An Investigation of the Current Loopholes in Bank ABC's Cybersecurity System: Supporting a More Resilient and Trustworthy Cybersecurity System

Master Of Philosophy

By

Humaid Almansoori

Strathclyde University

2024

An Investigation of the Current Loopholes in Bank ABC's Cybersecurity System: Supporting a More Resilient and Trustworthy Cybersecurity System

by

Student Name: Humaid Almansoori

In Partial Fulfillment of Requirements

For the Master Of Philosophy

Under the Supervision of Dr. Karen Renaud

2024

Ethics Application Approval Number: 1393

Contents

Abstract

This dissertation extensively analyses ways to make UAE financial institutions more resilient to cyber-attacks. The primary objective is to assess and enhance these institutions' cyber-risk resilience and preparedness, offering valuable insights applicable not only to the financial sector but across various industries. As the Statistical Significance of robust cyber defence cannot be overstated, the research is vital in countering cyber threats, making it imperative for UAE institutions to develop comprehensive and effective internet security measures.

The research addresses four pivotal concerns in understanding the vulnerabilities within banks situated in Dubai. In the UAE, In particular, it explores how organizational resilience affects cyber-risk mitigation, the linkages between various cyber hazards, the efficacy of management technologies, and the Statistical Significance of human factors in cyber-security. To address these concerns, the researcher employs an inductive problem-solving approach and a positivist realist philosophy supported by quantitative data on the examined variables.

In explaining the underlying epistemological considerations, the research adopts an academic approach. Data collection involves an email survey conducted among employees of Bank ABC situated in the UAE with subsequent analysis using exploratory factor analysis (EFA) and multiple regression to uncover the correlation matrix structure and outcomes. This analytical technique

reveals the relationships between latent and observable elements, reinforcing the research's primary assumptions.

The findings suggest that many UAE financial institutions demonstrate commendable cyber resilience, underscoring the importance of employee cyber-threat preparedness and skill in determining an institution's overall resilience.

Using data derived from Staff of Bank ABC, this research contributes substantially to cyber-resilience knowledge, enabling UAE banks to assess their preparedness and operational deficiencies by leveraging cyber security frameworks. The research commences with a survey exploring the relationship between organizational resilience and preparedness in UAE banks while evaluating employee awareness and preparedness regarding cyber threats.

Acknowledgements

I, Humaid Almansoori, extend my deepest gratitude to my supervisor, Dr. Karen Renaud, for her invaluable guidance, patience, and expert advice throughout the duration of this research. Their mentorship was crucial in shaping both the direction and success of my work. I am profoundly thankful for their support and encouragement.

List of Figures

List of Tables

Definition of Key Terminologies

Access Control: The selective restriction of access to a system or network, ensuring that only authorized individuals or systems can interact with resources (Guo et al., 2021).

Cybersecurity: The practice of protecting computer systems, networks, and data from unauthorized access, attacks, damage, or theft (Juliana De Groot, 2023).

Denial of Service (DoS) Attack: An attack that aims to make a computer or network resource unavailable to its intended users by overwhelming it with traffic (Guo et al., 2021).

Encryption: Converting data into a code to prevent unauthorized access, providing confidentiality and data security (RiskOptics, 2023).

Endpoint Security: The protection of endpoints (devices like computers and smartphones) from malicious activity and cyber threats (RiskOptics, 2023).

Firewall: A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules (www.cisco.com).

Incident Response: The structured approach to addressing and managing the aftermath of a cybersecurity incident or breach (RiskOptics, 2023).

Malware: Malicious software designed to harm or exploit computer systems, including viruses, worms, Trojans, and ransomware (www.cisco.com).

Multi-factor Authentication (MFA): A security process that requires users to provide two or more authentication factors, enhancing access control and reducing the risk of unauthorized access (www.cisco.com).

Loophole: A loophole in cybersecurity refers to a vulnerability, weakness, or oversight in a computer system, network, or protocol that can be exploited to bypass security measures. Loopholes allow attackers to gain unauthorized access to systems and data, often through unexpected or unintended means. (Asaad, 2021)

Patch Management: Regularly update and apply patches to software systems to fix vulnerabilities and improve security (www.cisco.com).

Penetration Testing: The practice of simulating cyberattacks on a computer system, network, or web application to identify vulnerabilities that could be exploited by real attackers (www.cisco.com).

Phishing: A fraudulent attempt to obtain sensitive information, such as usernames, passwords, and credit card details, by disguising it as a trustworthy entity in electronic communication (Alexander, 2023).

Security Audit: A systematic evaluation of an organization's information system, assessing its security policies, processes, and controls to identify and rectify vulnerabilities (www.cisco.com).

Threat: Any potential danger that can exploit a vulnerability, leading to a security breach or compromise (RiskOptics, 2023).

Vulnerability: A weakness or flaw in a system's design, implementation, or configuration that could be exploited by a threat to compromise the system's security (ISO 27005).

Zero-day Exploit: An attack that takes advantage of a software vulnerability on the same day it becomes known to the public before a fix or patch is available (Guo et al., 2021).

Definitions Of Different Cyber Risk Categories

Authentication and Authorization Risk: The risk associated with weaknesses in authentication and authorization mechanisms, including inadequate access controls, could lead to unauthorized access and data breaches (RiskOptics, 2023).

Cloud Security Risk: The risk related to storing, processing, and accessing data and applications in cloud environments, including concerns about data privacy, compliance, and the security of cloud service providers (www.cisco.com).

Critical Infrastructure Risk: The risk associated with cyber threats targeting essential services and infrastructure, such as energy, transportation, and healthcare, which could have severe consequences on public safety and national security (www.cisco.com).

Cyber Espionage Risk: The risk of unauthorized access and theft of sensitive information or intellectual property by nation-states, competitors, or cybercriminals for political, economic, or strategic purposes (RiskOptics, 2023).

Data Breach Risk: The potential for unauthorized access, acquisition, or disclosure of sensitive information, leading to the compromise of individuals' privacy and organizational data (Guo et al., 2021).

Denial of Service (DoS) Risk: The risk of cyber attackers disrupting or overwhelming a network, system, or service, rendering it temporarily or permanently unavailable to legitimate users (Guo et al., 2021).

Emerging Technology Risk: The risk associated with the adoption and integration of new and emerging technologies, such as artificial intelligence, blockchain, or quantum computing, may introduce novel security challenges (Merriam-Webster.com).

Incident Response Preparedness Risk: The risk of inadequate planning and preparedness to effectively respond to and mitigate the impact of cybersecurity incidents, leading to prolonged disruptions and increased damage (RiskOptics, 2023).

Insider Threat Risk: The risk associated with employees, contractors, or other insiders intentionally or unintentionally causing harm to an organization's cybersecurity, often by exploiting their access privileges (Guo et al., 2021).

Internet of Things (IoT) Risk: The risk arising from the interconnectedness of devices in the IoT ecosystem, where vulnerabilities may be exploited to gain unauthorized access, disrupt operations, or compromise data (RiskOptics, 2023).

Malware Risk: The likelihood of malicious software, including viruses, ransomware, and spyware, infiltrating computer systems to cause damage, steal data, or disrupt operations (Merriam-Webster.com).

Mobile Device Security Risk: The risk associated with the use of mobile devices, including smartphones and tablets, which may be vulnerable to attacks and unauthorized access, leading to data breaches or other security incidents (www.cisco.com).

Phishing Risk: The potential for cybercriminals to use deceptive emails, messages, or websites to trick individuals into divulging sensitive information, such as passwords or financial details (Merriam-Webster.com).

Physical Security Risk: The risk of unauthorized access or damage to physical infrastructure, hardware, or devices, which could lead to a compromise of cybersecurity (www.cisco.com).

Ransomware Risk: The risk of malicious software encrypting an organization's data, demanding a ransom for its release, and potentially causing significant operational and financial damage (ISO 27005).

Regulatory Compliance Risk: The risk of failing to comply with relevant cybersecurity regulations, industry standards, or legal requirements, which may result in fines, legal consequences, and reputational damage (ISO 27005).

Social Engineering Risk: The risk associated with attackers manipulating individuals through psychological tactics to deceive them into divulging sensitive information or performing actions that compromise security (ISO 27005).

Supply Chain Risk: The risk arising from vulnerabilities in the supply chain, where cyber attackers exploit weaknesses in third-party vendors, partners, or service providers to gain access to the target organization's systems (ISO 27005).

Third-party Software Risk: The risk associated with using or relying on third-party software or applications, which may have vulnerabilities that could be exploited by cyber attackers (RiskOptics, 2023).

Zero-day Exploit Risk: The vulnerability arises from attackers exploiting undisclosed and unpatched software flaws, posing a risk before security updates or patches are available (RiskOptics, 2023).

Chapter One

Introduction

1.1 Introduction

This dissertation investigates loopholes and level of cyber-risk resilience in Emirati banking, aiming to shed light on how effectively employees and management can mitigate the consequences of cyberattacks resulting from loopholes in an institution's cyber resilience. The primary objective of this project is to motivate and guide Emirati financial institutions towards implementing robust cyber-risk resilience measures to cover up any loopholes that might leave them prone to attacks. The UAE government's determination to modernize the economy via growing dependence on Information and Communication Technology (ICT) is shown in the case study organization, Bank ABC, in Dubai, UAE.

1.2 Motivation and Research Scope

The Statistical Significance of cyber-resilience has been underscored by researchers for decades (Li & Liu, 2021), with studies like Munusamy et al. (2023) recently confirming its importance. Despite this attention, a lack of comprehensive understanding of the dangers of loopholes in the banking cybersecurity system often leads to negligence, posing a significant threat to e-commerce institutions, as Akter et al. (2022) emphasized. Recent research has shown that a more profound comprehension of technology-related risks can substantially reduce vulnerability, as Yuchong et al. (2021) indicated. This dissertation investigates current loopholes in Bank ABC's cybersecurity

system, proposes mitigation strategies, and explores emerging cybersecurity concerns within the UAE's banking industry.

1.3 Background of Research

The prioritization of cyber-resilience is underscored by the research conducted by Fang-Yi Lo et al. (2020) and Myriam et al. (2023). who argue that a system cannot be considered secure solely based on perceived security. Resilience, although unable to prevent attacks, aids in the swift recovery of businesses following a security breach. The UAE's Telecommunications Regulatory Authority (TRA) unveiled "The UAE's National Cybersecurity Strategy" in 2020, demonstrating a commitment to creating a secure cyber-infrastructure for inhabitants and businesses. This strategy, controlled by the TRA, encompasses five pillars and 60 programs. The primary goal of this dissertation is to thoroughly examine the current cybersecurity systems and protocols at Bank ABC by identifying vulnerabilities, flaws, loopholes, or weaknesses. The ultimate objective is to provide key recommendations and guidance supporting a more resilient, robust and trustworthy cybersecurity infrastructure and systems at Bank ABC.

Kaspersky (2022) has identified cybersecurity vulnerabilities in the UAE, with Emirati institutions and other critical sectors fearing cyberattacks, often targeting Western governments and established economies. The newly established Cyber Security Centre (2020), under the TRA, reports that the UAE ranks as the second most targeted country after the United States, facing attacks from criminal organizations, intelligence agencies, and terrorist groups. According to the Cyber Security Centre (2020), state-owned energy companies and smaller financial institutions are particularly vulnerable to cyber-attacks. Data from Kaspersky (2022) also reveals that two million Emiratis are vulnerable to cyberattacks, positioning the UAE as the nineteenth most vulnerable

country worldwide. This vulnerability underscores the logical efforts of the UAE government, spearheaded by the TRA, to safeguard critical infrastructure from potential attacks. This research focuses on cyber-resilience and awareness to protect UAE financial institutions and enhance overall cybersecurity.

Previous works by Yunhan et al. (2022) and Zengwang (2022) have delved into aspects of cyber-resilience. However, the BSI/ISO (2022) and COSO (2023) provide recent comprehensive cyber-security frameworks, though integration into a conceptual framework still needs to be explored. This refers to information security and risk management standards published in 2022 by the International Organization for Standardization (ISO) and Germany's Federal Office for Information Security (BSI). These provide best practices for implementing holistic cybersecurity. The COSO (2023) framework stands for the Committee of Sponsoring Organizations of the Treadway Commission, which published its updated enterprise risk management framework in 2023. This covers guidance across cybersecurity, compliance and operational resilience. These two frameworks comprehensively articulate cybersecurity controls, governance, risk assessment, etc., but there remains room for further integration into a conceptual model synthesizing their fundamental elements. Previous topic-specific works exist but do not deliver robust, holistic cybersecurity frameworks that the ISO, BSI and COSO provide; however, integrating these frameworks into a single unifying conceptual model can be further explored.

The loophole refers to a gap or weakness in the cybersecurity frameworks ISO/BSI and COSO provided. While these frameworks are comprehensive, they must be integrated into a unified conceptual model (Asaad, 2021).

The ISO/BSI frameworks prioritize technical controls and IT security, whereas the COSO framework strongly emphasizes risk management and governance. Nevertheless, there exists a

chance to amalgamate the fundamental components of these frameworks into a comprehensive cybersecurity model.

Some potential loopholes include:

1. Lack of guidance on organizational culture and human factors related to cybersecurity
2. Insufficient integration of operational resilience and business continuity practices
3. Absence of a standardized methodology for cyber risk assessments
4. Need for further contextualization based on organization size, industry, risk appetite

The loophole represents an opening in the current frameworks that could be filled through additional research. By integrating existing standards like ISO, BSI and COSO, there is potential to develop a more robust, overarching cybersecurity framework.

Properly addressing this loophole would involve delineating the boundaries and intersections of the current frameworks and synthesizing their components into a unified model. This conceptual framework will provide holistic guidance tailored to organizational contexts and needs. Overall, the loophole highlights an opportunity for further research and theory-building to advance cybersecurity frameworks and practices.

This research also examines the intricate interplay of various factors to assess how different variables impact cyber-resilience, focusing on the ability to deliver the intended outcome despite continuous adverse cyber events. Cyber-attacks, system failures or human errors are inevitable - and damaging. Cyber resilience enables preparation and adaptation to disruptions to meet shifting threats and maintain operations during crises. Cyber-resilience has been widely adopted. However, many cyber-risk management frameworks should emphasize detecting and mitigating threats more

than the advantages of constructing a cyber-resilient system, as Yunhan et al. (2022) point out. Existing cyber-security conceptual frameworks, such as BSI (2022), must adequately prioritize cyber resilience and awareness of prevalent cyber threats, limiting their applicability in the UAE.

The relationship between cyber resilience, awareness, and vulnerability mitigation remains underexplored, as Carías et al. (2020) highlighted. This knowledge gap hinders the assessment of cyber-resilience within organizations and its connection to cyber-risk awareness. Further research is needed to address this gap and enhance understanding, emphasizing multidisciplinary cooperation and idea integration to establish a robust foundation for the UAE's financial sector and critical infrastructure.

The UAE government's aspiration to attract foreign direct investment underscores the need for a secure cyberspace (UAE Government, 2020). Protecting vital services and the financial sector from cyberattacks of all sizes is of the utmost importance. This research's foundation lies in fully grasping an issue before attempting to solve it. The existing knowledge gap in the UAE banking industry's cyber risk awareness and resilience necessitates swift action, and this dissertation aims to elucidate the issue and offer relevant insights for its resolution.

1.4 Problem Statement

Cyber-resilience is essential for the banking sector and other critical infrastructure, as noted by Yunhan et al. (2022). Existing cyber-risk management strategies and recommendations prioritize detection and mitigation over resilience enhancement (Taherdoost, 2023). This research addresses

two key research challenges while providing comprehensive recommendations to the UAE financial industry:

1. UAE financial institutions lack a specific cyber-resilience measurement tool, even though plausible methods have been proposed, as Carías et al. (2020) suggested. This gap is especially critical given the rapid expansion of the Internet of Things (IoT), which introduces significant security challenges because of the access it creates for the free sharing of information over the Internet through interconnected devices and networks without much interference (Taherdoost, 2023).

2. Human, technological, and organizational factors collectively render all cyber-systems vulnerable, as articulated by Shaikha et al. (2021), and according to these researchers, analyzing these factors at an institutional level is complex due to the diverse range of personality characteristics.

1.5 Aim and Objectives

This project aims to develop a novel conceptual framework for cyber-resilience that can be customized to meet the specific requirements of Bank ABC. It will also develop tools to help UAE financial sector management assess the nature and extent of external and internal cyber risks and the efficacy of existing responses and resilience systems. This research aims to develop a

theoretical framework for evaluating cyber resilience in UAE financial institutions. The following research aims were designed to accomplish these goals:

1. Design a theoretical structure for rating a system's resilience against cyberattacks.

2. Recognize emerging cyber-risks and investigate the connection between cyber-risk awareness and resilience.

1.6 Research Questions

This research addresses the following research questions:

1. How can cyber-risk resilience be assessed and enhanced without compromising existing solutions or increasing vulnerabilities and weaknesses?

2. How can existing standards be leveraged to develop a cyber-risk resilience framework that addresses dependent variables such as organizational resilience, vulnerabilities, and weaknesses?

1.7 Dissertation Outline

The structure of this dissertation is organized as follows:

Chapter Four: Results and Analysis (Data Collection and Analysis)

Chapter Five: Discussion (Overview of Findings, Validity, Discussion of Hypotheses)

Chapter Six: Conclusions and Recommendations (Accomplishments, Contributions, Implications, Limitations, Future Research)

Chapter 1: Introduction

The first chapter of this research will describe our analyses' scope, context, logic, goals, and objectives. The study will specify parameters to define its scope and limit our investigation. Define the principal domains and aspects to be explored. The background section will examine the loopholes and cyber resilience, highlight relevant past studies, and identify gaps in current understanding to provide context. This research aims to explain the Statistical Significance and relevance in the contemporary setting, so emphasizing practical applications will accomplish this. The research will also outline its goals to give a logical framework for its desired results, ensuring the objectives match the research goals. The design of research questions will guide the investigation and help attain research objectives. These questions will guide the study and provide a framework for analysis and discussion in the following chapters.

Chapter 2: Literature Review

Chapter 2 will situate the study within the scholarly discussion, making it vital as it focuses on cyber-resilience, risk concepts, and cyber frameworks. The cyber-resilience discourse will examine numerous definitions and conceptualizations and how institutions survive and recover from attacks. This chapter will also examine cybersecurity risk in all its forms, including threats, vulnerabilities, and mitigation strategies; it seeks to create a solid theoretical foundation for cyberspace risk and evaluate cyber frameworks, including the NIST Cybersecurity Framework,

ISO 27001, and others. Corporations use established standards and best tactics to improve their cybersecurity.

Chapter Three: Research Design and Methodology

Chapter Three details the research approach and methodologies used in this study. This will illuminate the steps to conduct a thorough investigation at several levels. The following section will explain the sampling methods used to pick research participants and data sources and justify the approach. The methodology section will describe the data gathering and analysis methodologies and tools. The study proposal would also include ethical issues and procedures to conduct the research responsibly. This study will also describe the research site, including the physical or virtual settings where data was collected.

Chapter Four: Results and Analysis

Chapter Four presents the data collection and analysis results, representing the research's culmination. This section will use tables, graphs, and other graphics to explain the research findings.

Chapter Five: Discussion

Chapter Five lays the groundwork for analyzing research results. The report will begin with a concise overview of Chapter Four's key results. This study will critically assess the research's validity, focusing on the reliability and trustworthiness of data collection and analysis methods. This chapter will thoroughly examine the hypotheses to see if the results support or refute them.

Any contradictions, unexpected results, reasons, or implications will be scrutinized. This section will discuss the study's more significant ramifications and relevance to existing understanding.

Chapter Six: Conclusions and Recommendations

This dissertation will summarize the research's findings, stressing its substantial contributions to cybersecurity and related fields. This study will also analyze the implications of the findings for field workers, politicians, and researchers, emphasizing their practicality. This chapter acknowledges the restrictions encountered throughout the study, identifying areas that need further study. Further research will be suggested in the report to expand and overcome current limitations.

Chapter Two

Literature Review

2.1 Introduction

This literature review is designed to provide a comprehensive and up-to-date overview of the key concepts and research related to cyber resilience and cyber risk in the context of Bank ABC. The review is the foundation for our research, focusing on recent developments and insights to support our objectives. This chapter's primary objective is to thoroughly analyze the underlying concepts of cyber resilience by reviewing the existing literature. An organization's ability to rebound from cyber-attacks is assessed through utilizing a cyber resilience matrix and various other

methodologies. The capacity to adapt to novel situations, expertise in gathering and evaluating data, and creating robust defensive mechanisms are all of the highest importance in this endeavour.

2.2 Cyber Resilience

Cyber-attacks are a significant problem for modern businesses all around the world. This menace spreads its tentacles across several spheres, including business, government, academia, and the public. A new area of study, cyber resilience, has arisen to deal with broadening and deepening cyber dangers beyond the purview of traditional cybersecurity (Ross et al., 2021). According to Ross et al. (2021), cyber resilience refers to an organization's ability to rebound from significant cyberattacks, and it is particularly critical for entities such as governments and financial institutions that are high-priority targets. The repercussions of a cyberattack on the financial industry can be devastating, making cyber resilience a top priority. In essence, it becomes the lifeline for an organization's survival in the face of coordinated cyberattacks.

When we consider cyber resilience's role in safeguarding digital spaces and the physical processes that underpin our lives, its Statistical Significance becomes increasingly apparent. Threats to human life, ecological stability, and the continuity of physical activities can all be precipitated by

incidents involving essential infrastructure and systems. Cyber resilience is becoming increasingly important to keep these vital parts of our lives safe (Ross et al., 2021).

2.3 Cyber Risks and Security

Cyber risks and security involve sensitive customer/employee records, intellectual property, system logs, databases, emails, archives, etc. Risks, including data theft, leakage, corruption, deletion or ransomware, have evolved rapidly, with cyber risk now recognized as a top corporate concern (Akter et al., 2022). In recent years, organizations have experienced a growing reliance on digital business operations, necessitating enhanced cyber threat protection. While security remains essential for cyber defence, it is crucial to consider the paradoxical nature of security. Secured data becomes less available over time, while available data becomes less secure, highlighting the delicate balance that institutions must maintain to protect their assets.

Insurance coverage to safeguard institutions against cyber threats is now possible, although the focus should extend beyond insurance to resilience. In this context, resilience refers to an organization's ability to sustain its operations following cyberattacks (Ross et al., 2021). This highlights the necessity of professional response teams to manage such attacks. The increasing frequency and complexity of cyberattacks have presented unique challenges for standards organizations and frameworks, such as Velocity of change, Increasing complexity, Lack of

historical precedents, and Constraints around precision. These challenges include addressing the evolving nature of cyber threats and their impact on organizations.

2.4 Statistics on Cyber-attacks in the UAE

1. The trend toward remote work has resulted in a 190% rise in cyber-attacks in the UAE, including 15.8 million brute force attempts on Remote Desktop Protocol (RDP) (ITP, 2021).

2. In 2020, the Middle East saw more than 2.57 million phishing attacks, with the UAE seeing a substantial 250% increase in phishing attacks that year, primarily due to phishing and

ransomware instances. ITP (2021) estimates that 72% of CISOs in the UAE are unprepared to cope with phishing attempts in their organizations.

3. The UAE's economic toll from cyber-attacks reached $1.4 billion in damages in 2020. These findings highlight the critical need to strengthen cybersecurity measures and increase resilience in the face of increased cyberattacks (ITP, 2021).

