st-VSM.html.

Hofstede, G. (1991). Cultures and organisations: Software of the mind. New York: McGraw-Hill.

Hofstede, G. (1984). Culture's consequences: International differences in work-related values (Vol. 5). Newbury Park, Calif: Sage Publications.

Hofstede, G. (1980). Culture's consequences: International differences in work-related values. Thousand Oaks, CA: Sage.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). Cultures and organisations: Software of the mind (3rd ed.). New York: McGraw-Hill.

Hofstede, G., & Bond, M. H. (1988). The Confucius connection: From cultural roots to economic growth. Organisational dynamics, 16(4), 5-21.

Hofstede, G., & Minkov, M. (2010). Cultures and Organisations: Software of the Mind (Rev. 3rd ed.). New York: McGraw-Hill.

Hooijberg, R. & Choi, J. (2001). The impact of Organisational Characteristics on Leadership Effectiveness Model: An Examination of Leadership in a Private and a Public Sector Organisation. Adminitration and Society, 33(4), 403-431.

House, R. J., Hanges, P. J., Javidan, M., Dorfman, P. W., & Gupta, V. (2004). Culture, Leadership and Organisations: The GLOBE Study of 62 Nations. Thousand Oaks, CA: Sage.

Howard, P. D. (2003). The Security Policy Life Cycle: Functions and Responsibilities, Information Security Management Handbook, Edited by Tipton & Krause.

Howard, J. D. (1997). An Analysis of Security Incidents on the Internet 1989 - 1995. Ph.D. Thesis, Carnegie Mellon University. Available Online at: http://www.cert.org/research/JHThesis/Start.html.

Hvidman, U., & Andersen, S. C. (2013). Impact of performance management in public and private organisations. Journal of Public Administration Research and Theory, 24(1), 35-58.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organisational Culture, Decision Sciences, 43 (4), 615-659

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2007) The role of external and internal influences on information system security - a neo-institutional perspective, Journal of Strategic Information System, 16(2), 153-172.

Humphreys, E. J., Moses, R. H., & Plate, A. E. (1998). Guide to risk assessment and risk management. British Standards Institution. Available Online at: HYPERLINK "http://shop.bsigroup.com/en/ProductDetail/?pid=000000000001408924"

Hussey, J. & Hussey, R. (1997). Business research: a practical guide for undergraduate and postgraduate students. Basingstoke: Macmillan.

Hutchings, K., & Weir, D. (2006). Understanding networking in China and the Arab World: Lessons for international managers. Journal of European Industrial Training, 30(4), 272-290.

Hayes, B., Bonner, A., & Douglas, C. (2013). An introduction to mixed methods research for nephrology nurses. Renal Society of Australasia Journal, 9(1), 8-14.

Ilvonen, I. (2011, July). Information Security Culture or Information Safety Culture-What do Words Convey?. In European Conference on Cyber Warfare and Security (p. 148). Academic Conferences International Limited.

Ikonen, M., & Savolainen, T. (2013). Does it enhance human resource management? A narrative approach to trust development in work relationships. In Proceedings of the International Conference on Management, Leadership and Governance (pp. 174-178).

ISACA. 2012. COBIT 5 for Information Security. Available: https://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf .ISO/IEC 27000:2014. (2014). International standard. Information technology - Security techniques Information security management systems - Overview and vocabulary. Haettu 28.4.2014 osoitteesta HYPERLINK "http://www.iso27001security.com/html/27000.html"

ISO/IEC 17799 (BS 7799-1) (2005). Information technology. Security techniques. Code of practice for information security management, Britain.

ISO/IEC 27001 (BS 7799-2) (2005). Information technology. Security techniques. Information security management systems—requirements, Britain

ITA- Information Technology Authority. "Annual Report 2015." 2015.

Jacobsen, D. I. (2002). Vad, hur och varför: Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen. Studentlitteratur, Lund Sverige.

Jasim, A. (1978). Mohammed: Al-Haqqaha Al-Kubra (Mohammed: The Greatest Truth). Dar Al-Andalas, Beirut.

Jermier, J. M., Slocum Jr, J. W., Fry, L. W., & Gaines, J. (1991). Organisational subcultures in a soft bureaucracy: Resistance behind the myth and facade of an official culture. Organisation science, 2(2), 170-194.

Johan, V. N., & Rossouw, V. S. (2006). Organisational learning models for information security. reviewed at http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/043.pdf.

Johanson, G. A., & Brooks, G. P. (2010). Initial scale development: sample size for pilot studies. Educational and Psychological Measurement, 70(3), 394-400.

Johansson, J., & Mattsson, L. G. (1987). Interorganisational relations in industrial systems: a network approach compared with the transaction-cost approach. International Studies of Management and Organisation, 17(1), 34-48.

Johansson, J., & Riley, S. (2005). Protect Your Windows Network from Perimeter to Data. Upper Saddle River, NJ: Addison Wesley.

Johnson, R. B. (1997). Examining the validity structure of qualitative research. Education, 118(2), 282-292.

Johnson, R. B., & Christensen, L. B. (2004). Educational research: Quantitative, qualitative, and mixed approaches. Boston, MA: Allyn and Bacon

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. Educational researcher, 33(7), 14-26.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. MIS quarterly, 549-566.

Joia, L. A. (2003). Key success factors for electronic interorganisational co-operation between government agencies. Proceedings of the 4th IFIP International Work ning Conference on Knowledge Management in Electronic Government, M.A. Wimmer (Ed.), Proceedings (Vol. 2645, p. 76). Springer.

Jones, P., Simmons, G., Packham, G., Beynon-Davies, P., & Pickernell, D. (2014). An exploration of the attitudes and strategic responses of sole- proprietor microenterprises in adopting information and communication technology. International Small Business Journal, 32, 285-306.

Jonsen, K., & Jehn, K. A. (2009). Using triangulation to validate themes in qualitative studies. Qualitative Research in Organisations and Management: An International Journal, 4(2), 123-150.

José, A., (2005). Security Metrics and Measurements for IT. The European Journal for the Informatics Professional, 6(4).

Jung, J., Su, X., Baeza, M., & Hong, S. (2008). The effect of organisational culture stemming from national culture towards quality management deployment. The TQM Journal, 20(6), 622-635.

Jung, T., Scott, T., Davies, H. T., Bower, P., Whalley, D., McNally, R., & Mannion, R. (2007). Instruments for the exploration of organisational culture. National Health Service, UK, 67-367.

Jung, J. Y., Qiu, J. L., & Kim, Y. C. (2001). Internet connectedness and inequality: Beyond the "divide". Communication Research, 28(4), 507-535.

Kainda, R., Flechais, I., & Roscoe, A. (2010). Information Security Theory and Practice. Security and Privacy of Pervasive Systems and Smart Devices, volume 6033 of WISTP 2010. Lecture Notes in Computer Sciences, chapter Secure and Usable Out-Of-Band Channels for Ad hoc Mobile Device Interactions, 308-315.

Kajava, J., Anttila, J., Varonen, R., Savola, R., & Roning, J. (2006, November). Senior executives commitment to information security-from motivation to responsibility. In Computational Intelligence and Security, 2006 International Conference on (Vol. 2, pp. 1519-1522). IEEE.

Kalliath, T. J., Bluedorn, A. C., & Strube, M. J. (1999). A test of value congruence effects. Journal of Organisational Behavior, 20(7),1175-1198.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. International journal of information management, 23(2), 139-154.

Kaplan, R. (2007). A matter of trust. Information Security Management Handbook,, 295-310.

Kaplan, B., & Duchon, D. (1988). Combining qualitative and quantitative methods in information systems research: a case study. MIS quarterly, 571-586.

Kark, K., Stamp, P., Penn, J., Koetzle, L., & Mulligan, J. A. (2007). Defining A High-Level Security Framework. Putting Basic Security Principles To Work. Forrester Research, Cambridge.

Karlsson, F., Goldkuhl, G., & Hedström, K. (2015). Practice-based discourse analysis of InfoSec policies. In IFIP International Information Security Conference (pp. 297-310). Springer, Cham.

Katz, F. H. (2005). The effect of a university information security survey on instruction methods in information security. In Proceedings of the 2nd annual conference on Information security curriculum development (pp. 43-48). ACM.

Kayworth, T., & Whitten, D. (2010). Effective Information Security Requires a Balance of Social and Technology Factors. MIS Quartely Executive. 9(3), 303–15.

Khalfan, A. M. (2004). Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. International Journal of Information Management, 24(1), 29-42.

Kilmann, R.H. (1985). Managing your organisation's culture. The Nonprofit World Report, 3(2), 12-15.

Kirk, J., & Miller, M. L. (1986). Reliability and validity in qualitative research. Newbury, CA: Sage.

Knapp, K. J., Morris Jr, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organisational-level process model. Computers & Security, 28(7), 493-508.

Knapp, K. J., Marshall, T. E., Kelly Rainer, R., & Nelson Ford, F. (2006). Information security: management's effect on culture and policy. Information Management & Computer Security, 14(1), 24-36.

Kolkowska, E. (2011). Security subculture in an organisation – Exploring value conflicts. Proceedings of the 19th European Conference on Information Systems – ICT and Sustainable Service Development, Helsinki, Finland. Available Online at: http://aisel.aisnet.org/ecis2011/237.

