University of Strathclyde Glasgow

IMPROVING CYBERCRIME REPORTING IN SCOTLAND

PhD Dissertation

PhDr Juraj Sikra, M.A.(Hons), MSc., CIPD Assoc.

Strathclyde Cyber Security Group (StrathCyber)

Department of Computer and Information Sciences

University of Strathclyde, Glasgow

14 May 2025

A dissertation submitted for the Degree of Doctor of Philosophy

DECLARATION OF AUTHENTICITY

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

PhDr Juraj Sikra, M.A. (Hons), MSc., CIPD Assoc.

Abstract

This dissertation aims to improve cybercrime reporting in Scotland, a responsibilised society, where the state has rolled back its support for cybervictimised populations. The main research questions is: **"What is required to improve cybercrime reporting in Scotland."** Firstly, a systematic literature review (SLR) was completed, which defines a victim typology and cybercrime reporting approaches. The SLR concludes that improving reporting requires a social rather than a purely technical approach. Secondly, interviews using the victim typology were conducted (N=10). Factors that improved (e.g., fund reimbursement, increased awareness and "best practices") and impeded reporting (e.g., lack of support from the police) were identified. Thirdly, a victimised private institution from the prior study received a research-driven bespoke cybercrime training. This training improved some work practices but did not improve reporting, which was connected to a lack of state support. Fourthly, work into Responsibilised Non-Policing Agencies (RNPAs for short) was completed. These varied agencies stem from multidisciplinary work and substitute the police in the cybercrime arena. Qualitative interviews on Scottish (N=10) and Italian (N=4) RNPAs were conducted to use their expertise to improve cybercrime reporting. As a result, it was found that the Scottish state supports victims to a greater degree than the Italian state post-victimisation. The overall discussion ties the material together by contrasting the frameworks from the SLR with the collected data. It was found that cybercrime reporting is unaffected by Police Scotland's organisational politics, but it is affected by responsibilisation. It is recommended that future work focuses on the needs of SMEs and continues to develop the expertise of RNPAs both from policy as well as technological perspectives. It is concluded that research into improving cybercrime reporting has enduring potential because it addresses the major economical and psychological costs of cybercrime victimisation in Scotland.

Acknowledgements

In 2019, the Scottish Institute for Policing Research (SIPR) allocated funding towards this PhD to investigate cybercrime reporting in Scotland (Thomas, D.R., Collier, B., and Renaud, K.V. 2019). By the time this PhD dissertation was first submitted in 2024, reported cybercrime had increased by 300% (Scottish Government 2024), which demonstrates the urgency of the current research.

Therefore, I would like to thank my primary supervisor Dr Daniel R. Thomas and secondary supervisor Prof Karen V. Renaud for their consistent availability and support both practical and emotional, which by far exceeded the formal requirements.

In addition, I thank my tertiary supervisor, Dr Ben Collier for helping me understand the unique and exciting context of contemporary Scottish policing as well as the University of Strathclyde, SIPR, SICSA (The Scottish Informatics and Computer Science Alliance) and Dr Jean Carletta from the University of St Andrews for their support and funding.

Contents

Chapter 1

Introduction

> There is no room for complacency about the severity of state-led threats or the volume of the threat posed by cyber criminals. The defence and resilience of critical infrastructure, supply chains, the public sector and our wider economy must improve.
>
> Richard Horne, Head of GCHQ's NCSC, December 2024

The purpose of this research was to understand the problem of cybercrime under-reporting in Scotland by using a multi-disciplinary research approach to investigate how to improve cybercrime reporting in Scotland, which it connects with barriers to reporting.

Investigating how to improve cybercrime reporting is crucial, because current statistics describe the increasing levels of harm caused by cybercrime on Scotland. According to Scottish Government 2024, in the year of 2023–2024 alone, 16 890 frauds were recorded by Police Scotland, of which 59% (9 890) were cybercrimes. This is an 16% increase in cybercrime from 2022–2023 (Scottish Government 2024).

These figures reflect only those cases where people felt able to come forward to report cybercrime. The research, along with prior work, demonstrates that victims often face barriers to coming forward and reporting cybercrime (Leukfeldt, E.R., Notte, R.J., and Malsch, M. 2020; Police Scotland and Scottish Police Authority 2020). Hence, the actual prevalence is likely to be much higher.

Therefore, the main research question is: **"What is required to improve cybercrime reporting in Scotland."** The question was selected to reflect the needs of Scotland and SIPR, which funded this investigation. Specifically, the funding statement by Thomas, D.R., Collier, B., and Renaud, K.V. 2019 justified the need for this project as a: "direct response to an emerging issue and strategic priority for Police Scotland"

This research focuses on determining what is required to improve the reporting of economic cybercrime that contains dishonesty such frauds and scams in their varied forms. Cybercrimes of dishonesty are important because dishonesty is at the root of all other cybercrime, yet they are often seen as less serious by society if they do not contain a violent or sexual component. I will also touch on other crimes that are carried out for an economic incentive such as selling illegal booter services (Collier, B., Thomas, D.R., Clayton, R., and Hutchings, A. 2019).

Cybercrime victimisation in Scotland affects a wide range of victims who fear to speak out, which perpetuates the under-reporting problem. For example, cybercriminals may impersonate British public institutions via their online communication, which they follow-up with credible looking printed correspondence delivered via Scottish victims' letter boxes (§4.2.2). Also, under-funded Scottish charities, which support extremely vulnerable people, can find their systems locked by cybercriminals who threaten to expose the identities of their clients if

they do not pay a ransom (§4.2.4). Even though these strategies are known, problems with insufficient cybercrime reporting worldwide result in both economical and psychological harms. Improving cybercrime reporting on a population scale is a critical step towards successful investigations, conclusive prosecutions and ultimately victim compensation.

The main research question of: **"What is required to improve cybercrime reporting in Scotland."** will be answered from multiple angles in the upcoming chapters with the use of sub-themes and sub-questions. In particular, the research question will be answered via a systematic literature review, which will serve as the basis for a qualitative study of cybercrime victims. Subsequently, a study into the cybersecurity training needs of an attacked Scottish company will look at whether training can improve reporting. Finally, an investigation into organisations that substitute the police will uncover the role of the multi-agency approach in improving cybercrime reporting in Scotland.

This multi-faceted approach is chosen because the problem of cybercrime under-reporting is not homogenous. Rather, the upcoming chapters are all anchored in the current Scottish policy landscape which is marked by the retraction of the state from victim support. Instead of supporting victims, the state delegates this responsibility or, as some would say, empowers the victims alongside the non-governmental and charity sector in addressing the problem.

Using Scotland as a case study will go beyond addressing the problem on a national level. In fact, it enables scholars, intelligence and law enforcement professionals to make inferences about other nations, too. Thanks to prior international research it is already known that inadequate cybercrime reporting mechanisms can be to blame for cybercrime under-reporting (Bidgoli, M., Knijnenburg, B.P., Grossklags, J., and Wardman, B. 2019) however experiences of social isolation also inhibit people from reporting cybercrime (Van de Weijer, S., Leukfeldt, R., and Van der Zee, S. 2020a). Yet there is a relative lack of data on cybercrime reporting overall and in Scotland, in particular (MacDonald, K. 2019), which justifies the use of prior UK and global research as a starting point for extrapolating lessons for Scotland.

A significant portion of this dissertation will include the extrapolation of data from all of the UK onto Scotland. I have done this assuming that prior UK research includes research on Scotland too unless stated otherwise. This is especially relevant in cybercrime reporting, whereby, until 2019, Scotland used Action Fraud - the UK's centralised cybercrime reporting mechanism (MacDonald, K. 2019). Yet, due to the devolution of policing in Scotland (and subsequent separation from Action Fraud), I distinguish between UK research and research on Scotland. I will also address the uniqueness of the Scottish policing context in section 1.3.

In section 1.3, I describe the modern changes in Scottish policing within the context of UK policing and how both connect to improving cybercrime reporting in Scotland. Then, section 1.4, covers how the counting of crime evolved over time and what this implies for improving incidence of cybercrime reporting in Scotland.

1.1 STATEMENT OF CONTRIBUTION TO KNOWLEDGE

The following is a statement of original contributions to the body of knowledge in the area of improving cybercrime reporting, provided within this dissertation.

1. The §3 Systematic literature review (SLR) chapters have effectively collated and analysed peer-review articles in connection to cybercrime research, victims and reporting by creating victim typology and cybercrime reporting frameworks that I used to inform both the structure of my dissertation but also work that I co-authored on real victims (see: Table 1.1). These frameworks can be used by subsequent researchers too for organising policies and laws.

   An important contribution of these chapters is in explaining the differences between victim types. These differences are meaningful because they increase insights into victims' needs, which can be used to improve reporting. Lastly, these chapters contribute with the insight that improving cybercrime reporting is also a social process not merely a technical one.

2. The §4 Scottish victims of cybercrime (SVC) chapter has built on the findings from the SLR and shed light on the experiences of typologically distinct victims (i.e., Individuals, Private institutions and Public institutions) via qualitative interviewing and thematic analysis. These qualitative interviews informed further empirical work on a quantitative survey of 380 Scottish victims of cybercrime, which I co-authored and which has been published (see: Table 1.1). The findings from this article will be useful for Scottish policy makers as they draw on multiple sources of evidence.

   An important contribution of this chapter is in extracting factors that (§4.2.5) improve and (§4.2.6) impede cybercrime reporting based on the interviews of the different victims, which is tied to genuine case studies.

3. The §5 Client-centred cybercrime training (CCCT) chapter reconnected with a victimised Private institution from the SVC and co-designed a bespoke cybercrime training for the purposes of building organisational resilience, which included guidance on cybercrime reporting. This case study resulted in a peer-reviewed publication (see: Table 1.1), which was accepted on the basis of addressing a research gap since this research aimed to support a Scottish SME from a deprived area. This approach adds to knowledge because currently the cybersecurity costs of running SMEs are not reflected as obstacles in government research as I go on to explain in section 8.1. This is likely to mean that there is substantial expenditure from SMEs for their cybersecurity, which could be more effectively harnessed if their cybersecurity needs were recognised by the government.

   An important contribution of this chapter is in showing that cybercrime training can improve some cybersecurity workplace practices, but did little in terms of improving cybercrime reporting to the police.

4. The §6 Responsibilised non-policing agencies (RNPAs) chapter builds on the principles of multi-agency work in a novel way by extending its principles into the cybercrime reporting arena in Scotland. This work has made multiple contributions to the existing body of knowledge because I have demonstrated how the non-policing agencies can be harnessed to improve cybercrime reporting in areas previously catered to by Police Scotland. Moreover, this work was presented and widely accepted across a range of conferences and is currently under under review post-submission in a peer-reviewed journal (see: Table 1.1). Personally, I also like to recollect at the moment when I presented this

work to Assistant Chief Constable to Police Scotland - Andy Freeburn, who described it as being: “Bang on the money.”

An important contribution of this chapter is in using the know-how of non-policing agencies to articulate a best practices strategy for improving cybercrime reporting in Scotland, which shares points of overlap with existing literature.

1.2 EVIDENCE FOR THE CONTRIBUTION TO KNOWLEDGE

In Table 1.1, I present my publication activity over the course of my PhD. Whilst I am the first or sole author of all the mentioned work, I am remain grateful to my supervisors without whom none of this would have been possible. In particular, the publication Identifying Factors that Promote or Deter Cybercrimes Reporting in Scotland, which was published by the *Journal of Economic Criminology (JEC)* has been substantially improved thanks to the help of Prof Karen Renaud, who has enriched it with the MINDSPACE framework.

Dissertation chapter	Peer-reviewed submission	Submission status	Non-peer-reviewed submission	Submission status
Chapter 3 Systematic literature review (SLR)	UK cybercrime, victims and reporting: a systematic review/ *Commonwealth Cybercrime Journal*	Published	Improving Cybercrime Reporting in Scotland: A Systematic Literature Review/ University of Strathclyde [Pre-print]	Published
			Improving cybercrime reporting in Scotland: a systematic literature review/ DSMS 2022 [Abstract]	Published
Chapter 4 Scottish Victims of Cybercrime (SVC)	Investigating what promotes and deters Scottish cybercrime reporting/ *Journal of Economic Criminology (JEC)* **Note**: Contains a quantitative survey on 380 Scottish victims of cybercrime not included in the dissertation due to the use of the MINDSPACE behavioural influence model agreed on by secondary authors.	Published	Improving cybercrime reporting in Scotland: the victims' perspective/ DSMS 2023 [Abstract]	Published
			Identifying Factors that Promote or Deter Cybercrimes Reporting in Scotland/ *7th Strathclyde International Perspectives on Cybercrime Summer School* **Note**: Presents the abstract from the accepted article to the JEC.	Published
			Book review: Insider Risk and Personnel Security: An Introduction: Paul Martin/ *The RUSI Journal* **Note**: Uses the original book to connect with the concept of "insiders" in Case study 2. of Chapter 4.	Published

			Book Review: The Rules of Security: Staying Safe in a Risky World: Paul Martin/ *The RUSI Journal* **Note**: Uses the original book to connect with the discussion section of Chapter 4.	Published
Chapter 5 Client-centred cybercrime training (CCCT)	Client-centred cybercrime training: C-C Cybercrime Training/ *The 2024 Dewald Roode Workshop (2024 DRW) on Information Systems Security Research, Kennesaw, Georgia, United States*	Published	Client-centred cybercrime training for Scottish Small-to-Medium Sized Enterprises (SMEs)/ University of Strathclyde **Note**: Contains the downloadable booklet, which was used as a handout to the staff of the attacked SME from 2024 DRW peer-reviewed submission.	Published
	Delivering an interactive university curriculum during Russia's invasion of Ukraine/ 13-16. *VII International Scientific Conference Military Psychology In The Dimensions Of War And Peace* **Note**: The methodology within informed the Client-centred cybercrime training and is cited in the publication.	Published		
	Evaluating an interactive university curriculum delivered during Russia's invasion of Ukraine/ *The Bulletin of Taras Shevchenko University of Kyiv Social Work* **Note**: The methodology within informed the Client-centred cybercrime training and is cited in the publication.	Published		

Chapter 6 Responsibilised Non-Policing Agencies (RNPAs)	Cybercrime reporting and the role of Responsibilised Non-Policing Agencies (RNPAs) in Scotland and Italy/ *International Journal of Cybersecurity Intelligence and Cybercrime* **Note**: Contains a quantitative survey on 151 Scottish and 136 Italian victims of cybercrime. The survey is not included in the dissertation due to a novel conceptual angle agreed on by secondary authors.	Manuscript accepted	The role of Responsibilised Non-Policing Agencies (RNPAs) in improving cybercrime reporting in Scotland/ *Cambridge Cybercrime Centre: Sixth Annual Cybercrime Conference* [Abstract and talk]	Published
			The role of RNPAs in improving cybercrime reporting in Scotland/ *Scottish Institute for Policing Research (SIPR): Annual Report and Accounts 2022/23 for the Academic Year Ending 31 August 2023* [Abstract]	Published

Table 1.1: Related publications. Note: This table covers only those chapters that included original and publishable research.

1.3 POLICE SCOTLAND

It is important to introduce Police Scotland. According to Police Scotland n.d.(a), the organisation was founded on 1 April 2013 with the aim of policing all of Scotland. It currently employs over 22 000 staff and aspires to protect people in line with the organisation's values of integrity, fairness, respect and with human rights (Police Scotland n.d.[a]).

Within Police Scotland, reporting cybercrimes of dishonesty is done via the non-emergency 101 phone number, this has longer waiting times rather than the 999 number, which grants instant access to the police's staff (Police Scotland n.d.[b]). This deters people from reporting to the police. Moreover, as I go on to demonstrate in section 4.1 the police and court systems of Scotland prioritise cybercrimes that contain sexual abuse over cybercrimes of dishonesty. This also makes victims of non-sexual scams invisible to the justice system in Scotland.

When discussing the democratisation of the UK police, Jones, T., Newburn, T., and Smith, D.J. 1996 put forward the arguments that the police cannot be effective without adequate supervision of public service processes. This pro-active supervisory approach should always be prioritised over a reactive after the fact strategy, which should only come as a second option. They also viewed the effective collaboration between the police and local communities as a key condition of democratic policing.

Taking into account the Scottish context in particular, in a research paper on the subject of rural policing, Wooff, A. 2015 described the interactions between the police and their local community on cases of anti-social behaviour. With the use of vignettes, Wooff, A. 2015 showed how police differently use discretion to respond to escalating violence. In the first vignette, the police officer used compassionate mentoring towards a group of youths that were engaged in verbal aggression, which de-escalated the situation. In the second vignette, the police officer arrested the individual who was behaving antisocially due to the continued repetition of the problem behaviour. I argue that in both cases the police officers tried to behave in ways that increased cohesion in the community be it with the use of compassion or offender exclusion respectively. Police officers who are able to embody these qualities will be particularly well placed to build trust with their citizens to increase cybercrime reporting because people will feel confident to approach them after a crime.

In a follow-up research, Wooff, A. 2016 has contextualised rural policing within the evolution of Scottish policing, which has undergone a major reform in 2013. During 2013, 8 regional forces were centralised under one Police Scotland. This has created new challenges for rural policing which Wooff, A. 2016 analysed using the prism of "soft" versus "hard" policing. Soft policing is based on the idea of police collaborating with the community to resolve shared issues. Hard policing is akin to the police enforcing the law and combating crime. Whilst Wooff, A. 2016 warns against collapsing "rural policing" and "soft policing", the author sees the terms as complimentary. In his view, soft policing exploits localised expertise, which is required for rural policing. This is an important piece of research because it goes some length to show that centralised hard policing practices carry the risk of losing precious insight into the social dynamics of communities. Importantly, these insights will contain information about who is most vulnerable to cybercrime. This is why I argue that soft approaches to policing are better placed at improving cybercrime reporting in Scotland than hard approaches.

In remaining with the subject of the 2013's centralisation reforms in Police Scotland, Henry, A., Malik, A., and Aydin-Aitchison, A. 2019 argued that centralisation is best conceptualised as a process rather than event. The authors state that local policing is historically tied to the municipal structure of services and therefore honours a democratic system, which need not be completely abolished moving forward. This is because according Henry, A., Malik, A., and Aydin-Aitchison, A. 2019 policing should remain at its heart democratic even if

effective centralist reforms are put into place.

In order to preserve a balanced debate about the unification of modern policing in Scotland, I include a captivating viewpoint on this subject by Murray, K. and Harkin, D. 2017. Unlike, Wooff, A. 2016, Murray, K. and Harkin, D. 2017 view the centralisation of Police Scotland under the nationalist government as a constructive manoeuvre. They argue that policing prior to this reform was devoid of effective scrutiny, which created problems for maintaining high standards of practice. I agree with the claim that localisation is not without its challenges, namely the discretion component frequently referenced by Wooff, A. 2015 and Wooff, A. 2016 is a double-edged sword when embraced uncritically. In other words, discretion is by definition about having power over an environment rather than about exercising that power ethically, which is an important distinction. Hence, police officers with privileged knowledge into their local communities are also in a far better position to abuse that knowledge than someone following centralised procedures of agreed best practice.

In parallel with the subject of centralisation of Police Scotland is the recent shifting away from the UK's centralised cybercrime reporting mechanism – Action Fraud. The latter is described as the fraud reporting system put into place by the Home Office and manned by City of London Police (MacDonald, K. 2019). In response to a Freedom of Information request to Dyson, I. 2019, MacDonald, K. 2019 supplied the evidence-based analysis which resulted in Scotland severing its relationship with Action Fraud. This is connected to centralisation. Firstly, Action Fraud was the central reporting system for England, Wales, Northern Ireland and Scotland until Scotland discontinued its membership. Secondly, by discontinuing its membership with Action Fraud, Scotland effectively centralised its cybercrime reporting systems under its devolved government.

In terms of the factors in favour and against remaining with Action Fraud, Police Scotland considered several of issues. Firstly, if the force were to remain with Action Fraud, Police Scotland would have to contribute £459 324 per year to the upkeep of the service. The advantages of this would include benefiting from a UK wide anti-fraud service and avoiding cases where the national police would conduct its own investigations. The disadvantages of this would include paying too much for a service that has been assessed as poor (MacDonald, K. 2019). Secondly, if the force were to refuse paying Action Fraud, then it would have to pave a new strategic direction for Police Scotland, which would include redirecting fraud complaints using the 101 non-emergency police helpline. The advantages of this would be victims receiving a tailored service including a vulnerability assessment and there would be no attached fees to Action Fraud. The disadvantages of this would include the risk of duplicate investigations in a situation where the central oversight of Action Fraud was removed. After weighing up the pros and cons, Police Scotland decided to move away from Action Fraud and follow their own approach (MacDonald, K. 2019).