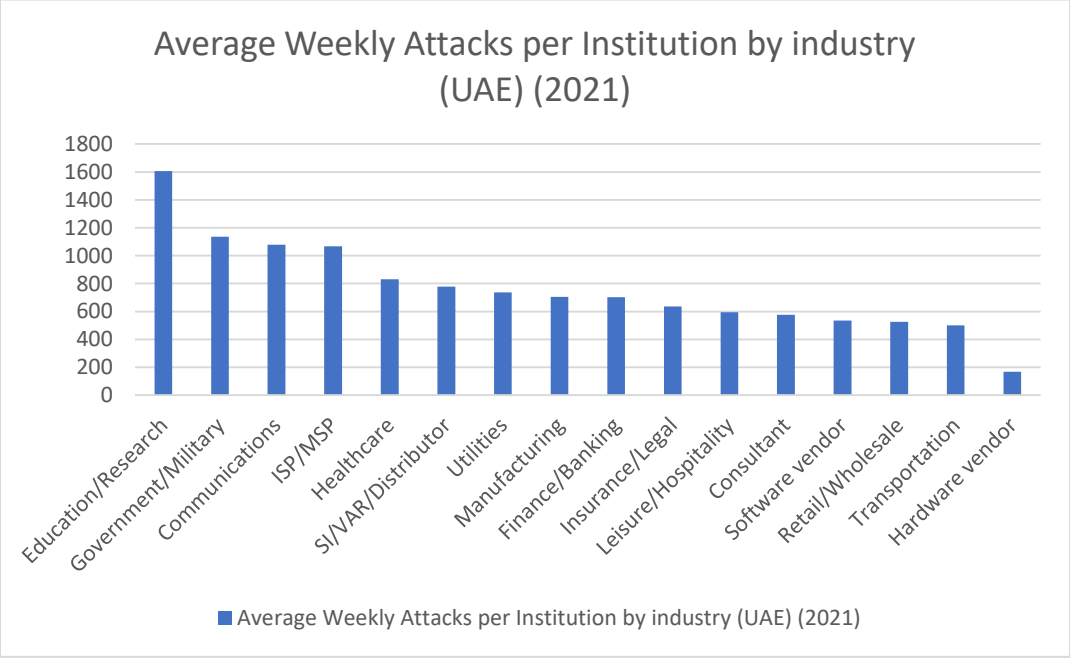

Figure 2:1: Average Weekly Attacks per institution by industry (UAE) (2021)

Source: www.techxmedia.com

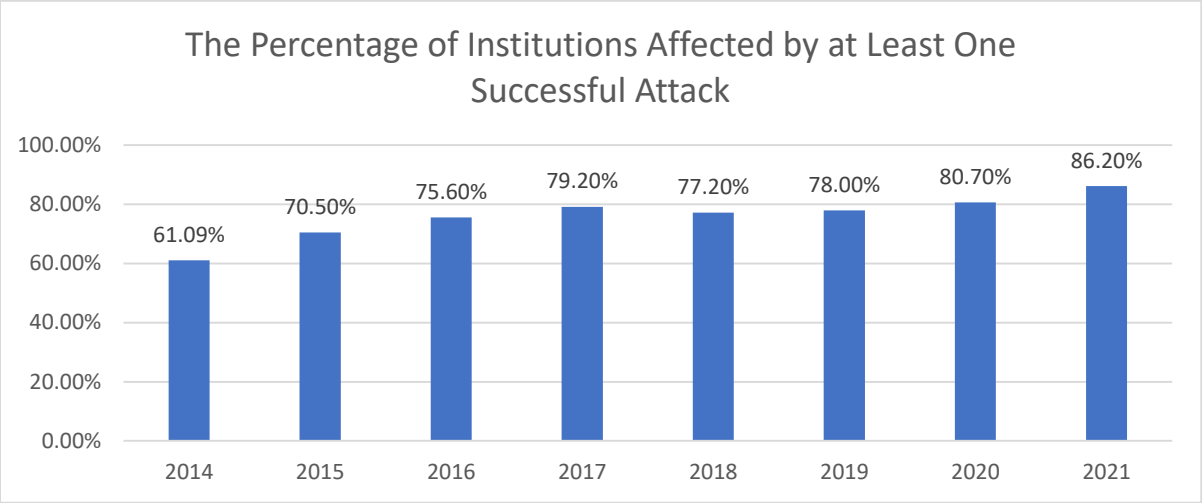

Figure 2.2: The percentage of institutions affected by at least one successful attack.

Source: www.comparitech.com

2.5 Existing Frameworks for Cyber-Risk Management

In the digital age, institutions connected to the internet must have adequate cyber protection and detection systems (Allianz, 2023). A cybersecurity framework refers to standardized guidelines, best practices, and processes that help organizations manage cyber risks and improve their cybersecurity posture (Ross et al., 2021). As Ross et al. (2021) define, "A cybersecurity framework provides a common language and mechanism for organizations to describe, manage, and improve their cybersecurity risk management processes."

Cybersecurity frameworks help organizations align and prioritize their cybersecurity initiatives to reduce vulnerabilities, detect threats, respond to incidents, and strengthen resilience against cyber-

attacks. As Munusamy et al. (2023) discuss, frameworks provide structured guidance to develop "holistic cybersecurity and cyber-resilience risk management" customized to different industry sectors.

A range of established cybersecurity frameworks globally serve as helpful reference models for organizations. Examples include the ISO/IEC 27001 standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which focuses on information security management. The US National Institute of Standards and Technology (NIST) also defines the widely adopted NIST Cybersecurity Framework. Tariq et al. (2023) explain that "The NIST framework characterizes cybersecurity activities into functions like identify, protect, detect, respond and recover." This aligns cybersecurity programs with business requirements, risk assessments, and improvement processes.

Other governance-focused frameworks like the COSO Enterprise Risk Management framework guide cybersecurity controls, compliance, resilience processes and integrating cyber risks into overall enterprise risk oversight (COSO, 2023). So, while various frameworks have different emphasis areas, they collectively enable systematic and strategic cybersecurity management aligned with organizational objectives. As Carías et al. (2020) summarize, frameworks facilitate evaluating "technological and procedural controls already implemented" and directing security investments.

However, generic security guidelines must often be revised to address specific issues. This research focuses on enhancing the comprehension of cyber risks and resilience among employees and within financial systems. Incorporating these concepts into organizational procedures may only partially align with emerging Cyber Resilience Management (CRM) frameworks. These frameworks aim not only to minimize the occurrence of cyber-attacks but also to mitigate their effects comprehensively. See Table 2.1 for cyber security and cyber resilience framework.

This literature review provides a contemporary understanding of cyber resilience and risks, setting the stage for our research. We will further investigate the relationship between cyber resilience and cyber risk readiness, with a particular focus on the role of employee skills and capabilities. These insights will inform our research methodology, align with best research practices and address ethical considerations.

Table 2.1 Cyber Resilience and Cyber Resilience Framework

Cybersecurity	Cyber Resilience
Definition: The term "cyber security" refers to the activity of protecting digital assets such computers, servers, mobile devices, electronic systems, networks, and data against intrusion (Kaspersky, 2023)	Definition: Resilience is defined as "the capacity of a system to detect, respond to, recover from, and adapt to stresses, attacks, or compromises on its cyber resources" (NIST SP 800-172).
Innovative solutions and protocols engineered to safeguard organizations against cybercrime.	Resilient technologies and protocols engineered to ensure uninterrupted service delivery despite cyber incidents.
Aims to protect the company from cybercrime and espionage and reduce the possibility of cyberattacks (www.securityboulevard.com).	Strives to maintain continuity across diverse domains, balancing cybersecurity and business imperatives (www.ibm.com)
Demonstrates efficiency while preserving the usability of other systems without compromise.	Demands a comprehensive organizational culture shift to integrate and normalize security best practices.
Incorporates a business continuity plan to ensure the resumption of operations in the event of a successful attack (www.ibm.com).	Mandates the institution to cultivate agility and adaptability in response to cyber-attacks and incidents.

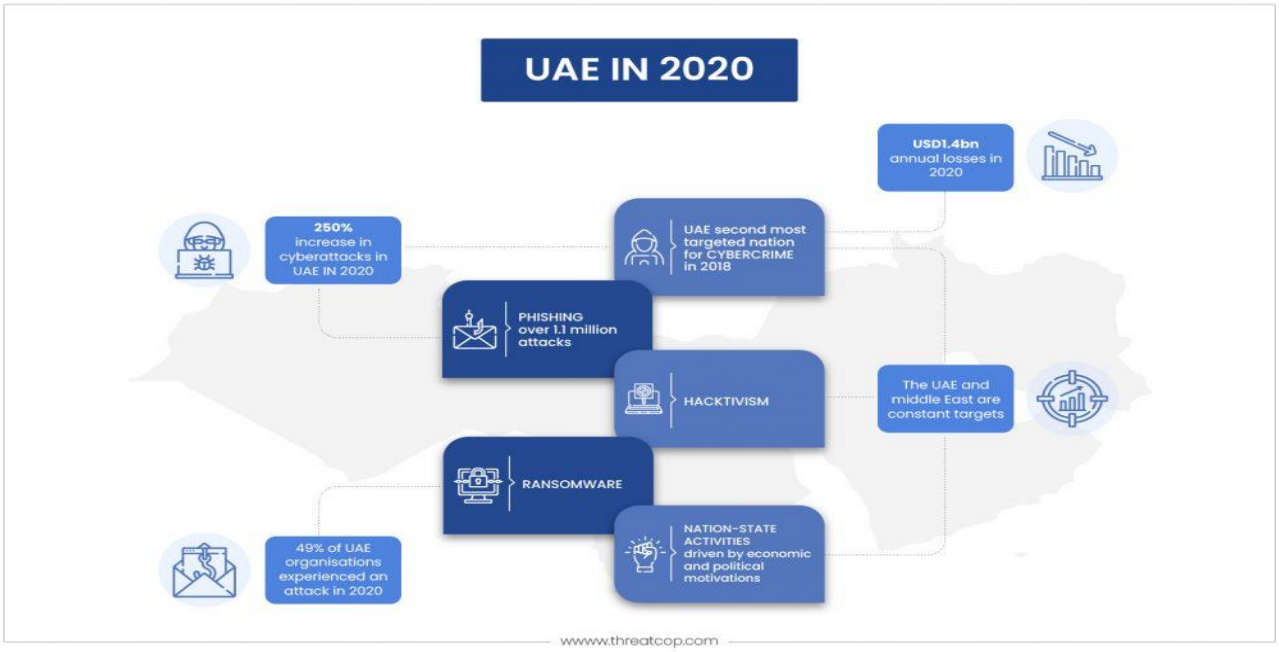

Figure 2.3. Rise in Cyber Attacks in UAE In 2020

Source: UAE News

2.6 Modern Terrorism and Cyber-Attacks

Cyber-terrorism aligns its strategic goals with traditional terrorism, with a primary objective being disrupting the functions of opposing governments or entities. While cyber-terrorism shares some similarities with its conventional counterpart, its defining characteristic lies in its execution mode, predominantly within the digital domain. As highlighted by experts in the field, such as Alok et al. (2022) and Alawida et al. (2022), much like traditional forms of terrorism, cyber-terrorism often requires financial support, which is frequently obtained through illicit means. While government websites and information centres are commonly targeted by cyber-terrorism due to their political and strategic Statistical Significance, ordinary commercial enterprises in the UAE must not underestimate the potential threat. Although cyber-terrorism is relatively new in the security

landscape, every new security framework should incorporate an awareness of its potential occurrence. This means vigilance is paramount in effectively managing this evolving and intricate risk.

Given that governments and organizations in the UAE continue to rely increasingly on digital infrastructure and online operations, the convergence of terrorism's objectives with cyber-attacks poses a multifaceted challenge. This underscores the need for continuous attention and proactive measures to safeguard against potential cyber-terrorism activities.

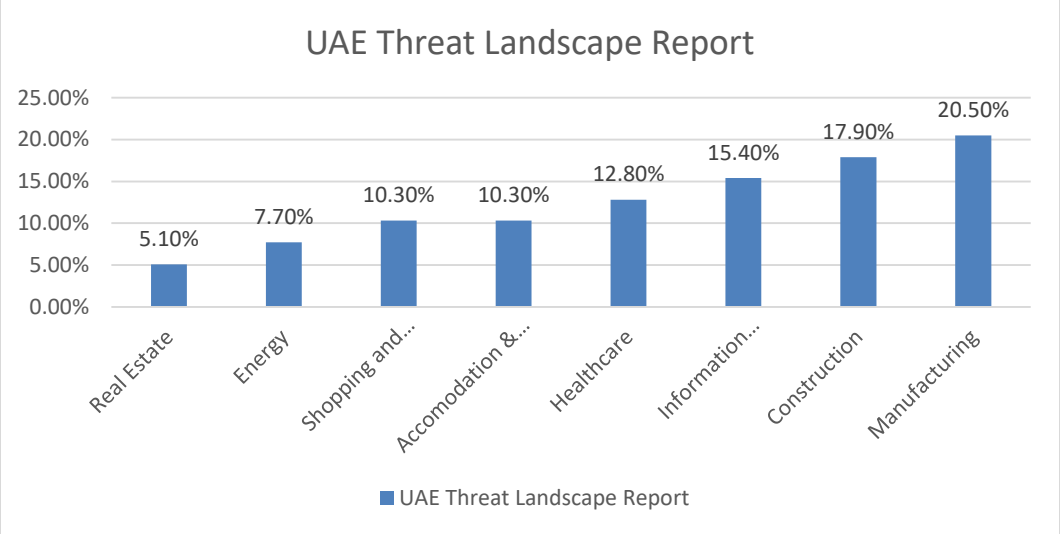

Figure 2.4 UAE Threat Landscape Report

Source: https://socradar.io

2.7 The Development of Cyber-Risk Management Frameworks

As modern institutions become increasingly reliant on interconnected digital systems for core operations, the imperative of cyber risk management continues to grow (Janna et al., 2023). Cyber

risks now refer to threats that can adversely impact confidential data, critical infrastructure, and service continuity due to reliance on cyberspace.

Initially, "critical infrastructure" pertained to essential physical and digital systems enabling key economic and financial activities (Joel, 2023). However, the scope has expanded to include sectors like banking, insurance, energy, water and communications that face cyber risks affecting both traditional and emerging business models.

Conventional risk management revolves around financial, hazard and insurance hedging. Failure to mitigate these risks can have disastrous consequences, especially with greater dependency on cyber systems (Janna et al., 2023). Therefore, specialized Cyber Risk Management (CRM) frameworks are needed to manage unique cyber threats. Probabilistic Risk Assessments (PRAs) have been proposed to quantify adverse cyber event likelihood and impact (RUI, 2022). However, CRM strategies have evolved further due to difficulties predicting rapidly emerging cyber threats. Advanced solutions like Hierarchical Holographic Modelling (HHM) filtering and ranking have been suggested, but CRM is an evolving field.

A key challenge is the interdependencies of threats, vulnerabilities and response mechanisms, traditionally treated as isolated domains. An integrated, system-wide perspective is required for cyber risk planning (Akter et al., 2022). As cyberspace intrinsically connects multiple stakeholders, institutions must coordinate CRM while managing their cyber risks. Emerging frameworks provide vital guidance to continuously evaluate controls, resilience processes and coordinated action against systemic cyber risks.

2.8 The Importance of a CRM Framework

According to Akter et al. (2022), effective cyber risk management is essential in today's interconnected business environment due to growing dangers. The complex computer systems that link suppliers, customers, and their networks form a "neural network" of interdependencies. This highlights the challenge of creating a universal protection framework and the scope of the issue. Smartphones have introduced new security weaknesses because background apps can compromise security, so it is understandable that Cyber Resilience Management (CRM) framework literature may only sometimes apply. Table 2.2 shows how the UAE's cyber laws differ from those in other developed countries.

Table 2.2 Analyzing cyber laws across nations, including the UAE, UK, USA, and South Korea.

	UAE	Other Developed Countries
Variant laws	A sole cyberlaw	South Korea has enacted a number of distinct laws to combat the vast array of potential cybercrimes.
Revisions	Revised in 2012	The cyber statutes of the United Kingdom, the United States, and South Korea undergo periodic revisions
Complexity	Simple and basic in nature	These cyber regulations are regularly updated and revised to account for changes in technology and the evolving nature of online threats
Magnitude of crime	It makes no distinction between accidental and purposeful violations of the agreement	The laws in the UK, the US, and South Korea all have distinct approaches to various forms of cybercrime
Type of breach	It makes no distinction between accidental and purposeful violations of the agreement	There is a distinct legal distinction between various forms of cybercrime under the laws of the United Kingdom, the United States of America, and South Korea
Financial damage	There is a lack of clarity on the punishment for monetary damages	The purpose of these laws is to ensure that those who commit cybercrime are held accountable for their acts and to

		offer victims with legal options to recoup whatever money they may have lost
Classification of offences committed online	The law does not yet have clear classifications for the many forms of online offences	Every nation crafts its own unique set of cyber laws, based on the particulars of its judicial system, the threats it faces, and its top objectives

Source: Gulf News

Alok et al. (2022) emphasized event readiness over prevention, as well-designed frameworks can prevent data breaches and other issues. Business continuity plans must incorporate cyber- and operational risks. Tech firms need catastrophe recovery plans, so these institutions must prepare for a cyberattack and have a thorough recovery and continuity plan. This kind of attack prevention system relies on employee data management knowledge.

A complete CRM strategy needs Human Resources, so governments and companies should work together to "secure cyber-space" (Tariq et al., 2023) and improve security, but no solution is risk-free. According to Alok et al. (2022), cyber threats often include people, so these risks rise with fraud, property theft, and harmful software and infections. This may impact how risks are viewed if disregarded. A robust cyber risk management framework must bridge technological systems, business processes, personnel capabilities, and procedural controls to minimize risk exposure. The proposed CRM model aligns with the direction of this framework to strengthen human-technology coordination and resilience against financial sector cyber risks. Evaluating employee awareness and organizational preparedness will inform the balanced implementation of the framework, specifically in the UAE context.

Cyber risk management should not disregard "human components," and the Chief Security and Information Security Officers manage employees and computers. Saxena et al. (2020) emphasize awareness while developing a new framework and argue that companies must confront " threats

from within their organization". The Cybersecurity and Infrastructure Security Agency (CISA, 2020) defines an insider threat as the risk that an individual with authorized access may, intentionally or unintentionally, cause harm to the department's mission, resources, personnel, facilities, information, equipment, networks, or systems. Violence, espionage, sabotage, theft, and cybercrime are just some of the many forms that insider threats can take. These precautions may not be adequate to thwart determined and sophisticated attacks; thus, banks should create an appropriate and effective Cyber Risk Management (CRM) framework.

2.9 The Dubai Vision of Cyber Safety

The Dubai Electronic Security Centre (2023) aims to make Dubai the leader in electronic and physical security. The ultimate goal is to make residents, employees, and tourists feel safe. This aim is implemented via risk awareness and timely responses to new and current physical or electronic threats. Dubai aims to be the safest place in the world for inhabitants and tourists by fostering proactive risk management and swift threat resolution.

2.10 Risk Awareness

Threat awareness also includes "human error" as a risk, so supervisors and workers may not know current dangers. As Allianz (2023) stated, emerging hazards are ideally discovered later than "hidden risks", and data system integration makes company operations unpredictable, making mergers and acquisitions risky (Akter et al., 2022). Data loss, distortion, and attack vulnerability can vary widely per system. According to research by Joel Witts, data integration gives hackers access to more information. (2023), present or former workers and contractors

pose the second largest cybersecurity risk. Risk awareness is the first step in risk avoidance or reduction, but only people aware of cyber risks can reduce hazards (Akter et al., 2022).

2.10.1 Human Error in Cybersecurity and Resilience

Accepting human mistakes and understanding human problems and causes is necessary to execute cybersecurity and resilience methods. Furthermore, a genuine commitment to solving these issues is essential. Problems with people are more complex to address than technological ones. According to Janna et al. (2023), personal concerns should be more straightforward than technological ones. The researchers recommended routinely updating user-credentialed application passwords, and they observed that postponing password changes and software upgrades undermines IoT device security. Yeo (2022) states that human errors cause fraud, phishing, and crime, while staff carelessness causes DoS attacks. Lack of motivation raises the likelihood of over-the-shoulder attacks (OSA) when an outsider discreetly watches an operator input a password (Vijay, 2022). Password strength allows workers to monitor their surroundings, so Vijay (2022) suggests "gesture passwords" and "swipe passwords" to decrease offline shoulder surfing, as strong passwords keep off unwanted access. Aratek (2022) recommends iris or fingerprint scans for computer access to combat laziness, as duplication and interchange are complex; therefore, biometric data is safeguarded. With biometric authentication, password changes are less critical as efficient access control decreases the risk of personnel having access credentials and ensures new hires have appropriate privileges.

2.10.2 Financial Fraud

The actions of auditors and accountants can significantly decrease internal financial fraud, but understandably, administrative staff with advanced computer skills can circumvent their actions to perpetrate fraud. Gov.uk (2022) indicated rising UK computer fraud as it showed that if there is to be success in curbing the unfortunate trend, then its success depends mainly on distinguishing "computer misuse" from "computer fraud". External risks are persistent, while internal threats are difficult to spot (Shaikha et al., 2021). However, a thorough audit and effective financial management can reduce these risks.

2.10.3 Criminal Elements

This attack was infrequent before 2000, and according to Alawida (2022), the frequency of cyber-attacks was shallow before 2000. The research also shows that young people are likelier to be behind the attacks. The report by Alawida (2022) stated that some of these youths think their actions are moral or lawful since no one is physically hurt. However, these events have enhanced cyber risk awareness. To reduce the possibility of being targeted by these criminals, the system's security has to be updated and enhanced and the human resources of financial institutions must handle employee complaints before they become organizational issues.

2.11 System Limitations and Vulnerabilities

Stephen (2020) describes vulnerability as three internal and external components, and the extent of damage depends on the attacker's knowledge, access, and ability to exploit system weaknesses. This shows that vulnerabilities exceed flaws, as inaccessible defects are not

vulnerabilities since they cannot be exploited. The 2017 MITRE SVE® standard (Stephen, 2020) classifies typical vulnerabilities and exposures. Shaikha et al. (2021) argue that cybersecurity's weakest link, such as human inefficiency and other internal security factors, determines the framework's strength. However, even the finest technology barriers can be overcome. Shaikha et al. (2021) stated that system complexity vulnerability is the key concern as most modern institutions employ more complicated and surprising mechanisms. This can mean that security and usability may collide, as security-focused systems may sacrifice usability, whereas usability-focused systems may lack security.

According to WEF (2022), resilience is the ability to endure inevitable challenges, and each event must be evaluated for vulnerabilities and weaknesses. Strict standards, established methods, and contemporary technology can fix every company's fault, but these flaws and vulnerabilities must be identified. Network vulnerabilities have increased with "smart" gadgets, so every corporate network equipment has to be examined before finding vulnerabilities or security issues. This activity requires regular monitoring and administration due to smart devices. The audit method examines authentication, password updates, and password recording instead of memorizing the details.

2.12 Bank ABC (MENA Location)

Over the past four decades, Bank ABC has established a notable presence in the MENA region. The bank has a history of fostering long-term partnerships and ensuring the success of its clients. With over 4,000 dedicated employees, Bank ABC remains steadfast in its commitment to fostering expansion. Bank ABC provides clients with a banking partner who understands their unique requirements and challenges. Utilizing its extensive network, comprehensive market

insights, robust presence in 15 countries across the MENA region, and key global financial centres such as New York, London, and Singapore, the bank offers practical and individualized assistance tailored to local markets. Bank ABC Islamic provides Shari'a-compliant banking services. Bank ABC serves individuals through retail branches in Algeria, Egypt, Tunisia, and Jordan, as well as its digital, mobile-only Bank in Bahrain and Jordan. Bank ABC has a strong and stable balance sheet, a secure footprint, and a well-respected reputation among regulators, clients, and competitors in the MENA region and beyond. The bank is committed to providing an exceptional client experience, nurturing collaboration across its global divisions, and upholding its core values consistently. Therefore, having explored fundamental cybersecurity principles and Bank ABC's strengths in previous chapters, Chapter 3 will detail the research methodology to assess the bank's resilience.

Chapter Three

Research Design and Methodology

3.1 Introduction

This section describes the methodology, research philosophy, paradigm, data-collecting design, process, and analytic tools are described. It also defends the quantitative methods and discusses pilot research techniques, sample selection, and ethics. This research aims to develop a cyber resilience framework and assess UAE bank's cyberattack resilience. The chapter introduces a new theoretical framework for developing financial institutions' cyber resilience.

To reveal areas where the research instrument may be inadequate in analysis, the research design first extensively evaluates the research's surroundings to understand where the research instrument may be inadequate in analysis. The research plan details UAE financial institutions' data collection and analysis, and careful sampling was done to increase research credibility. The research aim requires quantifiable data, such as the number of users with risk awareness and knowledge of recommended behaviors. Thus, creating a questionnaire that makes these questions clear to all consumers was sensible.