Kolkowska, E., & Dhillon, G. (2013). Organisational power and information security rule compliance. Computers & Security, 33, 3-11.

Kolkowska, E., & Dhillon, G. (2012). Organisational power and information security rule compliance. Computers & Security.

Koocher, G., P. (2009). Ethics and the Invisible Psychologist, Psychological Services, 6(2), 97-107.

Kothari, C. R. (2004). Research Methodology: Methods & Techniques (2nd ed.). Delhi: New Age International Ltd.

Krige, W. (1999). The usage of audit logs for effective information security management. Unpublished master's thesis. Port Elizabeth Technikon, Port Elizabeth, South Africa.

Krippendorf, K. (1980). Content Analysis: an introduction to its methodology.Beverley Hills, CA: Sage Publications

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. Computers & Security, 27(5), 224-231.

Kruger, H. A. & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers and Security, 25, 289-296.

Kvale, S. (1996). InterViews: An introduction to qualitative research interviewing.Thousand Oaks, CA: Sage.

Lacey, D. (2010). Understanding and transforming organisational security culture. Information Management & Computer Security, 18(1), 4-13.

Lamm, E., Gordon, J. R., & Purser, R. E. (2010). The role of value congruence in organisational change. Organisation Development Journal, 28(2), 49-64.

Landen, R. G. (1993). Oman -- Oman: Politics and Development by Ian Skeet. The Middle East journal, 47(3), 522.

Larsson, R., & Risberg, A. (1998). Cultural Awareness and National versus Corporate Barriers to Acculturation. In Gertsen, Söderberg & Torp (Eds.), Cultural Dimensions of International Mergers and Acquisitions, 85, 39.

Leach J. (2003). Improving user security behavior. Computers & Security, 22 (8), 685-692.

LeCompte, M. D., & Preissle, J. (1993). Ethnography and qualitative design in educational research. London, UK: Academic Press.

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. Computers & Security, 59, 60-70.

Lee, R. M., & Fielding, N. G. (1991). Computing for qualitative research: Options, problems and potential. In N. G. Fielding & R. M. Lee. (Eds.), Using computers in qualitative research (pp. 1-13). London: Sage

Lee, S. G., Trimi, S., & Kim, C. (2013). The impact of cultural differences on technology adoption. Journal of World Business, 48(1), 20-29.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information & Management, 41(6), 707-718.

Leech, N. L., & Onwuegbuzie, A. J. (2007). An array of qualitative data analysis tools: a call for data analysis triangulation. School psychology quarterly, 22(4), 557.

Leedy, P. D. (2005). Practical Research: Planning and Design (6th ed.). Upper Saddle River, N.J.: Prentice Hall.

Leedy, P. & Ormrod, J. (2001). Practical research: Planning and design (7th ed.). Upper Saddle River, NJ: Merrill Prentice Hall. Thousand Oaks: SAGE Publications.

Leenders, R. T. A. J. (2002). Modeling social influence through network autocorrelation: constructing the weight matrix. Social Networks, 24(1), 21-47.

Le Grand, C., & Ozier, W. (2000). Information Security Management Elements. Available Online at http:// www.itaudit.org/forum/auditcontrol/f305ac.htm.

Leidecker, J. K., & Bruno, A. V. (1984). Identifying and using critical success factors. Long range planning, 17(1), 23-32.

Leidner, D. E., & Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. MIS quarterly, 30(2), 357-399.

Levitin, T. (1973). Values. In: Robinson, J.P. & Shaver, P.R. (Editors). Measures of social psychological attitudes. Survey Research Center, Institute for Social Research, University of Michigan

Liang, H., Saraf, N., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. MIS Quarterly, 31(1), 59-87.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 394.

Liberti, L. (2008). CA Advisor Survey Results: Reduce Compliance Costs While Strengthening Security. Available Online at: http://www.ca.com/us/eitm/collateral.aspx?cid=181392

Lim, J. S., Chang, S., Maynard, S., & Ahmad, A. (2009). Exploring the relationship between organisational culture and information security culture. In Australian information security management conference (p. 12).

LINDUP, K. (1995). A new model for information security policies. Computers & Security. 14(8), p. 694.

Lin, Y.-H., Chen, C.-Y. and Chiu, P.-K. (2005). An Overview on Issues of Cross-Cultural Research and Back-Translation The Sport Journal, 8(4)

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. Beverly Hills, CA: Sage.

Lindholm, N. (2000). National culture and performance management in MNC subsidiaries. International studies of management & organisation, 29(4), 45-66.

Loch, K., Straub, D., and Kamel, S. (2003). Diffusing the Internet in the Arab World: the Role of Social Norms and Technological Culturation. IEEE Transactions on Engineering Management 50 (1), 45–63.

Lund, M. S., Solhaug, B., & Stølen, K. (2011). Model-Driven Risk Analysis. Model-Driven Risk Analysis: The CORAS Approach, ISBN 978-3-642-12322-1. Springer-Verlag Berlin Heidelberg, 2011.

Lundy, O., & Cowling, A. (1996). Strategic Human Resource Management. London: Thompson.

Ma, Q., & Pearson, J. M. (2005). ISO 17799:" Best Practices" in Information Security Management?. Communications of the Association for Information Systems, 15(1), 32.

Ma, Q. X., Schmidt, M. B., & Pearson, J. M. (2009). An integrated framework for information security management, Review of Business, 30(1), 58-70.

Malcolmson, J. (2009). What is security culture? Does it differ in content from general organisational culture? In 43rd Annual 2009 International Carnahan Conference on Security Technology, 2009 (pp. 361–366). doi:10.1109/CCST.2009.5335511

Maree, K., & Pietersen, J. (2007a). Surveys and the use of questionnaires. First steps in research. Pretoria: Van Schaik, 155-170.

Martin, J. (2002). Organisational culture: Mapping the terrain. Sage Publications. Thousand Oaks, CA

Martin, J., Feldman, M. S., Hatch, M. J., & Sitkin, S. B. (1983). The uniqueness paradox in organisational stories. Administrative Science Quarterly, 438-453.

Martins, N., & da Veiga, A. (2015). An Information Security Culture Model Validated with Structural Equation Modelling. In HAISA (pp. 11-21).

Martins, A., & Eloff, J. H. (2002). Information Security Culture. In Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives (pp. 203-214). Kluwer, BV.

Martins, A., & Eloff, J. (2002b). Assessing Information Security Culture. In ISSA. (pp. 1- 14).

Marshall, C. & Rossman, G. B. (2006). Designing Qualitative Research. (4th Ed.). Thousand Oaks, CA: Sage.

Marzigliano L. Advice (2013). Security vs Utility. Available Online at HYPERLINK "http://www.zigthis.com/145" http://www.zigthis.com/145.

Maxcy, S. J. (2003). Pragmatic threads in mixed methods research in the social sciences: The search for multiple modes of inquiry and the end of the philosophy of formalism. Handbook of mixed methods in social and behavioral research, 51-89.

Maynard, S., & Ruighaver, A. B. (2002). Evaluating IS Security Policy Development. In 3rd Australian Information Warfare and Security Conference.

McCarthy, M. P., & Campbell, S. (2001). Security Transformation: Digital Defense Strategies to Protect Your Company's Reputation and Market Share. McGraw-Hill Professional.

McDaniel, G. & IBM Corporation IBM dictionary of computing of Computing. (1994). New York NY. McGraw-Hill.

McIlwraith, A. (2016). Information security and employee behaviour: how to reduce risk through employee education, training and awareness. Routledge

Meglino, B. M., Ravlin, E. C., & Adkins, C. L. (1989). A work values approach to corporate culture: A field test of the value congruence process and its relationship to individual outcomes. Journal of Applied Psychology, 74(3), 424-432. doi:10.1037//0021-9010.74.3.424

Merkow, M. & Breithaupt, J. (2006). Information Security: Principles and Practices, Pearson Education Ltd., New Jersey.

Mertens, D. M. (1998). Research methods in education and psychology: İntergrating diversity wiht quantitative and qualitive approaches. Sage Publications

Miller, S., Batenburg, R. S., & van de Wijngaert, L. (2006). National culture influences on European ERP adoption. In J. Ljungberg & M. Andersson (Eds.), 14th European conference on information systems (pp. 1-12). Göteborg University, Chalmers University

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook (2nd ed.). Thousand Oaks, CA: Sage.

Mitnick, K. (2002). The art of deception. New York: CyberAge Books.

Mitnick, K., & Simon, W.L. (2002). The art of deception: Controlling the human element of security. New York: Wiley.

Mitnick, K. D., & Simon, W. L. (2005). L'arte dell'inganno. I consigli dell'hacker più famoso del mondo. Feltrinelli Editore.

Mohamed, U. K., White, G. R., & Prabhakar, G. P. (2008). Culture and conflict management style of international project managers. International Journal of Business Management, 3(5), 3-11.

Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2012). The "big picture" of insider IT sabotage across US critical infrastructures. In Insider Attack and Cyber Security (pp. 17-52). Springer, Boston, MA.