The question for practice is as follows: "What approach will work best to deliver on Police Scotland's ambition to prioritise the most vulnerable victims of cybercrime (Police Scotland and Scottish Police Authority 2020)?" The Cyber Strategy 2020 emphasises the need to pay closer attention to those who suffer with a disability or other form of adversity which puts them at greater risk of victimisation.

The prioritisation of vulnerability is not entirely new and is referenced in other literature where it is used to prioritise among high volume offences (Skidmore, M., Goldstraw-White, J., and Gill, M. 2020). In fact, Skidmore, M., Goldstraw-White, J., and Gill, M. 2020 found that 74% of police forces use the vulnerability of the victim to determine whether to proceed with an investigation. On the flip side, police officers were less likely to empathise with people who had played an active role in their victimisation. Increasingly, according to Skidmore, M., Goldstraw-White, J., and Gill, M. 2020 police forces have began to see more value in showing

support to the victims rather than proceeding with investigations, which was largely influenced by the difficulties to trace the cybercrime culprit.

The implementation of recommendations from the Cyber Strategy 2020 (Police Scotland and Scottish Police Authority 2020) is also not without its problems. Researchers have taken issue with how "vulnerability" is defined and what it means for those that are suffering with a condition which puts them at the intersection of the mental health and criminal justice system. Namely, Enang, I. et al. 2019 observed that vulnerability is context specific from the law enforcement perspective, which means that anyone can become vulnerable based on the situation that they find themselves in. In contrast, from a public health perspective vulnerability is viewed as a personal quality. The resulting effect of this conundrum is a fragmentation of the definition of "vulnerability" which makes its prioritisation in cybercrime complicated.

Based on the Cyber Strategy 2020 (Police Scotland and Scottish Police Authority 2020), cybercrime remains chronically under-reported. In the case of scam phone calls and viruses between 84% and 79% victims respectively did not report their experiences. In addition, the online theft of bank related details was the type of crime reported by 74% of victims, with approximately 95% from that group reporting to the banks and only 5-8% to the police (Police Scotland and Scottish Police Authority 2020).

The reasons for these discrepancies are debated in the literature in connection to "responsibilisation", which is the shifting of responsibility for security from the state onto the citizen (Garland, D. 2002a; Garland, D. 2002b). In topical research by Horgan, S. and Collier, B. 2016 the authors argued that security responsibilisation has been taking place since the 1980s. During this period the UK governments supported the privatisation of various policing services. This resulted in competition among private companies to sell more secure locks, CCTV and recently cybersecurity solutions. Moreover, other reasons for the lack of cybercrime reporting in Scotland can be that most government interventions are aimed at awareness raising, which contains victim blaming connotations. These only further alienate people.

The challenges with responsibilisation stretch into cybercrime. Take for example the research by Renaud, K., Flowerday, S., et al. 2018. The latter authors argued that the neoliberalist agenda resulted in governments adopting an approach whereby they advise citizens on cybersecurity issues, but let them face the consequences if they choose not to follow that advice. In the case of cybersecurity, Renaud, K., Flowerday, S., et al. 2018 take two main issues with this approach. Firstly, they argue that responsibilisation of cybersecurity is unreasonable because only a percentage of people have the expertise to behave safely online. Secondly, they argue that responsibilisation of cybersecurity is not judicious because the mistake of one person can result in the contamination of countless computers. Hence, one person's mistake can become many people's problem. This is why the state should adopt a more hands on approach to managing cybersecurity risks.

Furthermore, Renaud, K., Orgeron, C., et al. 2020 examined responsibilisation in countries from the "Five Eyes" coalition, which entail the United Kingdom, USA, Australia, New Zealand and Canada. They found that these countries impart cybersecurity advice to its individual citizens, but become disengaged thereafter. Critically, Renaud, K., Orgeron, C., et al. 2020 found that the "Five Eyes" invest substantial amounts of finances into the protection of businesses and research into cybersecurity, which exemplifies the disparity in their approach to citizens versus corporations.

Given the findings on responsibilisation, it should not come as a surprise that people struggled to connect their experiences of cybercrime with the Scottish police agenda (Horgan, S. 2021) making them reluctant to report it. This too points to the enduring effects of the discussed problem.

Before I close off this section, I will mention a successful example from the Hampshire

Constabulary, which provides a promising avenue for improving cybercrime reporting in Scotland. In the research by Karagiannopoulos, V., Sugiura, L., and Kirby, A. 2019 the researchers examined the Cyber Awareness Clinic, which was a two year university project funded by the Hampshire Constabulary. The aim of the clinic was threefold. Firstly, it was to impart cyber awareness to vulnerable groups such as young people, the elderly and small and medium sized companies. Secondly, the clinic improved the knowledge of risks that the latter communities faced from cybercrime. Thirdly, the clinic aimed to transfer its approach to clinics in other parts of the country. The pioneering clinic generated positive reviews at the formal assessment and was seen as effective in reducing cybercrime in the community. Hence, awareness raising clinics akin to the one above could increase people's reporting behaviour in Scotland.

1.4 Crime numeration

Now, I will discuss selected pieces from the literature on how crime numeration has evolved over time and how it ties into the current research. This matters because the approach within will utilise the upcoming information for structuring victimilogy research.

In a classical study by Maltz, M.D. 1977 the author analysed the evolution of crime counting in the USA from the 1930s onward and discovered several trends that defined this domain. Firstly, criminal data has shifted away from the system closer to the crime. This means that initially the source of crime data was court proceedings, gradually the main source of data became police reports, which had given way to victim reports. This change has become enduring as my project is still focused on the connection between the crime and the victim decades after this piece was published. Secondly, in the 1930s the USA dedicated funding to creating crime recording centres, which served to analyse data. Again, in some shape or form I observe this legacy in projects such as Action Fraud, which serve the exact purpose in modern times. Thirdly, when in the 1930s these changes were being put into place they were strongly criticised for their lack of accuracy much like in the 2020s, nearly 100 years later.

It is also worth considering what underlying circumstances prompt victims to report crime. Findings from the developed countries point to the fact that the crime type was the largest predictor of reporting behaviour in victims. Whilst the same researchers hypothesised that this effect may be varied by victim characteristics in developing countries, they were surprised to find no significant effect. Instead, the crime type in developing countries had the largest effect on subsequent reporting behaviour as well (Bennett, R.R. and Wiegand, R.B. 1994). This is an important piece of research for the current project because it suggests that low cybercrime reporting is due to the social perceptions surrounding the crime type rather than victims. Hence, to increase cybercrime reporting in Scotland, the way cybercrime is conceived has to become much more vivid.

Research by Tarling, R. and Morris, K. 2010 confirmed that the seriousness of the offence played the most important role in the decision to report it. Yet, the ratios have changed. Victims are less likely to report property crime and more likely to report violence than in the past. Interestingly, even though property crime has become more dominant, the reporting rate has plummeted. This lends insight into how society's values have shifted insofar as people have become much more sensitive to violent acts rather than low value scams, which can play into the under-reporting of cybercrime in Scotland.

I will conclude the section on crime numeration with a cautionary paper by Hall, M. 2021, who researched the adherence of police to best practice guidelines and the effect of this on the victims. Whilst the authors found encouraging evidence that the police showed strict adherence to the guidelines, they noted that instances where guidelines were not followed were seen as failing the victims. The authors cautioned against taking the best practices principle too far

because they speculated that it could be used to exercise undue control over the police. I think that whilst best practice principles play a role in victim care, it is important to maintain police autonomy as well. Hence, best practice guidelines also require police discretion.

1.5 SUMMARY

In summary, Police Scotland has undergone significant evolution since the nationalist's unification reforms in 2013, which have resulted in the amalgamation of the eight regional forces. This has resulted in some tension between the traditional and localised forms of policing versus the reformed centralised best practice approaches. When it comes to improving cybercrime reporting in Scotland, I will seek to exploit the best of both worlds.

The numeration of crime is also a part of this research. Crime reports have centred around the recorded experiences of the victims since the 1930s albeit with enduring inaccuracies. People are highly motivated to report those offences that are morally most salient which changes over time.

What follows now is chapter 2, which commences with the research paradigm (i.e., pragmatism), followed by the theoretical framework (i.e., responsibilisation), but mainly focuses on the four methodologies that were engaged during the empirical parts of this PhD. These methodologies have been designated into a separate chapter to ease the reader's orientation via the story lines of the subsequent chapters.

The following chapters of the dissertation will commence by guiding the reader through the §2 Methodology, which will speak about how the state's delegation of responsibility onto cybercrime victims is tied to the methodologies of the empirical studies for the purposes of improving cybercrime reporting.

Subsequently, the work will progress onto the (§3) Systematic literature review (SLR), which supplies the victim typology alongside the main cybercrime reporting approaches. An important contribution of the SLR is that improved reporting requires also social rather than purely technical approaches. The SLR is important because it paves the way into the (§4) Scottish victims of cybercrime (SVC) study, which is anchored in the victim typology developed via the SLR. The SVC study finds that fund reimbursement improves cybercrime reporting whereas lack of faith in police impedes it. The subsequent chapter about the (§5) Client-centred cybercrime training engages with a victimised private institution from the SVC research to develop a research-driven bespoke training in cybersecurity and cybercrime prevention post-attack and finds an improvement in work practices as result. Following on from that the (§6) Responsibilised non-policing agencies chapter focuses on engaging multi-agency work in the responsibilised cybercrime landscape whilst finding that Scotland supplies more support to its citizens versus Italy.

The (§7) Overall discussion, which contrasts data from the SLR with the empirical findings from the dissertation finds, among others, that cybercrime reporting remained unaffected by the strategic changes in Police Scotland. Finally, the (§8) Future work proposes a renewed focus on supporting attacked SMEs as well as developing technological solutions to improving cybercrime reporting. Lastly, the (§9) overall conclusion asserts the work's enduring relevance because of the deteriorating geopolitical landscape.

The remainder of the dissertation is dedicated to appendices Appendix A–Appendix E which are referenced throughout this work.

Chapter 2

Methodology

This chapter commences with explaining the pragmatic research paradigm, which is an umbrella term that encapsulates the diverse methodologies within this dissertation. It will then illuminate how the state's shifting of responsibility for cybercrime victimisation is used as the core assumption for the empirical methodologies within. These methodologies all serve the common purpose of answering the research question of what is required to improve cybercrime reporting in Scotland. The first study, which is the Systematic literature review (SLR) follows the empirical methodology by Pickering, C. et al. 2015 for conducting quantitative literature reviews. This methodology was chosen because it produces replicable and transparent results that can be verified by reviewers, which gives credence to its conclusions. The second study, which is the Scottish Victims of Cybercrime (SVC) follows the methodology by Braun, V. and Clarke, V. 2021 and Braun, V. and Clarke, V. 2022 for qualitative research from participant recruitment to interviewing and analysis. This methodology was chosen because it is a recognised guide to best practices for conducting research on participants that were chosen based on convenience as well as with a specific aim. The third study of Client-centred cybercrime training (CCCT) largely follows the methodologies of Sikra, J. 2022 and Sikra, J. 2023b that were derived from teaching online modules to war affected students in Ukraine. These methodologies were chosen because they were seen as being transferable due to their pastoral component, which was seen as useful in highly deprived areas. Moreover, the methodology of Bunge, E.L. et al. 2016 was used to evaluate Qualtrics quantitative surveys because it served as a guide to comparing pre-training and post-training scores. Braun, V. and Clarke, V. 2022's approach was also used to evaluate the qualitative interviews for the same reasons as in the second study. Fourthly, the Responsibilised non-policing agencies (RNPAs) study also followed the recommendations of Braun, V. and Clarke, V. 2022 as well as Ritchie and Lewis 2003 for participant recruitment, interviewing and analysis. Braun, V. and Clarke, V. 2022 was chosen for the reasons already mentioned whilst Ritchie and Lewis 2003 was chosen due to being an established resource for qualitative research (especially interviewing).

2.1 Research paradigm

Whilst the studies within this dissertation could be seen as falling under multiple paradigms, the dissertation itself addresses a singular problem, which is what is required to improve cybercrime reporting in Scotland. All of the studies included within address this problem from various angles and approaches that are flexibly adjusted to comply with the complexities of research in this area. Therefore, it is fitting to say that this dissertation is most aligned with the pragmatic paradigm, which serves as a common factor for researching a singular problem (Pretorius 2024). According to the pragmatic paradigm, reality is fluid and influenced by ex-

periences (i.e., ontology). This assumption is readily discernable from the following chapters particularly those that contain primary data (e.g., §4 Scottish victims of cybercrime (SVC)) because it is the participants' perspectives that have the leading role. Moreover, knowledge is assessed based on how useful it is as well as the results it delivers (i.e., epistemology). For example, in §5 Client-centred cybercrime training (CCCT) and §6 Responsibilised non-policing agencies (RNPAs) I use the feedback from the participants to formulate recommendations for training and policy makers respectively. Lastly, the pragmatic approach is value driven because values are critical in defining research aims with an eye on solving real world problems (i.e., axiology). For instance, the theoretical framework of responsibilisation (§2.2) is a socialist value-laden concept that underlines much of the reasoning within this piece. I believe that this approach enabled me to practice flexibility, which was essential for delivering on my research aims.

2.2 THEORETICAL FRAMEWORK: RESPONSIBILISATION

The main theoretical framework that is interwoven through this dissertation is that of responsibilisation (Garland, D. 2002a; Garland, D. 2002b; Garland, D. 2002c). According to David Garland the UK welfare state, which includes Scotland, started to diminish as the decades after World War II progressed. Responsibilisation was implemented as the need to follow a moral imperative, which made people feel like they should look after themselves in domains formerly catered to by the state (Peeters, R. 2019). These changes also permeated public health where people with unhealthy lifestyles were blamed for their illnesses without an effort to understand the underlying psychological reasons such as chronic stress (Brown, R.C.H., Malsen, H., and Savulescu, J. 2019). According to Done, E.J. and Murphy, M. 2016, responsibilisation was also observed in the teaching and educational profession whereby teachers were ascribed an increasing list of responsibilities whilst financial resources shrunk. Those teachers that struggled with the standards placed upon them were assessed by colleagues as a way to control them. I argue that this is a more severe case of control by using the moral imperative already mentioned within (Done, E.J. and Murphy, M. 2016; Peeters, R. 2019).

As a feature of the state's responsibilisation approach, new methods of crime control started to get rolled out, which shifted the responsibility for security onto the citizens. Initially, this manifested in the physical realm as an emphasis on the promotion of security devices such as more effective locks against break-ins (Horgan, S. and Collier, B. 2016). As technology progressed, responsibilisation encouraged people to buy house cameras and ultimately protective anti-virus software against cybercrime whilst also following governmental advice on how to keep themselves safe (Renaud, K., Flowerday, S., et al. 2018). Modern scholars now readily analyse the impacts of responsibilisation upon the vulnerable groups such as children. For example, Prior, S. and Renaud, K. 2023 argued that parents are prepared to act on safeguarding advice, but struggle to keep up to date with what is "best practice." Moreover, Jarvie, C. and Renaud, K.V. 2024 found that even though the UK government has stepped up its initiative to protect underage users, the deployed approaches violated children's privacy and were mistrusted by the public.

The real life results of cybercrime responsibilisation can be tragic. Tragedies like that of Molly (Kuenssberg, L. 2025), who was driven to suicide after viewing self-harm material online, serve as a stark reminder of what can happen when families are left unsupported. Moreover, the murder of teenage Brianna was also connected to her mental health, which deteriorated after viewing self-harm sites (Burns, J. and Crawford, A. 2024). Men can also face dangers online such as financial sextortion, which is the blackmail of a person with their intimate images (Cox, A. 2023). Yet, all of these cases have something in common apart from

being impacted by harmful content and cybercrime. In all instances, the parents and survivors impacted by this adversity decided to speak up and raise awareness. According to Garland, D. 2002a this is all responsibilised behaviour whereby it is the primary and secondary victims that take responsibility for the welfare of everyone else by going public, which can also trigger changes in the legislation process.

To summarise, responsibilisation is not new, but rather denotes a post-war phenomenon where the UK, including Scotland, has sought ways to shift governmental responsibilities onto the citizens. This has been observed in healthcare, education as well as crime and cybercrime control. The real life consequences in the area of cybercrime include tragedies to adolescent people, which contribute to awareness raising campaigns by the responsibilised primary and secondary victims.

2.2.1 Contribution of responsibilisation to scholarship

The contribution of responsibilisation theory to scholarship lies in its ability to challenge engrained automatic assumptions about notions such as various moral imperatives. The very phrase sounds positive yet from the perspective of responsibilisation theory it signals a reduction of the state's caring role. This can be illustrated beyond crime control with the research that described the responsibilising of patients for poor health outcomes on the grounds of an unhealthy diet (Brown, R.C.H., Malsen, H., and Savulescu, J. 2019). Not only does this approach overlook the root cause of poor health such as psychological stress, but it ignores other domains that may have been formerly the state's responsibility such as job creation and access to affordable healthy food. Therefore, it can be argued that the contribution of responsibilisation is that it offers a set of practical assumptions for policy recommendations, which can be transferred into practice and improve people's lives. The improvement to people's lives will come when the state gradually begins to reclaim some of its territories, which it had gifted to the private sector.

2.2.2 Limitations of responsibilisation

The main limitation of responsibilisation theory, which stems from socialism (Wyatt, G. 2003) is the same as the limitation of its polar opposite, which is neoliberalism stemming from capitalism (Reinsberg, B., Kentikelenis, A., and Stubbs, T. 2021). The limitation is that its success comes down to the people and their sense of ownership for the country they live in. If people understand the state as an extension of the social contract, which is in place, so that everyone can live happier, more equal and equitable lives, then responsibilisation theory will be helpful to aid that aspiration.

Nevertheless, we know from history that socialism has also resulted in distortions of the ideal such as the former Soviet Union, which was a genocidal dictatorship (Naimark, N.M. 2008). So, whilst "it is great" that researchers continue to articulate compelling arguments and advice for policy, at the end of the day, it comes down to the policy makers and everyday voters to decide how much of that advice is implemented into practice.

Hence, research into responsibilisation must remain current and relatable for the everyday person from the street. To achieve this, researchers must go out of their way to collect primary data from the general population. Sitting in an ivory tower for the purposes of writing articulate theoretical articles must be minimised.

To conclude, the main limitation of responsibilisation theory boils down to the people and society who have the most important say in terms of the framework's utility and legacy. This is not unique to responsibilisation, but applies to all theories that aim for social progress. The role of research in offsetting this limitation is in remaining current, practical and relatable to

everyday people. Responsibilisation theory was developed to improve lives and not for the accumulation of publications.

In the upcoming sections, the methodologies to the four empirical studies will be described in turn whilst the sections' titles link to the chapter with the corresponding results.

2.3 Systematic literature review (SLR) Methods

Using the principles of systematic research as outlined by Pickering, C. et al. 2015, I searched the databases Scopus, Web of Science and ProQuest with the use of Boolean variables and keywords identified below. The geographical scope was the UK and temporal scope was no earlier than 1 January 1999 (start of e-commerce) onwards, prioritising the most recent and cutting edge work.

The purpose of this review is to collect and analyse knowledge that will be used to in preparation for studies with the overarching research question of "What is required to improve cybercrime reporting in Scotland." Due to the relative lack of relevant literature from Scotland, this review will use research from the UK and further afield to build a picture about reporting cybercrime which is as close to the Scottish borders as possible. In §3.4 SLR Discussion, this research will be tied to policing in Scotland based on the articles from §1 Introduction with a focus on what gaps in knowledge need to be addressed to support the resolution of this problem in Scotland. In the §3.4.3 SLR Conclusion, I will provide the reader with a compendium of the themes within alongside their utility.

2.3.1 Cybercrime research in the UK

This subsection details the combinations of keywords and Boolean variables that I employed to conduct a systematic database search for analysing the first subtopic of §3.1 RQ1.: What is known about cybercrime research in the UK to date?, §3.1.1 Typology with the aim of answering the research question of what is required to improve cybercrime reporting.

RQ1 What is known about cybercrime research in the UK to date?

Keywords: "Cybercrime AND UK AND types"

Time range: The systematic search was carried out between 09 October 2021 - 30 October 2021 based on the records retrieved from Zotero.

Scopus: Using the above keywords, I revealed 11 articles in Scopus, which were screened for relevant titles and abstracts, which resulted in 8 articles being included in the review.

Web of Science: Using the above keywords, I revealed 21 documents in Web of Science, which were screened for relevant titles and abstracts, which resulted in the inclusion of 9. Subsequently, I reduced these to 5 after 4 were identified as being replicas of articles from the previous search on Scopus.