3.2 Layers of Research

Saunders et al. (2023) conducted a comparative analysis of studies, drawing an analogy to the multi-layered structure of an onion. The project can be positivist, realist, interpretivist, or pragmatic, and a researcher's perspective can influence the questions and conclusions. In

positivist/realist paradigms like this research, phenomena exist independently of human awareness and can be studied.

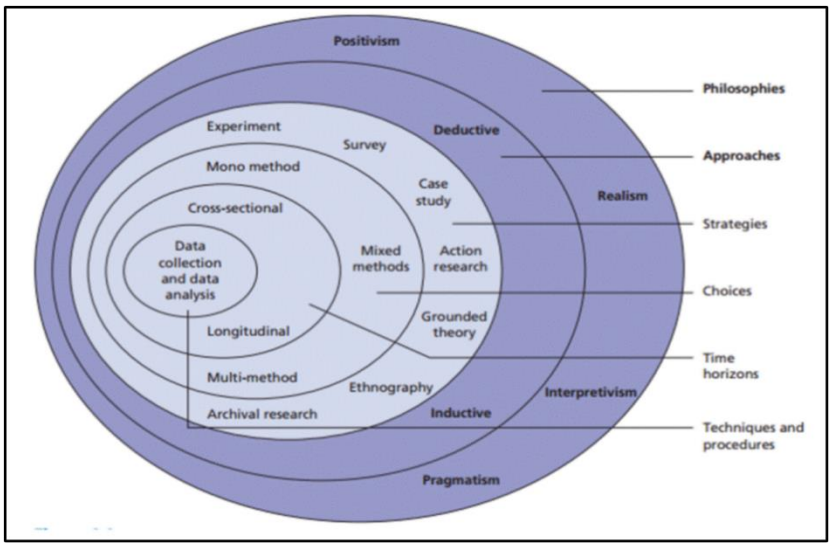

Figure 3.1 Layer of Research

(Source: Institut Numerique, 2012, n.p.)

3.3 Research Philosophy

The research employed a positivist/realist paradigm, a widely adopted approach in law and legal studies (Park et al., 2020). Deeper positivism describes the causes and procedures of law formation, and realism is positivism's most established form. The research uses a quantitative approach to analyze the organization's resilience (Wissem et al., 2020) for two reasons. There are two main reasons to examine resilience. The first goal is to objectively and quantitatively assess the situation. The second goal is to allow organizational management to compare and evaluate resilience immediately.

3.4 Selection of Samples

The sample was selected to represent the institution, and the survey would have been sent to all employees electronically. The final response rate determined the questionnaire's validity and reliability (Azraii et al., 2021). The questionnaire design may considerably impact response rates, so a rigorous approach is essential to increase response (Aithal et al., 2020).

The management and professional employees may be from the IT users' demographics, but manual employees' opinions were also acknowledged. The sample was primarily bank workers, although physical workers' accuracy and reliability were unaffected. A purposive sample was chosen (Ellen, 2022), and this plan covered operational, middle, and senior management.

The research hypothesis needed purposive sampling as, according to Ellen (2022), purposive sampling helps researchers find relevant persons or settings, and it is successful because it picks information-rich situations for detailed research.

The questionnaire was given to financial institutions' employees most likely to respond and offer helpful information as the goal was to reach potential participants. Thus, the purposive selection

technique involved vulnerable cyberattack victims and resilience concerns to address the research topic.

3.5 Rationale for Sample Size Determination

This research centres on Bank ABC as the case study within the UAE financial landscape. The study empirically investigates the cyber-risk resilience and readiness of financial organizations in the United Arab Emirates.

To ensure a focused and representative sample, purposive sampling was employed, selecting employees of Bank ABC as the research's primary subjects. The primary objective of this research is to establish a comprehensive framework for managing cybersecurity within the UAE's financial industry. Given practical constraints, a comprehensive industry-wide survey was not feasible.

In line with the findings by Quiera et al. (2021), which advocate a sample size of 100 or more for testing research assumptions, validating the conceptual model, and identifying variable correlations, the researcher adhered to established literature standards. This sample size ensures

the ability to draw valid conclusions about the broader population within the UAE financial industry.

3.6 Methodology of the Research

The research examined some selected employees of ABC Bank, utilizing firsthand data from individuals and secondary data from relevant literature and UAE government sources to assess the UAE financial sector enterprises' cyber-resilience.

The data came from 84 financial sector personnel who completed surveys. Quantitative or qualitative research and the investigator's research themes decide the data collection technique. Researchers must verify that data-collecting procedures create valuable data and conform to research paradigm philosophical assumptions (Park et al., 2020).

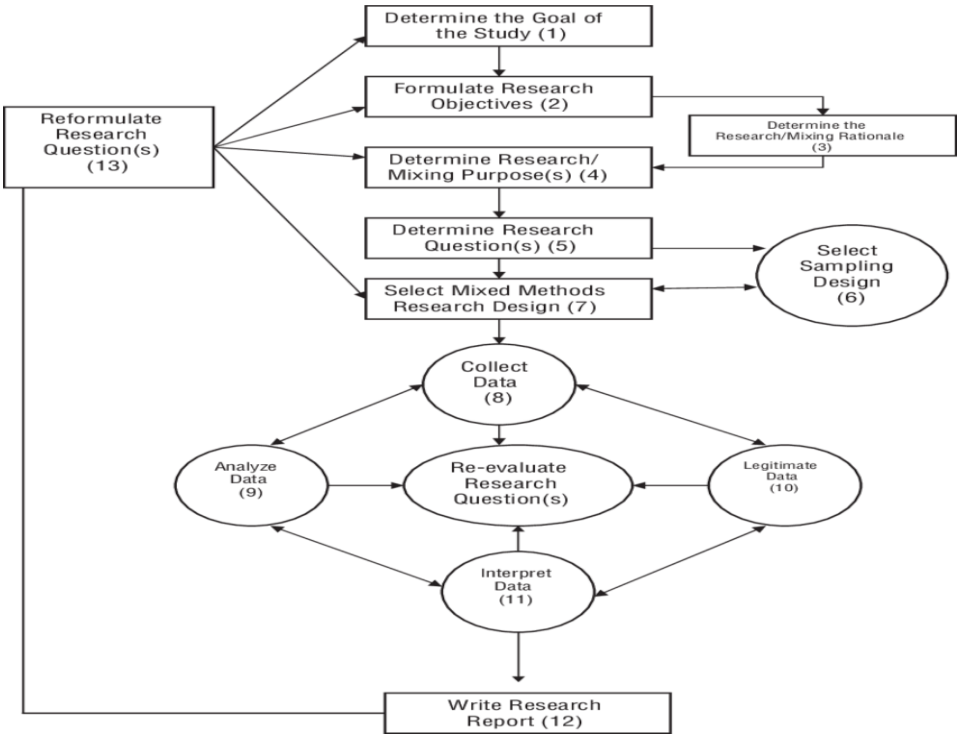

Figure 3.2 Research Design Process

Source: Rebecca K. Frels

The research's quantitative data is mostly on risk-aware and ethical users. It was reasonable since all clients could comprehend the questions. This technique eliminates qualitative aspects and uses validated survey methods (Taherdoost, 2021). The questionnaire assessed knowledge, conduct, and observations of others' behaviour, not views. The hypotheses of the research were examined

through the process of data analysis, and the findings were afterwards employed to fulfil the objectives of the research.

These are the hypotheses for the research:

Hypothesis 1: External threats cause vulnerabilities.

Hypothesis 2 Vulnerabilities and weaknesses pose internal hazards.

Hypothesis 3: Prepared responses reveal flaws.

Hypothesis 4: Responses reduce weaknesses and internal threats.

Hypothesis 5: Reaction mechanisms influence vulnerabilities, weaknesses, and external threats.

Hypothesis 6: Resilience within an organization minimizes weaknesses and risks.

Hypothesis 7: Resilience within an organization reduces vulnerabilities, weaknesses, and external threats.

3.7 Research Proposal

The three-phase research was extensive.

Phase 1: Framework Development

The variables were restructured, and contextual components were incorporated by the researcher in order to construct a comprehensive framework at an early stage. The objective was to construct

a survey that matched the UAE's workplace and met global standards. Initial testing with three microfinance banks and one commercial bank tested the questionnaire's validity.

Phase 2: Collection of Data

In this stage, the researcher randomly sampled the population. Participants self-administered the updated questionnaire using Survey Monkey after receiving it through email.

Phase 3: Evaluate and Validates Data

This phase is needed to draw meaningful conclusions and verify the findings. The vast operation's data were organized, checked, and improved. Cronbach's Alpha verified data validity, and unique descriptive statistical methods were employed to assess and validate results.

3.8 Research Location

This research analyzed Bank ABC, which is situated in Dubai. Dubai was chosen for data collection and analysis due to its financial prominence in the UAE, and a methodical approach was used to reach Dubai's financial institutions' decision-makers and stakeholders. The proximity of the employees made data collection efficient, giving a complete grasp of their cybersecurity techniques and policies.

It examined vital UAE financial institutions' cybersecurity environment and preparedness, particularly Dubai financial institutions. A localized methodology assessed context-specific elements and concerns that might impact these institutions' cybersecurity preparation. Local regulatory bodies and cybersecurity experts participated in the Dubai research. The research's

findings may strengthen UAE financial institutions' cyber resilience, making their digital environment safer for stakeholders.

3.9 Basis of Questionnaire

The hypotheses are based on the new framework's user-friendly elements. The goal was to acquire data on technology users in financial sector firms. This questionnaire was designed to obtain quantitative data. Thus, certain items were excluded because they are better for qualitative data. The survey's "informed consent" portion notified respondents of their right to opt out and assured them of anonymity. Participants were urged to email the researcher for research findings if they were interested.

3.9.1 Data Collection – Designing the Instrument

A meticulously crafted questionnaire was developed to gather empirical data for the research. Reviewing comparable surveys and adapting questions to guarantee questionnaire fit started the design process. The three independent criteria were Response in Place (RP), Organizational Resilience (ORe), and Vulnerabilities and Weaknesses.

3.9.2 Data Collection – Validating the Instrument

The Statistical Significance of doing pilot research in the validation of questionnaires is emphasized by Taherdoost (2021). The questionnaire questions were examined by a cyber-security specialist prior to the commencement of the pilot research. The objective of this step was to

establish a linkage between the questions in the questionnaire and the concepts to be evaluated. The measurement of questionnaire validity is often primarily assessed using the concept of alignment (Brinkman al., 2009). Once the principal questionnaire was validated, it was made available online, and participants were urged to complete it.

3.10 The Pilot Study

A questionnaire pilot study evaluated its efficacy before inviting participants to the main trial. Pilot studies assist researchers in testing question comprehensibility and answerability (Sekhon et al., 2022). Participants who do not seek challenges may need clarification on a question, but a well-designed questionnaire should require few or no adjustments before the primary survey.

3.10.1 The Pre-Pilot Surveys

The researcher checked the questionnaires with a statistics expert before commencing the pilot study to ensure they were relevant and met quantitative data analysis requirements. To guarantee suitability, senior and young academics carefully discussed the questionnaire. The researcher further performed a trial survey to evaluate the data collection process and approximate the anticipated time of the research, which was estimated to be one hour. The present phase of the pre-

pilot study involved revising the questionnaire and eliminating items that were found to be misleading.

3.10.2 Pilot Study Details

A six-person pilot study with three financial firms was done. The metric-maintained survey quality and question coherence. The firms had to be in Dubai, employ over 50 people, and have clear top, middle, and functional management. This pilot project only collected data from firms and individuals that accepted participation. Despite several reminders, only four of the twelve invited participants completed the survey. Six individuals left the research due to job and survey duration, and these individuals refused the event despite the deadline extension. Two top, one middle, and three operational managers completed pilot questionnaires. This indicated deliberate sampling in

rated businesses. The preliminary research corroborated the original research but got few responses.

3.11 Methods and Tools for Data Analysis

This research utilizes statistics and analysis tools for this investigation, and these methods were chosen for their consistency in producing compelling findings and supporting assertions. These processes are classified as:

3.11.1 Analytical Tools

Three methods assessed and merged the data:

- Survey Monkey is used for data collecting and analysis.
- IBM SPSS is utilized to analyze the analyzed charts.
- Microsoft Excel is utilized for analyzing.

3.11.2 Exploring Relationship Metrics

These metrics utilized two variables' characteristics and direction as this research used correlation and regression analysis. The Correlation coefficients and p-values measured variable correlation for this research. The linear regression model (Y=a+bX+e) of the dependent variable by

considering one or more independent variables. R2, the coefficient of determination, determined the two variables' correlation.

3.11.3 Coefficient of correlation

Pearson's System: r calculated variable correlation strength and direction. The analysis utilizes the SPSS science programme.

3.11.4 One-way ANOVA

One-way ANOVA was used to measure mean differences and evaluate nine null hypotheses. The researcher used ANOVA and SPSS for statistical analysis.

Source of Variation	Sum of Squares	Degrees of Freedom	Mean Squares (MS)	F
Within	$SSW = \sum_{j=1}^{k}\sum_{j=1}^{l}(X-\bar{X}_j)^2$	$df_w = k-1$	$MSW = \frac{SSW}{df_w}$	$F = \frac{MSB}{MSW}$
Between	$SSB = \sum_{j=1}^{k}(\bar{X}_j - \bar{X})^2$	$df_b = n-k$	$MSB = \frac{SSB}{df_b}$	
Total	$SST = \sum_{j=1}^{n}(\bar{X}_j - \bar{X})^2$	$df_t = n-1$		

Figure 3.3: ANOVA summary table

Source: //microbenotes.com/anova/

Chapter Four

Results and Analysis

4.1 Introduction

This section will describe the examination and analysis of the quantitative data in the research, providing a comprehensive explanation of the descriptive analysis conducted on the survey data. A comprehensive presentation of the outcomes of this analysis will also be provided, as well as some context and assumptions about the potential correlations between the conditions that led to the findings. A thorough exploratory factor analysis (EFA) was undertaken for this study. The present study relies on a dataset comprising 84 valid replies. The initial section of the chapter offers an elucidation of the basic protocols that must be completed before doing any analysis, and the procedures encompass several steps. Firstly, the data must undergo a reliability check. Secondly, an assessment of "normality" in terms of statistical normality is conducted, and lastly, the reliability of the measurement scales employed must be verified. In the event of missing values, an appropriate method is employed to replace them. Any outlying values are examined within their context and potentially eliminated.

4.2 Checking and Replacing Missing Values

Despite making significant efforts to assure data completeness throughout the study design and execution, it is practically certain that some data loss may occur, potentially leading to alterations in the research conclusions (Cisneros-Barahona et al., 2023). This phenomenon persists, regardless of the level of caution exercised, as it is inevitable that some degree of data loss will transpire. The

primary objective of the bulk of statistical research is to get reliable and valid results about the population under investigation. Fanny et al. (2020) conducted a study highlighting the implications of the missing data. The presence of missing data can lead to inefficiencies, challenges handling missing data, and the possibility of wrong estimators.

According to Cisneros-Barahona et al. (2023), reducing the likelihood of breaching the criteria for regression analysis is crucial for achieving a high level of trust in research findings. In response to this phenomenon, scholars have resorted to employing several examinations, including those about absent data and exceptional values, to enhance the accuracy of regression analysis (Mayo et al., 2022). Mayo et al. (2022) put forth two methodological techniques for investigating missing data: quantifying its occurrence rate and assessing its unpredictability. The presence of non-randomly missing data in the study may limit the generalization of the findings to a broader population. According to Cisneros-Barahona et al. (2023), it is essential to account for missing data in every variable within a research project.

Table 4.1: Details of the Factors

External Risk Factors (ERF)	External Risk - Cyber Attack (ERCA) External Risk - Cyber Advocacy (ER.CyA) External Risk - Social Engineering (ER.SE) External Risk - Fiscal Manipulation (ER.FM) External Risk - Illegal Activities (ER.IA)
Internal Risk Factors (IRF)	Internal Risk - Oblivious (IR.O) Internal Risk - Apathy (IR.A) Internal Risk - Fiscal Manipulation (IRFM) Internal Risk - Illegal Activities (IRIA)
Vulnerabilities and Weaknesses (VandW)	Vulnerabilities and Weaknesses (VandW) Organization Vulnerabilities and Weaknesses Physical and Digital Assets (VandWP)

Between 4.2 and 6.4 per cent of the sixty-two variables included in the sample needed more valid data. Based on the research conducted by Cisneros-Barahona et al. (2023), variables exhibiting a

missing data rate of 15% should be considered viable candidates for elimination. The primary deficiency in the available data pertained to the absence of ratings across many scales, including IR.O, IR.A, IRFM, IRIA, V, VP, RP, and OR.

In their study, Little (2021) introduced the Missing Completely at Random (MCAR) test to assess the degree to which the distribution of missing data adhered to a stochastic pattern. This test aimed to assess the extent to which the distribution of missing data adhered to a random pattern. If a result does not meet the Statistical Significance test using the p-value threshold of 0.05, this is probably due to random chance (Mayo et al., 2022). The Little (year) test utilized a Statistical Significance threshold of 0.719. The Chi-Square value obtained was 136.455, with 149 degrees of freedom. Hence, there was a lack of discernible discrepancy between the observed and expected data patterns, indicating a potential random absence of data. This phenomenon may be attributed to the possibility of random data absence.

To address the issue of incomplete data, the researcher employed two methodologies: Missing Value Analysis (MVA) and Expectation-Maximization (EM). The gaps in the dataset were filled by assigning values based on the highest likelihood probabilities using a specific technique. However, neither V6 nor OR3 fell within the anticipated ranges of 0.36 to 0.76, although it is worth noting that the absolute value of V5 exceeded 5.03. The observed discrepancies exceeded the acceptable range of 1-5, necessitating re-calibration to rectify the problem. The values were subsequently ascertained, drawing upon subsequent research findings. The test findings revealed that the Chi-Square statistic yielded a value of 9.836, accompanied by 10 degrees of freedom and a p-value of 0.2959. This discovery offers evidence in favour of the hypothesis that a similarity exists between the observed data pattern and the predicted unpredictability. The subsequent

calculations significantly demonstrated that the recommended numbers fell within the anticipated range of 1–5.

4.3 Test of Outliers

According to Mayo et al. (2022), outliers can arise from several factors, each of which might provide legitimacy or invalidity to their presence, making them a controversial subject. Due to their distinct attributes, outlier findings pose considerable challenges when making generalizations. Due to the potential atypicality of these samples about the broader population, it is advisable to gain a deeper understanding of the issue by examining pertinent contextual information and considering alternate explanations. Upon analyzing several statistical measures such as the arithmetic mean, the 5% trimmed mean, the standard deviation, the lowest and maximum values, the skewness, and the kurtosis, it was seen that the discrepancy between the 5% trimmed mean and the arithmetic mean amounted to a margin of 0.12. The unadjusted mean exhibited a 5% increase compared to the trimmed mean, yet it remained higher than the trimmed mean. The dependability assessment has significant importance, as highlighted by Elder et al. (2023) since it determines the level of precision with which commodities, reagents, and activities accurately represent the population.

4.4 Reliability Test

In developing a robust and theoretically grounded technical framework, it is imperative to consider the inherent limitations associated with the measurement apparatus. The precision of the measurements may be compromised due to intrinsic faults. This change in viewpoint offers a resolution to the difficulties arising from both random and systematic alterations of parameters.

The reliability of a measuring instrument can instil confidence in its accuracy. Elder et al. (2023) state that recorded or measured scores encompass actual values and measurement errors.

The present study included a reliability analysis that conforms to the guidelines established by Cisneros-Barahona et al. (2023), and the tables utilized in the analysis demonstrate internal consistency. Removing even a single item from a collection might jeopardize its overall quality. Based on the research conducted by Elder et al. (2023), it was determined that Cronbach's alpha coefficient for each evaluation item was above the threshold of 0.75. This suggests that the data collected was subject to thorough investigation and may be considered trustworthy.

Table 4.2: The Cronbach's Alpha coefficients associated with the research's measures.

Factor	Cronbach's Alpha (α)
Internal Risks - Oblivious	0.973
Internal Risks - Apathy	0.973
Internal Risks – Fiscal Manipulation	0.909
Internal Risks – Illicit Acts	0.892
External Risks – Cyber Attack	0.912
External Risks – Cyber Advocacy	0.938
External Risks – Social Engineering	0.939
External Risks – Fiscal Manipulation	0.941
External Risks – Illicit Activities	0.958

4.5 Assessing Statistical Normality

The degree to which numerical data follows the Gaussian distribution, often known as the bell curve, is what is meant by the term "normality" (Mayo et al., 2022). The term above originates

from the domain of statistics. Due to the distribution's symmetry, the central point and the median coincide precisely. The essential advantage of the normal distribution is its simplicity in representing the likelihood of the occurrence of data points. This approach utilises the characteristics of a larger population in order to analyse a smaller group.

The distribution of responses for a continuous variable can be ascertained by employing descriptive analytic techniques. Statistical tests can only be deemed credible if the data exhibit normality. The evaluation of the normalcy of real-world data relies heavily on both skewness and kurtosis. This phenomenon is that skewness is a statistical measure representing the degree of asymmetry in a distribution. Distributions exhibiting positive skewness coefficients tend to display a right-skewed tendency, while distributions with negative skewness coefficients tend to exhibit a left-skewed tendency. According to a study conducted by Orjiakor et al. (2023), it was observed that when the skewness values approach zero, the mean of a distribution tends to shift away from the central point of the distribution. These specialists also said that it is desirable for the skewness and kurtosis to approximate a value of 1 while performing forecasting. Orjiakor et al. (2023) reported that the skewness measure for 83 items and the kurtosis measure for 74 items satisfy the first requirement.

Suleyman (2022) posits that scientific data exhibiting a normal distribution is commonly regarded as having a skewness value of two or below. According to a statement made by Suleyman (2022), consistent use of these devices yields unexpected scientific findings. This notion is substantiated by the observation that administering the same instrument to various groups might provide divergent outcomes. Due to the inherent unpredictability of the legal process, those responsible for drafting legal documents must grapple with many sources of uncertainty and ambiguity, resulting in diminished accuracy and dependability of the data (Elder et al., 2023). Extensive research on this variability has led to the formulation of many equations that may be employed to assess the

dependability of scholarly communication. Dependability necessitates the presence of fundamental prerequisites, including internal coherence, stability, equivalence, and correctness.

Table 4.3: Internal Consistency Measures

Scales	Cronbach's Alpha
External Risks – Cyber Attack (ERCA)	0.942
External Risks – Cyber Advocacy (ER.CyA)	0.912
External Risks – Social Engineering (ER.SE)	0.910
External Risks – Fiscal Manipulation (ER.FM)	0.901
External Risks – Illicit Acts (ER.IA)	0.943
Internal Risks - Oblivious (IR.O)	0.930
Internal Risks - Apathy (IR.A)	0.939
Internal Risks – Fiscal Manipulation (IRFM)	0.912
Internal Risks - Illicit Acts (IRIA)	0.894

4.6 Descriptive Statistics

Presentations that incorporate variables, counts, or percentages sometimes include comparisons of sample sizes, which are aligned with the relative frequencies discussed. The data is subsequently classified based on subject matter via computational techniques. Due to the statistical significance of obtaining precise data, putting missing information for "all surveys" is not feasible.

Approximately 30.8% of the participants expressed concerns regarding cyber security. Out of the available choices, the response labeled as "likely" was chosen by participants in the study with a frequency of 32.1%. This observation implies that the involved parties comprehensively comprehend the gravity associated with the potential harm posed by cyberattacks originating from foreign nations. In the case of "high improbability," relatively more minor groups were assigned

more excellent ratings, with the group exhibiting the lowest likelihood of receiving the maximum score of 10.1 (7.8%).

The disengagement mechanism of the security system involving ERCA2 evoked the most pronounced reaction. In reality, 34 individuals, comprising 39.35 per cent of the sample, demonstrated identification with or concurrence with the statement. A mere 0.9% of participants in the study expressed scepticism on the likelihood of seeing ERCA4, which refers to service outages.

Table 4.4: External Risks - Cyber Attack (ER.CA). n = 84.