Morris, M. G., & Venkatesh, V. (2000). Age differences in technology adoption decisions: Implications for a changing work force. Personnel psychology, 53(2), 375-403.

Mujtaba, B. G., Khanfar, N. M., & Khanfar, S. M. (2009). Leadership Tendencies of Government Employees in Oman: A Study of Task and Relationship based on Age and Gender. Public Organisation Review, 1-18.

Munter, M. (1993). Cross-cultural communication for managers. Business Horizons. 36(3), 69-78.

Myers, M. D., & Avison, D. E. (Eds.). (2002). Qualitative research in information systems: a reader. Sage.

Myers, M. D., & Avison, D. E. (1997). Qualitative research in information systems. Management Information Systems Quarterly, 21, 241-242.

Nardi, P. M. (2014). Doing survey research: A guide to quantitative methods (3rd ed.). Boulder, CO: Paradigm Publishers.

Narasimhan, R., Nair, A., Griffith, D. A., Arlbjørn, J. S., & Bendoly, E. (2009). Lock-in situations in supply chains: A social exchange theoretic study of sourcing arrangements in buyer–supplier relationships. Journal of Operations Management,27(5), 374-389.

Neal, M., Finlay, J. L., Catana, G. A., & Catana, D. (2007). A comparison of leadership prototypes of Arab and European females. International Journal of Cross Cultural Management, 7(3), 291-316.

Neubauer, T., Klemen, M., & Biffl, S. (2006, April). Secure business process management: a roadmap. In Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on (pp. 8-pp). IEEE.

Neubauer, T., Klemen, M., & Biffl, S. " Business process-based valuation of IT-Security"; Vortrag: 7th International Workshop on Economics-Driven Software Engineering Research EDSER'05, St. Louis, Missouri; 15.05. 2005.

Neuman, W. L. (2009). Social research methods: Qualitative and quantitative approaches (7th ed.). Boston: Allyn & Bacon.

Niglas, K. (2009). How the novice researcher can make sense of mixed methods designs. International Journal of Multiple Research Approaches, 3(1), 34-46.

Niskanen, W. (1971). Bureaucracy and representative government, Aldin-Atherton, Chicago.

NIST (2006). Information Security Handbook: A Guide for Managers. NIST Special Publication 800-100, Gaithersburg, MD: National Institute of Standards and Technology. From http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

Norris, P. (2001). Digital divide: Civic engagement, information poverty, and the Internet worldwide. Cambridge University Press.

Nosworthy, J. D. (2000). Implementing information security in the 21st century: Do you have the balancing factors? Computer & Security, 19(4), 337-347.

Nutt, P. C. (1993). Organisational publicness and its implications for strategic management. Journal of Public Administration Research and Theory, 3(2), 209-231.

Nydell, M.K. (2006). Understanding Arabs: A Guide for Modern Times. Intercultural Press.Yarmouth. ME.

O'Donnell, O., & Boyle, R. (2008). Understanding and Managing Organisational Culture. Institute of Public Administration: Dublin.

Olson, I., & Abrams, M. (2001). Essay 7: Security Policy. Information Security: An Integrated Collection of Essays. IEEE computer Society press.

Olsen, W. (2004). Triangulation in social research: qualitative and quantitative methods can really be mixed. Developments in sociology, 20, 103-118.

"Oman" World Encyclopedia. Philip's, (2008). Oxford Reference Online. Oxford University Press. Available at HYPERLINK "http://www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t142.e8421". Accessed 29th October 2009.

Onwuegbuzie, A. J., & Leech, N. L. (2005). On Becoming a Pragmatic Researcher: The Importance of Combining Quantitative and Qualitative Research Methodologies. International Journal of Social Research Methodology, 8(5), 375-387.

O'Reillys III, C. A., & Puffer, S. M. (1989). The impact of rewards and punishments in a social context: A laboratory and field experiment. Journal of Occupational Psychology, 62(1), 41-53.

O'Reilly III, C. A., & Weitz, B. A. (1980). Managing marginal employees: The use of warnings and dismissals. Administrative Science Quarterly, 25(3), 467-484.

Orshesky, C. M. (2003). Beyond technology–The human factor in business systems. Journal of business strategy, 24(4), 43-47.

Ostroff, C., Shin, Y., & Kinicki, A. J. (2005). Multiple perspectives of congruence: Relationships between value congruence and employee attitudes. Journal of Organisational Behavior, 26(6), 591-623.

Ousmanou, K. (2007). A Method for the Articulation of Users' Requirements for Personalised Information Provision (Doctoral dissertation, University of Reading).

Pagnucco, M. (1995). Conjunctive versus disjunctive abduction-a pragmatic difference between abduction and inverse resolution.

Pahnila, S., Siponen, M. & Mahmood, A. (2007). Employees' Behavior Towards IS Security Policy Compliance, Proceedings of the 40th Hawaii International Conference on System Sciences, Los Alamitos, CA, 156-166

Pahnila, S., Siponen, M., & Mahmood, A. (2007b). Which factors explain employees' adherence to information security policies? An empirical study. Pacific Asia Conference on Information System (PACIS) 2007 Proceedings, 73.

Paine, K. D. (2003). Guidelines for measuring trust in Organisations. The institute for public relations, 2003, 9-10.

Park, S., Ahmad, A., and Ruighaver, A. B. (2010). Factors influencing the implementation of information systems security strategies in organisations. in Proceedings of the 2nd International Conference on Information Science and Applications, Seoul, pp. 1-6.

Parker, D. B. (1998). Fighting computer crime: A new framework for protecting information (pp. I-XV). New York: Wiley.

Parker, D. (1981). Computer Security Management. Reston, VA: Reston Publishing Company.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2014). The influence of organisational information security culture on information security decision making. Journal of Cognitive Engineering and Decision Making, 9, 117-129.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environment (No. DSTO-TR-2484). Defence Science and Technology Organisation Edinburgh (Australia) Command Control, Communications and Intelligence Div.

Patel, S. (2015). The research paradigm – methodology, epistemology and ontology – explained in simple language. Available at: HYPERLINK "http://salmapatel.co.uk/academia/the-research-paradigm-methodology-epistemology-and-ontology-explained-in-simple-language"

Patten, M. L. (2012). Understanding research methods: An overview of the essentials (8th Ed.). Glendale, CA: Pyrczak Publishing.

Patton, M. Q. (2005). Qualitative research. John Wiley & Sons, Ltd.

Peat, J. (2002). Health science research: a handbook of quantitative methods. Sage Publications Inc., Thousand Oaks Ca: Sage

Pederson, W. D. (2002). Oman Under Qaboos. From Coup to Constitution, 1970-1996. Journal of Third World Studies, 19(1), 259.

Peltier, T., R. (2013). Information Security Policies, Procedures, and Standards: guidelines for effective information security management: CRC Press.

Peltier, T.R., Peltier, J.& Blackley, J. (2005). Information security fundamentals. Auerbach Publications, Boca Raton, Fla.

Perry, C. (2012). A Structured Approach to Presenting Theses: Notes for Students and Their Supervisors. Paper on Structuring a Thesis, Southern Cross University, Lismore.

Perry, J. L., & Rainey, H. G. (1988). The public-private distinction in organisation theory: A critique and research strategy. Academy of management review, 13(2), 182-201.

Petter, S., DeLone, W., & McLean, E. (2008). Measuring information systems success: models, dimensions, measures, and interrelationships. European journal of information systems, 17(3), 236-263.

Peters, T. J., Waterman, R. H. (1982). In search of excellence: Lessons from America's best-run companies. Harper & Row.

Pfhleeger, C. P., & Pfleeger, S. L. (1997). Security in Computing, Second edn, Prentice Hall, United States of America.

Peirce, C. S. (1878) How to make our ideas clear. Popular Science Monthly 12, pp 286-302.

Peirce, C. S. (1902). Logic as semiotic: The theory of signs. Philosophical writings of Peirce, 100.

Pieters, W. (2011). The (social) construction of information security. The Information Society, 27(5), 326-335.

Pietersen J & Maree K 2007. Standardisation of a questionnaire. In: K Maree, First steps in research, 183-196. Pretoria: Van Schaik.

Pink Elephant (2008). IT service management tools: compatibility considerations. [Online], <https://www.pinkelephant.com/NR/rdonlyres/3C232863-4423-

430E-B5C6-
8358A2D217B9/4340/PinkVERIFYServiceWhitepaperV333.pdf>

Pinto, J., Leana, C. R., & Pil, F. K. (2008). Corrupt organisations or organisations of corrupt individuals? Two types of organisation-level corruption. Academy of Management Review, 33(3), 685-709.

Pizam, A. (1993). Managing Cross-Cultural Hospitality Enterprises. The International Hospitality Industry: Organisational and Operational Issues. John Wiley, NewYork, NY.

Plano Clark, V. L. (2010). The adoption and practice of mixed methods: US trends in federally funded health-related research. Qualitative Inquiry, 16(6), 428-440.

Ponemon Institute. 2014 . 2014 Cost of Data Breach. IBM. Available at: http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

Ponemon, L. (2009). Trends in Insider Compliance with Data Security Policies-Employees Evade and Ignore Security Policies. Ponemon Institute.