ProQuest: Using the above keywords, I revealed 14 779 documents in ProQuest. Due to this number being very high, I applied numerous other filters on ProQuest before I could proceed with a search of titles and abstracts. The additional filters were *Subject: Internet crime*, which reduced the articles to 1 585. This excluded the following subjects: risk 3 389, risk management 2 064, earning per share 1 926, computer security 1 570, stockholders 1 501, crime 1 457, dividends 1 119, corporate profits 1 013, stock exchanges 1 013, financial statements 1 002 as well as other subjects populated by less than 1000 articles per subject. *Limit to peer reviewed*, which reduced the articles to 383. This excluded the category of "Full text." *Location: United Kingdom*, which reduced the articles to 56, *Limit to articles*, which reduced the articles to 45. This also excluded the document types: Feature 363 and others under 10 pieces per document type. Subsequently, I screened the 45 articles for titles and abstracts,

which resulted in 11 articles, and as there were no replicas from the previous searches, all 11 were included.

Taken together, using the principles of a systematic literature review, I revealed 23 articles that were included in the literature review §A.1 Prisma 1.

The next section details the keywords and Boolean variables that I employed to conduct a systematic search for analysing the first subtopic of §3.1 RQ1.: What is known about cybercrime research in the UK to date?, §3.1.2 Policing with the aim of answering the research question

RQ1 What is known about cybercrime research in the UK to date?

Keywords: "Cybercrime AND UK AND policing"

Time range: The systematic search was carried out between 09 October 2021 - 30 October 2021 based on the records retrieved from Zotero.

Scopus: Using the above keywords, I revealed 23 articles in Scopus. These were screened for relevant titles and abstracts, which resulted in 14 articles identified as suitable for the systematic review.

Web of Science: Using the above keywords, I revealed 26 articles in Web of Science. These were screened for relevant titles and abstracts, which resulted in 6 articles being added after the additional exclusion of those that surfaced from the previous search.

ProQuest: Using the above keywords, I revealed 4 046 documents in ProQuest. Due to this number being very high, I applied numerous filters on ProQuest before I could proceed with a search of titles and abstracts. The additional filters were *Subject: Internet crime*, which reduced the articles to 301. This excluded the following subjects: risk 2 095, risk management 1 101, crime 1 087 as well as other subjects populated by less than 1000. *Limit to peer-reviewed*, which reduced the articles to 119. This excluded the category of "Full text." *Location: United Kingdom*, which reduced the articles to 25 and *Limit to articles*, which resulted in 21. This excluded the document types: Feature 23 and others that contained 1 article each. Subsequently, I screened the 21 articles for titles and abstracts, which resulted in 1 article being added after the exclusion of replicas from previous searches.

Taken together, using the principles of systematic literature review, I revealed 21 articles that were included in the literature review §A.2 Prisma 2.

2.3.2 Cybercrime victims in the UK

The subsequent subsection details the combinations of keywords and Boolean variables that I employed to conduct a systematic database search for analysing the second subtopic of §3.2 RQ2.: What is known about cybercrime victims in the UK to date?, §3.2.1 Victim profiles with the aim of answering the research question **RQ2:** What is known about cybercrime victims in the UK to date?

Keywords: "Cybercrime AND UK AND victims"

Time range: The systematic search was carried out between 09 October 2021 - 15 November 2021 based on the records retrieved from Zotero.

Scopus: Using the above keywords, I revealed 19 articles in Scopus. These were screened for relevant titles and abstracts, which resulted in 12 articles identified as suitable for the systematic review, 11 of which were added as they were available for free. From the 11 added, 4 already surfaced during the previous searches on the first subtopic, but they are still being treated as new searches in the current one.

Web of Science: Using the above keywords, I revealed 20 documents in Web of Science, which were screened for relevant titles and abstracts, which resulted in the inclusion of 1 article.

ProQuest: Using the above keywords, I revealed 9 252 documents in ProQuest. Due to this number being very high, I applied numerous filters on ProQuest before I could proceed with a search of titles and abstracts. The additional filters were *Subject: Internet crime*, which reduced the articles to 1 513. This excluded the subjects: risk 2 765, risk management 1 498, crime 1 482, computer security 1 261 and other subjects populated by less than 1000. *Limit to peer-reviewed* which reduced the articles to 334. This excluded the category "Full text." *Location: United Kingdom*, which reduced the articles to 55 and *Limit to articles*, which resulted in 43. This excluded the document types: Feature 50 and others that contained 3 to 1 articles each. Subsequently, I screened the 43 articles for titles and abstracts, which resulted in 4 articles being added after the exclusion of replicas from previous searches.

Taken together, using the principles of systematic literature review, I revealed 16 articles that were included in the literature review §A.3 Prisma 3.

The consequent section details the combinations of keywords and Boolean variables that I employed to conduct a systematic database search for analysing the second subtopic of §3.2 RQ2.: What is known about cybercrime victims in the UK to date?, §3.2.2 Victim experiences with the aim of answering the research question

RQ2: What is known about cybercrime victims in the UK to date?

The abbreviation of "UK" was dropped entirely from this search due to the fact that the searches were coming back with 0 results across the databases. Hence, in this section I will make an extrapolation from research on the Western population (i.e. Europe, USA and Australia) onto the UK population.

Keywords: "Cybercrime AND victim AND experiences"

Time range: The systematic search was carried out between 09 October 2021 - 15 November 2021 based on the records retrieved from Zotero.

Scopus: Using the above keywords, I revealed 39 articles in Scopus, which were screened for relevant titles and abstracts, which resulted in 10 articles being included in the review.

Web of Science: Using the above keywords, I revealed 71 documents in Web of Science, which were screened for relevant titles and abstracts, which resulted in the inclusion of 3 articles.

ProQuest: Using the above keywords, I revealed 11 683 documents in ProQuest. Due to this number being very high, I applied numerous filters on ProQuest before I could proceed with a search of titles and abstracts. The additional filters were *Subject: Internet crime*, which reduced the articles to 1 870. This excluded the subjects: risk 2 555, computer security 1 818, crime 1 348 and other subjects populated by less than 1000. *Limit to peer-reviewed*, which reduced the articles to 399. This excluded the category "Full Text." *Location: United Kingdom*, which reduced the articles to 25 and *Limit to articles*, which resulted in 22. This excluded the document types: Feature 23 and others that contained 2 articles each. Subsequently, I screened the 22 articles for titles and abstracts, which resulted in 0 articles being added after the removal of duplicates.

Taken together, using the principles of systematic literature review, I revealed 13 articles that were included in the literature review §A.4 Prisma 4.

2.3.3 Cybercrime reporting

The next subsection details the keywords and Boolean variables that I employed to conduct a systematic search for analysing the first subtopic of §3.3 RQ3.: What is known about cybercrime reporting to date?, §3.3.1 Cybercrime reporting approaches with the aim of answering the research question **RQ3:** What is known about cybercrime reporting to date?

Keywords: "Cybercrime AND reporting"

Time range: The systematic search was carried out between 29 November 2021 - 17 December 2021 based on the records retrieved from Zotero.

Scopus: Using the above keywords, I revealed 67 articles in Scopus, which I have screened the titles and abstracts which have resulted in the addition of 13 articles.

Web of Science: Using the above keywords, I revealed 309 documents in Web of Science, these were then filtered down according to the most recent years i.e., 2022 (1), 2021 (31), 2020 (59) and 2019 (48), which together amounted to 144 articles. I have then screened the 144 articles based on their titles and abstracts and included 6 articles.

ProQuest: Using the above keywords, I revealed 21 568 documents in ProQuest. Due to this number being very high, I applied numerous filters on ProQuest before I could proceed with a search of titles and abstracts. The additional filters were *Subject: Internet crime*, which reduced the articles to 3 054.This excluded subjects: risk 3 383, computer security 2 753, earnings per share 2 607, stockholders 2 425, crime 1 894, risk management 1 859, corporate profits 1 588, software 1 536, covid-19 1 392 as well as other economic and investment type subjects unrelated to cybercrime. *Limit to peer-reviewed*, which reduced the articles to 374. This excluded the category "Full Text." *Location: United Kingdom*, which reduced the articles to 36 and *Limit to articles*, which resulted in 29.This excluded the document types: Feature 33 and others that contained 3 articles each. Subsequently, I screened the 29 articles based for titles and abstracts, which resulted in 0 articles being added after the removal of duplicates.

Taken together, using the principles of systematic literature review, I revealed 19 articles that were included in the literature review §A.5 Prisma 5.

The next section details the keywords and Boolean variables that I employed to conduct a systematic search for analysing the second subtopic of §3.3 RQ3.: What is known about cybercrime reporting to date?, §3.3.2 Cybercrime reporting results with the aim of answering the research question **RQ3:** What is known about cybercrime reporting to date?

Keywords: "Cybercrime AND reporting AND results"

Time range: The systematic search was carried out between 29 November 2021 - 17 December 2021 based on the records retrieved from Zotero.

Scopus: Using the above keywords, I revealed 16 articles in Scopus. These I have screened for their titles and abstracts which have resulted in the addition of 4 articles.

Web of Science: Using the above keywords, I revealed 104 documents in Web of Science. I have then screened the 104 articles based on their titles and abstracts and included 4 articles.

ProQuest: Using the above keywords, I revealed 18 179 documents in ProQuest. Due to this number being very high, I applied numerous filters on ProQuest before I could proceed with a search of titles and abstracts. The additional filters were *Subject: Internet crime*, which reduced the articles to 1 637.This excluded subjects: risk 3 374, earning per share 2 593, stockholders 2 399, computer security 1 920, risk management 1 834, crime 1 704, corporate profits 1 571, financial statements 1 367 as well as other economic and investment type subjects unrelated to cybercrime. *Limit to peer-reviewed*, which reduced the articles to 341. This excluded the category "Full Text." *Location: United Kingdom*, which reduced the articles to 30 and *Limit to articles*, which resulted in 25.This excluded the document types: Feature 27 and others that contained 3 articles each. Subsequently, I screened the 25 articles based for titles and abstracts, which resulted in 0 articles being added after the removal of duplicates.

Taken together, using the principles of systematic literature review, I revealed 8 articles that were included in the literature review §A.6 Prisma 6.

2.4 Scottish victims of cybercrime (SVC) Methods

This section describes the methodology for the Scottish victims of cybercrime study.

2.4.1 Design

This methodology was selected to help me understand what gets in the way of reporting cybercrime, so that the processes can be adjusted to serve victims' needs as well as to increase reporting. To achieve this, I collected data via semi-structured interviews with people who have been victimised by online scams in a way that captured the victims' views as real people caught out amid going about their daily business. The interviews focused on collecting information around victims' experiences and reasons around reporting the crime with supplementary questions, to aid understanding the victim as a person. The interview questions were informed by discussions with my supervisors and are featured in the (§B) SVC Appendix. This project involves interviews of three groups of victims: **SVC – Individuals**, **SVC – Private institutions** and **SVC – Public institutions**.

The interviewing processes was based on person-centred values and approaches that I developed during years of practice within the field of mental health. The participants were sent a §B.1 SVC Participant information sheet and a Privacy Notice for Participants in Research Projects 2025 alongside the §B.2 SVC Consent form in advance of the interview. After they have read the first two documents in their own time, then they sent back a signed Consent form, which was scanned and uploaded onto the University of Strathclyde's One Drive. The interviews lasted between 20–45 minutes. Participants were thanked for their contribution to the research. A debriefing form was not supplied as the research did not include any deception and all aspects of the research were communicated in advance.

The interviews were recorded and stored on the University of Strathclyde's One Drive until they were transcribed by myself as soon as possible, after which they were deleted. Recordings where participants have chosen to have their camera switched on added extra value to the research because they offered more social cues in terms of what the participant was going through, but also how I interacted with the participant. Through these video cues I learned from and improved my research practice, which formed a part of my professional development. People who have chosen to have their camera switched off had their preference respected and they benefited from the same polite and person-centred approach as everyone else. In such cases, I was guided merely by the tone of the participants' voice to gauge changes in emotions to guide the subtleties of my approach. I did not collect biographical or other data that could be traced to specific people. Optionally, participants' age range and gender was collected at the outset hence the only way of directly identifying participants was via the actual video/audio recordings, which were deleted as soon as they were transcribed.

The approach to (§4.2.1) was qualitative whereby the recorded interviews were analysed via specialised software and according to methodological best practices.

2.4.2 Participants

There were three types of participants, which were recruited in different ways: **SVC- Individuals**, **SVC- Private institutions** and **SVC- Public institutions**.

Participant recruitment According to Braun, V. and Clarke, V. 2022, the principles underlying participant selection fit within both "convenience sampling" and "purposive sampling"

approaches (p.14). The former involves recruiting easily recruitable participants and the latter involves recruiting participants with a specific profile. Consecutively, I recruited who was available and in accordance with the victim typology of Individuals, Private institutions and Public institutions.

Firstly, all available news coverage of cybercrime was followed up and potential **SVC- Private institutions** and **SVC- Public institutions** were contacted to request participation. The proposed contact of victims based on news coverage did not pertain to **SVC- Individuals**. I presumed that if the information regarding their attacks was published in the news, then it is appropriate to follow this up using publicly available contact information. The identifiable information relating to these institutions was anonymised.

Secondly, all the researchers' private connections were explored to see whether **SVC- Individuals** can be recruited in that manner.

Thirdly, snowballing participants was used based on the good relationships with former participants. The manner of "snowballing" utilised within was the following: I asked past interviewees whether they were aware of a victim of cybercrime, if they confirmed that they are aware, then the current point of contact was used to reach out to the victim and ask whether the victim if it was okay to have their details shared with the myself and only then the contact person shared the victim's details with me.

Fourthly, CIS Departmental, StrathCyber and staff personal social media accounts were used to advertise the study to potential participants.

Participant information In this section, I will discuss some descriptive information about the 10 interviewed participants alongside the dates and values of the cybercrime. When referring to the values of cybercrime I refer to the monetary value that the cybercriminals sought to extract via their offending activity. I distinguish the value of cybercrime from other monetary as well as non-monetary costs such as the cost of human resources required to reset the corrupted systems for example. The interviewed participants varied in terms of educational attainment and social class although these aspects constituted my mere observations and were not separately analysed.

The first group, §4.2.2 SVC – Individuals consisted of 3 (2 males and 1 female) participants victimised between 2012 – 2022. The first participant suffered harm of £1 000, the second participant suffered harm of £5 240 and the third participant was suffered harm of £20.

The second group, §4.2.3 SVC – Private institutions were 2 organisations that were represented by their managers both of whom were male and in charge of a Small-to-medium-sized enterprise (SMEs). The first SME was victimised by cybercrime in 2015. The value of ransom was £1 000. The loss to business was estimated at £20 000. The second SME was victimised by cybercrime in September-October 2022. The value of the ransom was an unspecified amount of BitCoins. The loss to business was a non-financial cost to human resources required to reset the corrupted systems.

The third group, §4.2.4 SVC – Public institutions were 5 organisations (2 *Educational institutions*, 2 *Charities for vulnerable people* and 1 *National governance structure*) that were represented by their managerial and IT functions and, in one case, a person involved in incident response post-victimisation.

Educational institutions: The first victim was a university represented by its IT security officer (male), which was attacked in March 2021. The value of the cybercrime was zero- the attackers sent an underdeveloped ransomware. The loss to the institution was a non-financial cost to human resources required to reset the corrupted systems.

The second victim was a high school represented by a male head, which was attacked by cybercrime in June 2021. The value of cybercrime was zero- the investigation found a vindictive incentive. The loss to the institution was a temporary challenge to its reputation.

Charities for vulnerable people: The first charity for vulnerable people was represented by its managerial function (male) and had fallen victim to cybercrime in December 2021. The value of the cybercrime was £11 000 transferred by the charity based on a fake invoice although this was later successfully claimed back via the bank who managed to reverse the transaction. Therefore, the loss to the charity was zero. The second charity for vulnerable people was represented by its managerial function (male) and had fallen victim to cybercrime in March 2022. The value of the cybercrime was no stated during the interview. However, the charity did not comply with the ransomware request. Therefore, the loss to the charity was the psychological distress of its staff from the *dumping* (i.e., publicising) their personal details on the Dark Web as retribution.

National governance structure: I also interviewed a person from the incident response team (male) who supported an organisation, which plays a major role within the national governance structure of Scotland. This structure had fallen victim to cybercrime in 2020. The value of the cybercrime was not stated during the interview. The cost to the organisation was extensive system compromise, but also psychological distress of its staff from being interviewed under caution by Police Scotland.

2.4.3 Ethics

This study required multiple ethics applications predominantly due to the unexpected problems with victim recruitment. Hence, most applications to the departmental ethics committee were simply requests to extend the duration of the study whilst others were connected to various conceptual adjustments that reflected the unpredictable terrain of working in a sensitive area with victims. Hence, I applied and received approval for 7 updated versions of the current study spanning from 22 April 2022 until 09 January 2023. Much of the ethics application is contained within the current §2.4 Scottish victims of cybercrime (SVC) Methods hence it is not necessary to regurgitate the information separately in here. Nevertheless, I will briefly touch upon two factors that I considered when demonstrating consent ethically. Firstly, the study had taken place over Microsoft Teams Zoom or Skype online or in person using an Olympus WS-853 Voice recorder. The participant had the option to keep their camera turned off during online interviews to mitigate any possible anxiety. Secondly, the participants were emailed the consent form prior to the interview and then I briefly covered the points on the form during the actual recorded interview to ensure that the participants have a shared understanding of informed consent. Participants were also brought the form in physical format to sign during in-person interviews.

2.5 Client-centred cybercrime training (CCCT) Methods

2.5.1 Design

Quantitative section: The purpose of this research was to evaluate a client-centred cybercrime training for victims who are §4.2.3 SVC – Private institutions, which I interviewed as a part of

the §4 Scottish victims of cybercrime (SVC) study.

I compiled two Qualtrics questionnaires for this training. The aim of the pre-training questionnaire was to gather the staff's requirements for training. The results from this questionnaire served to devise the cybercrime client-centred cybercrime training. The aim of the post-training questionnaire was to gather staff's feedback after the training. Subsequently, I compared the pre-training and post-training questionnaires to evaluate the effectiveness of the client-centred cybercrime training. The questionnaire questions were informed by discussions with my supervisors and are featured in the (§C) CCCT Appendix.

I used the Qualtrics as a part of an integrated dissertation whereby I investigated the reasons for low training uptake and leadership in a major Scottish charity (Sikra, J. 2021). In the latter work I formulated recommendations about how to increase engagement with training by interpreting the empirical data via the lens of past research. Some of these are relevant for the development of the current training such as making it engaging and playful (Huang, R.-T. 2015). Next, I also have experience of designing (Sikra, J. 2022) and evaluating (Sikra, J. 2023b) an academic course that was delivered during the Russian invasion of Ukraine, which was student led, and which also serves as a source of valuable know-how and expertise.

Moreover, as a part of my PhD, I completed a paid part-time consultancy post with the University of St Andrews (21 February - 27 May 2022), where I investigated the Cyber Resilience Curriculum for Scotland with the use of a literature review. My findings from the unpublished theoretical work were especially important in underpinning the development of current questionnaires and introductory section of this work.

Take for example research that focused on designing a student-led curriculum to cyber-resilience (Pike, R.E. et al. 2020). These findings underpin the current research because I have taken the view that participants themselves ought to identify their learning needs to which the training will be reflexive. Additional findings were also accessed when envisaging the current training, mainly my emphasis on the use of real-world examples will form an important part of how the material is illustrated (Payne, B.K. et al. 2021).

Following on from that, I also made important insights for the questionnaire design by highlighting the influence of computer anxiety as a mediating factor over IT performance (Thatcher, J.B. and Perrewé, P.L. 2002). Hence, I integrated three Likert scales measuring depression, anxiety and confidence with respect to preventing cybercrime in the pre-training and post-training questionnaires.

Qualitative section: This segment of research aims to evaluate how people's views and practices in cybersecurity evolved since they have received the training after a period of at least three weeks or more. I aimed to enrich the research into client-centred cybercrime training as it was merely based on quantitative surveys. Hence, introducing the qualitative interviews aided a more holistic evaluation of this approach. The interview questions were informed by discussions with my supervisors and are featured in the (§C) CCCT Appendix.

The participants received the information sheet, consent form and the questions they would be asked in advance. There was a clear rationale to supplying the questions in advance. This was to make them more comfortable but in addition there was no added value to spontaneity. In fact, it was useful from the perspective of evidence if participants made some sort of notes prior to the interview to prime their memory accurately. The entire training approach was based around people being able to ask questions, so there was an opportunity to answer those. I also advised that I will be available for follow-up questions about cybersecuring the company circumstances allowing.