External Risks- Cyber Attack							
	ER.CA	**ER.CyA**	**ER.SE**	**ER.FM**	**ER.IA**	**IR.O**	**IR.FM**
Very Unlikely	5.70%	3.80%	1.80%	0.90%	6.70%	7.60%	6.70%
Unlikely	30.70%	26.00%	21.10%	21.10%	28.80%	22.00%	14.30%
Neutral	30.10%	28.00%	24.00%	23.00%	20.10%	18.20%	25.90%
Likely	24.90%	38.40%	39.30%	35.50%	28.80%	32.60%	30.70%
Very Likely	8.60%	3.80%	3.80%	9.50%	5.70%	9.50%	12.40%

External Risks – Cyber Attacks (ER.CA)
External Risks – Cyber Advocacy (ER.CyA)
External Risks – Social Engineering (ER.SE)
External Risks – Fiscal Manipulation (ER.FM)
External Risks – Illicit Acts (ER.IA)
Internal Risks - Oblivious (IR.O)
Internal Risks - Apathy (IR.A)
Internal Risks – Fiscal Manipulation (IRFM)
Internal Risks - Illicit Acts (IR.IA)

According to estimations, financial institutions face significant levels of external risk. While there is a possibility that the institutions of the participants may not possess the capacity to withstand cyberattacks, it is noteworthy that they demonstrate a complete understanding of the associated risks. A mere 2.9% of participants reported infrequent disruptions to their company caused by

intruders. Many individuals in the financial industry know the potentially catastrophic consequences of external factors.

A total of 32.9% of the participants mentioned external threats, whereas 5.8% of those individuals believed that the occurrence of a cyber advocacy event was very improbable. The study revealed that a significant % of individuals, namely 44.2%, lacked sufficient safeguards to prevent reverse engineering. The cause for these hazards was attributed to the belief of three respondents, which accounts for 0.9% of the total, that they were sufficiently safeguarded from the risks associated with heavy traffic.

According to the ER.SE poll, a significant proportion of respondents, namely 32.3%, expressed varying degrees of concern over the potential occurrence of phishing incidents. A mere 5.0% of the respondents selected the alternative designated as "very implausible", according to the poll

results. Merely 3% of the respondents agreed with the proposition, notwithstanding its nature as a phishing strategy aimed at illicitly acquiring personal data.

Table 4.5: External Risks – Cyber Advocacy (ER.CyA). n = 84

	ER.CyA 1	**ER.CyA 2**	**ER.CyA 3**	**ER.CyA 4**	**ER.CyA 5**	**ER.CyA 6**
Very Unlikely	12.2	1.1	8.6	4.5	5.4	5.3
Unlikely	25	21.9	19.5	17.4	19.5	24.4
Neutral	20.1	21.3	27.8	24.3	35.3	12.6
Likely	22.0	36.3	25.8	35.3	24.1	36.7
Very Likely	10.7	9.4	8.3	8.3	5.9	11.1

Table 4.6: External Risks – Social Engineering (ER.SE). n = 84.

	ER.SE 1	**ER.SE 2**	**ER.SE 3**	**ER.SE 4**	**ER.SE 5**	**ER.SE 6**
Very Unlikely	6.3	6.2	1.5	0.7	8.3	4.9
Unlikely	8.8	12.6	19.5	20.2	21.4	20.6
Neutral	25.7	24.2	27.6	14.4	18.4	24.0
Likely	35.7	32.9	28.6	41.5	29.4	33.1
Very Likely	13.6	14.5	12.6	13.3	12.6	7.4

According to the survey results, a significant proportion of respondents, namely 29 per cent, indicated the presence of a heightened risk of external threats related to fiscal manipulation in their comments. The position deemed "very implausible" had the lowest average score of 8.9 out of 10, or 6.6%, indicating that it had the most minor influence among the three positions. Approximately 49.9% of the respondents regarded the concept, which involves the misuse of assets and the theft of information, as plausible. Only a small proportion of respondents, namely 1.9%, had a negative outlook towards human vulnerability and trust issues.

Table 4.7: External Risks – Fiscal Manipulation (ER.FM). n = 84.

	ER.FM 1	ER.FM 2	ER.FM 3	ER.FM 4	ER.FM 5	ER.FM 6
Very Unlikely	5.4	1.9	1.9	4.9	6.8	5.5
Unlikely	17.5	9.4	22.2	29.5	23.1	21.3
Neutral	20.5	13.6	32.3	21.0	22.2	28.5
Likely	37.2	49.7	30.8	24.4	28.7	24.1
Very Likely	13.2	15.1	4.7	10.2	9.2	10.5

The responses to the ER.IA survey about external risks exhibited comparable tendencies. The average frequency of 28.7, accounting for 29.5% of the total responders, indicates that a significant portion of the participants perceived these threats to have a notably high likelihood. The position classified as "highly improbable" had an average rating of 9.6 out of a potential 10.0. Given the focus of the study on the probability of inaccurate and unreliable information, it was found that 39% of the whole sample expressed a degree of confidence in the research findings. Merely 1.9% of the individuals surveyed strongly believed that the occurrence of extensive data mining, monitoring, and social engineering endeavours was highly improbable.

Table 4.8: External Threats - Illicit Acts (ER.IA). n = 84.

Based on the results of the research entitled "Internal Risks - Oblivious (IR.O)," it was observed

	ER.IA 1	**ER.IA 2**	**ER.IA 3**	**ER.IA 4**	**ER.IA 5**	**ER.IA 6**
Very Unlikely	12.1	21.0	10.7	7.3	8.5	9.3
Unlikely	28.7	23.1	27.5	20.3	16.4	35.6
Neutral	12.6	15.4	16.4	29.8	28.9	20.2
Likely	25.9	17.3	25.8	24.8	28.6	13.5
Very Likely	10.7	13.2	9.6	7.7	7.7	11.4

that around 34.4% of participants had a moderate inclination to see the situation as 'probable.' The opinion categorized as 'extremely implausible' obtained the lowest mean score, 8.3%. One of the key findings of this study is that 51.9% of the entire sample expressed the belief that there was a high likelihood of a reporting policy gap. This finding has significant importance in concluding the research. A marginal proportion of participants, namely 0.9% in both scenarios, believed that this explanation possessed high credibility. Furthermore, a notable proportion of the participants

(0.9%) expressed scepticism on the level of danger, attributing it to the insufficient availability of situational awareness materials and security protocols.

Table 4.9: Internal Risks - Oblivious (IR.O). n = 84.

	IR.O1	**IR.O 2**	**IR.O 3**	**IR.O 4**	**IR.O 5**	**IR.O 6**
Very Unlikely	2.5	17.0	3.8	0.5	0.7	10.3
Unlikely	23.2	17.2	20.2	24.2	20.0	16.2
Neutral	22.2	22.0	40.4	26.2	29.7	24.1
Likely	37.4	31.9	30.8	40.6	37.8	38.6
Very Likely	12.7	9.8	2.8	6.5	9.8	10.8

The highest attainable average score for the Internal Risks - Apathy (IR.A) question was 28.5, with 27.6% of participants selecting this option. The opinion categorized as 'extremely improbable', endorsed by 11.4% of the participants, exhibited the lowest mean score. A significant proportion of participants, namely 34.6%, believed that a deficiency in risk culture may result in inadequate access control measures, as well as infrequent software updates and update patching. In conclusion, the information above leads to the finalization of this discourse. A minor fraction of

participants, namely 5.8% of the entire sample, expressed that the system's lack of clearly delineated power for users was deemed "highly improbable."

Table 4.10: Internal Risks – Apathy (IR.A). n = 84.

	IR.A 1	**IR.A 2**	**IR.A 3**	**IR.A 4**	**IR.A 5**	**IR.A 6**
Very Unlikely	10.4	10.3	6.9	12.2	10.1	9.9
Unlikely	21.4	22.4	28.6	15.3	20.3	21.4
Neutral	30.6	29.5	27.7	26.8	29.9	22.2
Likely	27.8	30.9	25.1	34.9	31.9	29.7
Very Likely	9.9	6.9	11.6	10.8	7.1	17.4

Based on the data obtained from the respondents, the Internal Risk-Fiscal Manipulation (IRFM) had an average score of 31.6, suggesting a substantial probability of its manifestation. Approximately 34% of the participants exhibited a certain degree of danger about this matter. In contrast, it was determined that the minimum average for perspectives classified as "very unlikely" was 9.6, equivalent to a percentage of 9.2%. Hardware theft emerged as a significant sub-variable, as around 36.5 per cent of the entire sample believed in the likelihood of such an occurrence. However, a mere 4.8% of the individuals polled expressed a high level of certainty, assigning an

"extremely probable" rating about the likelihood of never committing an error during their professional endeavours.

Table 4.11: Internal Risks – Fiscal Manipulation (IRFM). n = 84.

	IR.FM 1	**IR.FM 2**	**IR.FM 3**	**IR.FM 4**	**IR.FM 5**	**IR.FM 6**
Very Unlikely	13.3	5.5	7.3	8.4	6.4	6.2
Unlikely	22.0	17.6	25.1	25.1	20.5	26.3
Neutral	25.1	31.5	26.2	26.1	28.6	26.7
Likely	26.7	35.7	27.7	29.7	36.6	35.9
Very Likely	12.8	9.7	13.8	10.8	7.8	4.9

The mean score of 29.4 suggests a substantial likelihood of the Internal Risks - Illicit Acts (IRIA) category occurring. The impact of this phenomenon was experienced by around 33% of the population. Nevertheless, the numerical value 5.9 denoted a proportion of 5.6% about the entirety, exhibiting the lowest average value. This observation suggests a noteworthy level of unlikelihood. Most respondents (39.4%) answered this, expressing their belief in possible revenge attacks from

unfamiliar individuals. Based on the collected data, only 1.9% of the population regarded the episode in question as "highly improbable" based on the collected data.

Table 4.12: Internal Risks – Illicit Acts (IRIA). n = 84.

	IR.IA 1	**IR.IA 2**	**IR.IA 3**	**IR.IA 4**	**IR.IA 5**	**IR.IA 6**
Very Unlikely	6.5	1.7	2.8	14.2	4.9	5.5
Unlikely	27.8	14.6	29.9	27.8	22.0	17.5
Neutral	24.3	34.4	29.5	22.4	32.5	28.9
Likely	29.5	39.5	25.2	24.3	23.2	27.8
Very Likely	11.8	9.7	12.6	11.2	17.4	20.3

The upper limit of the average score for Vulnerabilities and Weaknesses (VandW) was 31.0, a value within the range associated with 'likely' outcomes. 29.8% of participants obtained the previously specified score, reflecting the diverse range of perspectives about this subject matter. It is easy to see the disparity between the improbability and the mean value of 10.7, which accounts for 10.3% of the whole. Concerns about the lack of an independent testing procedure and the restrictions imposed on utility programs and apps were raised by over 42 per cent of survey respondents. Only three people out of a sample of one hundred (2.9%) agreed with the statement, "The existence of e-mail protection systems was judged as very probable or highly imaginable." The general public seemed least enthusiastic about this idea. In terms of protecting physical and digital assets, the key metric used to do so provided an average score of 27.4, indicating a "probable" degree of hazard. This constitutes around 26.4% of the total number of contributors. There was expected to be a 9.5 per cent decrease, as indicated by a chance of 9.9 per cent for reaching a low point. A significant proportion of participants, comprising 35.6% of the total

responses, expressed a neutral stance towards hard drives, indicating a lack of emotional solid inclination towards this technology. In contrast, the prevalence of the response "unlikely" was found to be the least frequent among computers, as just four respondents (accounting for 3.8% of the total sample) provided this response. The response "unlikely" frequency was the lowest among all other categories.

Table 4.13: Vulnerabilities and Weaknesses (VandW). n = 84.

	VandW1	VandW2	VandW3	VandW4	VandW5	VandW6
Very Unlikely	3.5	6.5	5.6	6.5	7.4	18.0
Unlikely	20.5	30.9	19.3	14.5	13.8	38.8
Neutral	32.5	25.1	32.8	42.4	26.6	38.3
Likely	31.8	26.1	30.6	26.8	42.5	23.3
Very Likely	11.6	11.4	11.7	9.7	9.7	3.9

The findings of this study, which evaluate the correlation of the identity matrix, exhibit similarities to the results reported by Hidayah et al. (2020), which are indicative of the necessary conditions for accurate extrapolation. Reliable and precise extrapolation requires the use of significant test results and the application of lower Statistical Significance criteria, often below 0.05. When submitted to factor analysis, the data set under consideration had a Kaiser-Meyer-Olkin (KMO) measure of 0.851. Furthermore, the Chi-square value obtained for the dataset was 839.6, with a corresponding degree of freedom of 91. The chosen level of Statistical Significance for this analysis was set at 0.001.

Factors and factor loadings measure how strongly one variable is associated with another. Variables with high loading scores have a considerable capacity to accurately anticipate cyberattacks, as seen by their superior accuracy rate of 0.792. The concept of social networking

has been shown to exhibit a factor loading of 0.807%. Finch (2019) posits that for a variable to load on a single component significantly, its loading value should exceed 0.5 and ideally approach a value of 1. The initial covert cluster comprises seven variables about "attack systems."

One of the foremost external hazards that contemporary companies encounter is cyber advocacy, sometimes called hacking, to instigate political or social transformation. The first two components account for 62.3% of the total variance, with eigenvalues above 1. The 15 most significant variables collectively decreased their informative density by 37% compared to their prior levels. While the first factor explained 37.7% of the variation we saw, the second factor explained 62.3%. The calculated KMO score of 0.930 is within the typical range (0.5 to 1.0) in factor analysis. A Chi2 of 1012.6 with 105 degrees of freedom, as Bartlett's sphericity test suggested, indicates Statistical Significance at the 0.001 level. Therefore, factor analysis may be applied to the data set with little difficulty.

This statistic elucidates the potential for hostile actors to exploit vulnerabilities in software integration testing and offers an illustrative scenario. A deficit in proficient IT personnel and security equipment (loading of 0.768) exhibits a substantial correlation with Factor 2, as evidenced by factor loadings over 0.5, demonstrating a noteworthy link between the two variables. By employing this particular approach, we successfully identified two latent clusters of ER. CyA (External Risks-Cyber Advocacy). The initial cohort consisted of eleven digital variables that were devoid of any form of violent content. The subsequent set of themes, denoted as "inadequate preparation," has four distinct subtopics. Both recently identified latent clusters met the rigorous reliability threshold of 0.8.

This research also uses the supplemental statistical measures of Mean Squared Variance (MSV) and Average Shared Variance (ASV). The dependability coefficient (CR) exhibited a range of

values spanning from 0.843 to 0.908, all above the minimum acceptable threshold of 0.7. This finding indicates that the measurements used in the study exhibit good dependability. The observed average variance extracted (AVE) for Factor 1 exhibited values between 0.477 and 0.574. These values were statistically significant at the anticipated value of 0.5. Factor 2 exhibited a notable discrepancy between the MSV and ASV ratios. Specifically, the MSV value (0.694) surpassed the AVE value, but the ASV value (0.554) was comparatively lower. Consequently, subsequent research was conducted to assess the convergent validity of Factor 1, but Factor 2 did not pose similar issues. Despite the observation that the Maximum Shared Variance (MSV) surpasses the Average Variance Extracted (AVE), indicating that not all observable variables account entirely for the understanding of Factor 1, this worry has limited Statistical Significance due to the higher magnitude of the MSV compared to the AVE.

Table 4.14: Average Variance Extracted (AVE), Composite Reliability (CR), Maximum Shared Variance (MSV), and Average Shared Variance (ASV) For ER.CyA.

Parameters	Factor 1	Factor 2
CR	.906	.845
AVE	.478	.572
MSV	.696	
ASV	.556	

External Risks - Social Engineering (ER.SE), or phishing, represents a prevalent form of external threats organizations encounter. The first eigenvalue in the total variance table represents the first-factor analysis result that exceeds one threshold. As mentioned earlier, the component accounted for 71% of the variability observed in the data, suggesting that just 28% of the original information

from the first collection of eight variables needed to be captured. Furthermore, this particular element had a significant role in encompassing the entirety of the 5.7 variables.

The 0.890 KMO number is inside the valid range for use in factor analysis, which is between 0.5 and 1.0. A Chi-square value of 704.7 with 24 degrees of freedom was found after using Bartlett's sphericity test. The obtained score exhibits Statistical Significance at a level of 0.001. Consequently, we have determined that factor analysis is suitable for assessing the dataset above.

The overall reliability score of 0.952 is significantly higher than the criterion of 0.7, suggesting high consistency among data points. The extracted value of the average variance demonstrates convergent validity since it exceeds the minimal threshold of 0.5. The estimated value was determined to be 0.716. On average, the extracted variance for Factor 12 is determined to be 0.712, notably lower than the maximum shared variance of 0.782. No issues were identified regarding the convergent validity of the findings. The discriminant validity exhibited considerable strength, as shown by the mean shared variance surpassing the average extracted variance. It was shown that the extracted variance exhibited a higher average magnitude than the shared variance, suggesting the presence of limitations on the discriminant validity.

4.6.1 External Risks – Fiscal Manipulation (ER.FM)

During the first inquiry, it was seen that only the first two components had eigenvalues over 1, therefore accounting for 68.6% of the total variance. Due to the omission of these 13 initial criteria, a significant proportion of the original data, precisely 31.4%, had to be excluded. Complete research indicated the presence of 8.2 different variables, wherein the significant component

contributed to 46.3% of the observed variance, while the secondary component accounted for 68.6% of the overall variation.

Since values between 0.5 and 1.0 are often considered sufficient, a KMO score of 0.922 is appropriate for component analysis. The estimated Chi-square value (996.8) with 84 degrees of freedom demonstrates Statistical Significance at the 0.001 level based on the findings obtained using Bartlett's sphericity test. Consequently, component analysis arises as a viable approach for examining intricate information.

All items had factor loadings greater than 0.6, and the variables were sorted according to the factor or component with the highest loading. Two novel classifications of External Risks have been identified, linked to fraudulent activities in the financial industry. The initial category encompasses a set of variables and parameters associated with "economic fraud." In contrast, the subsequent category comprises a collection of parameters and variables about "financial scams." The latent clusters that have been recently discovered exhibit reliability scores that surpass the established criterion of 0.8. This suggests that these clusters demonstrate a reasonable degree of regularity and precision.

The study revealed that the composite dependability values exhibited a range between 0.816 and 0.934, all surpassing the minimal threshold of 0.7 per the established criteria. All of the average variance estimations above the cutoff value of 0.5, ranging from 0.566 to 0.624, all of which were greater than this threshold. Factor 2 had a lower mean shared variance (0.598) than Factor 1 (0.712), whereas Factor 1 had a higher mean shared variance (0.720) than Factor 2.

4.6.2 External Risks – Illicit Acts (ER.IA)

The eigenvalues of the initial three components exceeded the value of 1, indicating that they accounted for a majority (67.9%) of the total variance. Due to this phenomenon, 21 out of the initial 33.1% of variables were removed from the dataset. A total of 11.7 separate factors were found, with the first component accounting for 29.3%, the second for 49.3%, and the third for 67.9% of the total variation. The result of 0.928 provided by KMO's computations indicates that the sample size is enough for performing factor analysis. This value falls within the acceptable range of 0.5 to 1.0, with the sample size being 1798. The result obtained for Chi (2) when Bartlett's sphericity test was conducted on a sample with 200 degrees of freedom was 8. This finding was statistically significant at the 0.001 level of Statistical Significance. Hence, factor analysis was deemed suitable in this particular scenario for examining the aforementioned numerical data—all loads except for the ER.IA factor exhibited values over 0.5, with the ER.IA factor being the sole exception with a load of 0.489. The cumulative sum of all the loads exceeded 0.5. A new development has brought to light the existence of three underground criminal organizations, which were revealed due to substantial external threats, referred to as ER.IA. The initial latent cluster identified in the study was labeled as "Felonious actions" and had ten distinct factors. Upon conducting more inquiries, it was determined that unauthorized access and unlawful behaviour included two distinct clusters, each comprising six contributing parts. The observed consistency of the three latent clusters that were recently discovered exceeded 0.87, suggesting that they may be considered sufficiently reliable.

The range of overall dependability scores varied from 0.807 per cent to 0.904 per cent. After a thorough study and careful consideration of all pertinent elements, we have determined that the Mean Squared Variance, with a value of 0.676, is superior to the Average Variance Extracted, which possesses a value of 0.560. Each constituent encountered challenges in establishing either convergent or discriminant validity.

4.6.3 Internal Risks - Oblivious (IR.O)

Based on the variance table, a significant proportion, precisely 69.4%, of the total variation can be attributed to two distinct factors. The variance was decreased by surrendering 30.6% of the original information contained in the set of 25 variables. The initial component accounted for 69.4% of the total variance in a dataset consisting of 1.6 variables, whereas the subsequent factor accounted for 37.9% of the overall variation in a dataset including 15.8 variables.

Following factor analysis, the Kaiser-Meyer-Olkin (KMO) value of 0.921 was satisfactory since it fell within the permissible range of 0.5 to 1.0. Bartlett found Statistical Significance at the 0.001 level in his sphericity test. With 300 DOF, the resulting Chi-square value was 2670. As a result of this, it became apparent that factor analysis was a viable method that could be employed to assess the data.

All items placed on the bigger scale have a weight exceeding 0.5. The International Research Organization (IR.O) currently consists of four discrete factions, as opposed to its prior configuration of only two. The primary emphasis of the first inquiries revolved around the inadequate availability of the procedures. Still, competing research tackled the issue of poor observation of security mechanisms with a more basic approach. The reliability of the two newly identified latent clusters is more significant than 0.95, indicating a high degree of dependability.

The Composite Reliability and the Average Variance Extracted for every independent variable are more than 0.5. Furthermore, the average values of both measures were above 0.8. The highest shared variance (0.744) and the average shared variance (0.632) exhibit superior performance compared to the extracted average variance. The presence of a robust association between the two cohorts raised concerns regarding the test's discriminant validity. Identifying a connection between

these variables, which should ideally not be seen, raises concerns about the test's discriminant validity.

4.6.4 Internal Risks - Apathy (IR.A)

The initial list of 18 variables was reduced by 29.9% due to the influence of the first significant component. This factor explained 70.1% of the variance with just 12.6% of the variables. The Kaiser-Meyer-Olkin (KMO) score of 0.964 from the present study's factor analysis is within the generally recognized 0.5–1.0 range. The Chi-square result for the Bartlett sphericity test was 2048.8, with 120 degrees of freedom. This value has been seen at the 0.001 level of statistical significance. As a result, factor analysis may be performed on the data.

All observed factor loadings have values greater than 0.7. A dissection procedure was conducted, wherein the internal risk factors (IR.A) were systematically analyzed and deconstructed into their constituent elements. However, the study's findings indicated the presence of just one underlying cluster, leading to the proposition of "risk apathy" as a plausible explanation. The cluster had a reliability level of 0.98 or above, suggesting a substantial degree of overall dependability.

4.6.5 Internal Risks - Fiscal Manipulation (IRFM)

The component above that has been previously expounded upon the first set of seven independent variables was found to explain just 34.2% of the observed variance, leaving the remaining 65.8% unexplained. The KMO factor study yielded a result of 0.884, considered acceptable as it falls within the acceptable range of 0.5 to 1.0. The chi-square statistic obtained for Bartlett's sphericity

test was 452, with a corresponding Freedom Parameter of 0.001. Therefore, including factor analysis in the data analysis process may be a viable consideration.

All factor loadings have values more than 0.6, demonstrating their Statistical Significance. A single latent cluster is associated with the word "Internal Risks - Fiscal Manipulation" (IRFM). The present incident has been classified as "internal financial fraud" based on identifying six discrete components, each of which contributed to the emergence of this situation. The system exhibited a high level of reliability, surpassing 0.9, indicating a commendable performance. The total dependability and extracted variance had an average value exceeding 0.5. The overall dependability exhibited a statistically significant value of 0.934, surpassing the established barrier of 0.7.

Similarly, the mean extracted variance showed a statistically significant value of 0.658 over the designated threshold of 0.5. The average recovered variance was 0.738, whereas the average transmitted variance was 0.658. The observation that the mean square variance exceeded the average variance obtained in the study led to the inference that there were concerns with discriminant validity.

4.6.6 Internal Risks - Illicit Acts (IRIA)

By utilizing the variance table that spans the whole dataset, focusing specifically on a significant aspect becomes feasible. One particular component accounted for 62.1% of the total observed variance. Nevertheless, due to the inherent limitations of the model's explanatory capacity, which

is based on a mere 4.3 variables, the researcher needed help to retrieve 37.9% of the original information. The factor analysis demonstrated a satisfactory match with a KMO score of 0.882. The Chi-square test for sphericity, as proposed by Bartlett, yielded a value of 424 with 26 degrees of freedom.