Posner, B. Z. (2010). Another look at the impact of personal and organisational values congruency. Journal of Business Ethics, 97(4), 535-541.

Posthumus, Shaun, y. von Solms and Rossouw. (2004). A framework for the governance of information security. Computers & Security. 23(8), 638-642.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. MIS Quarterly, 34(4), 757-778.

Purser, S. (2004). A practical guide to managing information security. Artech House.

Rabi, U. (1997). Oman: Politics and Development / Trade and Empire in Muscat and Zanzibar: Roots of British Domination. Middle Eastern Studies, 33(4), 800.

Ragu-Nathan, B. S., Apigian, C. H., Ragu-Nathan, T. S., & Tu, Q. (2004). A Path Analytic Study of the Effect of Top Management Support for Information Systems Performance. Omega, 32, 459- 471.

Rainey, H., Backoff, R., and Levine, C. (1976). Comparing Public and Private Organisations, Public Administration Review, 36(2), 233-244.

Rainey, H. G., & Bozeman, B. (2000). Comparing public and private organisations: Empirical research and the power of the a priori. Journal of public administration research and theory, 10(2), 447-469.

Ramachandran, S., Rao, S. V., & Goles, T. (2008). Information security cultures of four professions: A comparative study. Paper presented in Hawaii International Conference on System Sciences, Proceedings of the 41st Annual (pp. 454-454). IEEE.

Rastogi, R., & von Solms, R. (2012). Information Security Service Branding–beyond information security awareness. Systemics, Cybernetics and Informatics, 10(6), 54-55.

Ratner, B. D., Cohen, P., Barman, B., Mam, K., Nagoli, J., & Allison, E.H. (2013). Governance of Aquatic Agricultural Systems: Analyzing Representation, Power, and Accountability. Ecology and Society, 18(4), 59.

Rees, C.J., Althakhri, R. (2008), Organisational change strategies in the Arab region: A review of critical factors. Journal of Business Economics and Management, 9(2), 123-132.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. Computers & Security, 27(7-8), 241-253.

Richards, D.A., Oliphant, A.S., & Le Grand, C.H. (2005), GTAG1:Information Technology Controls, The Institute of Internal Auditors IIA). Available at: http://www.theiia.org/guidance/standards-andguidance/ippf/practice-guides/gtag/gtag1/ .

Richards, T. J., & Richards, L. (1994). Using computers in qualitative research. Handbook of qualitative research, 2, 445-462.

Ring, P. S., & Perry, J. L. (1985). Strategic management in public and private organisations: Implications of distinctive contexts and constraints. Academy of management review, 10(2), 276-286.

Robbins, S. P. (2003). Organisational Behavior: Prentice Hall's Self-assessment Library. Prentice Hall.

Robbins, S. P &Judge, T. A. (2008). Organisational behavior (Organisational Behavior), terjemahan. Jakarta : Salemba Empat.

Robbins, S. P. & Judge, T. A. (2007). Organisational behavior. (12th ed.). Upper Saddle River: New Jersey: Pearson Prentice Hall.

Robson, C. (2011). Real world research 3 rd Ed. UK: Wiley.

Robson, C. (2002). Real World Research: A Resource for Social Scientists and Practitioner-Researchers., 2nd edn. (Blackwell Publishing: Oxford, UK.).

Rockart, J. F. (1979). Chief executives define their own data needs. Harvard Business Review, 57(2), 81-93.

Rowlands, B. H. (2005). Grounded in practice: Using interpretive research to build theory. The Electronic Journal of Business Research Methodology, 3(1), 81-92.

Rousseau, D. M. (1990). New hire perceptions of their own and their employer's obligations: A study of psychological contracts. Journal of organisational behavior, 11(5), 389-400.

Rossman, G. B., & Wilson, B. L. (1984). Numbers and words: Combining quantitative and qualitative methods in a single large-scale evaluation study. Evaluation review, 9(5), 627-643.

Rotvold, G. (2008). How to create a security culture in your organisation. The Information Management Journal, 42(6), 32–38.

Rubin, H. J., & Rubin, I. S. (2011). Qualitative interviewing: The art of hearing data. Sage.

Rubin, H. J., & Rubin, I. S. (2005). Qualitative interviewing: The art of hearing data (2nd ed.). Thousand Oaks, CA: Sage.

Rugh, W. A. (1999). Past, Present and future leadership. Middle East Policy, 6(4), 30.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. Computers & Security, 26(1), 56-62.

Sagiv, L., Schwartz, S., & Arieli, S. (2011). Personal values, national culture and organisations: Insights applying the Schwartz value framework. In The handbook of organisational culture and climate. Second Edition (pp. 515-537). SAGE Publications.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in Organisations. Computers & Security, 53, 65-78.

Sampieri, R. (1991). Research Methodology. Mexico: McGraw - Hill

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT technology journal, 19(3), 122-131.

Sasse, M. A., Ashenden, D., Lawrence, D., Coles-Kemp, L., Fléchais, I., & Kearney, P. (2007). Human Vulnerabilities in Security Systems. Human Factors Working Group, Cyber Security KTN Human Factors White Paper.

Saunders, M. N. K., & Tosey, P. C. (2013). The Layers of Research Design. Rapport, (Winter), 58-59.

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research Methods for Business Students (5th Eds) Essex: Pearson Education Ltd.

Saunders, M., Lewis, P., & Thornhill, A. (2007). Research Methods for Business Students (4th Eds) Harlow: Pearson Education.

Saunders, M., Lewis, P. and Thornhill, A. (2003). Research Methods for Business Students, Prentice Hall (3rd Ed)

Saunders, M., Lewis, P & Thornhill, A. (1997). Research Methods For Business Students, Pitman, London, United Kingdom.

Scandura, T. A., & Williams, E. A. (2000). Research methodology in management: Current practices, trends, and implications for future research. Academy of Management journal, 43(6), 1248-1264.

Schein, E. H. (2010). Organisational culture and leadership (Vol. 2). John Wiley & Sons.

Schein, E. H. (1999). The Corporate Culture Survival Guide. San Francisco: Jossey-Bass.

Schein, E. H. (1996a). Culture: The Missing Concept in Organisation Studies. Administrative science quarterly, 229-240.

Schein, E. H. (1996b). Three Cultures of Management: The Key to Organisational Learning. Sloan Management Review, 38(1), 9-20.

Schein, E. H. (1995). Organisational and managerial culture as a facilitator or inhibitor of Organisational transformation.

Schein, E. (1992). Organisational Culture and Leadership (2nd edn). San Francisco, CA:
Jossey-Bass Publishers.

Schein, E. H. (1988). Organisational Socialization and the Profession of Management. Sloan Management Review, 30(1), 53-65.

Schein, E. H. (1985). Organisational Culture and Leadership (1st ed.). San Francisco: Jossey-Bass.

Schlienger, T., & Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. In Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on (pp. 405-409). IEEE.

Schlienger, T., & Teufel, S. (2002). Information Security Culture: The Socio-Cultural Dimension in Information Security Management. In Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives (pp. 191-202). Kluwer, BV.

Schneider, B. & Barbera, K.M. (2014). Organizational Climate and Culture, Oxford University Press, p730..

Schneier, B. (2000). Secrets and Lies, New York: John Wiley & Sons.

Schneier, C. J. (1974). Behavior modification in management: A review and critique. Academy of Management Journal, 17, 528-548.

Scholtz, T. (2004). The Business Value of Information Security. META group.

Schostak, J. F. (2006). Interviewing and Representation in Qualitative Research Projects. Maidenhead: Open University Press.

Schultz, E. (2005). The human factor in security. Computers & Security, 24, 425-426.

Schwartz, S. H. (1994). Beyond individualism/collectivism: New cultural dimensions of values. Sage Publications, Inc.

Scott, P. G., & Falcone, S. (1998). Comparing public and private organisations: an exploratory analysis of three frameworks. The American Review of Public Administration, 28(2), 126-145.

Sekaran, U. (2003). Research methods for business: A skill-building approach (4th ed.). Chichester: John Wiley.

Senglaub, M., Harris, D., & Raybourn, E. M. (2001). Foundations for reasoning in cognition-based computational representations of human decision making. Albuquerque, New Mexico (NM): Sandia National Laboratories. Operational Decisions, 75.

Sharma, S. K. (2014). Adoption of e-government services: The role of service quality dimensions and demographic variables. Transforming Government: People, Process and Policy, 9(2), 207-222.

Sharma, N. K., & Dash, P. K. (2012). Effectiveness of ISO 27001, as an information security management system: an analytical study of financial aspects. Far East Journal of Psychology and Business, 9(3), 42-55.

Sharma, R., & Yetton, P. (2003). The contingent effects of management support and task interdependence on successful information systems implementation. MIS quarterly, 533-556.

Shaw, G.B. (1944). Everybody's Political What's Wath?: By Bernard Shaw. Constable.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92-100.

Shuttleworth, M. (2008). Quantitative and Quantitative Research Design. Available OnLine at: HYPERLINK https://explorable.com/quantitative-research-design.

Silverman, D. (2010). Doing qualitative research: a practical handbook (3rd ed.). Thousand Oaks, CA: Sage Publications Ltd.