2.5.2 Participants

The participants consisted of 9 staff members which engaged with the development of training, 6 staff members attended and only 5 supplied feedback. Therefore, it is argued that a gradual drop-out pattern was present throughout.In addition, 2 staff members were qualitatively interviewed. The study was conducted under the strict departmental ethical regulations.

2.5.3 Ethics

This study required two ethics applications, which were submitted to the departmental ethics committee.

Quantitative section: the departmental ethics submission was made on the 05 March 2023 and received unconditional approval on the 13 March 2023.

Much of the ethics application is contained within the current §2.5 Client-centred cybercrime training (CCCT) Methods hence it is not necessary to regurgitate the information separately in here. Nevertheless, I will briefly touch upon what factors I considered when demonstrating informed consent and how I justified those within the ethics application.

This part of the study employed an online pre-training (see: §C.3 CCCT Pre-training questionnaire) and post-training questionnaire (see: §C.4 CCCT Post-training questionnaire) which contained the necessary §C.1 CCCT Participant information sheet, a Privacy Notice for Participants in Research Projects 2025 and §C.2 CCCT Consent form. Before the participant could progress from the Participant information sheet onto the Privacy Notice for Research Participants, they had to indicate that they have read the piece of documentation. If they did not indicate that they read the documentation, then they could not progress. Consent was demonstrated by the typing of the participants' full name in the Consent form in both the pre-training and post-training questionnaires. Apart from demonstrating consent, this was put into place so that the data from both questionnaires could be matched and compared during analysis.

Qualitative section: the departmental ethics submission was made on 12 May 2023 and received unconditional approval on the 06 June 2023.

This section employed a semi-structured interview (see: §C.7 CCCT Qualitative interview) which contained the necessary §C.5 CCCT Participant information sheet, a Privacy Notice for Participants in Research Projects 2025 and §C.6 CCCT Consent form. Even though the initial plan was to interview the participants in person. Due to practical constraints placed upon the SME, both members of management decided to submit written responses to the interview questions.

2.5.4 Analysis

Quantitative section: The data were designated for analysis with Qualtrics by comparing pre-training and post-training questionnaires to get an indication of the training effectiveness (Bunge, E.L. et al. 2016). In addition, the pre-training Likert scale scores will be contrasted with post-training scores in cases where participants have submitted both sets of scores for visual rather than statistical purposes.

Qualitative section: The data were designated for analysis in accordance with Braun, V. and Clarke, V. 2022's description of "coding reliability thematic analysis (TA)", which is an approach where: "Themes are developed early in the analytic process prior to or following some data familiarisation, and often reflecting data collection questions (p. 6)." Hence, in line with Braun, V. and Clarke, V. 2022's theorising, the identified themes are best understood as summaries of particular topics, mainly in connection to the training effectiveness and improved cybercrime reporting. In identifying my TA approach, I will also follow the best practices

guidelines by Braun, V. and Clarke, V. 2021 who urged all researchers to "clearly demarcate which TA approach they are using (p.335)."

2.6 RESPONSIBILISED NON-POLICING AGENCIES (RNPAS) METHODS

2.6.1 Design

This study contained two comparative components, which were internationally varied. The major component pertained to Scottish RNPAs. I refer to this component as major because most interviews (11 in total) pertained to Scottish RNPAs and also the interview process was much more thorough. The minor component pertained to RNPAs who were Italian lawyers (4 in total), which accept reports of cybercrime.

I designed this study in response to the fact that an increasing number of people are victimised by online scams, which they are reluctant to report for various reasons. I did this study to understand what gets in the way of reporting this type of crime so that the processes can be adjusted to serve victims' needs as well as to increase reporting. To achieve this, I needed to collect data via interviews with people that work for RNPAs.

Scottish RNPAs The interviewing processes were based on person-centred values and approaches that I developed during years of practice within the field of mental health. The participants were sent a §D.1 RNPAs Participant information sheet and a Privacy Notice for Participants in Research Projects 2025 alongside the §D.2 RNPAs Consent form in advance of the interview. After they have read the first two documents in their own time, then they sent back a printed, signed and scanned §D.2 RNPAs Consent form, which was uploaded onto the University of Strathclyde's One Drive. The interviews lasted between 20– 45 minutes each. As a part of debriefing participants were thanked for their participation and the contribution to the current research. A debriefing form was not supplied as the research did not include any deception and all aspects of the research were communicated in advance.The interview questions were informed by discussions with my supervisors and are featured in the (§D) RNPAs Appendix

The interviews were recorded and stored on the University of Strathclyde's One Drive until they were transcribed by myself after which they were deleted. Recordings where participants have chosen to have their camera switched on added extra value to the research because they offered more social cues in terms of what the participant was going through, but also how I interacted with the participant. The current research had also taken into consideration my own approach to the study and how effectively I managed to interact with the participants therefore having a video record of an interaction offered additional insight into my approach when responding to a participant. Thanks to this I learned from and improved my research practice, which formed a part of my professional development. I transcribed the interview as soon as it had been carried out, thereby enabling the deletion of the sensitive recordings. People who have chosen to have their camera switched off should have felt that their preference was respected and they benefited from the same polite and person-centred approach as everyone else. In such cases, I was guided merely by the tone of the participants' voice to gauge changes in emotions to guide the subtleties of my approach. Any remaining recordings were stored until August 2023 after which they were all be transcribed by myself and erased. I did not collect biographical or other data that could be traced to specific people. Only the participants' age range and gender was collected at the outset hence the only way of directly identifying par-

ticipants was be via the actual video/audio recordings, which were deleted as soon as they are transcribed.

Italian RNPAs Originally, the Italian lawyers were meant to participate in a focus group where they would discuss five questions. These questions were developed in conjunction with my supervisors, whose views informed how they were articulated. However, due to the ethics of the legal profession the lawyers required that they answer the focus group questions individually and in writing. Hence, they firstly received the §E.1 RNPAs- Italian lawyers PIS and Consent form, §E.2 RNPAs- Italian lawyers Privacy Notice for Research Participants and §D.3 RNPAs Interview questions via e-mail in both English and Italian translations. The latter questions were translated by Dr Federica Casarosa which enabled the Italian lawyers to respond. These responses were then translated by Dr Federica Casarosa back into English and sent to me.

2.6.2 Participants

There were five types of participants, which were recruited in different ways: RNPAs – Banks, RNPAs – State-sponsored charities, RNPAs – Regulators of commerce, RNPAs – Private institutions and RNPAs – Italian lawyers.

Participant recruitment

Scottish RNPAs: *Firstly*, all available news coverage of cybercrime was followed up and potential RNPAs were contacted to request participation using publicly available contact information. The identifiable information relating to these institutions was anonymised.

Secondly, all the researchers' private connections were explored to see whether RNPAs can be recruited in that manner.

Thirdly, snowballing participants was used based on the good relationships with former RNPAs. The manner of 'snowballing' utilised within was the following: I asked past interviewees whether they were aware of other supporting organisations, if they confirmed that they are aware, then the current point of contact was used to reach out to the RNPA and ask whether the RNPA was okay to have their details shared with the myself and only then the contact person shared the victim's details with me.

Fourthly, CIS Departmental, StrathCyber and staff personal social media accounts were used to advertise the study to participants.

Italian RNPAs: Participants, which were §2.6.2 RNPAs – Italian lawyers were recruited by Dr Federica Casarosa and Prof Stefano Chessa from the University of Pisa as a part of a £2570 Saltire Emerging Researcher Scheme grant, which I was awarded to run an in-person comparative study in Italy from 03 June until 21 July 2022. These were known industrial contacts from Tuscany that were approached by Dr Federica Casarosa.

Participant information According to Braun, V. and Clarke, V. 2022, the principles underlying participant selection fit within both "convenience sampling" and "purposive sampling" approaches (p.14). The former involves recruiting easily recruitable participants and the latter involves recruiting participants with a specific profile. Consecutively, I recruited organisations' available representatives in accordance with the criterion that they must accept reports of cybercrime and substitute the policing function of the state.

In here, I will discuss some descriptive information about the 15 interviewed participants (9 males and 6 females), which represented different RNPAs. The interviewed participants varied in terms of educational attainment, social class and nationality although these aspects constituted my mere observations and were not separately analysed. My initial plan was to negotiate the publicising of the RNPAs identities as this would allow me to chart out a very detailed map of how the cybercrime agenda was shifted outside the government and hence outside of policing in a new territory of responsibilised non-policing agencies (RNPAs). Only some RNPAs agreed to have their identifiable details published. Hence, I anonymised all RNPAs. The following RNPAs were included in this study:

RNPAs – Banks This study includes 1 interview with a male representative from an established UK bank, which operates in Scotland. The interviewee worked with the bank's anti-fraud team, which made him especially suitable for explaining what information is reported to banks as well as other the analysis of other cybercrime data.

RNPAs – State-sponsored charities This study includes 6 interviews with state-sponsored charities, which receive, process and evaluate cybercrime reports. This group is heterogeneous and hence warrants a detailed description. I will begin by explaining my definition of "state-sponsored charity." I define the latter as a non-governmental organisation, which is predominantly if not entirely dependent from government funding in order to complement or substitute some form of state function. My conceptualisation ties closely to what Garland, D. 2002b described as the "third sector" on p. 170, where he goes on to explain how it evolved alongside the government to substitute its role. In regards to the latter, Garland, D. 2002b specifically states that: "It consists mainly of networks and coordinating practices – local authority panels, working groups, multi-agency forums, and action committees – whose primary task is to link up the activities of existing actors and agencies and direct their efforts towards crime reduction." RNPAs – State-sponsored charities fit this definition and are largely synonymous with the third sector, however in the case of Scotland, these are specifically paid for by the Scottish and UK government. Therefore, my terminology is more specific.

In the instance of cybercrime, I argue that these state-sponsored charities have been responsibilised by the government to tackle cybercrime even though in 5 out 6 cases they were not set-up for this purpose. Only 1 (male interviewee) out of the 6 organisations that I interviewed was deliberately established for tackling cybercrime. The remaining 5 had other dominant vocations such as being a legal charity (1 male interviewee), a consultation charity (1 male interviewee), a university (2 female interviewees), an elderly people's IT charity (1 male interviewee). Collectively, these interviewees received cybercrime reports via different social ports of access. For example, one charity was specifically tasked with supporting SMEs post cyberattack, but another charity supplied generic advice on a range of issues whilst yet another one sought to upskill pensioners' in IT. This is something you would expect to see in cases where a substantial governmental agenda has been shifted outside of the state's perimeter.

RNPAs – Regulators of commerce This study includes 3 interviews (1 female and 2 males) with regulators of commerce, which form a part of governmental functions in this area. I will begin by explaining my definition of "regulators of commerce." The purpose of these institutions is to safeguard the purchasers of goods and services from malpractice and fraud. With the advancement of technology these government functions have been responsibilised with tackling cybercrime, namely cyber-enabled fraud.

RNPAs – Private institutions This study includes 1 interview (male interviewee) with a representative of a private institution who was specifically established as a first-responder to victims attacked by cybercrime.

RNPAs – Italian lawyers This study includes 4 interviews (2 females and 2 males) with Italian lawyers, which receive reports of cybercrime from their clients who are predominantly seeking legal defence during cases where they are being blamed for falling victim to cybercrime which has affected their corporate context.

2.6.3 Ethics

Scottish RNPAs: The major study required multiple ethics applications predominantly due to the unexpected problems with RNPAs recruitment. Hence, most applications to the departmental ethics committee were simply requests to extend the duration of the study whilst others were connected to various conceptual adjustments that reflected the unpredictable terrain of working in a sensitive area with RNPAs that support victims. Hence, I applied and received approval for 7 updated versions of the current study spanning from 22 April 2022 until 09 January 2023. Much of the ethics application is contained within §2.4 Scottish victims of cybercrime (SVC) Methods. Nevertheless, I will briefly touch upon two factors that I considered when demonstrating consent ethically. Firstly, the interviews took place over Microsoft Teams, Zoom, or Skype online; or in person using an Olympus WS-853 Voice recorder. The participants had the option to keep their camera turned off during online interviews to mitigate any possible anxiety. Secondly, the participants were emailed the consent form prior to the interview and then I briefly covered the points on the form during the actual recorded interview to ensure that the participants have given informed consent. Participants were also be brought the form in physical format to sign by the researcher during in-person interviews.

Italian RNPAs: The minor Italian study required two ethics applications. The first ethics application was approved on 26 May 2022 and focused on interviewing victims of cybercrime. However, it was not possible to recruit any victims in Italy. Hence, the second ethics application focused on RNPAs – Italian lawyers and was approved on 06 July 2022.

2.6.4 Analysis

Scottish and Italian RNPAs: The analysis of interview data was designated for analysis by NVivo 1.3 using the rationale for small sample sizes by Ritchie and Lewis 2003 and methodology that fits closely with how Braun, V. and Clarke, V. 2022 describe "coding reliability thematic analysis (TA)", which is an approach where: "Themes are developed early in the analytic process prior to or following some data familiarisation, and often reflecting data collection questions (p. 6)." Hence, in line with Braun, V. and Clarke, V. 2022's theorising, the upcoming themes will be best understood as summaries of particular topics, mainly in connection to what improves and impedes reporting. In identifying my TA approach, I will follow the best practices guidelines by Braun, V. and Clarke, V. 2021 who urged all researchers to "clearly demarcate which TA approach they are using (p.335)."

Chapter 3

Systematic literature review (SLR)

I have explored what is required to improve cybercrime reporting in Scotland by conducting a systematic literature review. Even though Scotland is a part of the UK, it was meaningful to think of it separately since Scottish policing is devolved. Due to the lack of data on Scotland, I have frequently extrapolated from both the UK and the West.

The research questions were: 1. What is known about cybercrime in the UK to date? 2. What is known about cybercrime victims in the UK to date? 3. What is known about cybercrime reporting to date? The answers were retrieved by combining Boolean variables with keywords into Scopus, Web of Science and ProQuest.

This resulted in the analysis of 100 peer-reviewed articles, which was a coincidental round number. This analysis revealed a common trend, a novel taxonomy, and an original conclusion.

The common trend is that of responsibilisation, which is the shifting of responsibility for policing cybercrime from the government onto the citizens and private sector, which will inevitably responsibilise consumers.

The novel taxonomy is for classifying cybercrime reporting systems according to three pillars, which I referred to as Human-To-Human (H2H), Human-To-Machine (H2M) and Machine-To-Machine (M2M).

I answer the main research question by concluding that to improve cybercrime reporting in Scotland, the process needs to be treated also as a social one rather than a purely technical one.

3.1 RQ1.: What is known about cybercrime research in the UK to date?

It is important to understand the cybercrime research to date to improve cybercrime reporting, because prior research informs what is known as well as any gaps in knowledge.

The following subsection is thematically organised as follows: §3.1.1 Typology and §3.1.2 Policing.

3.1.1 Typology

Whilst the creativity of cybercriminals is prolific, I have used this systematic review to reveal specific categories of offences that have affected the UK: §3.1.1 Cybercrime against Individuals, §3.1.1 Cybercrime against Private institutions and §3.1.1 Cybercrime against Public institutions.

Cybercrime against Individuals

This type of cybercrime is most prominently represented in the literature search in connection to the UK. A summary of the crimes committed against individuals is provided in Levi, M. 2017 who states that individuals were most likely to experience bank card fraud (66% of all incidents) and online shopping fraud (28% of all incidents). In contrast, 12 months prior to this research being conducted in 2014-15, 5% of people in Scotland reported incidents of bank card fraud (Levi, M. 2017). Other research has identified that Denial of Service Attacks (DoS) also feature prominently as a cybercrime against individuals who are usually gamers (Collier, B., Thomas, D.R., Clayton, R., and Hutchings, A. 2019). There are at least two actors involved in this modus operandi. The illegal booter service where the customer can purchase the attack and then the actual customer who launches the attack on their victim. This type of crime can result in a simple nuisance that requires the gamer to postpone the game until the attack ceases, but it can also cause actual harm in the household (or to other bystanders) depending on what other technology is affected.

Moreover, people can be targeted by criminals using a romantic or sexual incentive. Victims can be scammed into sending money to apparently attractive people in exchange for sexual photos and videos as a form of a transactional sexual encounter. In fact, they are communicating with a cybercriminal who has purchased a packet of fake photographs via a criminal network to commit an offence referred to as eWhoring (Hutchings, A. and Pastrana, S. 2019; Pastrana, S. et al. 2019). Whilst eWhoring is the communication with a fake profile, romantic scams can involve interactions with actual attractive offenders who exploit the emotional needs of potential victims into sending them finances (Whitty 2018).

Previous research by Correia, S.G. 2019 and Correia, S.G. 2020 also draws attention to the varied effect of cybercrime on individuals. For example, data shows that females are significantly likelier to report Advance fee fraud, whereas as the effect is more pronounced in older people. In contrast, individuals reporting crimes of Hacking, Computer software service fraud, Malware and DoS tended to be younger. The details of cybercrime victims will be covered robustly in the upcoming section §3.2 RQ2.: What is known about cybercrime victims in the UK to date?.

Individuals have been affected by cybercrime even more due to increased loneliness and isolation brought on by the COVID-19 pandemic (Buil-Gil, D. and Zeng, Y. 2021). Crimes against the elderly during the pandemic also received attention in UK research (Cross, C. 2021). She found that the elderly were subjected to the same fraud techniques as in the pre-pandemic period, but that the pandemic was used as ruse to practice those techniques. Lastly, an unusual form of fraud that surfaced during the COVID-19 pandemic was devised to respond to people searching for their lost pets online. As a part of this scam, the offender contacts the owner of a pet that has been advertised as lost and falsely claims that they have found it and will return it for a fee (Levi, M. and Smith, R.G. 2021).

Cybercrime against Private institutions

In the past, these included attacks on banks, which meant submitting forged cheques which were electronically scanned and cashed before being identified as fake (Fisher, J. 2008). Increasingly, companies are targeted also via the vulnerabilities of their staff. In a fraud type referred to as Business E-mail Compromise (BEC), also known colloquially as "CEO Fraud", cybercriminals successfully impersonate the e-mail of a CEO requesting a speedy transfer of funds from the employee (Lord, J. 2016). As a result of this, companies suffer economic harm on reimbursements. In connection to this, SMEs were identified by Levi, M. and Williams, M.L 2013 as particularly vulnerable to cybercrime due to the having limited cyber safety

awareness and dispensable funds.

Another type of cybercrime is when cybercriminals steal customer data and the firm's intellectual property which results in losses that are profound, but also very difficult to calculate precisely (Lord, J. 2016). According to a financial analysis by Levi, M., Doig, A., et al. 2017 the largest financial losses were incurred by companies rather than individuals via crimes such as business trading fraud, pension fraud, financial investments and insolvency and bankruptcy frauds. In terms of the situation in the UK, Leukfeldt, E.R., Kleemans, E.R., and Stol, W.P. 2017 identified that criminal networks are most likely to carry out high tech crime against institutions, but also that their outreach is more international in comparison to other criminal networks elsewhere in the world. Yet a cautionary note is in place when referring to criminal networks as Lavorgna, A. 2019 warned against overestimating the extent of organised cybercrime in the UK lest public funds be unnecessarily depleted. Also, In her critical piece, the author pointed out that the media use the term "organised crime" alongside "cybercrime" to amplify the emotional effect of their message. In my personal opinion, this is an important analysis because the arbitrary use of strong language amplifies a sense of threat in society, which leads to anxiety. This type of anxiety can also influence people's decisions to withdraw from the use of technology, which can have a detrimental impact as well.

Cybercrime against Public institutions

A significant example of the latter cybercrime comes from Wirth, A. 2018 who explained the devastating effect of the WannaCry ransomware on the National Health Service (NHS) in 2017. Specifically, WannaCry impacted 81 out of 236 hospital trusts and 597 out of 7 545 GP surgeries, which resulted in the cancellation of 20 000 appointments. It is perhaps cases like this one that prompted some reflection regarding the importance in distinguishing between traditional crime and cybercrime as there has been a tendency to label the adjunct cyber- as something 'sexy' rather than explanatory (Cross, C. 2019). I also uncovered that employees from within organisations were responsible for criminal behaviour albeit with a weak or non-existent financial motive. In this regard, previous research by Hutchings, A. and Collier, B. 2019 lists women as being responsible for 32% data breaches in the Police and 67% data breaches in the Health and public sector. Men were responsible for 66% of data breaches in the Police and 33% of data breaches in the Health and public sector. Whilst this analysis is insightful on the one hand, what is lacking in the research by Hutchings, A. and Collier, B. 2019 is the gender ratio in the Police and Health and public sector, which would allow for more precise conclusions. Instead, the authors supply that the Police participants were a total of 51 people, 13 people from health services and 11 from other public bodies. Additionally, men were responsible for 2% of malware attacks against the Police with the other 98% of attacks lacking a financial incentive. Both sexes were found to have committed no offences against their public sector employer, which would have had a clear monetary incentive (Hutchings, A. and Collier, B. 2019).