Even though all factor loadings are above 0.6, a singular latent cluster, known as Internal Risks - Illegal Acts (IRIA), was recently discovered inside the dataset. We will use the following set of seven variables to analyze this cluster. Consequently, "internal criminal acts" emerged as the preferred terminology to elucidate the events. Based on the data analysis, it can be inferred that the reliability of the cluster surpasses the acceptable level of 0.89. There was a notable rise in the general reliability and the mean extracted variance, with the values changing from 0.8 to 0.6, respectively. When comparing the mean squared variance (0.786) to the mean shared variance (0.618), it is evident that the former exhibits a higher value. There were specific issues regarding the validity of employing a discriminant based on comparing the highest shared variance and the average extracted variance.

4.6.7 Vulnerabilities and Weaknesses (V)

This section outlines the criteria for choosing the four primary components that account for 67.6% of the variance. The KMO value of 0.764 was deemed within the acceptable range of 0.5-1.0 for its use in factor analysis. The sphericity test, as done by Bartlett, resulted in a Chi-square score of 522.4 with 90 degrees of freedom. The observed value of this number exhibited a statistically significant deviation from zero, with a Statistical Significance level of 0.001. Consequently, the data may be subjected to factor analysis. In Factor 4, all of the items exhibited loads beyond 0.5.

However, among these items, the variable associated with the presence of anti-virus and anti-malware programs employed to detect attacks displayed the highest load, surpassing 0.956.

The V matrix identified four novel vulnerabilities and problems inside the system. The "system usage" cluster has four distinct quantitative factors. Social security was the critical concern under consideration in the subsequent set of variables. The cluster called 'functional weakness' was tasked with managing three variables. In contrast, the 'protective software' cluster managed only one variable. Three of the recently revealed latent clusters exhibit a higher level of dependability than the remaining two, as shown by values exceeding 0.70. The scores on the Critical Reading (CR) section exhibited a range spanning from a minimum value of 0.777 to a high value of 0.914. The AVE markings exhibited considerable variability, spanning a range of 0.41 to 0.91. The average variance estimates (AVEs) for all components, except for Factor 2 (0.415), exceeded 0.5. By excluding Factor 2, all variables exhibited a mean squared variance (MSV) above the average variance (AVE) of 0.326. Notwithstanding this, concerns regarding the discriminant and convergent validity of Factor 2 persisted. The annual mean deviation was around 0.5, with few fluctuations.

4.7 Summary of Descriptive Statistics

A comprehensive examination of the data that was not available was conducted, and the Expectation-Maximization (EM) algorithm was employed to fill in the gaps and provide a more complete representation. The research data set contained all the values. However, six items had a maximum value above 5, while four items had a minimum value below 5. Once again, Little's Missing Completely At Random (MCAR) test failed to reveal any statistically significant differences. The second calculation projected that these values would range from 1 to 5. Identifying

outliers involved the computation of the absolute deviation from the untrimmed mean, followed by the subtraction of this deviation from the mean that had undergone a 5% trimming. The most absolute difference that could be established was 0.12.

Consequently, the dataset lacked outliers, and all control factors were duly accounted for. The reliability of each component and item was established by assessing their Cronbach's alpha coefficient, with a threshold of 0.75 or higher indicating a satisfactory level of dependability. The study considered five potential outcomes: highly improbable, unlikely, neutral, likely, and extremely likely. The researcher calculated the frequencies and percentages associated with each of these categories. The vast majority of the variables examined in the study did not violate the assumption of normalcy, as assessed by the rule of 1 normality. The normality assumption is justified since all variables exhibited skewness values below two and kurtosis values below three. Nevertheless, a few variables exceeded the established threshold, indicating that this assumption cannot be generalized to all variables.

4.8 Exploratory Factor Analysis (EFA)

Exploratory factor analysis (EFA) was used to establish the hypothesis and investigate the correlation matrix's latent factor structure. The limited information on the concept of interest necessitated exploratory factor analysis (EFA). Therefore, EFA was used to reveal the latent factors underlying the observable variables and investigate the connections between them. The results of the EFA were then used as independent variables in a subsequent regression analysis.

Exploratory factor analysis (EFA) was performed on 84 people, with data extracted using Principal Component Analysis (PCA). After that, Kaiser Normalization was performed to the Varimax rotation. These measures were taken so that the EFA could better understand the composition of

the 14 dimensions. Items with loadings on the primary criteria higher than 0.50 were retained. It was decided to use the Varimax rotation technique to produce orthogonal factors, maintaining a 90-degree angle between the axes (IBM, 2022). The claim that Varimax rotation provides simpler mathematical processes gained substantial sway for the bulk of the 20th century when exploratory factor analysis (EFA) was performed manually or with limited computing capabilities (Pablo, 2021).

4.9 External Risks - Cyber Attack (ERCA)

To summarize a large number of independent variables into a smaller number of components, principal component analysis (PCA) was used. The comprehensive analysis of the decision-making process for choosing the three essential components is shown in Table 4.15 of the Total Variance. Examining the initial three components accounted for about 68.2% of the total variation. Three components were extracted from the original set of 14 variables, accounting for 68.2% of the observed variation. Of the total variance, the first component accounted for 29.9%, the second for 51.6%, and the third for 11.2%.

Table 4.15 Total variance explained by the components of ERCA

Hidden Variables	Eigenmode Frequencies			Total Variance Explained			Communality		
	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion
1	6.695	47.821	47.821	6.695	47.821	47.821	4.188	29.918	29.918
2	1.842	13.160	60.981	1.842	13.160	60.981	3.031	21.651	51.569
3	1.013	7.234	68.215	1.013	7.234	68.215	2.330	16.646	68.215

4	0.703	5.024	73.239						

Factor Analysis Approach: Principal Component Analysis

The Kaiser-Meyer-Olkin (KMO) value is employed to determine the necessity of doing factor analysis due to its ability to assess the sample's representativeness accurately. Noora and Noora (2021) assert that values ranging from 0.5 to 1.0 indicate suitability. We use Bartlett's Sphericity Test to check if data is suitable for factor analysis. The approach relies on the identity status of the correlation matrix to test the lack of a link between the variables in the population, the null hypothesis. Significant findings, as demonstrated by a test statistic more than a crucial value and a reliability level less than 0.05, are those found by Hidayah et al. (2020). The KMO score of 0.851 made it possible to perform factor analysis. The Statistical Significance threshold for the Chi-square statistic for Bartlett's test of sphericity is 0.001, with a value of 839.6 and 91 degrees of freedom. This evidence demonstrates that factor analysis was viable for examining the given data.

Table 4.16 KMO Measure and Bartlett’s Test for ERCA

KMO Measure		0.849
	Asymptotic Chi-Square	837.6
	Freedom Parameter	89
	Statistical Significance	0.000

Table 4.16 presents the factors and factor loads, which indicate the extent to which each variable is associated with each factor. The strength of the load is used to indicate the extent to which another accurately represents one variable. Substantial burdens align with the concept that the variable effectively represents the factor. The variable ERCA1 has the highest loading (0.792) in Factor 1, indicating its association with breaches that result in the inability to use computers and the internet. Factor 2 accounts for 80.7% of the variance observed in ERCA8 (Social networking).

It is optimal for all variables to exhibit loading on a single factor, with loadings exceeding 0.5 and approaching 1 to the greatest extent possible. However, a value of 0.4 is often regarded as an acceptable or rational estimate.

The data shown in Table 5 represents the results of categorizing each variable based on the loading component or factor with the highest contribution. The results of this investigation on External Risks caused by Cyber Attacks (ERCA) revealed the existence of three distinct latent clusters. The factors that contributed to establishing each cluster are delineated in Table 4.16. The initial cluster of latent attack systems (ERCA1) was assigned seven elements, whereas the subsequent cluster (ERCA2) focused on four variables associated with social contact. The third cluster (ERCA3) specifically examined three variables about direct engagement. The performance of the three recently discovered latent clusters exhibited exceptional results, as reported by IBM in 2022, and the dependability of these clusters surpassed a value of 0.8.

The EFA's convergent and discriminant validity may be examined to determine its reliability and validity. As a result of the lack of validity and reliability displayed by its components, the assessment of the causal model needs to be made meaningful. Composite reliability (CR), average variance extracted (AVE), maximum shared variance (MSV), and average shared variance (ASV) are only a few of the metrics that may be used to evaluate validity and reliability.

Coefficient of Reliability, or CR for short, is a statistical measure used to evaluate the trustworthiness of a survey. As a strong indicator of convergent validity, the average variance extracted (AVE) is often deemed reasonable if it is more than 0.7. The rigour of the relevant standard is greater than that of the CR. The criterion exceeds the cutoff value of 0.5. If the average variance extracted (AVE) is less than the mean shared variance (MSV), then discriminant validity has been demonstrated. Each metric's CR, AVE, MSW, and ASV values are listed in Table 4.18. Each CR score was more than 0.7, with values as high as 0.881. The AVE values varied from

0.511 to 0.516, all more than 0.5. The average variance (AVE) (0.477) is lower than the median standard deviation (MSV) (0.566), indicating considerably more considerable variability.

Conversely, the ASV performs significantly worse than the other two measures (0.477). This maintained the validity of both the convergent and discriminant measures. The problem with the factor's convergent validity suggests that a complete explanation of the factor cannot be attained by looking at its parts in isolation. One or more variables likely correlate more with variables outside their parent factor than with variables within it if problems occur with the model's discriminant validity. Table 4.17 shows that the mean square variance (MSV) was somewhat higher than the average variance extracted (AVE) for the given case.

Table 4.17 Average variance extracted (AVE), composite reliability (CR), maximum shared variance (MSV) and average shared variance (ASV) of the scale ERCA.

Parameters	**Factor 1**	**Factor 2**	**Factor 3**
CR	0.881	0.808	0.755
AVE	0.516	0.515	0.511
MSV	0.566		
ASV	0.477		

According to the research by Shwadhin et al. (2022), human error is primarily absent in commercial domains, such as network intrusion detection. This finding suggests a potential for automation or computerization to replace human involvement in these areas effectively. The human factor, however, continues to be the system's most obvious weak point and vulnerability in many contexts. The research done by Shwadhin et al. (2022) suggests that simultaneous consideration of usability and security is challenging. Human-centred computing and human-computer interaction have been used to address this problem, but they have failed.

Implementing best practices and security procedures within organizations can take time due to various factors. Employee turnover, lack of knowledge, interpersonal dynamics within teams, organizational norms and practices, routines and procedures, data access controls, and the lack of awareness on the part of executives are all contributors (Shwadhin et al., 2022).

External Risks – Cyber Advocacy (ER.CyA)

The selection of two principal components for this feature is evident in Table 4.18, which presents the overall variance. Because the initial two components had eigenvalues beyond the value of 1, our capacity to account for the variance in the data was limited to 62.3%. As a result of the 15 factors, we lost 37.7% of the data we started with. In alternative terms, the determinants influencing the outcome of the matter can be reduced to a mere two. Upon considering all 8.3 components, it was seen that the initial component accounted for 37.7% of the variance, whilst the subsequent component accounted for 62.3% of the variance.

Table 4.18 Total variance explained by the components of ER.CyA

Hidden Variables	Eigenmode Frequencies			Total Variance Explained			Communality		
	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion
1	8.324	55.493	55.493	8.324	55.493	55.493	5.662	37.748	37.748
2	1.017	6.777	62.270	1.017	6.777	62.270	3.678	24.522	62.270
3	0.906	6.037	68.307						

Factor Analysis Approach: Principal Component Analysis

The calculated KMO value of 0.930 was within the factor analysis's margin of error. Bartlett's test of sphericity results is displayed in Table 4.19; a Chi-square value of 1012.6 with 105 degrees of freedom demonstrates Statistical Significance at the 0.001 level. Therefore, factor analysis became a plausible option for examining this dataset.

4.19 KMO Measure and Bartlett's test of sphericity for ER.CyA

KMO Measure		0.928
	Asymptotic Chi-Square	1010.6
	Freedom Parameter	103
	Statistical Significance	0.000

Values for CR, AVE, MSW, and ASV are shown for each measure in Table 4.21. Coefficient of reliability (CR) values were more than 0.7, with a spread of 0.843 to 0.908. The AVE values were all less than 0.5, with some variation between 0.477 and 0.574 for Factor 1. By dividing the Mean Squared Variance (MSV) by the Average Shared Variance (ASV), we get the Average Variance Extracted (AVE) value of 0.694. As a result, Factor 1's convergent validity suffered, whereas Factor 2's was unchanged. There were no problems with discriminant validity, though, as the MSV (mean shared variance) was higher than the AVE (average variance extracted). This suggests that there may be a stumbling block regarding the observed variables' ability to account for Factor 1.

Table 4.20 Average variance extracted (AVE), composite reliability (CR), maximum shared variance (MSV) and average shared variance (ASV) for ER.CyA

Parameters	**Factor 1**	**Factor 2**
CR	0.906	0.841
AVE	0.475	0.572
MSV	0.692	
ASV	0.552	

According to Tamar et al. (2020), using digital technology in a non-violent manner has been proposed as a kind of 'legal protest.' However, the authors caution that such a mode of protest may yield unforeseen consequences for the target of the protest. This action may be undertaken to advocate for a particular concept or express dissent towards a recently implemented governmental policy or legislation. According to the study conducted by Shekhar et al. (2022), conducting a comprehensive examination of the organization's cyber security is of utmost Significance before detecting any possible threats.

External Risks – Social Engineering (ER.SE)

The process of selecting a singular significant component is further elucidated in Table 4.21 of the comprehensive variance report. Approximately one-third of the information initially included in the eight variables was lost, as only the first component had an eigenvalue exceeding 1. However, this component accounted for 71.2% of the variance. Furthermore, this particular variable accounted for explaining an extra 5.7 variables.

Table 4.21: Total variance explained by the components of ER.SE

Hidden Variables	Eigenmode Frequencies			Total Variance Explained		
	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion
1	5.693	71.158	71.158	5.693	71.158	71.158
2	0.678	8.477	79.635			

Factor Analysis Approach: Principal Component Analysis.

Kaiser-Meyer-Olkin (KMO) values between 0.5 and 1.0 are typically used in factor analysis, and the value discovered to be 0.890 is within this range. Table 4.22 displays the results of a Chi-square test of sphericity using the data from Table 4.21; the result is a value of 706.7, statistically significant at the 0.001 level. As mentioned earlier, 28 number was calculated by noting that there

were 28 possible motions. As a result, factor analysis became a practical method for investigating the data.

Table 4.22 KMO Measure and Bartlett's test of sphericity for ER.SE

KMO Measure		0.888
	Asymptotic Chi-Square	704.7
	Freedom Parameter	26
	Statistical Significance	0.000

Table 4.23 lists the possible CR, AVE, MSW, and ASV values for the single component. Extracted average variance (AVE) and composite reliability (CR) had values over 0.7. The exact values for the CR and AVE were 0.952 and 0.712, respectively. Compared to the average variance extracted (AVE), the mean squared variance (MSV) of Factor 12 is more significant at 0.788. While the overall variance is significant, the average shared variance (ASV) is just 0.711. As a result, we found no evidence of problems with convergent validity. Maximum Shared Variance (MSV) is superior to Average Variance Extracted (AVE) when evaluating discriminant validity, while Average Shared Variance (ASV) is superior to MSV.

Table 4.23 Average variance extracted (AVE), composite reliability (CR), maximum shared variance (MSV) and average shared variance (ASV) for ER.SE

Parameters	**Factor 1**
CR	0.950
AVE	0.710
MSV	0.786
ASV	0.709

External Risks – Fiscal Manipulation (ER.FM)

Table 4.24 exhibits the total variance, indicating using two main components. Even though the initial two components had eigenvalues beyond 1, accounting for 68.6% of the variance, this outcome was achieved at the expense of the original set of 13 variables, which retained 31.4% of the information. The initial factor accounted for 46.3% of the overall variance observed in 7.8 distinct variables, whereas the subsequent factor accounted for 68.6% of the total variation observed in 1.2 distinct variables.

Table 4.24 Total variance explained by the components of ER.FM

Hidden Variables	Eigenmode Frequencies			Total Variance Explained			Communality		
	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion
1	7.771	59.779	59.779	7.771	59.779	59.779	6.023	46.330	46.330
2	1.150	8.849	68.628	1.150	8.849	68.628	2.899	22.298	68.628
3	0.660	5.081	73.708						

Factor Analysis Approach: Principal Component Analysis

For use in factor analysis, the calculated KMO value of 0.921 is within the allowable range of 0.5 to 1.0. With 78 degrees of freedom, the Chi-square result for Bartlett's sphericity test was 996.7. The Statistical Significance level of this finding was determined to be 0.001 (Table 4.25). Therefore, factor analysis became a plausible option for examining this dataset.

Table 4.25: KMO Measure and Bartlett's test of sphericity for ER.FM

KMO Measure		0.919
	Asymptotic Chi-Square	994.7
	Freedom Parameter	76

	Statistical Significance	0.000

Each metric's CR, AVE, MSW, and ASV values are shown in Table 4.27. The CR value is more than 0.7, ranging from 0.826 to 0.931. As a bonus, the AVE value was more significant than 0.5, ranging from 0.576 to 0.614. While the average variance extracted (AVE) was determined to be 0.690, the mean squared variance (MSV) was 0.730. Similarly, the average squared variance (ASV) was also higher than the AVE at a value of 0.597 for Factor 2.

On the other hand, the AVE was found to be higher than the ASV for Factor 1. Consequently, no issues about convergent validity were observed. Nevertheless, concerns were expressed regarding the discriminant validity of Factor 1. This implies that some variables had higher associations with those excluded from the overarching factor than others included. However, the observed disparity was only marginally significant.

Table 4.26: Average variance extracted (AVE), composite reliability (CR), maximum shared variance (MSV) and average shared variance (ASV) for ER.FM

Parameters	**Factor 1**	**Factor 2**
CR	0.929	0.824
AVE	0.574	0.612
MSV	0.728	
ASV	0.595	

External Risks – Illicit Acts (ER.IA)

The total variance is displayed in Table 4.27 and explains how the three primary factors were determined. Eigenvalues more significant than 1 for all three main components indicate that they account for over half of the variance (67.9%). However, the descriptive power of the other 21 variables decreases by 32.1%. Of the overall variance, the first component accounted for 29.3%, 49.3%, and 67.9%; the second factor explained 1.4% of the variance; the third factor explained 1.1% of the variance.

Table 4.27: Total variance explained by the components of ER.IA

Hidden Variables	Eigenmode Frequencies			Total Variance Explained			Communality		
	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion
1	11.764	56.018	56.018	11.764	56.018	56.018	6.159	29.327	29.327
2	1.400	6.667	62.684	1.400	6.667	62.684	4.191	19.955	49.283
3	1.089	5.186	67.871	1.089	5.186	67.871	3.903	18.588	67.871
4	0.854	4.066	71.937						

In the context of factor analysis, the KMO value of 0.908 is within the allowable range of values between 0.5 and 1.0. Table 4.28 displays the results of Bartlett's sphericity test. A Chi-square statistic of 1798.6 was found, with 210 associated degrees of freedom. The chosen Statistical Significance threshold for the statistical analysis was set at 0.001. Consequently, factor analysis emerged as a viable approach for analyzing this dataset.

4.28: KMO Measure and Bartlett’s Test for ER.IA

KMO Measure		0.906
	Asymptotic Chi-Square	1796.6

	Freedom Parameter	210
	Statistical Significance	0.000

Table 4.29 presents a comprehensive summary of each participant's CR, AVE, MSW, and ASV contributions. The average variance extracted (AVE) values exhibited a lower range, spanning from 0.416 to 0.489. The composite reliability (CR) scores fell within the higher half of the 0.7 range, explicitly ranging from 0.807 to 0.904. Upon considering all relevant factors, it can be concluded that the MSV score of 0.686 exhibits superior performance compared to the AVE score of 0.560. Consequently, it is plausible that every constituent encountered challenges about its convergent or discriminant validity.

Table 4.29: Average variance extracted (AVE), composite reliability (CR), maximum shared variance (MSV) and average shared variance (ASV) for ER.IA

Parameters	**Factor 1**	**Factor 2**	**Factor 3**
CR	0.902	0.823	0.805
AVE	0.487	0.485	0.414
MSV	0.684		
ASV	0.558		

Internal Risks - Oblivious (IR.O)

As shown in Table 4.30, the overall variance was utilized to choose the two principal components that explained 69.4 per cent of the variation. However, this selection led to a loss of 30.6 per cent of the information included in the initial set of 25 variables. The initial factor accounted for 37.9% of the overall variability observed in 15.8 variables. In contrast, the subsequent factor accounted for 69.4% of the total variability observed in a set of 1.6 variables. Both components were utilized in the analysis of the identical data set.

Table 4.30: Total variance explained by the components of IR.O

Hidden Variables	Eigenmode Frequencies			Total Variance Explained			Communality		
	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion
1	15.769	63.076	63.076	15.769	63.076	63.076	9.482	37.927	37.927
2	1.569	6.276	69.352	1.569	6.276	69.352	7.856	31.425	69.352
3	0.996	3.986	73.338						

Factor Analysis Approach: Principal Component Analysis

The calculated KMO value of 0.931 is adequate for factor analysis, falling within the allowable range of 0.5 to 1.0. A Chi-square score of 2670.4 (with 300 degrees of freedom) is statistically significant at the 0.001 level, as shown by Bartlett's sphericity test results. The data is displayed in Table 4.31. Therefore, factor analysis became a plausible option for examining this dataset.

Table 4.31: KMO Measure and Bartlett's test of sphericity for IR.O

KMO Measure		0.929
	Asymptotic Chi-Square	2668.4
	Freedom Parameter	298
	Statistical Significance	0.000

Table 4.32 provides a thorough breakdown of all contributors' contributions in terms of CR, AVE, MSW, and ASV. The AVE and CR were more than 0.5, indicating high dependability. The CR was in the 0.921–0.938 range, while the AVE was in the 0.504–0.544 range. The mean squared variance (MSV) is more significant than the average variance extracted (AVE), showing a value

of 0.742. Similarly, the average shared variance (ASV) demonstrates a value of 0.630, again above the AVE. The discriminant validity of both components was compromised due to an unexpected and substantial association between them despite the absence of an anticipated relationship.

Table 4.32: Average variance extracted (AVE), composite reliability (CR), maximum shared variance (MSV) and average shared variance (ASV) for IR.O

Parameters	**Factor 1**	**Factor 2**
CR	0.936	0.919
AVE	0.502	0.542
MSV	0.7400	
ASV	0.628	

Internal Risks - Apathy (IR.A)

The breakdown of the entire variance is depicted in Table 4.33, showing that a significant proportion of 70.1% may be traced to a singular fundamental component. As a result, 29.9% of the data about the original set of 18 variables has been eliminated. The initial component accounted for 12.6% of the aggregate variables considered during the study.

Table 4.33: Total variance explained by the components of IR.A

Hidden Variables	Eigenmode Frequencies			Total Variance Explained		
	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion
1	12.614	70.077	70.077	12.614	70.077	70.077
2	0.740	4.109	74.186			

Factor Analysis Approach: Principal Component Analysis

Because it is within the preferred range of 0.5 to 1.0, the estimated KMO value of 0.934 may be used in factor analysis. There were 153 degrees of freedom, and a Chi-square of 2049.2 was found when using Bartlett's sphericity test. Table 4.34 indicates that this finding is statistically significant at the 0.001 level of Statistical Significance. Therefore, factor analysis became a plausible option for examining this dataset.

Table 4.34: KMO Measure and Bartlett's test of sphericity for IR.A

KMO Measure		0.932
	Asymptotic Chi-Square	2047.2
	Freedom Parameter	151
	Statistical Significance	0.000

The CR, AVE, MSW, and ASV values for the variables are presented in a unified table (Table 4.35). Above the 0.7 cutoff for the composite reliability (CR) and the average variance extracted (AVE). There is a CR of 0.977 and an AVE of 0.701%. The average variance extracted (AVE) is 0.701, whereas the mean squared variance (MSV) measures 0.841. However, compared to the average variance (AVE), the average shared variance (ASV) has a lower value of 0.701. Because MSV is higher than AVE, there are concerns about its discriminant validity.