Siponen, M. T. (2001). Five Dimensions of Informstion Security Awareness. Computers and Society, 31(2): 24-29.

Siponen, M. T. (2000). A conceptual foundation for organisational information security awareness. Information Management & Computer Security, 8(1), 31-41.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 38(1), 60-80.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. Computer, 43(2).

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study *New Approaches for Security, Privacy and Trust in Complex Environments*. In IFIP International Information Security Conference (pp. 133-144). Springer, Boston, MA.

Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee systems security policy violations. MIS Quarterly, 34(3), 487-502.

Smith, P. B., & Bond, M. H. (1998). Social psychology across cultures. Paris; Prentice Hall Europe.

Smith, S., & Jamieson, R. (2006). Determining key factors in e-government information system security. Information systems management, 23(2), 23-32.

Smith, A. R., Colombi, J. M., & Wirthlin, J. R. (2013). Rapid development: A content analysis comparison of literature and purposive sampling of rapid reaction projects. Procedia Computer Science, 16, 475-482.

Sowa, J. F. (2000). Knowledge representation: logical, philosophical, and computational foundations (Vol. 13). Pacific Grove: Brooks/Cole.

Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. Management Information Systems Quarterly, 34(3), 503-522.

Spears, J. L. (2005). A holistic risk analysis method for identifying information security risks. In Security management, integrity, and internal control in information systems (pp. 185-202). Springer, Boston, MA.

Srite, M., & Karahanna, E. (2006). The role of espoused national cultural values in technology acceptance. MIS Quarterly, 30(3), 679-704.

Srite, M., Straub, D., Loch, K., Evaristo, R., & Karahanna, E. (2004). Inquiry into definitions of culture in IT studies. In H. Gordon & T. Tan (Eds.), Advanced Topics in Global Information Management (pp. 30-48). Hershey, PA, USA: Idea Group Pub.

Stake, R.E. (1985). Case Studies, Chapter 14. In N.K. Denzin & Y.S. Lincoln (Eds.), Handbook in Qualitative Research. Beverly Hills, California: Sage Publications, Inc., 236-247.

Stan, S. (2007). Beyond Information Security Awareness Training: It Is Time to Change the Culture. In H. F. Tipton (Ed.), Information Security Management Handbook (pp. 555-565). Hoboken: Auerbach Publications.

Straub, D. W. (1990). Effective IS security: An empirical study. Information Systems Research, 1(3), 255-276.

Straub, D. W. (1988). Organisational structuring of the computer security function. Computers & Security, 7(2), 185-195.

Straub, D., Loch, K., Evaristo, R., Karahanna, E., & Srite, M. (2002). Toward a Theory-Based Measurement of Culture. Journal of Global Information Management (JGIM), 10(1), 13-23.

Straub, D., Loch, K. D., & Hill, C. E. (2001). Transfer of Information Technology to the Arab World: A Test of Cultural Influence Modeling. Journal of Global Information Management (JGIM), 9(4), 6-28.

Stukat, S. (2005). Att skriva examensarbete inom utbildningsvetenskap. Studentlitteratur: Lund. ISBN, 978-91.

Su, X., Bolzoni, D., & van Eck, P. (2007). Specifying Information Security Needs for the Delivery of High Quality Security Services. In Business-Driven IT Management, 2007. BDIM'07. 2nd IEEE/IFIP International Workshop on (pp. 112-113). IEEE.

Suar, D., & Khuntia, R. (2010). Influence of personal values and value congruence on unethical practices and work behavior. Journal of Business Ethics, 97(3), 443-460.

Szilagyi, A.D., & Wallace, M.J. (1990). Organisational Behavior and Performance: (5th Ed.) Scott, Foresman and Company, Illinois.

Talbot, S., & Woodward, A. (2009). Improving an organisations existing information technology policy to increase security.

Talmy, S. (2010). Qualitative interviews in applied linguistics: From research instrument to social practice. Annual Review of Applied Linguistics, 30, 128-148.

Tarimo, C. N. (2006). ICT security readiness checklist for developing countries: A social-technical approach (Doctoral dissertation, Institutionen för data-och systemvetenskap (tills m KTH)).

Tashakkori, A., & Teddlie, C. (Eds.). (2010). Sage handbook of mixed methods in social & behavioral research. Sage.

Tashakkori, A., & Teddlie, C. (2008). Quality of inferences in mixed methods research: Calling for an integrative framework. Advances in mixed methods research, 101-119.

Tashakkori, A., & Teddlie, C. (1998). Mixed methodology: Combining qualitative and quantitative approaches. Applied Social Research Meth- ods Series (Vol. 46). Thousand Oaks, CA: Sage.

Tayeb, M. (1997). Islamic revival in Asia and human resource management. Employee relations, 19(4), 352-364.

Tettero, O, (2000), Intrinsic Information Security: Embedding security issues in the design process of telematics systems, Ph.D. thesis, Twente University.

Terry, W. (2005). Information security policy's impact on reporting security incidents. Computers& Security. 24(6), p. 449.

Thibaut, J. W., & Kelley, H. H. (1959). The social psychology of groups. Oxford, England: John Wiley.

Thietart, R. A. et coll. (2003). Methods of research in management, 2nd edition, Dunod, Paris.

Thomson, K. L., von Solms, R., & Louw, L. (2006). Cultivating an organisational information security culture. Computer Fraud & Security, 2006(10), 7-11.

Thomson, M. E. & Von Solms, R. (1998). Information security awareness: educating your users effectively. Information Management & Computer Security, 6(4), 167-173.

Tipton, H. F., & Krause, M. (2009). Information security management handbook, (6th ed., Vol. 3). Boca Raton, FL: Auerbach Publications.

Torres, J., Sarriegi, J., Santos, J., & Serrano, N. (2006). Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness, in Information Security, S. Katsikas, J. López, M. Backes, S. Gritzalis and B. Preneel (eds.), Springer Berlin Heidelberg, pp. 530-545.

Trost, J. (2005). Qualitative Interviews Lund: Student litteratur: University Press

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness Programs. Computers & Security, 52, 128-141. doi:10.1016/j.cose.2015.04.006

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: research and practice gaps. Information Security Journal: A Global Perspective, 17(5-6), 207-227.

Tuohy, D., Cooney, A., Dowling, M., Murphy, K., & Sixsmith, J. (2013). An overview of interpretive phenomenology as a research methodology. Nurse Researcher, 20(6), 17-20

UNESCAP (United Nations Economic and Social Commission for Asia and the Pacific). (2008). Information Security for Economic and Social Development, BANGKOK.

Ursula K. Le Guin, (1974). "The Dispossessed". New York Harper & Row Pub.

Van de Ven, A. H. (1986). Central problems in the management of innovation. Management science, 32(5), 590-607.

Van Loenen, J. (2015). Information Security Awareness. Research World, 54(53).

Van Maanen, J., & Schein, E. H. (1979). Toward a theory of organisational socialization. In Research in Organisational Behavior 1, 209-264.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. Computers & Security, 29(4), 476-486.

Van Niekerk, J. F., & von Solms, R. (2006). Understanding Information Security Culture: A Conceptual Framework. In ISSA (pp. 1-10).

Van Niekerk, J. F., & von Solms, R. (2005). A holistic framework for the fostering of an information security sub-culture in organisations. Paper presented at the 4th Annual ISSA Conference South Africa.

Vedder, J. N. (1992). How much can we learn from success?. The executive, 6(1), 56-66.

Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. Information Systems Management, 24(4), 361-372.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. MIS Quarterly, 37(1), 21-54.

Verizon Business, R. I. S. K. (2009). Team.(2009). Data breach investigations report. Retrieved online from: http://www.verizonbusiness.com/resources/security/, reports/2009databreach rp.pdf;2009.

Von Roessing, R. (2010). The ISACA Business Model for Information Security: An Integrative and Innovative Approach. In ISSE 2009 Securing Electronic Business Processes (pp. 37-47). Vieweg+ Teubner.

Von Solms, B. (2005) Information security governance-compliance management vs operational management, Computers & Security, 24(6), 443-447.

Von Solms, B. (2000). Information security—the third wave?. Computers & Security, 19(7), 615-620.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371-376.

Von Solms, R. (1997). Driving safely on the information superhighway. Information management & computer security, 5(1), 20-22.

Von Solms, S.H. (2005a). Information Security Governance - Compliance management vs operational management, Computers & Security, 24(6): 443-447.

Von Solms, S.H. (2005b). Information Security Governance in ICT Based Educational Systems, Proceedings of the 2005 Conference in Bangkok. 109-119.

Von Solms, S.H. (2001a). Information Security - A Multidimensional Discipline Computers & Security, 20(6): 504-508.

Von Solms, S.H. (2001b). Corporate Governance and Information Security, Computers & Security, 20(3): 215-218.

Von Solms, S.H. (1999). Information Security Management through Measurement, in Proceedings of the SEC99 conference, Johannesburg, South-Africa.

Von Solms, S.H., & Eloff, J.H.P. (2004). Information Security. University of Johannesburg, Johannesburg, South-Africa.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioral complaince. Computers and Security, 23(3), 191-198.

Vroom, C., & von Solms, R. (2002). A Practical Approach to Information Security Awareness in the Organisation. In Security in the Information Society (pp. 19-37). Springer, Boston, MA.