3.1.2 Policing

I grouped the various aspects of cybercrime policing in the UK using the following research themes: §3.1.2 Models, §3.1.2 Organisation, §3.1.2 Human resources and §3.1.2 Jurisprudence.

Models

Research by Hunton, P. 2011 has developed a model for cybercrime policing which contains eight stages. In Stage 1 the investigation of the offence is started and what is known about the cybercrime becomes established. During Stage 2 the cybercrime is modelled which also includes the technology that was used throughout the offence. During Stage 3 a specialist assessment of what is known takes place. The purpose of Stage 4 is risk assessment of the potential harms. Investigation planning takes place as a part of Stage 5. The activities in Stage 6 are focused on assessing how to handle the technological data to prevent the interference with evidence. Stage 7 is the carrying out of the intervention and Stage 8 is the reporting on the results.

Hunton, P. 2012 also identified five policing roles within the investigation framework. Here they are presented in an ascending order in terms of the expertise and risk requirements. Role 1 is the technical enquirer who can perform less sophisticated tasks as well as open-source searches. Role 2 is the network investigator, who covers networked technology. Role 3 is the forensic technician who can perform a range of expert skills including the retrieval of evidence. Role 4 is the digital forensic examiner who will be capable of conducting advanced analysis of the data including running experiments on it. The technical domain expert is role 5, which is an expert in a particular field of cybercrime.

The main strengths of Hunton, P. 2012's model are its functional specialisation and seemingly effective division of labour. Yet, it seems to me as if the model was based on a fixed hierarchical principle. This may be effective with traditional crime where the modus operandi evolves only very gradually over time and therefore radical shifts in tactics are rarer. With cybercrime however, a fixed hierarchical model can tempt team leaders to become rigid and constrained by the hierarchically organised roles. Cybercrime confers more opportunities for creativity than more traditional crimes and hence teams should operate on a flexible rather than a fixed principle. As a part of this flexible principle, even the most junior roles should have an opportunity to contribute to the investigation strategy.

Organisation

A major organisational challenge to policing cybercrime is that the police were not originally set-up for this kind of work. According to Wall, D.S. 2013 the police are navigating their activity in a sector that originally fell under the private sector, who used responsibilisation (§2.2) to shift cybersecurity onto the users thereby creating victims of cybercrime. The use of the term "responsibilisation" by Wall, D.S. 2013 is an adaptation from its original meaning. The original meaning denotes a shift of responsibility from the government towards the citizens. Take an example as a refresher of the canonical meaning: The local council refuses to invest in traffic lights, so that people learn to be more careful when crossing the road. The local council has made people responsible for road safety in a way that they were formerly responsible to avoid purchasing a new set of lights. In contrast, Wall, D.S. 2013 uses responsibilisation to signify a shift of responsibility from the commercial sector onto the consumer. This denotes a shift where corporations take on many of the roles previously filled by the government whilst developing the same techniques used by the latter.

In an example of the increasing controversy surrounding this merger, Johnson, D. et al. 2020 observed a trend whereby the police rely on the private sector to assist with cybercrime policing- an initiative promoted to the force. Yet, the members of the police were aware that private companies who receive potential access to data lacked the legal mandate to handle it.

Another organisational challenge comes from the Northeast of England, where the police have evaluated the effectiveness of local policing, which is supposed to be embedded within

the broader national framework such as with the National Crime Agency (NCA) (Doig, A. 2018). The researcher found that the force deals with frauds as well as DoS attacks and malware attacks, yet it does not have an established line of communication with NCA. From an organizational perspective the local police are left to their own devices when tackling the evolving challenges of cybercrime.

It is also worth noting examples from the literature which highlight the strengths of the police force in tackling cybercrime (Shan-A-Khuda, M. and Schreuders, Z.C. 2019). The researchers used statistical analysis to draw connections between demographics and cybercrime victimisation, which resulted in significant results. They found that victims of economic cybercrime were more likely to be male (56%) and from areas populated by full-time students and the Asian minority. The extent to which this a true reflection of the situation can be debated. I would argue that what is reported in the research is an under-representation of the problem. Instead, I would expect that the actual figures are considerably higher as suggested by the following research piece.

Herein, the under-reporting of cybercrime was seen as an important issue in policing research (Johnson, D. et al. 2020). The lack of effective reporting resulted in the police being unable to measure the extent of crime and compile robust statistics to assess the problem. Constructively, Horgan, S., Collier, B., et al. 2021 envisioned a way out of this conundrum by exploiting the negatives brought on by the COVID-19 pandemic. Examples of COVID-19 related negatives included a 72% increase in fraud 52% increase in other, predominantly narcotic offences, between the year 2019 and 2020 in Scotland. Specifically, they suggested that the links between the local police and communities provide a network that can work together to improve cybercrime reporting in a democratic way. These points will be further elaborated on in a separate section §3.3 RQ3.: What is known about cybercrime reporting to date?.

As a part of the organisational assets in policing cybercrime, the role of Action Fraud (AF), the UK National Fraud and Cybercrime Reporting Centre occupies an important place in the policing system that covers England, Wales and Northern Ireland, but not Scotland anymore. The role of AF is to serve as the nation's key centre for reporting economic cybercrime such as fraud. AF will not conduct enquiries into reports of other crimes such as thefts of vehicles, hate speech or suspicious behaviour towards a minor. As mentioned in the §1 Introduction in §1.3 Police Scotland, Police Scotland have separated from AF and therefore a separate procedure needs to be followed when people are victimised by fraud in Scotland. As a part of its reporting function, AF publishes monthly statistics about fraud and cybercrime data. These have served the important purpose of highlighting the dramatic spike in cybercrime against individuals during COVID-19 (Buil-Gil, D., Miro-Llinares, F., et al. 2021).

Lastly, it is worth considering some of the organisation's unique approaches to policing cybercrime such as 'influence policing' which is based around the idea that the digital footprint of at-risk Internet users is used to tailor deterrence ads that are meant to discourage the engagement in cybercrime. If this intervention fails, then on the next level at risk Internet users are approached by officers from the NCA in their homes who offer guidance on how to avoid criminality online (Collier, B., Thomas, D.R., Clayton, R., Hutchings, A., and Chua, Y.-T. 2021).

This approach raises some ethical questions, which I contrast with an analogy from the non-online domain. Imagine an 18 y.o. male whom I will refer to as "X." X goes to his local supermarket nearly every day to buy a single chocolate bar. Unbeknown to anyone apart from X, the protagonist has been tempted to shop lift. Therefore, his daily visits to the supermarket are actually a reconnaissance mission. He is not tempted by need or poverty. He is loved by his close ones both emotionally and materially. X simply has a nihilistic propensity towards boredom and risk taking behaviour. Ultimately, X's fear of reprisal takes over and he abandons

his intention. Yet, the supermarket keeps a log of visits, which it analyses to make inferences about customer behaviour. Security decides that X was acting suspiciously. Therefore, they warn him about what lays ahead for those who shop lift. How would we, as a society, feel about X being spoken to by security if he was well within his rights to behave in the way that he did?

From my perspective, a miss is as good as a mile and this applies to the use of influence policing as well. I do not believe that it is the role of the police to make assumptions about people's thoughts based on their online behaviour when it comes to economic cybercrime. Also, the act of being spoken to by the police may alienate X even further, which can then lead to an offending pathway. As someone who has worked in criminal mental health, I appreciate the elusive distinction between anti-social thoughts and actions. Why some people have thoughts of scamming and fraud, but never do, whilst others act to the contrary, remains, for lack of a better word, a mystery. The role of the police is not to disentangle this mystery, but to collect evidence of economic cybercrime post hoc.

The chances are that we will never know how many people planned to carry out a fraud, but at the last minute turned back and did not. In contrast, the thing that we find out about eventually, is approximately how many people were snooped on by the state via one of its extended arms to keep the rest of us safe. That ratio, defined as zero public knowledge about who chooses to be good when driven to be bad, versus thousands of people that can be placed under surveillance, is the essence of what could go wrong if the majority's safety is prioritised over the individual's freedom to think and act as he or she chooses.

Human resources

Some of the literature available on the subtopic is best understood as issues in HR. A candid piece by Sommer, P. 2017 says that what gets in the way of cybercrime policing can range from inter-agency competition to lack of resources to hire specialised staff. According to Sommer, P. 2017 people would struggle if taxes increased to fund additional cyber specialists.

Whilst citizens want to avoid higher taxes, the way their current taxes are redistributed should also be taken into account. It may not be the responsibility of the citizens to pay more tax if they want better policing, or the responsibility of the police to carry out a first class volume service on a tight budget. Rather, the government should consider how to redistribute taxes in a way that improves policing without increasing the economic burden on the citizen. Sommer, P. 2017 also states that companies who have been victimised by fraud should not blame the police for collapsed investigations if they have not collected the evidence of the crime precisely enough. Once again, this is an example of responsibilisation where the author automatically presumes that victims will proceed more pedantically in cases of cybercrime than they would if they were burgled. I cannot imagine a police officer telling off a burglary victim for accidentally interfering with a crime scene, so why is it acceptable in cases of economic cybercrime?

An integral part of HR is staff development and the London Met have rolled out the Ncalt training package, which is an online training to educate officers in how to deal with cybercrime. Critical research has revealed various caveats in how this training was harnessed (Forouzan, H., Jahankhani, H., and McCarthy, J. 2018). Most police officers from their study did not feel adequately trained to respond to cybercrime challenges and felt that the Ncalt training was not an effective way to upskill the workforce. About one third of the police officers were not even aware that the Ncalt package existed. The authors perplex over the fact that the London Met does not monitor the training uptake since it is the only training on the subject that is meant to be used by the entire force.

Problems with training are a theme that re-emerges in Forouzan, H., Jahankhani, H., and

McCarthy, J. 2018 and Schreuders, Z.C. et al. 2020 the former of which also identifies that HR problems stretch to recruitment and working across agencies. Interestingly, Loveday, B. 2018 supplies an example where a local police force boosted its expertise by hiring a former hacker as a staff manager and resolving staff shortages by engaging with qualified volunteer groups. Apart from such innovative HR solutions, since 2003 the problem of cyber fraud was also policed by vigilantes who congregated on forums of concerned citizens and publicly shamed people whom they assumed to be committing fraud (Button, M. and Whittaker, J. 2021).

More optimistic evidence has emerged, which found that constables did engage in some level of cybercrime training and this increased their feelings of preparedness and competence when responding to cyber frauds (Bossler, A.M. et al. 2020). Nevertheless, these successes seem to be localised as time and time again in other research a lack of training, knowledge, resources, and improper cybercrime recording come up as obstacles in the way of effective policing (Buil-Gil, D. and Zeng, Y. 2021). The paper by Cockroft, T. et al. 2021 sheds light on the issues with the training in policing cybercrime. The latter authors have found that training that is delivered face-to-face as opposed to online is viewed as more effective by the force. The evidence from within the research suggests that the effectiveness was actual rather merely perceived. This conclusion can be drawn based on the thematic analysis, which showed that 58.77% of the attendees appreciated clarification as the most important component of face-to-face learning. When evaluating online training, 33.5% stated that they liked the flexibility, but 28.31% said that online training was superficial. Hence, the conclusion that face-to-face training is more effective seems justified although more detailed information about the content of online training would be helpful.

In terms of the macro level in HR, previous research has found that police forces would benefit from clear policies and procedures when responding to cybercrime as a form of best practices approach (Bossler, A.M. et al. 2020). The difficulty with this, according to Johnson, D. et al. 2020, is that the English system is highly decentralised and therefore there is a lack of consensus as to who should have the final say over what best practices in cybercrime policing should look like. This approach has some pros and cons. The pros of decentralisation are that different approaches can be trialled in different regions to see what works best. The cons of decentralisation are that if regions do not communicate effectively, then important lessons get missed.

The last piece that fits within the HR section is from Wilson-Kovacs, D. 2021 who explored the new role of 'Digital Media Investigator' (DMI) in England and Wales. The DMIs were created by upskilling police officers to use technology to relieve the specialised teams from the more unsophisticated tasks. Whilst the idea was seen as pioneering by some, issues concerning the role content were raised by others. Specifically, the lack of rigorous recruitment, the lack of support to sustain digital skills, the lack of supervisors' cyber awareness and tensions between DMIs and accredited forensic specialists were all critiqued.

Jurisprudence

In Sampson, F. 2014, the author argues that current legal approaches focus on conceptualising the systems of crime but struggle to catch up with individual offenders, hence what might be required are dedicated police constables that will patrol the cyber area in a similar fashion as they do physical spaces. In the online domain, this would require dedicated offices that are populated with people that can use specialised software to monitor behaviours on the most prominent chat forums and domains. There are however various unanswered questions in regards to this approach. For example, would the constables identify themselves via a username so that they could be approached by the chat users? Even if they did identify themselves via a username, would it be possible to effectively safeguard the identifiers of police constables

from impersonation? These questions were not answered in the article, but are key for the implementation of police constables online.

Furthermore, the current legal approaches can also create various pitfalls for policing cybercrime, which can have unintended negative consequences for the police (Lyle, A. 2016). Examples of pitfalls include using a fake social media profile to access information on social media, which is an offence under the Computer Misuse Act 1990 or the seizure of a family PC for investigation purposes, which can violate the privacy rights of the rest of the family. To minimise the risk of this happening, Lyle, A. 2016 articulated six rules as guidance. Firstly, the police must apply the correct legislation to specific offences rather than a one-size fits all approach. Secondly, caution is urged when carrying out open-source investigations because different laws apply when this information is used by the police as opposed to the regular person. Thirdly, open-source investigations may conflict with privacy rights, which is why the justification must be rigorously established beforehand. Fourthly, the collection and storage of data needs to comply with relevant legislation whereby the data protection principles have the overriding power. Fifthly, the taking, analysis and display of evidence must be highly regulated in an evidenced way. Sixthly, all such activity must be appropriately recorded so that it can be scrutinised in the interest of transparency.

Additionally, specific national differences in legal definitions impact not just on the how but also if an offence will be investigated by the police and subsequently prosecuted in court. Take for example the problem of organised cybercrime (Leukfeldt, E.R., Lavorgna, A., and Kleemans, E.R. 2017). Imagine an organised cybercrime group of three individuals who coordinate an attack on bank customers. Investigating these individuals as an organised crime group in the UK would not be possible unless their offence was punishable with at least seven years in prison because the organised crime laws would not apply to them. Therefore, the police must remain extremely careful in how they bring forward charges because an organised group of cybercriminals in the UK may not legally constitute a form of organised crime. Moreover, a careless delegation of public resources towards a fight against organised crime caused by a moral panic would result in an unnecessary dent in the state's budget (Lavorgna, A. 2019).

The last article concerned the effects of Brexit on jurisprudence in cybercrime (Stevens, T. and O'Brein, K. 2019). Among the various concerns of Stevens, T. and O'Brein, K. 2019 were that Brexit will affect UK's capabilities in terms of policing and sentencing cybercrime. The former will be affected by the loosening of ties with Europol and the latter will come into effect as a result of severing ties with the European court system. The authors highlight that the UK alongside Germany is the highest contributor to cybercrime intelligence in Europol. Whilst the UK is not exiting the security alliances associated with the EU, its position within them will change as a result of Brexit. The question remains how this will effect the vulnerable users of technology regardless of what they voted for in Brexit? In my view, the reconfiguration of cybersecurity ties with the EU is likely to increase cybersecurity threats to the UK and the EU during the implementation phase of the transition.

3.2 RQ2.: What is known about cybercrime victims in the UK to date?

It is important to have an understanding of what is known about cybercrime victims in the UK to date because understanding victims needs will help tailor solutions that can be harnessed to improve cybercrime reporting in Scotland.

The following subsection is thematically organised as follows: §3.2.1 Victim profiles and

§3.2.2 Victim experiences.

3.2.1 Victim profiles

I will dedicate this subheading to compiling the characteristics of the various victim profiles. Due to our evolving understanding of cybercrime victims, we currently define victims based on a very limited number of characteristics, for example as individuals or private sector institutions. In contrast, we tend to attribute many characteristics to victims, particularly individuals, in traditional crime. For example, in the latter type of crime, society stresses that a victim was "a loving mother", "a passionate and bubbly teen" or "a reliable and quirky grandad." I want to use this section to emphasise the humanity of cybercrime victims and put them at the centre of this subheading, which will be organised using the following themes: §3.2.1 From elites to the masses, §3.2.1 Routine Activity Theory (RAT), §3.2.1 Psychological perspective and §3.2.1 Correlation with age.

From elites to the masses

I feel that it is fitting of the world we are living in to commence this review by a high profile case. It takes a high profile victim to bring attention to the adversity affecting the masses. Specifically, in 2008, the shadow home secretary David Davis, criticised the UK government for being ineffective in tackling cybercrime after he became a victim of it himself (Hunter, P. 2008). The situation in 2008 bears some resemblance to the present situation. Then, cybercrime reporting was also a problem with Hunter, P. 2008 critiquing the lack of a dedicated centre for tackling cybercrime and the police's tendency to investigate only high value crimes. Things have since changed. The centre of cybercrime reporting was established under the name Action Fraud. However, the problem with investigating only high value offences persists. The difference being that Hunter, P. 2008 complained that only offences above £500 are investigated by the police. In 2019 that figure has increased to offences above £100 000 (Correia, S.G. 2019). The rhetorical question withstands the test of time: "Who are the current cybercrime reporting mechanisms really serving if not those that can afford to police themselves?"

The literature in connection to victims' profiles was also centred around the quantitative aspects of what it meant to be a victim in terms of defence costs (Bohme, R. 2013). In other words, the victims were defined in terms of what happened to them (e.g. the type of fraud they succumbed to) and how much it cost in pounds. Speaking of the victims' distress, the authors argued, is a practical matter that will be discounted because victims cannot sue for distress and hence it cannot be meaningfully connected to remuneration. I agree with Bohme, R. 2013 that it is difficult to put a price tag on distress. Yet, what victims go through tells us a lot about who they are as people. Discounting phenomenology means diminishing the victims' profile and humanity. Not only is this a problem from an ethical standpoint, but also because without accurate victims' profiles it is difficult to devise strategies to engage with victims in a way that would improve cybercrime reporting.

In their piece Bana, A. and Hertzberg, D. 2015 started by highlighting that between 2012 and 2014 a survey into the UK's top law firms showed that the importance they placed on cybersecurity doubled from 23% to 46%. This increase may have been influenced by an attack on ACS:Law, a prominent UK law firm, in 2010. The hacker group Anonymous attacked the firm based on knowledge that they were defending people accused of accessing illegal pornography, which resulted in the clients' confidential e-mails being made public. The law firm received a fine of £1000 reduced from £20 000 after it declared bankruptcy. This article is more informative about victim profiles than meets the eye. In chronological order, the first

victims were the lawyers who were paid for upholding the law. The second victims of the crime were the clients of the law firm who were vulnerable because the state has accused them of committing a crime and hence they were in a vulnerable position because their liberties and reputation were under threat. Thirdly, and these are the victims Anonymous have ignored, are any victims of molestation by proxy contained within illegal pornography. The latter are not molested once but every time when such a medium is viewed for sexual gratification. The only retribution for these victims is the chance that the creators and consumers of such media will be brought to justice. If, however, the right to a fair trail is compromised by publicising confidential information pertaining to the accused, the entire trial can collapse. Conclusively, what started as an attempt to punish elite lawyers may have easily resulted in damaging vulnerable victims of online molestation.

Routine Activity Theory (RAT)

In an attempt to compile an accurate victim profile, the research by Nasi, M. et al. 2015 is helpful. The researchers discussed the RAT which stands for Routine Activity Theory. The core assumption of the theory could be summarised as follows, people who behave less than safely online by opening links from unknown e-mail addresses and having insecure passwords such as "12345" are more likely to become victims of crime than those who avoid opening links from unknown e-mail addresses and who use complex passwords such as "Xde9Fq14."

In the study by Nasi, M. et al. 2015 the authors surveyed 999 respondents from the UK and matched their data with the assumptions from RAT. They found that being male, young, migrant, urban, not living with parents, unemployed with more social life online versus offline were all predictors of becoming a victim of cybercrime such as slander and violent threats. Economic cybercrime was represented as well, specifically 28% of respondents have become victims of fraud and a further 23% were victims of identity theft.