Table 4.35: Average variance extracted (AVE), composite reliability (CR), maximum shared variance (MSV) and average shared variance (ASV) for IR.A

Parameters	**Factor 1**
CR	0.975
AVE	0.699
MSV	0.839
ASV	0.699

Internal Risks – Fiscal Manipulation (IRFM)

The decision to choose a solitary main component is justified by the comprehensive variance table (Table 4.36), which explains 65.8% of the variation while retaining just 34.2% of the information included in the initial set of seven variables. The comprehensive analysis of the total variance table justifies choosing a single principal component. This particular component was tasked with elucidating a total of 4.6 variables.

Table 4.36: Total variance explained by the components of IRFM

Hidden Variables	Eigenmode Frequencies			Total Variance Explained		
	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion
1	4.607	65.808	65.808	4.607	65.808	65.808
2	0.704	10.056	75.864			

Factor Analysis Approach: Principal Component Analysis.

For this particular factor study, a KMO value of 0.894 was optimal. With 21 degrees of freedom, the Chi-square result for Bartlett's test of sphericity was 454.0. Table 4.37 shows that this result is statistically significant at the 0.001 level. Therefore, factor analysis became a plausible option for examining this dataset.

Table 4.37: KMO Measure and Bartlett's test of sphericity for IRFM

KMO Measure		0.892
	Asymptotic Chi-Square	452.0
	Freedom Parameter	19
	Statistical Significance	0.000

Each metric's CR, AVE, MSW, and ASV values are listed in Table 4.38. High levels of internal consistency are indicated by the composite dependability (CR) rating of 0.931. Similarly, the AVE

is 0.658, much over the minimum requirement of 0.5. According to the data, the MSV is higher than the AVE by a margin of 0.739 to 0.658, but the ASV is lower at 0.658. As a direct result of this, issues about discriminant validity have arisen, as evidenced by the mean square variance (MSV) exceeding the average variance extracted (AVE).

Table 4.38: Average variance extracted (AVE), composite reliability (CR), maximum shared variance (MSV) and average shared variance (ASV) of IRFM

Parameters	**Factor 1**
CR	0.929
AVE	0.656
MSV	0.737
ASV	0.656

Internal Risks - Illicit Acts (IRIA)

Table 4.39 displays the comprehensive variance, indicating the suitability of selecting a solitary primary component. As a result, the analysis accounted for 62.1% of the variance. Although the new component added some variation to the model, it only accounted for 4.3% of the total variables. We lost 37.9% of the information in the original seven variables set.

Table 4.39: Total variance explained by the components of IRIA

Hidden Variables	Eigenmode Frequencies			Total Variance Explained		
	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion
1	4.346	62.082	62.082	4.346	62.082	62.082

2	0.823	11.762	73.84 4			

The KMO value of 0.849 was determined to fall within the acceptable range (0.5-1.0) for its use in factor analysis. The chi-square value was 428.2, with 21 degrees of freedom. Additionally, the p-value for Bartlett's test of sphericity was determined to be 0.001, as presented in Table 4.40. Consequently, factor analysis emerged as a viable approach for analyzing this dataset.

Table 4.40: KMO Measure and Bartlett's test of sphericity for IRIA

KMO Measure		0.847
	Asymptotic Chi-Square	426.2
	Freedom Parameter	19
	Statistical Significance	0.000

Table 4.41 displays the CR, AVE, MSW, and ASV values for each metric. The composite reliability (CR) and the average variance extracted (AVE) exhibited values exceeding 0.7. Specifically, the CR was found to be 0.919, while the AVE was determined to be 0.621. The MSV (0.780) exhibits higher superiority than the AVE (0.620). However, the ASV (0.620) is shown to be inferior to the former. As a direct result of this phenomenon, issues about discriminant validity have surfaced, indicated by the manifestation of a higher magnitude of the measure's square root of average variance extracted (MSV) compared to the average variance extracted (AVE).

Table 4.41: Average variance extracted (AVE), composite reliability (CR), maximum shared variance (MSV) and average shared variance (ASV) for IRIA

Parameters	**Factor 1**

CR	0.917
AVE	0.619
MSV	0.778
ASV	0.618

Vulnerabilities and Weaknesses (VandW)

Table 4.42 presents the comprehensive variance, accompanied by a rationale for selecting these four crucial components, which collectively explain 67.6% of the variability in the dataset. As a result, 3.2% of the data, which constituted the set of 13 variables, could not be successfully retrieved. The dataset consisted of four variables, with values of 4.4, 2.1, 1.2, and 1.1. Only 24.5% of the total variation could be accounted for by the first component, 41.8% by the second, 59.1% by the third, and 67.6% by the fourth.

Total 4.42: Total variance explained by the components of VandW

Hidden Variables	Eigenmode Frequencies			Total Variance Explained			Communality		
	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion
1	4.409	33.914	33.914	4.409	33.914	33.914	3.180	24.462	24.462
2	2.088	16.062	49.977	2.088	16.062	49.977	2.252	17.323	41.786
3	1.194	9.188	59.165	1.194	9.188	59.165	2.248	17.295	59.081
4	1.093	8.408	67.573	1.093	8.408	67.573	1.104	8.491	67.573
5	0.811	6.239	73.812						

Factor Analysis Approach: Principal Component Analysis.

With a KMO of 0.785, the accuracy of the factor analysis performed was confirmed. At the 0.001 level of Statistical Significance, Bartlett's sphericity test yielded a Chi-square score of 508.5 with

78 degrees of freedom. The data above is displayed in Table 4.43. Consequently, factor analysis emerged as a viable approach for analyzing this dataset.

Table 4.43 KMO Measure and Bartlett's test of sphericity for VandW

KMO Measure		0.783
	Asymptotic Chi-Square	506.4
	Freedom Parameter	76
	Statistical Significance	0.000

The calculated values of the composite reliability (CR), average variance extracted (AVE), mean square within (MSW), and average shared variance (ASV) are shown in Table 4.44. Composite reliability (CR) and average variance explained (AVE) exceeded 0.7. The AVE varied from 0.415 to 0.914, and the CR was relatively wide, from 0.777 to 0.914. The AVE for all factors was more than 0.5, except Factor 2. The average variance extracted (AVE) was more significant than the mean squared variance (MSV) for all variables except Factor 2. The average variance extracted (AVE) was 0.326, while the observed value was 0.570. This revealed concerns about the factor's capacity to predict outcomes. Despite the AVE being less than 0.5, the observed discrepancy did not exhibit a substantial level of Statistical Significance.

Due to the inherent variability among companies and their unique combination of strengths and weaknesses, conducting a comprehensive analysis on a case-by-case basis is essential to assess any given element. While specific hazards persist, technology may be employed to minimize some of them, while audited processes and practices can be implemented to lessen others. Despite their inherent presence, specific hazards can be mitigated.

Table 4.44 Average variance extracted (AVE), composite reliability (CR), maximum shared variance (MSV) and average shared variance (ASV) for VandW

Parameters	**Factor 1**	**Factor 2**	**Factor 3**	**Factor 4**
CR	0.887	0.775	0.843	0.912
AVE	0.666	0.413	0.643	0.912
MSV	0.568			
ASV	0.324			

Organizational Vulnerabilities and Weaknesses: Physical and Digital Assets (VandWP)

Table 4.45 presents the selected vital components that explain 68.3% of the overall variation. Two main components were selected. As a result, a significant proportion of the data, precisely 33.3%, was excluded from further analysis, reducing the initial set of 14 variables under examination. The initial factor explained 52.1% of the collective variation seen in 8.1 variables, whereas the subsequent factor accounted for 68.3% of the variance observed in 1.5 variables.

Table 4.45: Total variance explained by the components of VandWP

Hidden Variables	Eigenmode Frequencies			Total Variance Explained			Communality		
	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion
1	8.084	57.742	57.742	8.084	57.742	57.742	7.337	52.409	52.409
2	1.477	10.550	68.293	1.477	10.550	68.293	2.224	15.884	68.293
3	0.938	6.702	74.995						

Factor Analysis Approach: Principal Component Analysis

In the context of factor analysis, the KMO value of 0.896 is within the normal range of values (0.5 to 1.0). Chi-square = 1195.7 with 91 degrees of freedom (Table 4.46) indicates Statistical

Significance at the 0.001 level for Bartlett's sphericity test. Therefore, factor analysis became a plausible option for examining this dataset.

Table 4.46: KMO Measure and Bartlett's test of sphericity for VandWP

KMO Measure		0.894
	Asymptotic Chi-Square	1193.7
	Freedom Parameter	89
	Statistical Significance	0.000

Table 4.47 shows the CR, AVE, MSW, and ASV values for each measure. The CR ranged from 0.523 to 0.956. Therefore, factor 2 was not over the critical value of 0.7. The magnitude of component 2's value was less than 0.5, whereas the AVE was between 0.447% and 0.688%. The Average Variance Extracted (AVE) exceeds the Mean Squared Variance (MSV) of 0.808 for Factor 2, but the ASV of 0.573 is greater than the MSV. Based on the data, problems with reliability, convergent validity, and discriminant validity are linked to Factor 2.

Table 4.47: Average variance extracted (AVE), composite reliability (CR), maximum shared variance (MSV) and average shared variance (ASV) for VandWP

Parameters	**Factor 1**	**Factor 2**
CR	0.954	0.521
AVE	0.686	0.445
MSV	0.806	
ASV	0.571	

Responses in Place (RP)

The chart illustrating the entire variance offers evidence in favour of selecting three key components. These components collectively explain 69.6 per cent of the total variation (chart

4.48). Due to this particular circumstance, 30.4% of the data, initially consisting of 18 variables, could not be retrieved. The initial component accounted for 32.1% of the entire variance. In contrast, the subsequent component accounted for 52.5% of the overall variation, and the third component accounted for 69.6% of the whole variation—the initial, subsequent, and final components comprised 8.3, 3.1, and 1.1 variables.

Table 4.48: Total variance explained by the components of RP

Hidden Variables	Eigenmode Frequencies			Total Variance Explained			Communality		
	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion
1	8.348	46.381	46.381	8.348	46.381	46.381	5.772	32.066	32.066
2	3.052	16.958	63.339	3.052	16.958	63.339	3.683	20.464	52.529
3	1.135	6.304	69.643	1.135	6.304	69.643	3.080	17.114	69.643
4	0.894	4.967	74.610						

Factor Analysis Approach: Principal Component Analysis

The KMO score of 0.897 demonstrated satisfactory adequacy for conducting factor analysis. The observed number exhibited Statistical Significance at the 0.001 level, as seen in Table 4.49. Using the Bartlett test of sphericity, a Chi-square value of 1370.8 was found with 153 degrees of freedom. As a result, factor analysis became a practical method for investigating the data.

Table 4.49: KMO Measure and Bartlett's test of sphericity for RP

KMO Measure		0.895
	Asymptotic Chi-Square	1368.8
	Freedom Parameter	151

	Statistical Significance	0.000

Table 4.50 presents the CR, AVE, MSW, and ASV values for each contributor. All the CR values observed were more than 0.7, spanning from 0.835 to 0.924. The AVE metric consistently exceeded 0.5 in all instances in which it was measured. Except for Factor 3, the Mean Squared Variance (MSV) demonstrates superiority over the Average Variance Extracted (AVE), with a value of 0.664. The Average Shared Variance (ASV) exhibits inferiority with a value of 0.443. Consequently, the most notable issues pertaining to discriminant validity were identified in Factors 1 and 2.

Table 4.50 Average variance extracted (AVE), composite reliability (CR), maximum shared variance (MSV) and average shared variance (ASV) for RP

Parameters	**Factor 1**	**Factor 2**	**Factor 3**
CR	0.912	0.833	0.922
AVE	0.516	0.558	0.750
MSV	0.662		
ASV	0.441		

As shown by Shwadhin et al. (2022), scholars have prioritized investigating and implementing detection and response mechanisms. The proponents posited that possessing comprehensive protection renders the vast majority of assailants incapable of doing substantial harm. Although internal audit measures can contribute to the prevention and identification of potential threats originating from within an organization, it is unavoidable that specific attacks may evade detection. This is due to the inherent imperfections of internal audit systems. Utilizing diverse operating systems does not provide foolproof security against malevolent hackers. Consequently, it is imperative to develop cyber defences with the assumption that cyber-attacks will transpire, and these defences should be engineered to detect and counteract such attacks swiftly. As a

consequence of this, the research and endeavours dedicated to detection are of utmost Statistical Significance.

Organizational Resilience (OR)

Table 4.51 comprehensively depicts the overall variance and furnishes ample details on the selection procedure for these three crucial components. The variables mentioned above explained 70.4% of the variance, leading to a decrease of 29.6% in data from the original set of 21 variables. Sequentially, the first, subsequent, and third elements were responsible for 34.3%, 53.2%, and 70.4% of the total variability seen among a collective of 1.2 variables, 12.2 variables, and 1.4 variables, respectively.

Table 4.51: Total variance explained by the components of OR

Hidden Variables	Eigenmode Frequencies			Total Variance Explained			Communality		
	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion	Total	Explained Variance	Cumulative Proportion
1	12.170	57.952	57.952	12.170	57.952	57.952	7.206	34.317	34.317
2	1.370	6.526	64.479	1.370	6.526	64.479	3.957	18.843	53.160
3	1.244	5.926	70.404	1.244	5.926	70.404	3.621	17.245	70.404
4	0.876	4.172	74.576						

Factor Analysis Approach: Principal Component Analysis

The KMO value of 0.930 is respectable within the factor analysis framework, where respectable values are often between 0.5 and 1.0. A Chi-square of 1012.6 was obtained using Bartlett's test of

sphericity, which is statistically significant at the 0.001 level (see Table 4.52). Therefore, factor analysis became a plausible option for examining this dataset.

Table 4.52: KMO Measure and Bartlett's test of sphericity for RP

KMO Measure		0.922
	Asymptotic Chi-Square	1837.8
	Freedom Parameter	208
	Statistical Significance	0.000

Each component's Mean Square Within (MSW), Average Squared Variance (ASV), Composite Reliability (CR), and Average Variance Extracted (AVE) are shown in Table 4.53. Nevertheless, the average variance extracted (AVE) values exhibited a range of 0.469 to 0.752, except Factor 1, which fell below the threshold of 0.5. All of the correlation coefficient (CR) values above 0.7, ranging from 0.813 to 0.924. The mean squared variance (MSV) exhibits a more significant value of 0.728 compared to the average variance extracted (AVE), except for Factor 3. The average shared variance (ASV) demonstrates a higher value of 0.579 than the AVE. As a result, issues arose about the convergent validity of Factor 1, but Factors 2 and 3 did not exhibit such difficulties. Additionally, concerns were raised regarding the discriminant validity of Factors 1 and 2.

Table 4.53: Average variance extracted (AVE), composite reliability (CR), maximum shared variance (MSV) and average shared variance (ASV) for OR

Parameters	**Factor 1**	**Factor 2**	**Factor 3**
CR	0.922	0.811	0.922
AVE	0.467	0.590	0.750
MSV	0.726		
ASV	0.577		

The Cronbach's alpha coefficients demonstrated high levels of reliability for all scales in the study. Specifically, the Internal Trait Consistency Assessment (ITCA) scale had a coefficient of 0.894, indicating strong internal consistency. Similarly, the Validity and Reliability of the Weights (VandW) scale exhibited a coefficient of 0.795, suggesting good reliability. Additionally, the remaining scales show coefficients equal to or greater than 1.000, further supporting their trustworthiness. Every scale included a range of unique components, varying from one to four. Additionally, the proportion of total variance explained by these components exceeded sixty per cent.

Given that all of the Kaiser-Meyer-Olkin (KMO) values were above the threshold of 0.785 and the chi-square probabilities were below 0.001, it was feasible to do a factor analysis on the dataset. Most commonalities had values beyond 0.6, whereas a negligible proportion demonstrated values below 0.4. In most cases, the composite dependability exceeded the minimal threshold of 0.7. Most of the scales, with a few notable outliers, demonstrated convergent and discriminant validity, particularly when compared to the ASV.

4.10 Summary

The investigation led the researcher to conclude that EFA and regression analysis would yield the best results. The statistical program SPSS, with the help of Hayes' macro (Hayes, 2018), was utilized for this investigation. Exploratory factor analysis (EFA) and regression analysis are the most appropriate methods for analyzing the moderating effects of the variables, which is why this chapter is included. Little (1988) introduced the missing ultimately at random (MCAR) test, which was used to fill in the gaps in the dataset. The results of the analysis indicated that the data adhered to a normal distribution. Due to the absence of abnormalities or outliers in the data, there was no

need to exclude or eliminate any records. This element enhances the overall validity of the research.

In this chapter, the presented evidence showcases the reliability of the data and its adherence to statistical standards for "normality." Consequently, this ensures that any deductions from the data are replicable, as another individual might evaluate the data and reach identical conclusions. This is due to the replicability of the data. The study's overall reliability and repeatability are notably enhanced, although the sample size is minimal. The sample is considered representative as its demographics closely resemble those of the federal entities under the supervision of the UAE Government. Consequently, it may be inferred that the collected information is likely to be representative, thereby enabling the generalization of the findings to the broader context of the United Arab Emirates government.

Chapter Five

Discussion

5.1 Introduction

The researcher will explain the research questions, data analysis methods, and research conclusions in this chapter. Relationships between variables, correlation analyses used to back up research hypotheses, and results are discussed in this chapter. This research proposes a framework for strengthening the UAE financial sector's Resilience to cyberattacks and gives an in-depth summary of the study's aims.

5.2 Research Overview – External and Internal Cyber-Threat Constructs

This research examined UAE financial sector employees' threat awareness and financial sector companies' resistance to external and internal cyber threats. The purpose was to strengthen cyber defenses and awareness with a conceptual framework. To achieve this, the researcher must examine these banks' employee perspectives and resilience practices. The researcher also aimed to assess a firm's cyberattack resilience and preparedness at the time of the research. It was commonly believed that such activities would improve awareness and make it easier to implement suitable measures.

5.2.1 Threats

According to Ross et al. (2021), it is posited that specific systems may experience an enhancement in Resilience as a result of hazards. For instance, the authors assert that enterprises operating within the financial sector must adopt cyber-threat resilience strategies and enhance their employees' comprehension of cyber risks to address cross-border cybercrime effectively. Implementing these techniques and enhancing staff comprehension regarding cyber-risks are essential in mitigating such criminal activities.

5.2.2 Vulnerabilities and Weaknesses

Given the inherent persistence of vulnerabilities and weaknesses (Akter et al., 2022), this study does not aim to achieve complete eradication, recognizing the impracticality of such an endeavor. In contrast, Hughes-Lartey et al. (2021) propose that an enhanced understanding of the potential dangers linked to technological progress and vulnerabilities inside systems has the potential to reduce the magnitude of these risks. The study conducted by Alawida et al. (2022) showed that gaining insight into individuals' inadvertent introduction of hazards can be crucial in mitigating potentially dangerous actions. Consequently, using the framework is expected to improve the performance of both workers and management. According to Allianz's findings by Allianz (2023), employees with this particular skill set have a decreased propensity to engage in unwarranted risk-taking behaviors, thereby mitigating the system's susceptibility to cyber-attacks.

5.2.3 Resilience

The final theoretical framework explored in this research (the integrated cyber resilience and risk management framework customized for the UAE financial sector) may be the most important. The UAE financial sector must be cyber-resilient to sustain investor faith in businesses seeking to operate here. Zengwang et al. (2022) have stressed Resilience and the research on cyber-resilience practices and compliance led to developing a measuring instrument. The framework will also help firms perceive cyber hazards and manage them.

5.3 Descriptive Analysis Findings

The online survey of Bank ABC employees received 84 valid surveys after 124 invitations were sent to potential participants. According to Aithal et al. (2020), 52% is a significant response rate. The demographic data met expectations, including high-level managers and data entry workers; the common denominator is an organization's decreased Resilience—its lack of belief in its capacity to withstand a cyberattack. Externally, there was a sense of tremendous risk. A lack of understanding of the risks, a poor culture, and indolence were recognized as concerns. The UAE banking industry may have fallen short of the new framework's criteria, but there was a definite propensity toward cyber-security.

The researchers used descriptive statistics to analyze the normal distribution to assist cross-validation. The Missing Completely at Random (MCAR) test by Little (2021) was used to detect random patterns in missing data. The testing showed that the answers were helpful and had a normal distribution with a few outliers.

5.4 Validity of the Results

The results may be genuine since statistical tests yielded results within the predicted range, and the participants' demographics matched UAE financial sector personnel's viewpoints. Presenting all assumptions and restrictions strengthened the new framework. The new framework creatively integrates old frameworks, yet the value and imports their value. The poll's anonymity encourages candid replies, making the data likely to be reliable.

5.5 Frequencies of the Research Constructs

In the data analysis chapter, research construct frequencies are given. However, a brief discussion of the consequences of these findings is required. The survey respondents' responses were scored on a one-to-five Likert scale on which a grade of one signified strong agreement with the statement or question, while five indicated strong dissent. Many participants disagreed with most survey items, as shown by mean values between 2.75 and 4. However, the research on normality in statistics and its presence increased data quality and trustworthiness.

5.6 Association Findings

According to the study's findings, there is a significant connection between these indicators and firms' internal and external risk management practices. This lends more credence to the notion that financial institutions must take measures to protect themselves against cyberattacks.

Even though most frameworks and standards are geared towards lessening the effect of attacks, and Resilience and mitigation are inextricably related, no paradigm has ever looked at an organization's Resilience before a threat is posed. Alok et al. (2022) strongly focus on the need

for early detection to mitigate the negative impacts of cyberattacks. When discovered early enough, cyberattacks may be defended against and recovered from.

An online survey was carried out to determine whether or not those working in the UAE's financial industry would be included in any future framework. Scales of the Likert type were utilized in the formulation of questions incorporating Hidden Variables. We sent out 124 electronic surveys and received 84 usable replies, giving us a response rate of 84%. A principal component analysis was performed to analyze and assess all 84 responses.

5.7 Discussion of Regression Analysis

The following sub-sections explain this research's independent-dependent variable connections, including direct and moderator effects.

5.7.1 The direct influence on external and internal threats, pre-existing responses, and organization adaptation and recovery.

Financial sector organizational resilience was statistically linked to internal and external threats, response strategy implementation, and quantitative analysis. A statistically significant component relationship corroborated the results. Superior solutions and organizational Resilience can help managers decrease internal and external risks to assets.

The hypothesis was investigated using a Pearson Correlation test to assess the independent-dependent connection. First, the organization's weaknesses and deficiencies were examined for external threats. Positive correlation between External Threats Risk Factor (ERF) and Financial Sector Organization Vulnerability and Weaknesses (VandW) and Statistical Significance (p-value below 0.01) suggest that external threats increase a company's vulnerabilities and weaknesses.

A positive correlation exists between the growing number of exposure locations and an elevated incidence rate factor. A statistically significant positive correlation ($p<0.01$) was observed between vulnerability (VandW) and IRF, suggesting a relationship between the two variables. Fotios et al. (2022) assert that implementing effective cyber-risk management within the financial industry necessitates the active involvement and oversight of management. Due to the potential reduction in future corporate targeting, organizations should cultivate a robust security culture. This may be achieved via conducting assessments to identify vulnerabilities and weaknesses and by enhancing top executives' knowledge and self-awareness.

Financial sector weaknesses positively and strongly correlate with responses in place (RP). More answers raise vulnerabilities and weaknesses. Shaikha et al. (2021) showed that early identification and response can minimize organizational attacks, and preventing every attack is tough. Hence, a timely response is essential.

5.7.2 Reaction mechanisms, external threats, and organizational resilience change vulnerabilities and weaknesses.

External risks (ERF) make financial sector firms more susceptible and faultier as they immediately impact financial sector shortcomings.

Exposure to varied dangers positively correlates with risk propensity (RP), showing that an organization's vulnerability to attack grows with its reaction. This research supports findings by WEF (2022) that halting a cyberattack immediately reduces long-term harm. However, a reaction plan does not prevent all external dangers, although it may reduce these risks.

The positive link between organizational Resilience (OR) and vulnerabilities and weaknesses shows that robust financial sector companies have more defects. This supports Richard's (2021)

assertion that Resilience is the ability of systems to anticipate and adjust to unexpected events and failures.