Walmsley, G., and Zald, M. (1973). The political economy of public organisations, Lexington Books, Lexington, MA.

Warkentin, M., Johnston, A.C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. European Journal of Information Systems, 20(3), 267-284.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems, 18(2), 101.

Warschauer, M. (2002). Reconceptualizing the digital divide. First monday, 7(7).

Webster, C. (1993). Refinement of the marketing culture scale and the relationship between marketing culture and profitability of a service firm. Journal of business research, 26(2), 111-131.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organisational, and technological challenges of IT security management. Information Management & Computer Security, 17(1), 4-19.

Whitman, M. E., 2004. In defense of the realm: Understanding threats to information security. Informational Journal of Information Management, Vol. 24, pp. 3-4.

Whitman, M.E. (2003). Enemy at the gate: threats to information security. Communications of the ACM, 46(8), 91-95.

Whitman, M.E., & Mattord, H.J. (2013). Management of Information Security. Delmar Cengage Learning.

Whitman, M.E., & Mattord, H. J. (2012). Principles of Information Security, 4th edition. Hands-on information security lab manual. Course Technology, Cengage Learning.

Whitman, M.E. & Mattord, H.J. (2009). Principles of Information Security. London: Cengage Learning.

Whitman, M.E. & Mattord, H. J. (2008). Management of Information Security. Thomson Course Technology, Canada.

Whitman, M.E., & Mattord, H.J. (2005). Principles of information security. (2nd ed.). Thomson.

Whitman, M.E. & Mattord, H.J. (2003). Principles of Information Security. Kennesaw State University: Thomson Course Technology

Williams, P. (2001). Information Security Governance. Information Security Technical Report, 6(3), 60-70.

Willison, R., & Siponen, M. (2009). Overcoming the insider: reducing employee computer crime through Situational Crime Prevention. Communications of the ACM, 52(9), 133-137.

Wilson, A. (2014). Being a practitioner: an application of Heidegger's phenomenology. Nurse Researcher, 21(6), 28-33.

Wipawayangkool, K. (2009). Security awareness and security training: An attitudinal perspective. SWDSI 2009, 266-273.

Wood, C., C. (2005). Information Security Policies: Distinct from guidelines and standards. Available online at www. searchsecurity. com

Wright, M. A. (2001). Keeping top management focused on security. Computer Fraud & Security, 2001(5), 12-14.

Yaghubi, S., & Modiri, N. (2014). The control model of security in the deployment of ERP systems. International Journal of Computer Science and Information Security, 12(6), 29.

Yin R. K. (2014). Case Study Research: Design and Methods, 5th edition, Los Angeles, CA: Sage.

Yin, R. K. (2003). Case study research: Design and methods (3rd ed.). Thousand Oaks, CA: Sage.

Yin, R. K. (2002). Case Study Research. Design and methods. Thousand Oaks, CA: SAGE.

Yin, R. K. (1994). Case study research: Design and Methods, Applied social research methods series, 5. Biography, Sage Publications, London.

Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. Communications of the Association for Information Systems, 24(1), 34.

Zakaria, N., Stanton, J. M., & Sarkar-Barney, S. T. (2003). Designing and implementing culturally-sensitive IT applications: The interaction of culture values and privacy issues in the Middle East. Information Technology & People, 16(1), 49-75.

Zakaria, M. S. (1994). A model of machine intelligence based on the pragmatic approach. Unpublished PhD Thesis, Department of Computer Science, University of Reading, UK.

Zakaria, O. (2006, May). Internalisation of information security culture amongst employees through basic security knowledge. In IFIP International Information Security Conference (pp. 437-441). Springer, Boston, MA.

Zakaria, O. (2004). Understanding Challenges of information security culture: a methodological approach issue. Paper presented at the Second Australian information secuirty management conference, Perth, Australia.

Appendix A. Information Security Survey Questions

A survey to determain and to measure the Information Security in the Omani organisations in different sectors

Invitation to Participate in Dissertation Research Survey

Mars 02, 2017

Purpose : Information Security is one of the most critical domains challenging in the Omani organisations, which facing an increasing variety of security threats, and to know the critical Information Security issues will help trying to get the right solution to solve or limit them. The purpose of this survey is to meet requirements for a PhD degree in Information Security, and it aims to investigate and measure the Information Security practices and awareness in the omani organisations in both sectors public and private, and to promote a better understanding of the most critical Information Security issues. Hopefully, the results from this survey will offer a practical value for the organisations and shed insight on the essential capabilities of an organisation that most influence the effective implementation of Information Security policy.

Anonymity: Your responses and any comments you may have will be treated with confidentiality. Information will be reported in an aggregated form, without identifying you or your organisation.

Appreciation: Your participation involves completing the survey (5) pages including some basic personal information. The survey will take approximately (15-20) minutes to complete. Your participation in filling this survey is greatly appreciated .

Please know that the information you provide is essential in understanding the effect of organisational capabilities on an organisation's drive toward using Information Security to create business value.

Thank you in advance for participating in this research.

Information Security Survey		
PART1	Nationality * :	
Personal Information	Gender* : ☐ Male ☐ Female	
	Organisation* : ☐ Public ☐ Private	
	Title/Designation :	
	Education* : ☐ H. school ☐ Diploma ☐ H. diploma ☐ BSc ☐ MSc/MB ☐ PhD	
	Age Group*: ☐ 15-25 ☐ 26-35 ☐ 36-45 ☐ 46-55 ☐ 56-65 ☐ More then 66	
PART2	Type	Tick the right option
Organisation Type	Governmental organisation	❑
	Banking, & Insurance	❑
	Consultancy	❑
	Information Technology/Security/Telecoms	❑
	Manufacturing	❑
	Medical/Healthcare-public or private	❑
	Consumer Products /Retail/Wholesale	❑
	Education/Training	❑
PART3	Employees	Tick the right option
Organisation Size	More than 15,000	❑
	From 7,501 to 15,000	❑
	From 2,501 to 7,500	❑
	From 501 to 2,500	❑
	500 or less	❑
PART 4	Experience	Tick the right option
Job Experience in the organisation	Less than one year	❑
	Between 1 and 5	❑
	Between 6 and 10	❑
	Between 11 and 15	❑
	Between 16 and 20	❑
	Between 21 and 30	❑

PART5	Information Security Policy	Yes	No	Not Sure	Not Aplicable
Organisation's Information Security Policy	Does the organisation have a strong and enforced Information Security policy?.	❑	❑	❑	❑
	If the answer for the above question is YES, do all levels of organisation' members must signed the Information Security policy?.	❑	❑	❑	❑
	Are there a hard copies of the Information Security policy distributed in all organisation' offices , so that all employees are aware of it ?.	❑	❑	❑	❑
	Are the organisation' Information Security policies periodically reviewed and updated to combat the latest Information Security vulnerabilities?	❑	❑	❑	❑
	Are necessary efforts made in the organisation to educate employees about any new and updated Security policies ?.	❑	❑	❑	❑
	does the organisation follow a periodically checking mechanism to make sure that the employees are not breaching the security policy.	❑	❑	❑	❑
PART6	Training and Awarness	Yes	No	Not Sure	Not Aplicable
Information Scurity Training and Awarness	Does the organisation conducts any adequate awareness and training programs on Information Security for all employees before they getting a network account and regularly thereafter?.	❑	❑	❑	❑
	Does the organisation hold a regular refreshing security programs and awareness activities to raise the security awareness levels among its employees at all levels?	❑	❑	❑	❑
	Does the organisation have a section (or security officer) that concerns with the Information Security?	❑	❑	❑	❑
	If the answer for the above question is YES , are those actors exercising their role to the fullest?.	❑	❑	❑	❑
	Is there any coordination between the organisation's HR section and the Information Security concerned staff during the new appointments or job termination?.	❑	❑	❑	❑
	Are the organisation's security staff updating their knowledge periodically by participating in different security courses and conferences?.	❑	❑	❑	❑
PART 7	Managers Support	Yes	No	Not Sure	Not Aplicable
Managers Support for IS	Are organization's managers at all levels support the Information Security policies and procedures?.	❑	❑	❑	❑
	Do you think Managers only care about Information Security when there is a breach of Security in the organization?.	❑	❑	❑	❑
	Does the organization specify an annual budget for the Information Security in the organization?	❑	❑	❑	❑