When using the RAT, caution should be exercised when discussing victim profiles so that the rhetoric does not slide into victim-blaming. For example, Waldrop, M.M. 2016 uses the example of GCHQ to highlight, what I will refer to as, a person-centred strategy to cybersecurity. GCHQ advised its managers to be thoughtful when requiring the workforce to constantly update their passwords to prevent exhaustion. In this respect, when talking about victim profiles, I want to re-emphasise that it is important to strike a balance between security and freedom. Anybody can become a victim regardless of how secure their passwords are. If people are going dedicate too much time to securing their computers, then that will interfere not only with their ability to work, but ultimately to live a meaningful risk tolerant life.

Remaining with the RAT, subsequent research discussed the unexpected dip in the amount of victims from the private sector despite the increased amount of attacks (CFS 2018). Small and medium sized companies (SMEs) that invested in cybersecurity experienced a marked decrease in harm during 2017, a year throughout which there was an increase in cybercrime attacks. The specific figures are interesting for illustrating how victims can effectively increase their locus of control by going down this route. In particular it was found that the amount of companies using a network perimeter firewall went up from 54% in 2016 to 75% in 2017. Additionally, the amount of companies enforcing cybersecurity policies went up from 26% to 51% from 2016 to 2017. Lastly, the sum of businesses with cyber-insurance went up double the amount resulting in 38% for small sized companies and 54% for medium sized ones. This is evidence that RAT holds water in the private sector so long as companies invest in their own cybersecurity.

A question worth asking with respect to the findings by CFS 2018 is: What is it about the victim profiles of SMEs that made them such desirable targets in 2017? The findings by Donegan, M. 2019 state that SMEs are specifically profiled by cybercriminals due to having

several vulnerabilities. Firstly, they often communicate payment correspondence via e-mails. Secondly, SMEs use of systems such as Office365 is another source of vulnerability. Thirdly, often SMEs have publicly available information on the web that pertains to information about staff. Cybercriminals will compile this information to inform their deception strategy.

Further support for RAT can be gathered from the results of Akdemir, N. and Lawless, C.J. 2020 who found that victims' online lifestyles were connected to the threat of cyber victimisation, which included the use of insecure Internet connections and public access computers. The risk of becoming a phishing victim was increased in people who both voluntarily and involuntarily shared personal information through social networking sites and online advertisement sites. Lastly, illegal activities such as downloading pirated media and streaming via illegitimate sites also increased the likelihood of becoming a cybercrime victim.

To conclude on the subject of RAT, Buil-Gil, D., Miro-Llinares, F., et al. 2021 examined the effect of COVID-19 on increased victimisation. It was found that people spend more time online and less time on the street, which resulted in a decrease of street violence and increase in cybercrime. Therefore, the COVID-19 pandemic created a novel set of circumstances that played into the core assumptions of the RAT theory, but also placed it into the online domain.

Psychological perspective

Next, I will analyse the research with the use of a psychological perspective to victims' profiles. In research by Jones, H.S. et al. 2019 the authors measured several psychological constructs to identify the hallmarks of a profile most susceptible to economic cybercrime. They found that people who were able to proceed with cognitive reflection (i.e. suppress incorrect information versus correct information) were moderately less prone to opening fraudulent e-mails. Additionally, people who scored high on sensation seeking were more inclined to give into automatic processes and open fraudulent e-mails. The authors have also argued that sensation seeking might be mediated by impulsivity, which triggered the erroneous responses.

Another route into the psyche of the cybercrime victims can be taken with the use of Rational choice theory (RCT) (Connolly, A.Y. and Borrison, H. 2020). The latter scientists examined the trade-offs in victims' decision making processes when deciding whether or not to pay off a ransomware attacker. Connolly, A.Y. and Borrison, H. 2020 found a rational basis for victims' decision making processes which they summed up in the following way. The first cluster of victims that paid ransom usually had ineffective backups, the data was critical to the business, there was a real risk of bankruptcy and they followed the advice of the IT consultant. The second cluster of victims that did not pay the ransom had effective backups, the data was not critical to the business, the police advised against paying the ransom, they found the perpetuation of crime unethical and the negotiations with the cybercriminal broke down.

In my opinion, this pattern of results is interesting because it can be interpreted as attesting to various rationalisations. For example, the survival motive was prominent in the first cluster, whereas this motive was absent in the second cluster. Hence, I would speculate that the moral reasoning behind refusing to perpetuate crime stemmed from the staff's basic survival needs being met despite being victimised.

The study by Connolly, A.Y. and Borrison, H. 2020 was followed up by research examining the impact of attacks on organisations (Connolly, A.Y., Wall, D.S., et al. 2020). The latter authors corroborated the findings from the previous article by finding the private institutions suffer much greater harm than public institutions and this was not only due to the former facing greater redundancies, but also because public institutions invested more in security. I would critique this side of the argument because I find its assumptions narrow. Whilst, yes, a public institution is going to carry on regardless of the size of the attack, what about the population its meant to be serving? I would have welcomed an emphasis on the suffering of those affected

by the lack of service during a ransomware attack on a public institution. Moreover, Connolly, A.Y., Wall, D.S., et al. 2020 found that made-to-measure attacks were more severe than generic ones based on the utilisation of background information about the victim's profile.

I feel it is suitable to round up with a qualitative psychological study that entails victims' phenomenological perspective. Indeed, the research by Button, M., Blackbourn, D., et al. 2021 uncovered evidence of both psychological and psychosomatic effects of becoming victimised. It was found that people experienced, headaches, flare ups of existing conditions such a fybromyalgia and Crohn's disease, withdrawal from relationships, isolation, depression, anxiety, and suicidality. People with existing mental health conditions reported a resurgence of difficulties. As can be seen from this information, the distress of the victims is profound. In some cases, unlike in the conclusions by Bohme, R. 2013, victims' adversity contains a measurable component such as a resurgence of an existing condition post-victimisation. Take for example the effect of victimisation on mental health. Changes in mental health can be empirically measured in a range of ways starting with psychometric questionnaires. If the expert witness willed it, psychometric questionnaires can contain concealed malingering questions to assess for instrumentality in responses. Broadly speaking, malingering questions are deliberately easy questions that the interviewee will definitely be able to answer. Malingering questions are used to assess insufficient effort or dishonesty. A less robust, but admissible way to measure changes in mental health can be via keeping a diary and recording changes in sleeping patterns to name but a few measures available to the general public. Justifiably, real measurable harm that can be proven through court is taking place.

Correlation with age

An important characteristic to consider during the compilation of victims' profiles is age and its effects. Thus, Correia, S.G. 2020 examined the demographics of repeat victims of economic cybercrime in the UK. The researcher found that in cases where repeat victimisation has occurred, more incidents were reported by men rather than women. An average repeat victim was older than an average single case victim. Both the median and the mean ages are higher for the repeat (median is 57, mean is 53.6) versus single case victims (median is 50, mean is 49.93). The advantage of this research is that it can be used to direct preventative resources more effectively. I would argue that these statistically significant findings are of a nuanced nature where both groups, that is repeat victims versus single case victims, are essentially people in their fifties. In my opinion, setting up an effective economic cybercrime reporting system is key before we move on to more nuanced differences within the victim groups.

Age was argued to play a significant correlation with respect to romance fraud during the COVID-19 pandemic (Buil-Gil, D. and Zeng, Y. 2021). An opposite pattern relative to the previous piece by Correia, S.G. 2020 was found. Mainly, younger people versus older people were more susceptible to romance fraud as a result of loneliness and isolation, which was reflected in their increased use of the Internet. The use of Internet for communication was the highest for the over 16s and then gradually toned down across the groups until reaching a minimum in the over 70s.

3.2.2 Victim experiences

In this section I will make an extrapolation from research on the Western population (i.e. Europe, USA and Australia) onto the UK and hence Scottish population due to there being an insufficiency of research from the UK. This section will be subdivided according to the geographical jurisdictions from which the respective research originates: §3.2.2 European Union,

§3.2.2 Australia and Canada, §3.2.2 United States of America and §3.2.2 International collaboration.

European Union

At the beginning of this section, I will supply an overview of cybercrime in the European Union since 2010 based on previous research that surfaced via the systematic analysis (Reep-van den Bergh, C.M.M. and Junger, M. 2018). In regards to economic cybercrime in the European Union it was found that online shopping fraud affected between 0.6–4% people annually. In comparison, online banking fraud was found to be less common at around 1–2%. Moreover, less than 1% of the population were victimised via advance fee fraud or identity fraud. Britain being in the EU at this point was also included in the research with the finding that 0.5% Brits were victims of an "Online Romance Scam." To complement these figures, the research by Huaman, N. et al. 2021 into Germany's SMEs found that 45.1% of interviewed employees reported that their SME had to respond to at least one cyber attack. Additionally, more than 50% (i.e., 1 842) were attacked on multiple occasions.

Bohme, R. and Moore, T. 2012 wrote an intriguing article concerning the experiences of people in the EU who have either been victimised by cybercrime or have heard about the threat of it. Bohme, R. and Moore, T. 2012 found that in people who have been victimised there was a 4–5% decrease in shopping and banking online. Moreover, people who have been exposed to information about the threats of cybercrime were twice as likely to diminish their online activity in comparison to those directly victimised. What I find interesting is that anticipatory anxiety is a stronger behavioural modifier than a crime actually occurring. This matters because anticipatory anxiety is not necessarily protective from economic cybercrime unless a person were to completely abstain from the Internet. Rather than suffering from anticipatory anxiety, the state should split the responsibility with its citizens. On the one hand, people should be supplied with easy to understand guidance on how to use the Internet. On the other hand, the state, banks and all of those that can really afford it, should make the Internet a safer place for all of those who cannot. This type of information could be imparted via regular state-sponsored awareness raising campaigns.

Another perspective considering Dutch victims' experiences is found in a study by (Van De Weijer, S.G.A. and Leukfeldt, E.R. 2017). This study examines how "The Big Five Model" of personality influences people's susceptibility to becoming victims of cybercrime. The aforementioned model is a contemporary and empirical model of personality, which presumes that every personality can be conceptualised with five factors, which are: Openness (to experience), Agreeableness, Neuroticism, Conscientiousness and Extraversion. The main idea is that every personality has all these traits to some degree, but the extent to which the traits are expressed defines the characteristics of the personality. Based on the results of Van De Weijer, S.G.A. and Leukfeldt, E.R. 2017 the authors concluded that people high on Neuroticism, low on Conscientiousness and high on Openness (to experience) were likelier to become victims of cybercrime. Whilst the research offers an interesting insight into the phenomenological experience of victims, clearer causal links between particular personality facets and types of cyber-victimisation would have been beneficial to avoid making assumptions about people based on their personality make-up. Another critique is that future studies should also entail the concept of self-awareness into their design. Whilst someone can be very open to experience and very low in conscientiousness, they may also be aware of these traits, which can result in making safer choices.

When discussing victims' experiences it makes logical sense to connect these with their needs as was done by Leukfeldt, E.R., Notte, R.J., and Malsch, M. 2020 on a diverse sample of Dutch victims. They evidenced that victims of economic cybercrime have pronounced

emotional needs, which revolve around receiving recognition from society and the police for their ordeal, which is linked to being able to tell their story. Fraud victims in particular have a need to remain informed about the court proceedings with all victims citing retribution as an important need. Victims also need to receive detailed information from the police about the processes that are triggered by their report. Then, victims also experience a range of practical needs that relate to requirements to liaise with banks, social media platforms, etc. to mitigate the effects of the crime. Understandably, financial needs are particularly high among victims of fraud, which can culminate into the endangerment of primary needs. Leukfeldt, E.R., Notte, R.J., and Malsch, M. 2020 described an example of a woman who lost all of her saving to dating fraud and could not afford to stay in her house and hence had to move in with her social circle to avoid homelessness.

How the victims' experience the crime also plays into whether they decide to report it or not. In particular, Van de Weijer, S., Leukfeldt, R., and Van der Zee, S. 2020a found that the type of cybercrime influences Dutch victims' motivation to report. Victims of various forms of economical cybercrime (e.g., fraud, romance scams etc.) were more likely to report the incident to the police, especially if they incurred some type of financial loss. This effect was more pronounced in serious versus less serious offences.

Australia and Canada

Despite the geographical distance between Australia and Canada, they have been collapsed in this section due to a significant piece of research included within that has been concurrently run in both countries.

The effectiveness of the calculative trust marker in phishing was explored by the subsequent piece (Lacey, D., Salmon, P., and Glancy, P. 2015). Using the example of a phisher impersonating Australia's post, the authors show how victims are misled into experiencing trust in forced choice paradigms. For instance, the phisher will force the victim to click on a link impersonating Australia's post because the link will purport to provide more information about a parcel, which will otherwise not be delivered. The victim is then drawn to believe that by clicking on the link they will merely receive additional information, which becomes the access point for the phisher. Hence, the experience of trust is an important antecedent to become a victim of phishing.

The next article by Cross, C. and Kelly, M. 2016 is an interesting example of the disassociation that victims experience between warnings regarding cybercrime and their experience of it. It was found that educating people about the specific types of cyberfraud was an ineffective protection strategy mainly because the recipients struggled to apply the messages into their lives. Citing examples of Ruth and Hazel, the researchers uncovered that in the first instance Ruth sent sums of money oversees to a person she thought she was in a relationship with despite knowing about romance fraud. The emotions Ruth invested in this pseudo-relationship stopped her from making the connection between what she knew about romance fraud and her specific situation. In the case of Hazel, she knew about investment fraud. Nevertheless, when she was approached by a scammer who disguised the crime as a contracted business opportunity, Hazel did not apply her knowledge of investment fraud to her situation and ended up loosing £300 000. Cross, C. and Kelly, M. 2016 advise that people should not be overloaded with information during awareness raising campaigns. Instead they should receive two key messages: First, do not share your details with anyone online. Second, never transfer money to anyone you met online. I agree with the general gist of Cross, C. and Kelly, M. 2016's advice because it takes into account people's preference to enjoy online communication, be it romantic or otherwise, whilst supporting them to do it safely.

Moving to a study of victims' experiences of reporting cybercrime to the Australian author-

ities, Cross, C. 2018 identified that people's experiences were often influenced by unrealistic expectations. The author referenced the "Merry-Go-Round effect" when victims approach an agency for assistance with fraud. Victims in this situation experience being referred from one agency onto the next one without getting any closure about what they have been through. Victims also experience confusion with respect to how the jurisdiction of the crime is assigned to the police jurisdiction. Victims do not realise that police forces with broad competencies, such as the Australian Federal Police in this instance, cannot investigate international fraud. As well as experiencing significant trauma, the victims often overestimated the force's information sharing capabilities expecting that their reports will quickly be sent to the correct addressee. Lastly, victims in Australia experienced what Cross, C. 2018 coined the "CSI" effect based on the popular TV show. This refers to the victims' expectations that the police have far greater technological and investigatory powers than is really the case.

Weighing against each other students' experiences of cybercrime victimisation versus knowledge of cybercrime and demographics Abdulai, M.A. 2020 examined a sample of 462 students to compare fear of credit card fraud. According to Abdulai, M.A. 2020, demographics have no effect on the amount of fear a person experiences in anticipation of a crime. The author takes this as evidence for the assumption that everybody is fearful of cybercrime in a similar way. Whilst one can, to some extent, control safety in the physical world (i.e., live in a better neighbourhood with burglar alarms), one finds it much harder to gain the same sense of safety in a world that is governed by online principles. Moreover, Abdulai, M.A. 2020 found that, understandably, this effect was more pronounced in people who were victimised by cybercrime.

The pattern of result from a study by Cross, C., Holt, T., et al. 2021 added to the generalisability of people's erroneous perception that they can effectively protect themselves against economic cybercrime. Cross, C., Holt, T., et al. 2021 found that communities perceived their risk of victimisation as low whilst at the same time most have reported being victimised by some form of cybercrime. The police, who were a control group, stated that they perceived people's ability to safeguard themselves as low, whereas the community members experienced high confidence to stay safe online. Hence, this is evidence of the type of disassociation that is present in other studies where people's perceptions of themselves differ from the evidence supplied by reality.

United States of America

A study from the USA on international students who were targeted by phone scams and Craigslist scams revealed some important components of the victims' experiences, in particular how a victim's lack of relevant knowledge can be used against them (Bidgoli, M. and Grossklags, J. 2017). On the one hand the majority of international students did not feel targeted because of their background. On the other hand, the participants felt targeted by the phone scams because the latter was connected to their immigration status in a threatening manner. Due to their lack of experiences with the FBI and the IRS, the students did not know that the agencies would not phone people to threaten them. In hindsight, the participants acknowledged that whilst they did not feel specifically targeted, being an international student put them in a vulnerable position. In my opinion this is a valuable piece of research because it goes some way to show that particularly vulnerable groups do not see themselves in that light, which can increase their vulnerability. There also seems to be some conceptual overlap with the findings by Cross, C. and Kelly, M. 2016 who also stated that the victims did not feel vulnerable albeit with a different argument in mind.

International collaboration

The last piece of research that will conclude the section on victim experiences is the result of an international collaboration between the U.S.A., Germany, Canada and UK. It is fitting of the subject matter that this piece by Monteith, S. et al. 2021 concerns the connection between victims' experiences and psychiatry because mental health is likely to be affected by economic cybercrime. Starting from the beginning Monteith, S. et al. 2021 found that the the COVID-19 pandemic caused a change in how people socially interact for professional, educational, health, financial and personal reasons. These changes interact with people's mental health in two cardinal ways. Firstly, even otherwise mentally unaffected individuals may slide into mental illness as a result of falling victim to cybercrime. This can be the result of anything from suffering dire financial consequences post-victimisation to not being able to effectively grieve after the loss of a romantic relationship with the cybercriminal. Secondly, people with pre-existing mental health conditions are particularly vulnerable to economic cybercrime. For instance, people with emotional instability can engage in risky behaviours but also people of an older age can become more vulnerable as their short term memory and cognitive abilities become affected. Taken together, the COVID-19 pandemic presented new risk factors for developing a mental illness as a result of cybercrime victimisation as well as an increase in risky behaviours by people with pre-existing psychiatric conditions.

3.3 RQ3.: What is known about cybercrime reporting to date?

It is important to understand and conceptualise cybercrime reporting approaches because that can help prioritise human vs. technological solutions to improving cybercrime reporting. For example, if people prefer to report to other people vs. machines, then solutions favouring a human component should be prioritised.

The following subsection is thematically organised as follows: §3.3.1 Cybercrime reporting approaches and §3.3.2 Cybercrime reporting results.

3.3.1 Cybercrime reporting approaches

The literature on this subsection is best grouped according to three classifications, which denote distinct approaches to reporting. The Human To Human (H2H) approach refers to traditional forms of reporting which are based on interactions between human actors. Human To Machine (H2M) approach relates to those forms of reporting and interventions where a human navigates a computer to report cybercrime. Machine To Machine (M2M) approach relates to automated interventions for improving cybercrime reporting and analysis.

Based on my knowledge, this taxonomy is entirely original and if it became established, then it would make a functional contribution to systematic analysis.

Being able to use abbreviations such as "H2H" in their keyword search would transport social psychologists to research, which is related to the interpersonal aspects of cybercrime reporting. In contrast, an IT engineer seeking to secure a system against breaches will key in "H2M" or "M2M" to focus on the intersection between human to machine, or machine to machine respectively.

Human To Human (H2H)

To begin this subsection, the research by Bidgoli, M., Knijnenburg, B.P., and Grossklags, J. 2016 serves as a series of explanatory case studies of how some of their participants reported economic cybercrime using the H2H approach. For example, one victim reported online shopping fraud to their bank in order to cancel their card, but also to Abercrombie & Fitch because the fraudulent website was mimicking the designer brand. A victim from another case study reported the computer virus to Dell customer service. Yet, none of Bidgoli, M., Knijnenburg, B.P., and Grossklags, J. 2016's participants reported the crime to the police.

As I highlighted in the previous subsections, §3.1.2 Organisation, §3.1.2 Jurisprudence, and responsibilisation (§2.2) resulted in changes to societal expectations as to who is responsible for making the Internet a safe space, which is free from economic cybercrime. In an interesting article by Jhaveri, M.H. et al. 2017 the authors put forward a framework for understanding the voluntary response to economic cybercrime. By using the phrase "voluntary response" I am referring to the reporting and resolving of cybercrime in an predominantly H2H manner amongst actors from private institutions. The incentives for participation are the protection of the brand and service reputation. It was argued in the article that the protection from disrepute outweighs the direct financial losses. Moreover, the private institutions participate willingly in sharing information about attacks among other firms because they receive intelligence about how their counterparts were attacked. Taken together, economic cybercrime has created solidarity among private sector institutions who were able to put competitive advantage to the side and assist each other with self-policing this toxic phenomenon.