5.7.3 Organizational Resilience, response strategy execution, and internal threats impact vulnerabilities and weaknesses.

IRF and VandW are firmly connected; increasing IRF makes the organization more vulnerable. Companies are more vulnerable to internal attacks than foreign ones, per Fang-Yi Lo et al. (2020). Because 90% of data breaches are employee-caused, secret information might hurt the company's reputation and earnings.

UAE financial companies should prioritize worker behaviour or intentions before a disaster. This step can lower internal dangers and protect the assets. A thorough assessment of workers' data access credentials is needed. Dissatisfied personnel, delays in career progression or wage increases, and other reasons may increase internal risks. UAE financial sector enterprises must rewrite their access authorization rules and internal operating processes to maintain functional interdependency and resistance to internal threats.

Fotios et al. (2022) advise management to promote cyber-risk awareness and management as the passion and skill of management generate a risk-conscious atmosphere that may increase business resilience.

5.7.4 This research explores whether organizational Resilience moderates internal-external risks, vulnerabilities, and weaknesses.

The results show that organizational Resilience and ERF bystander impact are connected. Additionally, organizational Resilience positively connects with the vulnerability and weakness dependent variable. This suggests that Resilience moderated ERF but did not diminish VandW. However, organizational Resilience increases vulnerability and weakness.

The research indicated that IRF negatively correlated with organizational Resilience. Organizational Resilience prevented internal attacks on vulnerabilities and weaknesses. Therefore, organizational Resilience buffers internal threats, vulnerabilities, and weaknesses.

5.7.5 Hypotheses

Eight threat-response-resilience architecture hypotheses were developed to answer research questions. The online poll of financial sector professionals assessed the eight hypotheses, and the validity of each hypothesis was tested.

Research Question 1. This research evaluates and enhances cyber-risk Resilience while preserving reaction mechanisms and reducing susceptibility and weakness.

First hypothesis: Weaknesses and vulnerabilities produce external threats. Positive associations support VandW = ERF.

Second hypothesis: Weaknesses and vulnerabilities produce internal threats. VandW = IRF is a well-known positive correlation. Failures are revealed via reaction measurements. VandW acceptance boosts RP. Vulnerabilities and weaknesses determine organizational Resilience. VandW's brand acceptability is linked to its quality and honesty.

Research Question 2: Given the research's dependent variables—current reaction, organizational Resilience, vulnerabilities and weaknesses—can established standards be used to create a cyber-risk management framework? The fourth hypothesis is that well-structured activities can reduce external and internal hazards. The equation VandW = IRF + RP shows a positive connection. The fifth hypothesis states that habitual reactions reduce risk. According to academics, the formula suggests a favorable relationship between VandW and ERF + RP. The seventh hypothesis states that organizational Resilience reduces threat vulnerability. VandW, IRF, and ORe can be related under certain situations. External dangers and hazards are mitigated by organizational Resilience. VandW = ERF + ORe is acknowledged, albeit with restrictions.

Hypothesis 1 (H1) External dangers cause vulnerabilities and weaknesses.

VandW's good correlation with external risks backed the idea.

Hypothesis 2 (H2) relates flaws and vulnerabilities to internal risks.

Internal risks corresponded strongly with vulnerabilities and weaknesses, supporting the hypothesis.

Hypothesis 3 (H3) relates reactions to flaws and vulnerabilities.

A positive correlation between context-specific reactions and vulnerabilities and weaknesses supported the idea.

Hypothesis 4 (H4) relates reactions to vulnerabilities, weaknesses, and internal risks.

Each measure correlated favorably, confirming the idea—moderator responses are associated strongly with vulnerabilities, weaknesses, and internal risks.

Hypothesis 5 (H5) As responses are contextualized, internal difficulties and external risks become less linked. Their close relationship supports the opinion. Moderator reactions closely correspond with external threats, vulnerabilities, and shortcomings.

Hypothesis 6 (H6): Organizational deficits improve Resilience.

It was analyzed and simplified into a formula. Organizational Resilience improves vulnerabilities and weaknesses, according to the research.

Hypothesis 7 (H7) Internal organizational flaws, vulnerabilities, and threats are linked to Resilience.

The positive connection between the factors supported the concept. Resilience in an institution mitigates internal risks, vulnerabilities, and weaknesses.

Hypothesis 8 (H8) Organizational Resilience mitigates vulnerabilities, weaknesses, and external threats.

Each measure correlated favorably, confirming the idea. Organizational Resilience reduces external threats and increases weaknesses.

5.8 Discussion of Findings and Results

The redesigned architecture can improve the UAE financial sector's cyber-security awareness, response, and Resilience after data analysis. Academic research and empirical data agree that early diagnosis and intervention build Resilience, and the findings show that early detection needs threat recognition.

All management levels may commit to and be aware of company-wide response and resilience mechanisms. This measure will reassure companies contemplating migrating to the UAE that the government will protect crucial national infrastructure from an attack, which may increase corporate migration.

5.8.1 Regression Test Conclusions

Although all hypotheses were confirmed, only two received complete validation from the dataset regression tests. The notion that the recently implemented framework is adequate and expected to fulfil its intended purposes effectively is substantiated. In conjunction with other findings about descriptive data, the inference above suggests that the framework possesses the potential to enhance cyber-security within the banking sector of the United Arab Emirates.

5.9 Validation of the New Framework

A thorough assessment of the present situation and explicit or implicit impediments must precede framework creation, as only then can the framework be fully validated. The dissertation must demonstrate that the framework can solve the issues above, but a clear, persuasive presentation is needed to prove this.

5.9.1 Cyber-Resilience and -Security in the UAE Financial Sector

The 2020 TRA, "The UAE National Cybersecurity Strategy", made the UAE a safe cyberspace for multinational enterprises. The UAE's TRA-managed Cyber Security Centre ranks second in

cyberattacks behind the US, with Darkmatter (2020) and Kaspersky (2022) deeming the country vulnerable. The introduction indicated that many UAE inhabitants felt uneasy, which inspired the methodology and investigation.

The full implementation of the new framework in the UAE is complex but has been carefully tested, and the research found Resilience to be excellent but improvable. The framework's relevance has been proven, but these hazards are dynamic. Thus, constant monitoring and assessment is the best strategy to identify and minimize dangers.

5.9.2 Acceptance of Validated Framework

Eight financial industry managers from the research population were contacted to confirm the findings, as this step verified the research findings and internal consistency of the research variable. Factors such as management level and cyber security experience determined the selection process. However, only five people responded to the invitation to partake in the research. These five people connected virtually via a video conferencing tool. The five participants had vital feedback after the session, but it is still being determined if all UAE financial industry entities immediately accepted the new conceptual framework. Participants will likely push for early adoption of the framework when it is developed and disseminated to UAE financial sector firms due to its optimistic outlook. This will further strengthen the cyber-resilience of the UAE financial sector and safeguard critical infrastructure.

Chapter Six

Conclusion and Recommendations

6.1 Introduction

This chapter presents the research's key results and research summary. It also synthesizes the research's significant results, examines the methodology, and rates its contribution. This chapter outlines the research's theoretical, practical, and methodological contributions. The contributions above are carefully analyzed before the second step, assessing the research's constraints and future prospects.

6.2 An Overview of the Research

The research highlighted the UAE financial sector and critical infrastructure cyber resilience but did not identify any resilience assessment method. With the unique paradigm, financial industry managers might study organizational resilience (ORe) and enhance cyber-resilience and cyber-security. After analyzing the literature, a new conceptual framework was needed to fulfil these aims.

The data originated from computer users in the UAE financial sector. The data analysis was concerning but consistent with earlier findings. The findings showed that the recommended strategy could evaluate ORe and increase cyber-security, which was proven using these methods. Sharing cyber threat and attack data is crucial and will help other firms be proactive and resilient.

6.3 The Accomplishment of the Research Objectives

Financial sector enterprises are expected to lead in cyber-awareness, cyber-protection, and cyber-resilience, and this research provides a veritable framework for attaining it. The following subsections describe the research's objectives and progress.

6.3.1 This initiative seeks to uncover new cyber-risks and investigate resilience and awareness.

Cyber threats evolve, especially for IoT and connected devices. Many are ignorant of their security risks despite their vulnerability to attacks, so promoting cyber-risk understanding is crucial for resilience (Hughes-Lartey et al., 2021). Data analysis should relate vulnerabilities and weaknesses (VandW) to operational risk events (ORe). The poll tested individuals' cyber-risk awareness, confirming the link, and this means that cyber-risk awareness must be emphasized

6.3.2 Formulate A Comprehensive Theoretical Framework for Assessing Resistance to Cyber-Risks

According to Kunz et al. (2021), establishing a risk-aware corporate culture necessitates the integration of accountability and awareness. This would enable the strengthening and mitigation

of system weaknesses. If applied effectively, the framework can enhance levels of accountability and vigilance, fostering a corporate culture that is more aware of cyber dangers.

6.3.3 This research investigates organizational vulnerability and cyber threats from external and internal sources, considering resilience and risk resolution.

Cyber risk evolves, advances, and transforms, according to this research. Regression research showed that internal or external risks create weaknesses and vulnerabilities, which degrade resilience until managed. While resilience may not reduce external threats, it may reduce internal risks and vulnerabilities or modify their relationship.

UAE's digital economy is booming, but this growth needs a secure, stable, and resilient infrastructure for long-term success. Business enterprises need safe, reliable, and robust infrastructure. The framework cannot create financial proof and cannot achieve this purpose. However, UAE financial sector managers can show critical infrastructure protection policies. The third aim will be met following system resilience enhancement.

6.4 Key Findings

The research found that the UAE's financial sector has high ORe levels; however, some sectors might improve. The findings show that financial sector personnel comprehend cyber risks and are cyber-resilient, but the existing frameworks detect or respond to cyber threats slowly.

Financial sector firms' IRF, ERF, RP, and ORe links have worsened framework problems, so a new paradigm that helps managers detect and mitigate internal and external risks and retain

organizational assets and infrastructure is much needed. The UAE financial industry must prioritize technology and management planning in strategic planning to improve business cyber-resilience.

The survey demonstrates significant cyber-risk awareness despite some significant IoT flaws. Financial sector employees and management should applaud the new strategy to increase cyber safety and cybersecurity. Financial sector personnel and management must embrace technology instead of ignoring it.

6.5 Research Novelty and Contribution

This research expanded cyber-security and cyber-resilience understanding, so the paradigm offers a unique conceptual approach to boosting UAE financial sector cyber-resilience, helping managers prepare their organizations. The method should aid future research by revealing UAE financial sector improvements.

According to Akter et al. (2022), the financial sector's abysmal cyber risks and resilience rates show an urgent need to address the situation. Thus, frameworks need ongoing evaluation and

improvement, and a new analysis will assess their declining relevance and new risk categories and raise digital risk awareness.

6.6 Research Achievement

By systematically verifying and validating results, this dissertation enhances cyber-resilience research. The research found that cyber-risk awareness boosts resilience, supporting UAE (2021) claims that the UAE financial sector entities support essential infrastructure.

The research indicated that strengthening either factor reduced vulnerabilities and weaknesses. However, increasing both components had a higher effect than each alone. Statistical methods verified the data's accuracy, and the research's conclusions supported the premise.

6.7 Research Implications

The objective of this research was to provide a comprehensive framework to enhance cyber-resilience and foster awareness of cyber threats within the banking sector of the United Arab Emirates. The outcomes of this research have the potential to provide benefits to many tiers within the financial industry.

6.7.1 Implications for Research and Theory

This theoretical research examined developing nations' financial sectors' organizational vulnerabilities, weaknesses, and resilience to external and internal cyber threats. In their research,

Fang-Yi Lo et al. (2020) conducted a comparative analysis of qualitative and quantitative research methodologies, concluding that the latter showed superiority over the former. The inclusion of scientific literature has also influenced the collection of quantitative data (Saunders et al., 2023), which enhances our understanding of cyber-resilience by combining methods to increase it and raise awareness of cyber risk.

6.7.2 Implications for Management.

The findings have an impact on those involved in the financial business. Operational teams, middle and senior management, government policy analysts, change management experts, and cyber-attack consultants and practitioners are all examples of the types of people considered stakeholders.

This research benefits all financial sector personnel who use computers or digital data. This suggests managers immediately provide training and awareness lectures for all employees, including themselves and due to cyber risk's dynamic nature, managers must keep everyone informed. Thus, annual refresher training or evaluations are required, as regular research suggests that cyber-risk awareness promotes cyber-resilience. Efforts to increase cyber-risk awareness, cyber-resilience, and cyber-security need the support of upper management, as stated by Cremer et al. (2005). Financial sector enterprise managers in the UAE must be cyber-resilient, cyber-risk

aware, and cyber-secure to use the framework. This means that UAE financial managers must embrace change and the new framework.

6.8 Research Limitations

Cyber risks and hazards, especially IoT-related ones, are challenging to research due to their fast growth. This covers all studies. Unfortunately, material under review for new or possible vulnerabilities may become old before investigation. The Internet of Things has information security experts rethinking connections, but neural networks are the most complex assets to protect. Thus, the research conclusions cannot be applied to other organizations and sectors of the economy.

6.8.1 Methodological Limitations and Recommendations

Despite being done with a thorough research methodology, this research did not encompass data from all employees within the UAE financial industry or provide comprehensive answers to all cyber-risk or cyber-resilience issues. In subsequent studies, researchers may employ larger sample sizes or explore alternative structural traits. Future research may develop the framework's principles to fulfil government ministry or financial sector agency aims. Any future or advanced academic project should measure resilience or cyber risk understanding. A different industry sample is advised for a new perspective and more robust research findings. A separate industrial sample supports this research's findings, so banks in the United Arab Emirates (UAE) must

proactively enhance cyber-resilience and promote risk education. However, incorporating research conducted by the private sector could contribute to these efforts.

6.8.1.1 Limitation of Sample Size

Due to quantitative data, researchers picked the largest sample size. It could not disseminate the online survey to all UAE financial sector employees and management, so a representative sample and reasonable return rate were necessary. This research follows Azraii et al.'s (2021) method for credibility and correctness, and to avoid prejudice or conformity, poll questions were non-controversial and anonymous. The key obstacle was the impracticality of engaging all financial industry personnel in the UAE. While 40 participants are appropriate for most quantitative studies (Cremer et al., 2022), the quantitative data sample size was only 84, indicating a low count. The twelve financial institutions from where data was collected revealed a tiny sample size.

6.8.2 Limitations for the Researcher and Recommendations

Access to data is limited as the UAE financial institution has done minimal research on cyber-security, resilience, and awareness. This prevents confirming or cross-checking the research's findings with others because the financial sector computer use and data accessibility were difficult to assess without statistics. This means that the sample size must be estimated rather than calculated.

Access to participants is limited, so UAE financial industry professionals were employed to determine names due to computer inaccessibility and data management skills. However, it is

assumed that certain employees of these institutions may need a professional email account due to their tasks.

Linguistic restrictions. Though English is the UAE's official language, many financial sector personnel use it as a second language, but the questionnaire needed clear, simple English.

6.9 Future Research Agenda

The extensive investigation neglected long-term effects. Due to fast development, this industry could only conduct cross-sectional research. Two main aspects affect the structure's use and effectiveness: A) Structure use and B) effectiveness.

At least two further investigations are recommended. The framework's efficacy must be assessed by monitoring and evaluating progress.

The following research ideas emphasize practical application:

1. All top management in the financial sector must adequately implement the new structure.

2. The researchers will analyze the intervention with a bigger sample size and more employees in a comparable survey.

References

Ahsan, Mostofa, Kendall E. Nygard, Rahul Gomes, Md Minhaz Chowdhury, Nafiz Rifat, and Jayden F Connolly. (2022). "Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review" Journal of Cybersecurity and Privacy 2, no. 3: 527-555. Retrieved on 5 October 2023 from https://doi.org/10.3390/jcp2030027

Aithal, Architha and Aithal, Sreeramana. (2020). Development and Validation of Survey Questionnaire Experimental Data – A Systematical Review-based Statistical Approach. Retrieved on 5 October 2023 from https://mpra.ub.uni-muenchen.de/103996/

Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. Annals of operations research, 1–26. Advance online publication. Retrieved on 5 October 2023 from https://doi.org/10.1007/s10479-022-04844-8

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University. Computer and information sciences, 34(10), 8176–8206. Retrieved on 5 October 2023 from https://doi.org/10.1016/j.jksuci.2022.08.003

Alexander S. Gillis, T. (2023). Phishing. Retrieved on 20 October 2023 from https://www.techtarget.com/searchsecurity/definition/phishing

Allianz. (2023). Allianz Risk Barometer 2023 -Rank 1: Cyber incidents. Retrieved on 5 October 2023 from https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2023-cyber-incidents.html

Alok Mishra, Yehia Ibrahim Alzoubi, Memoona Javeria Anwar, Asif Qumer Gill. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations, Computers & Security. Volume 120, 2022, 102820, ISSN 0167-4048. Retrieved on 5 October 2023 from https://doi.org/10.1016/j.cose.2022.102820.

Aratek. (2022). ‘Biometric Access Control System—A Complete Guide’. Retrieved on 5 October 2023 from https://www.aratek.co/news/biometric-access-control-system-a-complete-guide

Asaad, R. R. (2021). Penetration Testing: Wireless Network Attacks Method on Kali Linux OS. Academic Journal of Nawroz University, 10(1), 7–12. https://doi.org/10.25007/ajnu.v10n1a9987

Azraii, A.B., Ramli, A.S., Ismail, Z. et al. (2021). Validity and reliability of an adapted questionnaire measuring knowledge, awareness and practice regarding familial hypercholesterolemia among primary care physicians in Malaysia. BMC Cardiovasc Disord 21, 39 (2021). Retrieved on 5 October 2023 from https://doi.org/10.1186/s12872-020-01845-y

BSI (2022). The new ISO/IEC 27001:2022 standard. Retrieved on 5 October 2023 from https://www.bsigroup.com/en-US/ISO-IEC-27001-Information-Security/2022-revision/

Carías, Juan F., Saioa Arrizabalaga, Leire Labaka, and Josune Hernantes. (2020). Cyber Resilience Progression Model. Applied Sciences 10, no. 21: 7393. Retrieved on 5 October 2023 from https://doi.org/10.3390/app10217393

Cybersecurity & Infrastructure Security Agency (2020). Defining Insider Threats. Retrieved on 5 October 2023 from https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats#:~:text=The%20CybER.SEcurity%20and%20Infrastructure%20Security,equipment%2C%20networks%2C%20or%20systems.

Cisneros-Barahona AS, Marqués-Molías L, Samaniego-Erazo N. (2023). Multivariate data analysis: Validation of an instrument for the evaluation of teaching digital competence [version 1; peer review: 2 approved with reservations]. F1000Research 2023, 12:866. Retrieved on 5 October 2023 from https://doi.org/10.12688/f1000research.135194.1)

COSO (2023). COSO Releases New "Achieving Effective Internal Control Over Sustainability Reporting" (ICSR) Supplemental Guidance. Retrieved on 5 October from https://www.coso.org/new-icsr

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. The Geneva papers on risk and insurance. Issues and practice, 47(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Darkmatter. (2020). Smart and Safe Digital. Retrieved 22 August 2023, from https://www.zawya.com/en/press-release/uae-cyber-security-firm-darkmatter-to-protect-expo-2020s-digital-network-and-data-a3khzpyk

Dubai Electronic Security Centre. (2023). Retrieved on 5 October from https://www.desc.gov.ae/

Elder, J., Wilson, L., & Calanchini, J. (2023). Estimating the Reliability and Stability of Cognitive Processes Contributing to Responses on the Implicit Association Test. Personality and Social Psychology Bulletin, 0(0). https://doi.org/10.1177/01461672231171256

Ellen Webborn, Eoghan McKenna, Simon Elam, Ben Anderson, Adam Cooper, Tadj Oreszczyn. (2022). Increasing response rates and improving research design: Learnings from the Smart Energy Research Lab in the United Kingdom, Energy Research & Social Science, Volume 83, 2022. 102312, ISSN 2214-6296, Retrieved on 5 October from https://doi.org/10.1016/j.erss.2021.102312.

ERM (2022). Playbook: Enterprise Risk Management for the U.S. Federal Government (Fall, 2022 Update). Retrieved on 5 October from https://www.doi.gov/sites/doi.gov/files/erm-playbook-2022-update-final-508-compliant.pdf

Fang-Yi Lo, Andrea Rey-Martí, Dolores Botella-Carrubi. (2020). Research methods in business: Quantitative and qualitative comparative analysis. Journal of Business Research, Volume 115, 2020.Pages 221-224, ISSN 0148-2963. Retrieved on 5 October 2023 from https://doi.org/10.1016/j.jbusres.2020.05.003.

Fanny Bengtsson and Klara Lindblad. (2020). Methods for handling missing values. A simulation study comparing imputation methods for missing values on a Poisson distributed explanatory variable. Department of Statistics, Uppsala University. Retrieved on 11 October 2023 from https://www.diva-portal.org/smash/get/diva2:1520218/FULLTEXT01.pdf

Fotios Petropoulos, Daniele Apiletti, Vassilios Assimakopoulos, Mohamed Zied Babai, Devon K. Barrow, Souhaib Ben Taieb, Christoph Bergmeir, Ricardo J. Bessa, Jakub Bijak, John E. Boylan, Jethro Browell, Claudio Carnevale, Jennifer L. Castle, Pasquale Cirillo, Michael P. Clements, Clara CordeIR.O, Fernando Luiz Cyrino OliveIR.A, Shari De Baets, Alexander Dokumentov, Joanne Ellison, Piotr Fiszeder, Philip Hans Franses, David T. Frazier, Michael Gilliland, M. Sinan Gönül, Paul Goodwin, Luigi Grossi, Yael Grushka-Cockayne, Mariangela Guidolin, Massimo Guidolin, Ulrich Gunter, Xiaojia Guo, Renato Guseo, Nigel Harvey, David F. Hendry, Ross Hollyman, Tim Januschowski, Jooyoung Jeon, Victor Richmond R. Jose, Yanfei Kang, Anne B. Koehler, Stephan Kolassa, Nikolaos Kourentzes, Sonia Leva, Feng Li, Konstantia Litsiou, Spyros Makridakis, Gael M. Martin, Andrew B. Martinez, Sheik Meeran, Theodore Modis, Konstantinos Nikolopoulos, Dilek Önkal, Alessia Paccagnini, Anastasios Panagiotelis, Ioannis Panapakidis, Jose M. Pavía, Manuela Pedio, Diego J. Pedregal, Pierre Pinson, Patrícia Ramos, David E. Rapach, J. James Reade, Bahman Rostami-Tabar, Michał Rubaszek, Georgios Sermpinis, Han Lin Shang, Evangelos Spiliotis, Aris A. Syntetos, Priyanga Dilini Talagala, Thiyanga S.

Talagala, Len Tashman, Dimitrios Thomakos, Thordis Thorarinsdottir, Ezio Todini, Juan Ramón Trapero Arenas, Xiaoqian Wang, Robert L. Winkler, Alisa Yusupova, Florian Ziel. (2022). Forecasting: theory and practice, International Journal of Forecasting. Volume 38, Issue 3, 2022. Pages 705-871, ISSN 0169-2070. Retrieved on 5 October 2023 from https://doi.org/10.1016/j.ijforecast.2021.11.001.

Gov.Uk (2022). 'Official Statistics- Crime outcomes in England and Wales 2021 to 2022'. Retrieved on 5 October 2023 from https://www.gov.uk/government/statistics/crime-outcomes-in-england-and-wales-2021-to-2022/crime-outcomes-in-england-and-wales-2021-to-2022

Guo, Mingyu; Wang, Guanhua; Hata, Hideaki; Babar, Muhammad Ali (2021). "Revenue maximizing markets for zero-day exploits". Autonomous Agents and Multi-Agent Systems. 35 (2): 36. arXiv:2006.14184. doi:10.1007/s10458-021-09522-w. ISSN 1387-2532. S2CID 254225904.

Hadlington, Lee & Chivers, Sally. (2020). Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors. Policing: A Journal of Policy and Practice. 14. 479-492. 10.1093/police/pay027.