PART 8	Organizational Culture	Yes	No	Not Sure	Not Aplicable
The Effect of the Organizational Culture in The Information Security	Do you think most employees are familiar with the importance of the Information Security to the organization ?.	❑	❑	❑	❑
	Are practicing good Information Security is part of the shared beliefs of organization' members?.	❑	❑	❑	❑
	Does The organization have a successful Information Security culture?.	❑	❑	❑	❑
	Is Information Security a major concern in the organization?.	❑	❑	❑	❑
	Are Information Security' policies and procedures applied to all organization' members including managers in different levels ?.	❑	❑	❑	❑
	Are organization' employees often complain about Information Security procedures?.	❑	❑	❑	❑
	Is it a common practice in the organization that employees exchange passwords between each other?.	❑	❑	❑	❑
	Do you think the weakness of the employees' Information Security culture and awareness could be the cause of increased Information Security threats and vulnerabilities in the organization?.	❑	❑	❑	❑
	During the previous years in the organization, did you contribute with any suggestions to improve the Information Security policies and procedures?.	❑	❑	❑	❑
	Is it important to have a cooperation and a coordination between the various organization' departments and the Information Security staff regarding the application of the Information Security procedures?.	❑	❑	❑	❑
PART 9	Information Security' Procedures	Yes	No	Not Sure	Not Aplicable
Organization's Information Security Procedures	Are there an adequate Security background & references investigated and checked during recruitment for new employees and staff?.	❑	❑	❑	❑
	Is it a requirement that all organization' members (including system administrators), should have a unique username and password for tnetwork authentication?.	❑	❑	❑	❑
	Does the organization's policy requires that passwords be changed at least every "90" days?.	❑	❑	❑	❑
	Did the organization experienced any internal or external Information Security breach previously?.	❑	❑	❑	❑
	If the answer for the above question is "YES", did this breach happen more than once?.	❑	❑	❑	❑
	Do most employees allowed to use their mobile phones within the organization premises?.	❑	❑	❑	❑

	Are employees allowed to copy documents and data from their computers into external storage devices, such as memory stick, CDs,…etc ?.	❑	❑	❑	❑
	Does the organization uses access control to manage the separation of duties in the organization?,	❑	❑	❑	❑
	Are Short contract employees allowed to access the organization's network?.	❑	❑	❑	❑
	Are suppliers allowed to access the organization's network?.	❑	❑	❑	❑
	Does the organization follow a certain procedures to secure the laptops that use for the organization's internal and external meetings and other businesses?.	❑	❑	❑	❑
	Is there a certain security measures followed by the organization to secure classified documents?.	❑	❑	❑	❑
	Is "Need to Know" policy been used among the organization' employees when exchanging information?.	❑	❑	❑	❑
	Are disciplinary process applied in the organization when an Information Security violation repeated?.	❑	❑	❑	❑
	Does the organization motivate Employees when notify superiors in the event of an Information Security violation?.	❑	❑	❑	❑
	Are all access rights and network' accounts removed at employment termination?.	❑	❑	❑	❑
	Is There a complete physical separation between the organization's network and the Internet network?.	❑	❑	❑	❑
	Does the organization implement network Security measures, such as firewalls, ids/ips, etc.?.	❑	❑	❑	❑
	Are network firewall' logs and servers' logs regularly monitored for intrusion attempts?.	❑	❑	❑	❑
	Is there a ready Disaster Recovery Plan in the organization?.	❑	❑	❑	❑
	Is there any preventive measures to protect and secure the organization' information from sabotage, (Such as the availability of disaster recovery location)?.	❑	❑	❑	❑
PART10	Responsible Parties' duty	Yes	No	Not Sure	Not Aplicable
Information Security Responsible Parties Duties	Are the Information Security concerned bodies in Oman such as ITA & CERT guide the public and private sectors to apply the best Information Security practices in their organizations?.	❑	❑	❑	❑
	Did the organization previously receive any invitations from those bodies to attend Information Security' conferences and workshops?.	❑	❑	❑	❑
	Does the organization receive any periodically alerts from those bodies regarding any new detection of Information Security' vulnerabilities and threats?.	❑	❑	❑	❑

	Does the organization interested in consulting internal or external Information Security auditors to insure that full security is provided to it's projects and systems.	❑	❑	❑	❑
PART11	Other Factors	Yes	No	Not Sure	Not Aplicable
Other fctors that could affect the IS in the organisation	Do you think young employees in the organization are more willing to follow the Information Security procedures than the older one?.	❑	❑	❑	❑
	Do you think educated employees in the organization are more willing to follow the Information Security procedures than the less educated one?.	❑	❑	❑	❑
	Do you think women employees are more sensible and more responsible when dealing with Information Security?.	❑	❑	❑	❑
PART12	Information Security Challenges	Yes	No	Not Sure	Not Aplicable
The challenges that facing Information Security application in the organization	Are there any factors such as (financial, management, training or education) that affect the development of Information Security in the organization?.	❑	❑	❑	❑
	If the answer for the above question is "Yes", what do you think the most effective factor? - Finance - Management - Education and training	❑	❑	❑	❑
	Does the organization' Information Security facing a management lack of interest?.	❑	❑	❑	❑
	Does the age factor represent a challenge to the development of employees' Information Security knowledge in the organization?.	❑	❑	❑	❑
	Do you think the organization's working environment could limit the capability of raising the employees' sensation towards Information Security?.	❑	❑	❑	❑
PART13	Other Notes				
Applicants Notes					

Appendix B. Information Security Interview Guide

Name (optional):
Organization:
Position (optional) :

a- General Questions

Q1: Tel me about your work / Information Security Experience.
Q2: How many years have you been working in this Organization?
Q3: What do you feel are the main drivers for Information Security within your organization?

b- Organization's Information Security current state

Q1: From your experience could you describe the current state of Information Security in your Organization?

Q2: Do your organization suffered a major Information Security incident before? If yes, what is the average number of Information Security incidents occurred during the last two years?.

Q3: In your opinion what are the biggest threats to Information Security at your organization?

Q4: In your view, what do you consider to be the top three barriers or obstacles to achieving improved security compliance in your Organization?

Q5: Which of these do you think is more challenge for Information Security in your organization and why?.

Create policies, procedures and regulations
Educate management
Educate Employees
Define vision and objective

Q6: Are there a business continuity/ disaster recovery plan in place in your organization? If the answer is 'Yes' does this disaster recovery plan tested regularly

Q7: In your opinion which is harder to convince to follow the Information Security policies and regulations in your organization: management or the employees? Why?

Q8: Is there a qualified, known and defined responsible department/section for Information Security in your organization, which also part of their job is to review, maintenance and upgrade the Information Security policy?.

Q9: Is there a complete physical separation between the organization's network and the Internet network in your organization?.

Q10: Does your organization implement a network security measures, such as firewalls, ids/ips, etc?.

Q11: Are network firewall logs and servers logs regularly monitored for intrusion attempts?.

C- Organization's Culture

Q1: How do you think your current organization's culture originated, is it from the Management visions, or from employees' culture or both?.

Q2: How would you describe the effects of the organization's culture in the Information Security in your Organization?.

Q3: Does The organization have a successful Information Security culture?.

Q4: Does the organization's members recognize the value and importance of Information Security? and are practicing good Information Security is part of the shared beliefs of organization's members ?

Q5: Are Information Security policies and procedures applied to all organization's members including managers in different levels?.

Q6: Do you think all employees must have a shared understanding of security practices, to have a successful Information Security implementation?.

d- Organization's Management Support.

Q1: Do you think management adequately gets involved in the implementation of the Information Security's policies and procedures?.

Q2: Does management frequently demand progress reports or feedbacks on implementation of Information Security's policies and procedures?.

Q3: Are organization's managers at all levels support the Information Security policies and procedures? or they only care about Information Security when there is a breach of Security in the organization?

Q4: Are managements quick to review issues arising from the Information Security progress report?.

E- Awareness, Education and Training

Q1: Do you thinks the organization conduct any adequate awareness and training programs on Information Security for all employees before they getting a network account?.

Q2: Are awareness programs regularly conducted to ensure that organization's employees are aware of their security responsibilities?.

Q3: Are management regularly obliged they employees to attend awareness, education and training sessions?

Q3: Are awareness and training programs carried out together for all organization's members or for different categories of staff? .

Q4: Are necessary efforts made in the organization to educate employees about any new and updated Security policies?.

Q5: Does the organization follow a periodically checking mechanism to make sure that the employees are not breaching the security policy.

F- Motivation and Punishment

Q1: Does the organization motivate employees when notify superiors in the event of an Information Security violation?.

Q2 : What do you think about policy enforcement? and also is there any disciplinary actions in this organization when an Information Security violation repeated?

G- Information Security Policy.

Q1: Do you think an Information Security policy exists in the organization and it is known to all the employees?.

Q2: If the answer for the above question is 'YES', do all levels of organization' members must signed the Information Security policy?.

Q3: Are Information Security roles and responsibilities clearly defined and communicated?

Q4: In your organization is there an effective and tested process to deal with Information Security Incidents /emergencies?

Q5: Do you think the organization's policy maintains regularly and review process considers any new affecting changes like: significant security incidents, news risks, changes in organizational or technical infrastructure?

Appendix C. Consent Form

Consent Form

Name of department: Computer and Information Sciences

Title of the study: Exploring the Organisational, Social and Cultural Factors Influencing those Employee Attitudes and Behaviours That Impact the Implementation of an Information Security Culture within Omani Organisations.