H2H poses novel demands on the reporting infrastructure, which is accustomed to accepting complaints about traditional crime. Take Cross, C. 2020a and the problems of jurisdiction that victims and police have to face. As pointed out by the researcher herself, a criminal from country A can target a victim in country B by getting them to wire finances to country C. In what jurisdiction has the crime taken place? As a result victims who report cybercrime often have misconceptions about the various policing bodies in Australia. In order to mitigate this, The Australian Cybercrime Online Reporting Network (ACORN) was established in 2014 as centre for processing the aforementioned complaints. Yet, Cross, C. 2020a concludes by saying that greater transparency is needed about how ACORN processes individual reports as well as more awareness raising about the competencies and limitations of various police forces.

In a similar vein, Popham, J. et al. 2020 explored the extent to which economic cybercrime was reported by police based on complaints that they received from the public. The research found considerable variations in police reported cybercrime across Canada's jurisdictions with under-reporting being the overarching theme. One reason for this can be legislative. The authors argued that cyberlegislation is just traditional criminal law, which has received a jargon revamp whilst resting on unchanged principles. They argue that this causes problems for reporting due to the constantly evolving field of economic cybercrime. The latter cite an exception to the rule taken from a manual by the Canadian Centre for Justice statistics, which states that: "any fraud that involves the unauthorised use of a computer or use of a computer for illegal means" constitutes the basis for cybercrime reporting. Moreover, a dismissive viewpoint of cybercrime reporting was also considered as a source of variation.

Using a hypothetical and simulated setup, Van de Weijer, S., Leukfeldt, R., and Van der Zee, S. 2020b presented 595 participants with vignettes about cybercrime to explore who they would report to predominantly. Several interesting patterns of responses surfaced as a result. Within I will be concerned with just those connected to economic cybercrime. In all cases of economic cybercrime (i.e., malware, ransomware, phishing, online consumer fraud, online dating fraud) people were more likely to report the offence to an organisation other than the police. The exception being identity theft where people were equally likely to report the of-

fence to the police and another organisation. The distinction at hand is especially obvious in the case of phishing where 49.7% respondents would rather report to an organisation other than the police and only 9.4% would report to the police. Online consumer fraud, which is one of the most common economic cybercrimes, would get reported 36.7% to another organisation and 25.6% to the police. Van de Weijer, S., Leukfeldt, R., and Van der Zee, S. 2020b conclude that the take home message for the police is to strike up more effective multi-agency cooperation to increase people's reporting to the police.

In stark contrast to the hypothetical setup by Van de Weijer, S., Leukfeldt, R., and Van der Zee, S. 2020b the study by Yadav, H. et al. 2021 is based on a real world case study. The study is interesting because it illustrates the grey area when talking about cybercrime in a strictly economical sense. In fact, I prefer to think of crime as form of anti-social relationship between people where one party or multiple parties incur some form of harm. Yadav, H. et al. 2021 talked about the case of a cyberstalker who owned an art gallery in Los Angeles. The offender created abusive websites to target various actors in the business and managed to extort over $3 000 000 from his victims. Eventually, the cyberstalker was apprehended and sentenced to 60 months behind bars. This study is powerful because it uses a story to convey its point. It also contains an important weakness, which is the lack of specific details about the processes of reporting and investigation, which would allow me to align it with the systems under debate.

Sitting somewhere in between studies about H2H and H2M is a piece from Saudi Arabia by Alzubaidi, A. 2021, who touched upon reporting cybercrime among nationals. Based on the research findings, in a sample of 1230 respondents, 267 (21.7%) were victimised. From this percentage only 78 (29.2%) reported the offence to an agency. Alzubaidi, A. 2021 found that 31% would not know whom to report to, but would ask their friends, 15% would use the Saudi government e-portal and only 7% would report to the police directly. These data can be taken to mean that much like elsewhere in the world, people are confused about who to report to. Nevertheless, government's oversight in Saudi Arabia is more pronounced as a portion of the participants would report directly to its portal. Yet, as has been the case in previous research, people were not particularly likely to associate cybercrime victimisation with police reporting.

Human To Machine (H2M)

Heinonen, J.A., Holt, T.J., and Wilson, J.M. 2012 described the reporting to the U.S. Internet Crime Complaint Center (IC3). The IC3 receives complaints via its online interface from the public, but also other organisations such as PayPal for example. The IC3 also maintains a presence on the websites of the FBI and the National White Collar Crime Center (NW3C). The IC3 holds its own academic and industrial conferences but also engages with local communities and senior citizens to warn them about economic cybercrime. In addition, a diversified critique of IC3 was supplied by Bidgoli, M. and Grossklags, J. 2016 who highlighted the system's main strengths and weaknesses. The main strength is that it provides helpful advice and tips on how people should protect themselves online so that they do not fall into a trap and become victims of economic cybercrime. The main weakness is that the IC3's work is insufficiently publicised so people do not have as much access to the information as they would require. Also, Bidgoli, M. and Grossklags, J. 2016 argue that the IC3 is a federal platform, whereas a substantial amount of cybercrime is localised. Hence, reporting channels that serve particular communities would be better equipped to respond to the localised nature of economic cybercrime.

In a paper by Bidgoli, M., Knijnenburg, B.P., Grossklags, J., and Wardman, B. 2019 the authors streamlined a procedure for reporting cybercrime in the PayPal service. The outcome of their study was a reporting interface that was user-friendly for the lay person from the

street. Apart from the latter, the interface achieved two important goals. Firstly, it effectively connected reports within PayPal and outwith PayPal with the relevant entities. Secondly, the interface raised awareness of cybercrime among the company's customers. The model itself was tested using 523 Amazon Mechanical Turks who offered positive feedback. The interface was structured around three key criteria. The first criterion was that it had to match the real world, which meant that the creators defined relevant jargon (e.g., phishing) and used lay language wherever possible. The second criterion was higher user freedom and control, which was programmed into the system by allowing users to undo any mistakes by pressing the "Back" button at the bottom of the page. The third criterion was minimalism, which meant that the authors included only the minimum amount of information on the interface that was required by the user to progress through the report.

Similarly, Mapimele, F. and Mangoale, B. 2019 devised a H2M platform, which they named the cybercrime combating platform (CP3). The algorithms of the CP3 allow users to use the search bar to check whether any of their data has been compromised. The system, which is serviced by people makes use of databases to crawl through data of cybercrime activity online. The databases it engages are: HaveIBeenPwnd, Phishtank, Dshield and Breach Level Index.

Yet not all research that is out there is about how specialists can improve cybercrime reporting. To the contrary, Baror, S.O., Ikuesan, R.A., and Venter, H.S. 2020 realised that low cybercrime reporting can be caused by a lack of clear criteria that victims can follow when reporting a crime. Therefore, Baror, S.O., Ikuesan, R.A., and Venter, H.S. 2020 used their research to put forward a set of transparent criteria that could be utilised from the victim's end when inputting data into the designated platform. The criteria are: *1. Physical location*, which pertains to where the victim was physically in space when she was targeted by the scam text message. An example of a physical location is Glasgow (Scotland). *2. ISP/Cloud Provider* relates to the unique digital gateway via which the attack has occurred. *3. Nature of cybercrime*, which is the type of offence that has taken place such as cyberfraud. *4. Cybercrime description* refers to what is known about the attacks such as the language used by the offender as well as any other discernible characteristics that can be used to specify what has happened. *5. Estimated start time & end time* refers to the approximate time windrow during which the crime has happened. *6. Other specifiers* relates to any other material retained by the victim which can be used to assist with the investigation such as screen shots of chat logs. Lastly, *7. Digital investigation artefacts* are loose types of data such as registry keys, timestamps, files and so on. I consider these criteria to be a meaningful guide when designing reporting systems to ensure a high degree of specificity.

Returning to some of the information from the previous section §3.3.1 Human To Human (H2H) by Cross, C. 2020a a follow up study by the same author offered an independent analysis of the ACORN system, which has since been decommissioned (Cross, C. 2020b). She found that the victims who reported to the ACORN online system experience high levels of dissatisfaction, specifically 77% of complainants were unhappy with the outcome of their complaint. Also, according to the author, the data captured by ACORN was of poor quality and there were numerous reasons for this. Many people logged that someone attempted to scam them, but not actually succeeded. Also, victims viewed money that they were promised versus money that they lost as a form of crime. Moreover, victims inflated their actual losses to get the police's attention and victims submitted multiple reports in the hope of having a greater impact. Lastly, Cross, C. 2020b found that people struggled to keep within the remits of what ACORN was designed for, i.e. the reporting of economic cybercrime. In fact, out of the 65 000 incidents, 16% of reports related to illegal content found online such as sexual abuse and exploitation material, which further muddied the data.

Additionally, cybercrime reporting should not be reduced to merely passing on information about about an offence to a relevant body. Rather the way the information is stored and subsequently analysed should be included in the equation about reporting (Das, A. et al. 2021). The latter research identified the problem of how reports were stored. In the case of cybercrime, reports were stored in an unorganised text form where one document pertained to different criminal activities, which made the investigation of patterns very problematic. To make a step towards resolving this issue, Das, A. et al. 2021 used principles from Natural language processing to create a set of graphs that makes connections about offences in an analysis supportive way.

Preparing the ground for some of themes in the next subsection §3.3.1 Machine To Machine (M2M), Mackey, T.K. et al. 2020 investigated the proliferation of fake COVID-19 related health products on Twitter and Instagram. In order to report and analyse the scams, the authors first scraped Instagram and filtered through Twitter for keywords that are connected to the selling of fake COVID-19 remedies and tests. During the second stage, the data was analysed with the use of deep learning and Natural language processing (NLP), which is a multidisciplinary domain dedicated to teaching computers how to analyse large chunks of language. In total, Mackey, T.K. et al. 2020 analysed 6 029 323 tweets and 204 597 Instagram posts. After the application of deep learning and NLP, the authors identified 1 271 tweets and 596 Instagram posts connected to the dubious sales of questionable COVID-19 related health products.

Machine To Machine (M2M)

A novel approached pioneered by Carpineto, C. and Romano, G. 2020 designed an automated pipeline with two machine learning stages to identify sellers of counterfeit luxurious clothes. This prototype was found to be more effective than established trustworthiness systems and non-expert humans. This piece is included because it closely ties to two forms of economic harm caused by dishonesty. Firstly, the sellers of genuine brands lose profits to the fraudsters, but secondly people who think that they have landed a good deal on a designer purse, are actually scammed out of money. Taken together, this research shows a promising new direction in cybercrime reporting whereby automation of the reporting process can be streamlined.

Similarly, in a technical piece by Sheikhalishahi, M. et al. 2020 the authors offered an exploration and resolution of the problem of spam e-mail automated analysis and classification. In their article the authors put forward an automatic method and resulting framework founded on pioneering categorical divisive clustering, utilised for both classification as well as grouping of spam e-mails. Specifically, the grouping is harnessed to diagnose campaigns of comparable spam e-mails, whilst classification is used to name particular messages according to their intended purpose (e.g., phishing). The authors put forward the CCTree algorithm for grouping and classification in batch and dynamic forms to navigate via both large data sets and data streams. Subsequently, the CCTree was applied by the authors to spam to fulfil its intended purpose.

In remaining with the subject of phishing, a technological development by Singh, S. et al. 2020 delved into identifying the difference between the latter and a classical web page. This task was found to pose challenges due to the semantic structure involved. Singh, S. et al. 2020 managed to apply a phishing detection system with the utilisation of deep learning mechanisms to safeguard against these cyber assaults. The framework works using URLs via an application of the convolutional neural network (CNN) with an accuracy of 98%. The CNN is a type of deep learning algorithm capable of inputting, analysing and differentiating between images. Feature engineering, the process of using speciality knowledge to extract features, has been removed as the CNN pulls out features from the URLs via an automatic process through its hidden layers.

3.3.2 Cybercrime reporting results

The purpose of this subsection was to scrape up any remaining literature via the systematic approach and highlight any gaps not covered by the previous searches in this section. In doing so, a collage of findings surfaced which is presented chronologically below.

Closely tying into the previous subsection, the research by Nappa, A., Rafique, M.Z., and Caballero, J. 2015 looked at the results of cybercrime reporting in a design that explored drive-by downloads. These types of downloads refer to two main types of downloading. Firstly they are concerned with downloads triggered consciously but without an understanding of the consequences, secondly the download is triggered illicitly to install some form of malware. Drive-by downloads are rolled out via cloud based servers with 60% of servers hosted by specialised cloud hosting services. According to Nappa, A., Rafique, M.Z., and Caballero, J. 2015 the designated servers fall into two types. The first one is called a short-lived server, which launches attacks for about 16 hours, the second one is called a long-lived server which can carry on for multiple months. The researchers analysed reports to ISPs and hosting providers for 19 long-lived server. The result was that 61% of the reports did not even receive acknowledgement. For the reports that were acted upon, it was found a server lives for another 4.3 days after the report was submitted.

An interesting take on the results of cybercrime reporting was considered in a piece that analysed the effects of reports by technological specialists adapted by the media (Winder, D. and Trump, I. 2015). The authors found that the sensationalist reporting has shifted the focus in an unhelpful way. This was best expressed by a historical quote used in the paper, according to which: "The one that defends everything, defends nothing." Let me unpack the argument that is hidden behind this eloquent principle. They specifically argue that people's reluctance to disclose specific system vulnerabilities results in reports about grand attacks. Whereas, if people were more open about reporting what aspects of their systems were permeable, then this would allow a much more fine grained discussion about how to defend against such attacks. Therefore, Winder, D. and Trump, I. 2015 recommend that reports about cybercrime should be less grandiose and more specific if they are to result in an effective defence.

Returning to a more common perspective, on cybercrime reporting results, Prislan, K. et al. 2019's work can be used to speculate about what results people expected to see post-reporting. In their student sample, the vast majority experienced cybercrime as a form of psychological aggression (e.g., stalking). However, only 26.7% experienced cybercrime with an economic incentive such as online scams, bank frauds and sextortion. Most people expected to see positive results if they reported to a friend in hope of getting advice (77.9%) followed by the police (76%). The interesting aspect of Prislan, K. et al. 2019's findings was that whilst 38.4% of respondents would seek help from the Slovenian Computer Emergency Response Team (SI CERT), a reporting system similar to Action Fraud in England, 33.7% of participants had never heard of this centre. This is critical because it is another piece of research that highlights the international theme of people not interacting with cybercrime reporting centres. Consecutively, it can be difficult to follow-up on the results of cybercrime reporting, not just in Slovenia, but globally if citizens do not engage with the dedicated tools.

As I have shown before, various factors influence people's expectations of whether cybercrime reporting will bring about the desired results. In this respect, Van de Weijer, S.G.A., Leukfeldt, R., and Bernasco, W. 2019 used a Dutch population to show that males versus females reported fraud to the police more often, whereas females versus males reported identity theft more frequently to organisations other than the police. Furthermore, there was a general trend to report repeat victimisation to other organisations, but this trend was reversed when reporting to the police. Once again, this pattern of findings suggests that people do not expect the police to be deliver on the results of their cybercrime reports. Instead, if I were to

be optimistic, I would say that people feel that this responsibility is shared between the police and other organisations. The latter research connects effectively to its Belgian counterpart by De Kimpe, L. et al. 2021 who found that only 28% of respondents reported cybercrime in an official way and only 10.8% reported to the police.

A piece that carried out the painstaking task of tracing individual cybercrime reports to the offenders brought forward some interesting results (Buil-Gil, D. and Saldana-Taboada, P. 2021). The authors have focused on Bitcoin to investigate economic related cybercrimes such as blackmail, fraud, sextortion etc. It was evidenced that a relatively small number of offenders are responsible for a relatively large number of offences in cybercrime. A deeper analysis of these reported results revealed that the offenders that attracted the most reports are not always the same ones as the offenders which made most money. This is evidence of the type of results that can be generated when cybercrime reports are analysed as well as the kind of conclusions that can be gleaned. From this, I can also see that there is significant skills diversification among offenders whereby ones tend to launch multiple attacks as kind of fishing expedition whilst others are more sophisticated and precise.

In a rare qualitative article revealed via the systematic approach, Hadlington, L. et al. 2021 interviewed sixteen frontline police officers in order to examine the crucial aspects of cybercrime. The police staff found that they continued to struggle with how to define cybercrime, its constantly evolving nature and lack of appropriate training that would help them remain on the cutting edge. From this research it is clear to me that the police are in a similar place to the public when it comes to economic cybercrime. Also, in my view, I get the sense that the police have low self-confidence in their abilities based on the responses provided to the interviewers. If I think about some of the earlier studies from this section, where people said that they were unlikely to report cybercrime to the police, it seems plausible that the police's lack of confidence may have been a contributing factor.

Lastly, it seems fitting to conclude with a study that analyses the results of reports from Action Fraud during COVID-19. I say it is fitting because Action Fraud and its critique is responsible for driving some of my current research and, of course, COVID-19 remains the most pertinent challenge faced by society in terms of novel pandemics. A research paper by Kemp, S. et al. 2021 analysed the changes in cybercrime during the pandemic and found, as anticipated, that there was a significant increase in this type of offending. However, their findings were nuanced and warrant a couple of concrete examples. For instance, Kemp, S. et al. 2021 found that the closing of physical shops resulted in people shopping for clothes online, which resulted in increased shopping fraud. On the opposite side, a reduction in ticket related leisure activities and aviation resulted in a decline of ticket fraud. Additionally, the researchers found that organisations as opposed to individuals experienced decreased cybercrime. The explanations for this are speculative, but relate to the closing down of businesses and restructuralisation, which resulted in an inability to detect crime. Taken together, the article by Kemp, S. et al. 2021 is a fitting concluding statement because it brought this research right back to Action Fraud, which is partially effective at supplying descriptive data, but less effective at providing explanatory data.

3.4 SLR Discussion

At the beginning of the §1 Introduction I put forward three research questions with the aim of illuminating the cybercrime landscape where economical crimes of dishonesty prevail. The purpose of these questions was to target the main research question of: "What is required for improving cybercrime reporting?," from different angles. I have answered these questions exhaustively by discussing the articles revealed by the systematic approach. Now, I will discuss

the research from the systematic literature review in connection to the situation in Scotland as I analysed it in the §1 Introduction. The subsections are subdivided according to the three research questions. I will discuss only a small number of selected relevant articles from the main body.

What is known about cybercrime research in the UK to date?

My research seeks to address the improved reporting of high volume low value crimes, which is the type most likely to affect individuals (Levi, M. 2017). The modus operandi can stretch to involve a sexual incentive (Hutchings, A. and Pastrana, S. 2019; Pastrana, S. et al. 2019) or a romantic one (Whitty 2018). Moreover, the modus operandi will target particular vulnerabilities in the individual ranging from loneliness brought on by the COVID-19 pandemic (Buil-Gil, D. and Saldana-Taboada, P. 2021; Cross, C. 2021) to scamming people into sending money by falsely claiming to have found their beloved pet (Levi, M. and Smith, R.G. 2021). What these examples share in common is that all victims were targeted via their emotional needs. Improving cybercrime reporting in Scotland could entail an awareness raising campaign in community venues, which will help potential victims understand their needs and how those can be used against them by criminals (Karagiannopoulos, V., Sugiura, L., and Kirby, A. 2019).

When comparing these findings with Police Scotland's Cyber Strategy (Police Scotland and Scottish Police Authority 2020) it becomes clear that the callous criminals will target people who are vulnerable by a combination of age or disability, and loneliness. Therefore, to improve the reporting of cybercrime, effective identification of at risk people needs to take place. Such a risk assessment would include information about those in the community that are lonely and isolated as the two factors are major contributors to victimisation. Yet, identifying the latter type of people will be especially challenging as, by definition, if someone is lonely and isolated, then people are less likely to be aware of their existence, needs and vulnerabilities. Community police officers in combination with community mental health teams (CMHTs) are best placed to identify these people in Scotland. It is through their collaboration cybercrime can be prevented and reported more effectively. Indeed, prior research has shown that local officers possess significant background knowledge of the localities that they police, which can enable them to devise tailored policing measures (Wooff, A. 2015; Wooff, A. 2016).

In §3.1.2 Models I also engaged with Hunton, P. 2012's five policing roles investigation framework as a way of dividing functional specialisation within investigations into economic cybercrime. I said that the approach had a potential pitfall because team leaders could become constrained by the boundaries of the roles where a creative fully-flexible approach would be more helpful. In the context of the Scottish situation, models of functional specialisation support the 2013 centralisation reforms by the nationalists. This is owing to the fact that functional specialisation creates the conditions for accountability far more than fully-flexible teams. That is to say, if an officer has to meet the specific requirements of their role description, then it becomes easy to measure whether she has succeeded or failed based on a simple box ticking exercise. In contrast, if I were to take a fully-flexible team where everyone can offer their ideas, then I might find that some people are always driving the investigations whilst others are merely free-riding in the system whilst wasting tax payers' money. If improved cybercrime reporting is to take place in Scotland, then a balance needs to be struck between the need to remain flexible and open to new ideas on the one hand, but also having clear systems of accountability on the other.