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. Heliyon, 7(3), e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

IBM. (2022). Factor Analysis Rotation. Retrieved on 11 October 2023 from https://www.ibm.com/docs/en/spss-statistics/25.0.0?topic=analysis-factor-rotation

ITP (2021). Cyber-attacks in UAE increased over 190% following remote working shift. Retrieved on 5 October 2023 from https://www.arabianbusiness.com/industries/technology/460814-cybER.SEcurity-risks-rise-with-remote-working

Janna Anderson and Lee Rainie (2023). Themes: The best and most beneficial changes in digital life that are likely by 2035. Retrieved on 5 October 2023 from https://www.pewresearch.org/internet/2023/06/21/themes-the-best-and-most-beneficial-changes-in-digital-life-that-are-likely-by-2035/

Joel Witts. (2023). 'The Top 5 Biggest Cyber Security Threats That Small Businesses Face And How To Stop Them.' Retrieved on 5 October 2023 from https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/#:~:text=An%20insider%20threat%20is%20a,simply%20through%20ignorance%20and%20carelessness.

Juliana De Groot (2023). What is Cyber Security? Definition, Best Practices & Examples. Retrieved on 20 October 2023 from https://www.digitalguardian.com/blog/what-cyber-security#:~:text=Cyber%20security%20refers%20to%20the,Importance%20of%20Cyber%20Security

Kaspersky (2022). Kaspersky finds exploits in Middle East detected in 2Q 2022 increased compared to 1Q. Retrieved on 5 October 2023 from https://www.ec-mea.com/exploit-detections-in-the-middle-east-rise-8-in-q2-2022/

Kunz, J., and Heitz, M. (2021). Banks' risk culture and management control systems: A systematic literature review. J Manag Control 32, 439–493 (2021). Retrieved on 5 October 2023 from https://doi.org/10.1007/s00187-021-00325-4

Li, F. & Liu, B. (2021). The Growing Importance of Cyber-Resilience in the Digital Age. Journal of Information Security, 17(3), 201-215 https://doi.org/10.1093/jis/27.3.201

Little Roderick J. (2021). Missing Data Assumptions. Vol. 8:89-107 (Volume publication date March 2021) First published as a Review in Advance on August 21, 2020. Retrieved on 5 October 2023 from https://doi.org/10.1146/annurev-statistics-040720-031104

Mayo, D.G., & Hand, D. (2022). Statistical Significance and its critics: practicing damaging science, or damaging scientific practice?. Synthese 200, 220 (2022). Retrieved on 5 October 2023 from https://doi.org/10.1007/s11229-022-03692-0

Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/. Accessed 30 Nov. 2023.

Munusamy, Thavaselvi & Khodadadi, Touraj & Zamani, Mazdak. (2023). Enhancing Cyber Security in Organizations by Establishing Attributes Towards Achieving Cyber Resilience. Retrieved on 5 October 2023 from 10.20944/preprints202308.0901.v1.

Myriam Dunn Cavelty, Christine Eriksen & Benjamin Scharte. (2023). Making cyber security more resilient: adding social considerations to technological fixes. Pages 801-814 | Retrieved on 5 October 2023 from https://doi.org/10.1080/13669877.2023.2208146

Noora Shrestha. (2021). "Factor Analysis as a Tool for Survey Analysis." American Journal of Applied Mathematics and Statistics, vol. 9, no. 1 (2021): 4-11. doi: 10.12691/ajams-9-1-2. Retrieved on 11 October 2023 from http://article.sciappliedmathematics.com/pdf/ajams-9-1-2.pdf

ObserveIT. (2020). 2020 Cost of Insider Threats Global Report. Retrieved on 5 October 2023 from https://www.observeit.com/wp-content/uploads/2020/06/The-HiddenCosts-of-Insider-Threats-in-this-New-Infographic.pdf

Orjiakor, C. T., Sellbom, M., Keeley, J. W., & Bagby, R. M. (2023). Measurement invariance of the Personality Inventory for the DSM-5 (PID-5) for Nigerian and White American university students. Psychological Assessment, 35(8), 715–720. https://doi.org/10.1037/pas0001251

Pablo Rogers. (2021). Best Practices for Your Exploratory Factor Analysis: A Factor Tutorial. Revista de Administração Contemporânea Universidade Federal de Uberlândia, Brazil, vol. 26, no. 6, e210085, 2022. Retrieved on 11 October 2023 from DOI: https://doi.org/10.1590/1982-7849rac2022210085.en

Park, Y., Konge, L., & Artino, A. R. (2020). The Positivism Paradigm of Research. Academic medicine: journal of the Association of American Medical Colleges, 95 (5). http://dx.doi.org/10.1097/ ACM.0000000000003093 Retrieved on 5 October 2023 from https://journals.lww.com/academicmedicine/fulltext/2020/05000/the_positivism_paradigm_of_research.16.aspx

Quiera S Booker, Jessica D Austin, Bijal A Balasubramanian. (2021). Survey strategies to increase participant response rates in primary care research studies, Family Practice, Volume 38, Issue 5, October 2021, Pages 699–702. Retrieved on 5 October 2023 from https://doi.org/10.1093/fampra/cmab070

Richard I. Cook, Beth Adele Long. (2021). Building and revising adaptive capacity sharing for technical incident response: A case of resilience engineering, Applied Ergonomics. Volume

90, 2021, 103240, ISSN 0003-6870. Retrieved on 5 October 2023 from https://doi.org/10.1016/j.apergo.2020.103240.

RiskOptics (2023). Threat, Vulnerability, and Risk: What's the Difference? Retrieved on 20 October 2023 from https://reciprocity.com/blog/threat-vulnerability-and-risk-whats-the-difference/#:~:text=A%20threat%20refers%20to%20any,threat%20actors%20with%20malicious%20intent.

Rosado, David G., Antonio Santos-Olmo, Luis Enrique Sánchez, Manuel A. Serrano, Carlos Blanco, Haralambos Mouratidis, Eduardo Fernández-Medina. (2022). Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern, Computers in Industry, 10.1016/j.compind.2022.103715, 142, (103715).

Ross Ron, Victoria Pillitteri, Richard Graubart, Deborah Bodeau and Rosalie McQuaid (2021). "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach" (PDF). NIST Special Publication. 2 – via NIST. Retrieved on 5 October 2023 from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

Rui He, Jingyu Zhu, Guoming Chen, Zhigang Tian. (2022). A real-time probabilistic risk assessment method for the petrochemical industry based on data monitoring, Reliability Engineering & System Safety, Volume 226, 2022. 108700, ISSN 0951-8320, Retrieved on 5 October 2023 from https://doi.org/10.1016/j.ress.2022.108700.

Saunders, Mark & Bristow, Alexandra. (2023). 2023 Research Methods for Business Students Preface and Chapter 4.

Saxena, Neetesh, Emma Hayes, Elisa Bertino, Patrick Ojo, Kim-Kwang Raymond Choo, and Pete Burnap. (2020). Impact and Key Challenges of Insider Threats on Organizations and

Critical Businesses. Electronics 9, no. 9: 1460. Retrieved on 5 October 2023 from https://doi.org/10.3390/electronics9091460

Sekhon, M., Cartwright, M. & Francis, J.J. (2022). Development of a theory-informed questionnaire to assess the acceptability of healthcare interventions. BMC Health Serv Res 22, 279 (2022). https://doi.org/10.1186/s12913-022-07577-3

Shaikha Hasan, Mazen Ali, Sherah Kurnia, & Ramayah Thurasamy. (2021). Evaluating the cyber security readiness of organizations and its influence on performance, Journal of Information Security and Applications, Volume 58, 2021. 102726, ISSN 2214-2126. Retrieved on 5 October 2023 from https://doi.org/10.1016/j.jisa.2020.102726.

Shekhar Pawar, Dr. Hemant Palivela. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs), International Journal of Information Management Data Insights, Volume 2, Issue 1, 2022. 100080, ISSN 2667-0968. Retrieved on 11 October 2023 from https://doi.org/10.1016/j.jjimei.2022.100080.

Shwadhin Sharma, Eduardo Aparicio. (2022). Organizational and team culture as antecedents of protection motivation among IT employees, Computers & Security, Volume 120, 2022, 102774, ISSN 0167-4048. Retrieved on 11 October 2023 from https://doi.org/10.1016/j.cose.2022.102774.

Stephen Watts. (2020). 'What is CVE? Common Vulnerabilities and Exposures Explained.' Retrieved on 5 October 2023 from https://www.bmc.com/blogs/cve-common-vulnerabilities-exposures/

Suleyman Demir. (2022). Comparison of Normality Tests in Terms of Sample Sizes under Different Skewness and Kurtosis Coefficients. International Journal of Assessment Tools in Education 2022, Vol. 9, No. 2, 397–409. https://doi.org/10.21449/ijate.1101295

Taherdoost, Hamed. (2023). Security and Internet of Things: Benefits, Challenges, and Future Perspectives. Electronics 12, no. 8: 1901. Retrieved on 5 October 2023 from https://doi.org/10.3390/electronics12081901

Taherdoost, Hamed (2021). Data Collection Methods and Tools for Research; A Step-by-Step Guide to Choose Data Collection Technique for Academic and Business Research Projects. International Journal of Academic Research in Management (IJARM), 2021, 10 (1), pp.10-38. ffhal-03741847f. Retrieved on 5 October 2023 from https://hal.science/hal-03741847/document

Tamar Haruna Dambo, Metin Ersoy, Ahmad Muhammad Auwal, Victor Oluwafemi Olorunsola, Ayodeji Olonode, Abdulgaffar Olawale Arikewuyo, Ayodele Joseph. (2020). Nigeria's #EndSARS movement and its implication on online protests in Africa's most populous country. Retrieved on 11 October 2023 from https://doi.org/10.1002/pa.2583

Tariq, Usman, Irfan Ahmed, Ali Kashif Bashir, and Kamran Shaukat. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors 23, no. 8: 4117. Retrieved on 5 October 2023 from https://doi.org/10.3390/s23084117

Tobias Adrian, Caio Ferreira (2023). 'Mounting Cyber Threats Mean Financial Firms Urgently Need Better Safeguards Regulators and supervisors must act now to strengthen the prudential framework'. Retrieved on 5 October 2023 from https://www.imf.org/en/Blogs/Articles/2023/03/02/mounting-cyber-threats-mean-financial-firms-urgently-need-better-safeguards

TRA. (2020). Home. Retrieved on 25 August 2023, from Telecommunication Regulatory Authority: https://www.tra.gov.ae/en/home.aspx

UAE (2021). Infrastructure and Vision 2021. Retrieved on 5 October 2023 from https://u.ae/en/information-and-services/infrastructure/infrastructure-and-vision-2021

UAE Government. (2020). Cyber safety and digital security. Retrieved on 16 August 2023 from Information and Service: https://u.ae/en/information-and-services/justice-safety-and-the-law/cyber-safety-and-digital-security

Vijay Kanade. (2022). 'What Is Ransomware? Definition, Types, Examples, and Best Practices for Prevention, and Removal'. Retrieved on 5 October 2023 from https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-a-ransomware-attack/

WEF (2022). The Global Risks Report 2022 (17th Edition). Retrieved on 5 October 2023 from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Wissem Eljaoueda, Nesrine Ben Yahiaa, and Narjès Bellamine Ben Saouda. (2020). A Qualitative-Quantitative Resilience Assessment Approach for Socio-technical Systems, Procedia Computer Science, Volume 176, 2020. Pages 2625-2634, ISSN 1877-0509. Retrieved on 5 October 2023 from https://doi.org/10.1016/j.procs.2020.09.305.

Yeo, L. H., & Banfield, J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. Perspectives in health information management, 19(Spring), 1i. Retrieved on 5 October 2023 from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9123525/

Yuchong Li, & Qinghui Liu. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, Volume 7, 2021. Pages 8176-8186, ISSN 2352-4847. Retrieved on 5 October 2023 from https://doi.org/10.1016/j.egyr.2021.08.126.

Yunhan Huang, Linan Huang, Quanyan Zhu. (2022). Reinforcement Learning for feedback-enabled cyber resilience. Annual Reviews in Control, Volume 53, 2022. Pages 273-295, ISSN 1367-5788. Retrieved on 5 October 2023 from https://doi.org/10.1016/j.arcontrol.2022.01.001.

Zengwang Jin, Menglu Ma, Shuting Zhang, Yanyan Hu, Yanning Zhang, Changyin Sun. (2022). Secure State Estimation of Cyber-Physical System under Cyber Attacks: Q-Learning vs. SARSA, Electronics, 10.3390/electronics11193161, 11, 19, (3161).

Appendix I

Consent Sheet

Title of research: An Investigation of the Current Loopholes in Bank ABC's Cybersecurity System: Supporting a More Resilient and Trustworthy Cybersecurity System

Please consider contributing to this study. The purpose of this initial page is to describe the research to you before you choose to participate. Please contact the researcher if you have any questions or concerns about participating.

To indicate, check the box(es) or type in the initials

Before the researcher collects my data, I can withdraw from the study by informing them of my decision. Due to the nature of the data collection procedure, retracting my participation in the online survey may not be possible after it has begun.

By submitting this form, I consent to using my personal information as outlined in the privacy notice. I understand that all data processing will be done by the rules and regulations of the United Arab Emirates (UAE) regarding privacy and data protection.

I understand that a dissertation will be written outlining the findings of this study and that I can have a copy of it by emailing the researcher. It is OK if my information is stored indefinitely and used for research purposes.

Participant's statement:

I ……. join the research voluntarily. I have read the preceding remarks and the project's Information Sheet, and I fully grasp the nature of the research to be conducted.

Signed Date

Appendix II

Ethical considerations

Ethical treatment of participant confidentiality

The researcher will employ pseudonyms to conceal the participants' real names and safeguard their data's confidentiality.

Consent form and explanation

The research's participants had all completed a permission form, which the researcher used to learn the following:

Why I am doing this survey

How long will it take you to complete the survey?

The Participant may stop participating and decline to answer any questions.

Participation is optional, and they have the right to privacy and anonymity. The signed consent forms will be given to the research ethics committee and stored safely on campus at Strathclyde University for future review.

Confidentiality of collected data

Without participants' permission, the researcher will not release personally-identifying information. The researcher will use encrypted passwords on two external hard drives to save all the data acquired and recorded during the investigation. The information will be stored in many safe locations, and all digital copies will be destroyed after the doctorate is earned. The researcher shall always have a lockable filing cabinet where paper copies of the research data and participant identification will be kept. Participants' names, job titles, and information about their current or prior employers will not be collected throughout the survey. Any identifying information about

the participants will be eliminated, modified, or anonymize so that the presentation of the research results is not hampered.

Appendix III

Questionnaire

Dear Participant,

This survey is a component of my research for my dissertation at Strathclyde University, where I am a doctoral candidate. My research aims to investigate and analyze how UAE financial institution workers deal with cyber risk.

Most organizations today know that their cybersecurity initiatives are producing the expected results. When questioned, however, whether or not they are confident in their company's capacity to monitor, identify, and quantify internal breaches, confidence levels begin to plummet.

The primary objective of this research was to analyze how well United Arab Emirates financial institutions deal with cyber risk. This evaluation tool aims to help management figure out how far down the path to cyber-resilience their organizations are. These businesses can benefit from an

analysis of cyber-risk resilience by learning more about the efficacy of their present cyber-risk strategies in preventing and responding to intrusions.

We need your assistance in figuring out how banks handle cybersecurity. This, in turn, will aid in ensuring secure online services by establishing protocols to safeguard businesses and their clients.

It should take you about 20 to 25 minutes to finish the survey.

Individual replies will be kept anonymous, and the data from the entire research will be combined and evaluated. You are under no need to take part in this activity, but if you do, I will consider it a great honour. We will only provide abstracts of the research's findings to maintain privacy.

Thank you for participating in this survey; I appreciate your time and look forward to reporting the findings.

Yours sincerely,

Humaid Almansoori

Appendix IV

Title Of Research

An Investigation of the Current Loopholes in Bank ABC's Cybersecurity System: Supporting a More Resilient and Trustworthy Cybersecurity System

PRINCIPAL INVESTIGATOR

Name Strathclyde University

Address United Kingdom

Phone

Email

PURPOSE OF RESEARCH

You are being solicited to participate in research. Please read the following carefully to familiarize yourself with the research's goals and procedures before deciding whether or not to join. Please

take the time to read the details below. If you have any questions or require clarification, please ask the researcher.

This research aims to strengthen Bank ABC's cyber defences and make them more reliable and secure for their clients. For example, I will utilize Bank ABC, an enormous financial institution in Dubai that relies heavily on the Internet for its day-to-day operations.

Research Procedures

1. Risks

Filling out the form with personal information is optional. Leave out any identifying information, such as your name, phone number, or address. You are not obligated to answer any of the questions, and you can stop participating whenever you choose.

Benefits

There is no payoff in kind for taking part in this research. I sincerely wish that you would be eager to contribute and provide candid feedback.

Confidentiality

Your anonymity and the confidentiality of your replies to this poll are guaranteed. Do not include any personal details in your survey. The researcher will try to protect your privacy by discarding any survey materials once the data has been analyzed and the dissertation has been accepted.

Contact Details

The researcher's contact information is on the first page if you have any queries or suffer any side effects from participating in this research.

You are under no obligation to take part in this research. Your participation in this research is entirely voluntary. Participation in this research will require your signature on a permission form. You have the right to revoke your permission at any moment and for any reason after signing the form. Your current status in the researcher's eyes will remain the same if you decide to drop out of the research. If you leave the research before collecting your information, you will either get it back or erase it.

Consent

I have had the chance to read and comprehend the materials presented and pose pertinent questions. I know that my participation is optional and that I may stop at any moment without penalty or explanation. I acknowledge that a copy of this permission form will be provided to me. I consent to taking part in this research of my own free will.

Participant's signature _____ Date _____

Investigator's signature _____ Date _____

Appendix V

Questionnaire

Researcher requests permission to conduct the following survey; your cooperation is appreciated. There is no obligation to take part. All replies are confidential and will be kept under strict anonymity.

Section A: PERSONAL INFORMATION

Sex	
Male	
Female	

Age	
25 and below	
26 - 35	
36 - 45	
46 - 55	
56 and above	

Level of Educational Qualification	
High School or Less	

Diploma/Bachelor	
Master’s Degree	
Doctorate or above	

Job Level	
Employee	
Middle Management	
Top Management	

Nationality	
Emirati	
Non-Emirati	

Section B: To what extent do you believe the following cyber risks will affect your institution?

Please put (√) mark in the boxes that suits your response.

VL=Very Likely, L= Likely, N=Neutral, U=Unlikely, VU=Very Unlikely

	External Risks	VL	L	N	U	VU
External Risks - Cyber Attack						
6	Hacking attacks that render computers and the internet useless					
7	Separated security systems pose a significant risk.					
8	Power blackouts, accidents and hacked signals and controls.					
9	Services were interrupted					
10	Taking Charge of Crucial Mechanisms					
11	Rogue and feral mobile apps					
12	P2P file sharing/exchanging					
13	Social networking					
14	Individual webmail and email					
15	Device(s) with unappealing user interfaces.					
16	Poor handling of credentials					
17	Overuse of biometrics (such as facial recognition, iris scans, and fingerprint readers)					

Please put (√) mark in the boxes that suits your response.

VL=Very Likely, L= Likely, N=Neutral, U=Unlikely, VU=Very Unlikely

	External Risks	VL	L	N	U	VU
External Risks – Social Engineering						
18	Scam emails targeting any department					
19	Data theft in the workplace					
20	IDs have been stolen from people.					
21	The unauthorized disclosure of sensitive data (whaling scams).					
22	Malware, or malicious software					
External Risk – Fiscal Manipulation						
23	Institutionalized financial transaction manipulation					
24	Misappropriation of assets (theft of data)					
25	Reputational harm to the company's bottom line					
26	Problems with biometric entry points					
27	Weak methods of encrypting financial transactions					
28	Weak system for identifying potentially fraudulent financial dealings					
	External Risks – Illicit Acts					
29	Use of obscene and/or unethical content					
30	Theft of computer systems					
31	The absence of confidentiality agreements					
32	Industrial sabotage					
33	Theft of information through the use of intermediaries.					
34	Identity theft and signature forgery					
35	Phishing attack					

Please put (√) mark in the boxes that suits your response.

VL=Very Likely, L= Likely, N=Neutral, U=Unlikely, VU=Very Unlikely

	Internal Risks	VL	L	N	U	VU
Internal Risks – Oblivious						
36	Staff members are too complacent.					
37	Unavailable resources for gaining context					
38	There is a lack of information sharing and threat analysis					
39	No effort is made to maintain or update regulations.					
40	Insufficient reporting procedures					
41	Unauthorized connections					
42	Security flaws that are ignored					
43	Inadequate education in cyber defence					
44	Failure to adhere to data privacy regulations					
45	Inadequate safeguards during data input					
46	Inadequate safeguards at the biometric access					
47	Linking individual gadgets to corporate networks					
Internal Risk – Apathy						
48	Risk-based culture is not a focus in cybersecurity education.					
49	There is a lack of risk management policies.					
50	Insufficient disclosure of risks and weaknesses					
51	Insufficient employee responsibility and reaction time to emerging threats					
52	Lack of consistent bug fixes and new features in software					
Internal Risks – Fiscal Manipulation						
53	Financial and cyber-literacy gaps					
54	Former employees retain certain access even after they've left the company.					
55	Inappropriate personnel have access to financial records.					
56	Misappropriation of funds or sensitive data					

57	Employee errors					
Internal Risks – Illicit Acts						
58	Acts of retaliation by workers or former workers					
59	Intentional attacks					
60	Phishing					
61	Imposing Usage Restrictions					
62	Theft of property, including ideas and inventions					

Please put (√) mark in the boxes that suits your response.

VL=Very Likely, L= Likely, N=Neutral, U=Unlikely, VU=Very Unlikely

	Risks	VL	L	N	U	VU
Vulnerabilities and Weaknesses						
63	Cybersecurity threats increase with system size.					
64	Risk is never an issue with systems.					
65	A common issue is that private information is too easy to obtain.					
66	We do not disclose malfunctions or breakdowns in our systems.					
67	Attacks can be detected with the use of anti-virus and anti-malware software.					
68	There are safeguards in place for electronic mail.					

Section C: In What Ways Do You Believe The Organization's Weaknesses And Vulnerabilities May Affect Its Physical And Digital Assets?

Please put (√) mark in the boxes that suits your response.

VL=Very Likely, L= Likely, N=Neutral, U=Unlikely, VU=Very Unlikely

	Risks	VL	L	N	U	VU
Physical And Digital Assets						
69	Computers					
70	Hard disks					
71	Intellectual property					
72	RFID and barcode readers					
73	Credit cards/debit card/payment cards/'e-wallet'					
74	Scanners and detectors					

Section D: How Probable Are Each Of The Following Reactions To Cyberattacks From Outside Your Organization?

Please put (√) mark in the boxes that suits your response.

VL=Very Likely, L= Likely, N=Neutral, U=Unlikely, VU=Very Unlikely

	Risks	VL	L	N	U	VU
63	Take systems off-line					
64	Make a new password					
65	Verify all safety measures and firewalls					
66	Keep an eye on activity logs.					
67	Get rid of or modify all of the default passwords and unused accounts.					
68	Firewall external access needs regular checks					
69	Firewall external access should be checked often					
70	To avoid continued unauthorized access, occurrences must be categorized, logged, and tracked.					
71	Ensure secure authentication and data transfer by equipping the network with robust encryption.					

Section E: To What Extent Do You Agree That Each Of The Following Descriptions Fits Your Company?

Please put (√) mark in the boxes that suits your response.

VL=Very Likely, L= Likely, N=Neutral, U=Unlikely, VU=Very Unlikely

	Risks	VL	L	N	U	VU
72	Instantaneous detection and shutdown of cyberattacks					
73	Any unauthorized or otherwise suspicious attempts to access vital systems will be immediately flagged.					
74	A standard level of network activity is set.					
75	Unauthorized access, hardware, network activity, and program execution are all tracked.					
76	The area is constantly checked for signs of unauthorized entry.					
77	Timely notification of security incidents is provided as recommended.					
78	In accordance with industry standards, we promptly report any security incidents.					
79	Assessment results are used to determine the order of problems to be addressed and fixed.					
80	Independent audits of event logging procedures guarantee proper administration (including but not limited to access limits, retention, and upkeep).					