- I confirm that I have read and understood the information sheet for the above project and the researcher has answered any queries to my satisfaction.
- I understand that my participation is voluntary and that I am free to withdraw from the project at any time, without having to give a reason and without any consequences.
- I understand that I can withdraw my data from the study at any time.
- I understand that any information recorded in the investigation will remain confidential and no information that identifies me will be made publicly available.
- I consent to being a participant in the project
- I consent to being audio recorded as part of the project Yes/ No

(PRINT NAME)	Hereby agree to take part in the above project
Signature of Participant:	Date

Appendix D. Information Security Survey Answers (Public & Private Sector)

Total Responses Public + private = 155 - Pub. Particepants= 112 - Pr.Particepants = 43										
Male = 109 Female = 46 -Pub.Org= 92-– PROrg=35										
P1	Information Security Policy	Yes		No		Not Sure		Not Aplicable		Totals
		PU	PR	PU	PR	PU	PR	PU	PR	PU+PR
Organization's Information Security Policy	Does the organization have a strong and enforced Information Security policy?.	57	30	16	5	14	0	1	1	124
	If the answer for the above question is YES, do all levels of organization' members must signed the Information Security policy?.	24	26	30	3	15	3	13	4	118
	Are there a hard copies of the Information Security policy distributed in all organization' offices , so that all employees are aware of it ?.	18	17	54	9	12	7	3	3	123
	Are the organization' Information Security policies periodically reviewed and updated to combat the latest Information Security vulnerabilities?	22	21	35	6	26	8	4	1	123
	Are necessary efforts made in the organization to educate employees about any new and updated Security policies ?.	26	21	41	11	18	3	2	1	123
	does the organization follow a periodically checking mechanism to make sure that the employees are not breaching the security policy.	15	19	46	10	25	4	1	3	123

P2	Training and Awarness	Yes	No		Not Sure		Not Aplicable		Totals	
		PU	PR	PU	PR	PU	PR	PU	PR	PU+PR
Information Scurity Training and Awarness	Does the organization conducts any adequate awareness and training programs on Information Security for all employees before they getting a network account and regularly thereafter?.	29	23	40	8	10	2	0	2	114
	Does the organization hold a regular refreshing security programs and awareness activities to raise the security awareness levels among it's employees at all levels?.	24	21	47	8	7	4	1	1	113
	Does the organization have a section (or security officer) that concerns with the Information Security?.	58	28	9	2	9	3	1	2	112
	If the answer for the above question is YES , are those actors exercising their role to the fullest?.	19	22	26	3	20	6	8	3	107
	Is there any coordination between the organization's HR section and the Information Security concerned staff during the new appointments or job termination?.	18	22	30	4	26	8	4	1	113
	Are the organization's security staff updating their knowledge periodically by participating in different security courses and conferences?.	34	19	15	4	28	10	0	2	112
P3	Management Support	Yes	No		Not Sure		Not Aplicable		Totals	
		PU	PR	PU	PR	PU	PR	PU	PR	PU +PR
Oranization's Management Support	Are organization's managers at all levels support the Information Security policies and procedures?.	30	22	20	4	26	6	2	2	112
	Do you think Managers only care about Information Security when there is a breach of Security in the organization?.	36	10	14	15	27	8	1	1	112
	Does the organization specify an annual budget for the development of Information Security in the organization?	23	13	22	9	32	11	1	1	112

P4	Cultur Effects on IS	Yes	No		Not Sure		Not Aplicable		Totals	
		PU	PR	PU	PR	PU	PR	PU	PR	PU+PR
The Effect of the Organizational Culture in The Information Securty	Do you think most employees are familiar with the importance of the Information Security to the organization?	2	13	48	11	11	8	0	1	94
	Are practicing good Information Security is part of the shared beliefs of organization' members?.	4	23	26	6	15	3	0	1	78
	Does The organization have a successful Information Security culture?.	1	21	35	8	23	2	1	2	93
	Is Information Security a major concern in the organization?.	1	24	24	5	18	2	1	2	77
	Are Information Security' policies and procedures applied to all organization' members including managers in different levels ?.	2	19	34	8	16	4	1	2	86
	Are organization' employees often complain about Information Security procedures?.	4	7	18	17	21	6	4	3	80
	Is it a common practice in the organization that employees exchange passwords between each other?.	1	9	26	20	13	2	0	2	73
	Do you think the weakness of the employees' Information Security culture and awareness could be the cause of increased Information Security threats and vulnerabilities in the organization?.	3	24	1	2	10	3	0	4	47
	During the previous years in the organization, did you contribute with any suggestions to improve the Information Security policies and procedures?.	50	30	1	2	2	0	0	1	86
	Is it important to have a cooperation and a coordination between the various organization' departments and the Information Security staff regarding the application of the Information Security procedures?.	32	14	37	17	4	0	1	1	106

P5	Information Security Practices & Procedures	Yes	No		Not Sure		Not Aplicable		Totals	
		PU	PR	PU	PR	PU	PR	PU	PR	PU+PR
Organization's Information Security Practices and Procedures	Are there an adequate Security background & references investigated and checked during recruitment for new employees and staff?.	41	12	15	10	13	8	1	1	101
	Is it a requirement that all organization' members (including system administrators), should have a unique username and password for network authentication?.	62	26	3	3	5	0	0	2	101
	Does the organization's policy requires that passwords be changed at least every "90" days?.	47	28	15	2	8	0	0	1	101
	Did the organization experienced any internal or external Information Security breach previously?.	28	8	21	11	21	11	0	0	100
	If the answer for the above question is "YES", did this breach happen more than once?.	13	4	17	5	12	9	19	12	91
	Do most employees allowed to use their mobile phones within the organization premises?.	57	26	9	2	4	1	0	1	100
	Are employees allowed to copy documents and data from their computers into external storage devices, such as memory stick, CDs,…etc ?.	48	19	15	10	7	1	0	1	101
	Are Short contract employees allowed to access the organization's network?.	39	19	13	8	18	3	0	1	101
	Are suppliers allowed to access the organization's network?.	17	8	35	17	18	5	0	1	101
	Does the organization follow a certain procedures to secure the laptops that use for the organization's internal and external meetings and other businesses?.	31	20	22	9	14	1	2	1	100
	Is there a certain security measures followed by the organization to secure classified documents?.	34	20	17	4	19	6	0	1	101
	Is "Need to Know" policy been used among the organization' employees when exchanging information?.	20	14	25	8	22	8	1	1	99

	Does the organization motivate Employees when notify superiors in the event of an Information Security violation?.	13	10	36	12	19	7	2	1	100
	Are disciplinary process applied in the organization when an Information Security violation repeated?.	23	16	13	3	21	10	2	2	90
	Are all access rights and network' accounts removed at employment termination?.	36	24	9	3	25	3	0	1	101
	Is There a complete physical separation between the organization's network and the Internet network?.	29	15	24	14	16	1	1	1	101
	Does the organization uses access control to manage the separation of duties in the organization?,	38	19	20	7	12	2	0	1	99
	Does the organization implement network Security measures, such as firewalls, ids/ips, etc.?.	48	23	11	5	11	2	0	1	101
	Are network firewall' logs and servers' logs regularly monitored for intrusion attempts?.	24	21	11	3	15	5	0	1	80
	Is there a ready Disaster Recovery Plan in the organization?.	22	21	15	3	31	6	0	1	99
	Is there any preventive measures to protect and secure the organization' information from sabotage, (Such as the availability of disaster recovery location)?.	43	23	6	1	19	6	1	1	100

P6	Responsible Parties' duty	Yes	No		Not Sure		Not Aplicable		Totals	
		PU	PR	PU	PR	PU	PR	PU	PR	PU+PR
Information Security Responsible Parties Duties	Are the Information Security concerned bodies in Oman such as ITA & CERT guide the public and private sectors to apply the best Information Security practices in their organizations?.	36	12	18	7	12	10	0	2	97
	Did the organization previously receive any invitations from those bodies to attend Information Security' conferences and workshops?.	37	11	15	12	15	7	0	1	98

	Does the organization receive any periodically alerts from those bodies regarding any new detection of Information Security' vulnerabilities and threats?.	26	11	20	12	19	7	1	1	97
	Does the organization interested in consulting internal or external Information Security auditors to insure that full security is provided to it's projects and systems.	17	17	25	4	23	9	0	1	96
P7	Factors Could affected IS	Yes	No		Not Sure		Not Aplicable		Totals	
		PU	PR	PU	PR	PU	PR	PU	PR	PU +PR
Other fators that could affect the IS in the organization	Do you think young employees in the organization are more willing to follow the Information Security procedures than the older one?.	33	12	18	10	15	6	1	2	97
	Do you think educated employees in the organization are more willing to follow the Information Security procedures than the less educated one?.	44	21	7	3	13	4	2	2	96
	Do you think women employees are more sensible and more responsible when dealing with Information Security?.	16	9	20	11	28	8	3	2	97
P8	Information Security Challenges	Yes	No		Not Sure		Not Aplicable		Totals	
		PU	PR	PU	PR	PU	PR	PU	PR	PU+PR
The challenges that facing Information Security Implementation in the organisation	Are there any factors such as (financial, management, training or education) that affect the development of Information Security in the organization?.	46	22	13	7	8	0	0	1	97
	Does the organization' Information Security facing a management lack of interest?.	35	7	21	16	10	6	1	1	97
	Does the age factor represent a challenge to the development of employees' Information Security knowledge in the organization?.	43	13	15	12	8	4	0	1	96
	Do you think the organization's working environment could limit the capability of raising the employees' sensation towards Information Security?.	14	19	12	9	4	0	2	2	62