Johnson, D. et al. 2020 evidenced the enduring problem with the accurate counting and compilation of cybercrime reports. As I mentioned in the §1 Introduction in §1.4 Crime numeration the accurate recording and counting of crime has been a problem since the 1930s

(Maltz, M.D. 1977) and endures despite the dramatic advances in technology. This might be due to the fact that we have been looking at the problem of counting crime purely mathematically. Counting crime is very different from counting the amount of grain collected by an industrial agricultural machine. When we speak about "counting crime" we are inevitably describing a social interaction, which is why counting crime may be more of a qualitative exercise than meets the eye. I argue that it is these interpersonal complexities that result in poor cybercrime recording strategies because every crime is slightly different and hence capturing "the right information" is impossible if the police officer does not know what the complete mosaic will look like once it is finished. This is why it is important that police officers are not made to feel as if they let down their victims (Hall, M. 2021) if the systems that they are required to operate within are not setup for purpose. It follows that improving cybercrime reporting in Scotland will entail a discussion about the social components of reporting crimes and how to engage those for the benefit of accuracy and robustness.

In connection to problems with reporting and recording cybercrime, Horgan, S., Collier, B., et al. 2021 suggested harnessing the power of community links with the police. I can only add that the insider's view of the community police might be useful in filling many of the holes that are contained within cybercrime reports as the complaint taker may be less likely to make assumptions about the complainant concerning issues such as demographics and the like. This argument is in line with the favourable view that Wooff, A. 2015 and Wooff, A. 2016 have towards community policing as mentioned in §1.3 Police Scotland.

Subsequently, I supplied several relevant pointers for adjusting the people's side of improving cybercrime reporting in Scotland. I discussed how Forouzan, H., Jahankhani, H., and McCarthy, J. 2018 and Schreuders, Z.C. et al. 2020 found that a one-size-fits all online cybercrime training by the London Met was ineffective. In fact, over 33% of the police force did not even hear about it. Illuminatingly, the usefulness of the social element in cybercrime training was corroborated by Cockroft, T. et al. 2021 who found that face-to-face training delivery was more effective in preparing the police for responding to cybercrime. Hence, if cybercrime reporting is to improve in Scotland, then it is preferable that the training of police officers is face-to-face and interactive.

I believe that online cybercrime training perpetuates the problem it is meant to be solving by playing into the narrative of cybercrime being something that happens on a computer. I argue that the computer is just a medium, cybercrime can happen between people with personalities and life stories. The successful improving of cybercrime reporting will also require an ability to reclaim this social landscape from a purely technical interpretation. Much like in my proposed taxonomy for cybercrime reporting (i.e., H2H, H2M and M2M), actual cybercrime reflects a similar pattern. Whilst some crimes are carried out from human-to-human, such as when a malicious ex-partner goes on a shopping spree via an Amazon account of their ex, others can be human-to-machine, such as when a hacker attacks a computer with ransomware. Lastly, in a case of machine-to-machine, malware that incorporates computers into botnets is criminally making unauthorised use of computers, but the computers' authorised users may not know that this has happened or be directly impacted.

Finally, I have considered the research by Bossler, A.M. et al. 2020 who argued that cybercrime reporting could be improved with a set of best practice procedures and guidelines that would be rolled out across the board. To the contrary, this was disputed by Johnson, D. et al. 2020 who wrote that the decentralisation of the English force would make this difficult. Importantly, this is no longer applies to Scotland, which has undergone the centralisation of the eight regional divisions under one Police Scotland. In a research by Murray, K. and Harkin, D. 2017 this was lauded as a step towards more effective scrutiny and higher accountability of police staff as I have said in §1.3 Police Scotland. Whilst I do believe that cybercrime reporting is a

distinctly social phenomenon, I also think that a set of democratically negotiated best practice procedures would improve the situation across Scotland. This is a residual benefit from the nationalists' reforms that has yet to be harnessed.

3.4.1 What is known about cybercrime victims in the UK to date?

I have used the systematic approach to reveal information about the victims' profiles and experiences. Starting with a stark piece from 2008, Hunter, P. 2008 reported on a case study where a prominent MP was victimised by cybercrime, which prompted him to prioritise the problem as a part of public discourse whilst also critiquing the absence of a dedicated cybercrime reporting centre. As I wrote in §1.3 Police Scotland, the cybercrime reporting centre has been established as Action Fraud, however in 2019 Scotland chose to discontinue its membership with the centre due to receiving an overpriced and poor service (MacDonald, K. 2019). Leaving AF was a wise strategic move on behalf of Scotland which will enable it to set-up systems (both social and technological) that will improve cybercrime reporting whilst respecting its unique cultural landscape.

Next, I have discussed the research by Bohme, R. 2013 who discussed the quantitative aspects of victimisation in terms of how much victims could sue for in court. The research by Bohme, R. 2013 argued that victims' distress is difficult to account for in legal terms. I have argued that without considering the victims distress and their phenomenology it will be difficult to construct improved cybercrime reporting systems in Scotland. I find it hard to imagine how one could follow through with the Police Scotland's Cyber Strategy 2020 and focus on "vulnerability" whilst not seeing its connection to increased distress (Police Scotland and Scottish Police Authority 2020).

Then I have shifted the discussion to the Routine Activity Theory (RAT) as a framework that explains the probability of online victimisation based on insecure online behaviours. Take the following two examples. Firstly, the article by Nasi, M. et al. 2015 was used to shed light on what traits make people more vulnerable to cybercrime. It was found that being male, young, migrant, urban, not living with parents, unemployed with more social life online versus offline were all predictors of becoming a victim of cybercrime. Secondly, it was found that during the pandemic people spent more time online, which increased their risk of victimisation albeit decreasing the risk of being a victim of a violent crime in the street (Buil-Gil, D., Miro-Llinares, F., et al. 2021).

Subsequently, I was able to garner that victims of cybercrime often engage in sensation seeking behaviours with their cognition being less likely to suppress incorrect information when they come across it in phishing emails (Jones, H.S. et al. 2019). This research tied into findings by Button, M. and Whittaker, J. 2021 where the authors found that victims of cybercrime experienced a range of psychosomatic symptoms ranging from physiological deterioration all the way to psychiatric deterioration thereby suggesting that victimisation also increases vulnerability to serious illnesses.

Lastly, the systematic search revealed age to be a predictor of vulnerability towards cybercrime with older people being more likely to be victimised by economic scams (Correia, S.G. 2020) and younger people who were lonely during the COVID-19 pandemic were likelier to fall prey to romance scams (Buil-Gil, D. and Zeng, Y. 2021).

Conclusively, these findings should be linked in with the Police Scotland's Cyber Strategy 2020 as they all feed into the concept of "vulnerability" and as such are instrumental in understanding the victims of cybercrime (Police Scotland and Scottish Police Authority 2020).

An important theme from the §1 Introduction that stretches throughout this research is that of responsibilisation (§2.2) which is closely connected to cybercrime victims. As I have stated

before, due to there being an insufficiency of research on cybercrime victims from the United Kingdom, I have chosen to extrapolate findings from the West onto the UK and from the UK onto Scotland. For example, Bohme, R. and Moore, T. 2012 found that people who have been victimised by cybercrime or received information about its threat depressed their online activity. This points to the unintended effects of responsibilisation as Renaud, K., Flowerday, S., et al. 2018 and Renaud, K., Orgeron, C., et al. 2020 found that Western governments merely impart cautionary information onto their citizens but disengage thereafter. I would argue that people's decrease in activity points to feeling alone, vulnerable and unprotected whilst online, which is why they decrease their activity rather than seek protection. It is crucial to create such cybercrime reporting mechanisms that citizens will feel emboldened to come out of anonymity and share what has happened to them with the police without a fear of being judged.

Also, Leukfeldt, E.R., Notte, R.J., and Malsch, M. 2020 found that cybercrime victims have a real need to receive recognition from society and the police for the ordeal that they have been through. This includes receiving regular updates regarding the investigative process. The notion of recognition is something that I connect to responsibilisation because it suggests that recognition is still not a given. Rather, cybercrime victims are made to feel responsible for what has happened to them, which is why they do not receive the recognition that they deserve. Improved cybercrime reporting in Scotland is inevitably connected to helping victims restore their dignity and turn their adversity into a story of resilience.

Ironically, the very governments that responsibilise their citizens may be reluctant to admit that it is fake government websites that are used to target victims. This is important because on the one hand all Western governments enforce the law and expect citizens to abide by it, but if citizens are tricked by a scammer, then they run the risk of being blamed. Take for example the discussed study by Lacey, D., Salmon, P., and Glancy, P. 2015 who found that fraudsters impersonate the post office to force people to open phishing links purporting to provide extra information about a delivery. People should not be made to feel responsible for complying with the request. It is a similar scenario as if a criminal was to impersonate a post man in order to commit a burglary. In response, the victim would be blamed for not scrutinising their ID card in more detail via the key hole before they opened the door. The majority would not blame the burglary victim, so why do we do we blame cybercrime victims?

As I have shown throughout, the cybercriminals do not stop there. Indeed, in the USA they readily impersonate the IRS or the FBI in order to get international students with minimal knowledge of national laws to give up their details under the threat of criminalisation (Bidgoli, M. and Grossklags, J. 2017). This is another example of why the governments cannot bypass their responsibility to protect the innocent victims. The predatory behaviours of scammers will use the fear of the law against citizens if they know that their victims will be blamed for giving in. In order to improve cybercrime reporting in Scotland, people need to receive this information in places and from people that they know they can trust as the internet can be full of deception. This is why the social element of coming together and talking about these challenges in a community venue with the police can be so helpful. The citizens will know that the police officers are who they claim to be as they will have many years worth of memories with them being genuine police.

The ineffectiveness of responsibilisation strategies can also be seen in the research by Cross, C. and Kelly, M. 2016 which used two case studies that of Ruth and Hazel. They illustrate that whilst people receive information about how to protect themselves against cybercrime, they fail to do so if their emotions are invested in a pseudo-relationship or a pseudo-enterprise. Moreover, these single cases were backed up by community research where most people perceived the risk of cybercrime as being low whilst reporting widespread victimisation (Cross, C., Holt, T., et al. 2021), which suggests that the problem is societal rather than that of

Ruth and Hazel. This is evidence that the Western governments' approach to merely educating citizens about cybercrime is simply an insufficient.

It is ironic that governments which responsibilise their citizens invest finances into awareness raising campaigns on how to avoid cybercrime but do not invest in raising awareness of how to report crime and what to expect from authorities. This was illustrated by Cross, C. 2018 which described that people had unrealistic expectations from the police and were often moved on from one agency onto the other. If I were to conduct an awareness raising campaign as a part of this research, then I would focus it on who citizens should contact to report cybercrime and what they can expect thereafter.

3.4.2 What is known about cybercrime reporting to date?

Responsibilisation correlates negatively with people's desire to report cybercrime. As can be seen in studies by Bidgoli, M., Knijnenburg, B.P., and Grossklags, J. 2016 and Van de Weijer, S., Leukfeldt, R., and Van der Zee, S. 2020b people readily associate private companies with providing a resolution. Likewise, Jhaveri, M.H. et al. 2017 found that government's unwillingness to tackle cybercrime has brought together business rivals to form security coalitions with the aim of protecting businesses.

It is also important to consider findings from countries where (§2.2) responsibilisation is likely to be lower and control of the state higher. The research from Saudi Arabia by Alzubaidi, A. 2021 was interesting because whilst most of his participants did not report cybercrime to anyone, from those that did, most consulted a friend and then the government's e-portal. This raises interesting questions about trust towards governments in countries with distinct values. Citizens in the West are more inclined to report cybercrime to those agencies that aspire to sell them as much products as possible rather than the government to which they are paying taxes. This is a case of responsibilisation, which needs to be reversed. To the contrary, citizens in Saudi Arabia are slightly likelier to report to their government. The reasons for this distinction warrant further, ideally cross-cultural, research.

A key finding for my research comes from Cross, C. 2020a, which debated the challenges of jurisdiction in cybercrime reporting. She also explained the ACORN project, Australia's version of Action Fraud. The similarities between ACORN and AF are striking. Just like in the case of AF, ACORN was criticised for lack of transparency and poor customer service and poor incident recording. This rings all too familiar with the piece from in §1.4 Crime numeration by Maltz, M.D. 1977 who wrote about the problems with crime recording centres in the 1930s. It also corresponds closely to the strategic thinking behind Police Scotland's desire to separate from AF due to receiving a poor service (MacDonald, K. 2019). As I have argued before, I think that one reason these systems have problems is because they discount the social element of crime. I believe that if crime recordings engaged the person more holistically by including their emotions and so forth, then people would be more encouraged to provide accurate reports.

At least of the surface, the reporting centre IC3 in the USA (Heinonen, J.A., Holt, T.J., and Wilson, J.M. 2012) fares better than both ACORN in Australia and AF in the United Kingdom. As stated by Bidgoli, M. and Grossklags, J. 2016 its main advantage is that it provides awareness raising campaigns, but its main weakness is that it operates on a federal level whereas most cybercrime is localised. Out of three reporting centres discussed here (AF, ACORN, and IC3), I am most sympathetic to the IC3 because of its effort to interact with the citizens, which are most likely to need it rather than just dispersing information in the hope it finds its way to the correct receivers. In this respect, I see the IC3 as making very explicit steps to increase the social dimension in cybercrime reporting which I have spoken about.

I have also presented several studies that could be used to inspire a cybercrime reporting system in Scotland, which I summarise as follows. Firstly, cybercrime reporting systems must increase user cyber-awareness, provide user autonomy and avoid cognitive overload (Bidgoli, M., Knijnenburg, B.P., Grossklags, J., and Wardman, B. 2019). Secondly, to make cybercrime reporting more objective, systems must supply people with clear criteria regarding what information is sought (Baror, S.O., Ikuesan, R.A., and Venter, H.S. 2020). The second example might be helpful for those that prefer to communicate with a system rather than a police officer. However, people who are already intimidated by technology will miss the social element I have referred to before.

3.4.3 SLR Conclusion

I conducted a systematic review to identify what is required for improving cybercrime reporting in Scotland. I have contextualised current state of the art knowledge on the subject within the changing political landscape of Scottish policing. In this respect I have sought to connect much of my research to the notion of vulnerability to cybercrime. I have also looked at how crime numeration has evolved over time and that, despite unquestionable technological advancements, the problems with reporting remain unchanged for nearly 100 years (Maltz, M.D. 1977). This lead me to postulate that cybercrime reporting needs to be treated as a social phenomenon rather than a strictly numerical one. A common thread that stretched throughout the literature was that of (§2.2) responsibilisation and its damaging effects on cybercrime reporting. I explained that the paradigm needs to change and the state has to take ownership of policing cybercrime. Moreover, I have supplied an original taxonomy for classifying cybercrime, which could aid researchers in searching through the literature if it became widely adopted. Moreover, this taxonomy will be effective in understanding the literature on cybercrime reporting, which could aid the development of interventions.

Chapter 4

Scottish victims of cybercrime (SVC)

Using the frameworks from the §3 Systematic literature review (SLR), I have sought to understand Scottish victims of cybercrime (henceforth: SVC) to improve cybercrime reporting in Scotland. In the §4.1 SVC Introduction I hone in with relevant court and news stories before interviewing §4.2.2 SVC – Individuals, §4.2.3 SVC – Private institutions and §4.2.4 SVC – Public institutions. There were 10 SVC (9 males, 1 female): 3 Individual SVC who incurred cybercrime harm of £1 000, £5 240 and £20. 2 Private institution SVC who incurred cybercrime harm of over £20 000 and non-monetary harm. 5 Public institutions, represented by various functions. Their staff and equipment suffered psychological and technological harms. All the cybercrimes were from the years: 2012 (1), 2015 (2), 2017 (1), 2020 (1), 2021 (3) and 2022 (2), where the number of interviewees is in brackets. Then, the qualitative §2.4 Scottish victims of cybercrime (SVC) Methods guides the reader through the anatomy of the study. §4.2 Results describes victim case studies, which uncover the dominant impact of transnational cybercrime. The reporting trajectories varied and responsibilisation as well as scepticism towards the Police exerted their influence over the processes. The §4.3 SVC Discussion encapsulates this in detail and connects with what is required to improve national cybercrime reporting. The §4.5 SVC Conclusion argues that victims' expertise and a reduction in responsibilisation are needed to improve cybercrime reporting.

4.1 SVC Introduction

Cybercrime reporting in Scotland is a pertinent subject because, in 2021-22, almost half of all reported fraud cases (totalling 8 010) were cybercrimes. The number of cases in 2020-21 amounted to 8 630, a significant increase over 2019-2020 with 3 450 recorded cybercrimes (Scottish Government 2022).

The purpose of this study is to understand Scottish victims of cybercrime (henceforth: SVC) in context with the purpose of improving cybercrime reporting in Scotland. The central focus is on anybody in Scotland when they were victimised. The peripheral emphasis is on on victims within the UK in general and elsewhere if it augments the understanding of SVC.

To some extent this corresponds to the contemporary emphasis on the victim take centre stage as described by Garland, D. 2002b who on p. 179 states that: "The processes of individualisation now increasingly centre upon the victim. Individual victims are to be kept informed, to be offered the support that they need, to be consulted prior to decision-making, to be involved in the judicial process from complaint through to conviction and beyond." Yet, I diverge from this conceptualisation where I put forward the idea that there are two more victim types, namely Public and Private institutions.

I will occasionally touch upon the importance of (§2.2) responsibilisation in explaining

the behaviour of victims. I have spoken about this already in §1.3 Police Scotland, where I have explained how the state shifts responsibility for policing cybercrime onto the citizen (Horgan, S. and Collier, B. 2016), which manifests when neoliberal governments advise citizens about safe online behaviour but disengage post-victimisation (Renaud, K., Flowerday, S., et al. 2018). I will use Garland, D. 2002a's argument, who associated responsibilisation with recruiting the private sector as a substitute for the policing function of the state.

In §1.4 Crime numeration I cited a classical study by Maltz, M.D. 1977, who described the evolution of crime numeration. The original source of statistics were court proceedings, followed by police reports, which were replaced by impact statements, which moved reporting closer to the victim. Within, I borrow and modify this rationale by using selected court cases from Scots courts to introduce the subject of SVC as a way of getting closer to the victims. Moreover, the empirical part of this research is entirely focused on victims' reports of cybercrime and their surrounding experiences.

Creating closeness via court document analysis has precedent in cybercrime. Loggen, J. and Leukfeldt, E.R. 2022 did just that in a thorough and systematic analysis of Dutch court cases related to phishing. My use of their approach within is less ambitious and differently motivated. As opposed to conducting a systematic study of court cases, I focus on a selection of illustrative ones as a foundation for the qualitative empirical study which is being investigated. When searching the court data I proceeded in the following way: Accessing the website of Scot Courts, I initially used the search term: "cybercrime", which generated 4 cases connected to the possession of indecent images of children amounting in the High Court, a single case of fraud in a Sheriff Court, and a single case of a cyber unrelated sexual assault in National Personal Injury, but no cases in other courts. Thus, as of 13 December 2023, the term "cybercrime" did not feature in any court documents in connection to Internet crimes of dishonesty. The search terms "fraud" and "fraudulent scheme" revealed the six court cases discussed below. There may be further cases connected to economic cybercrime under other keywords as it is apparent that cyber terminology has not yet pervaded the Scots court system. The relative scarcity of written court judgements can be connected to the fact that most judged cases do not result in written judgements.

The news stories were found in a non-systematic manner using the Google News search function so that examples reflecting each of the three victim types could be extracted.

Moreover, within I engage the approaches from §3.1.2 Jurisprudence by Lavorgna, A. 2019, who analysed press releases in order to gauge the extent of moral panic in the UK in connection to organised cybercrime. Once again, I modify the author's approach to suit my aims, which is to create victim closeness. I do this with the use of illustrative news stories that summarise the misgivings of people victimised, mainly in Scotland, but also elsewhere in the UK. The current subsection will build closeness with SVC by analysing a selection of Scots courts' cases and press releases.

It became clear is that cybercrime reporting is often neglected, even in reports of genuine cybercrimes the reporting thereof is not mentioned. Only 3 out of the 14 court and news cases explicitly gave details related to reporting, a curious omission.

Next, I will supply these case examples following the structure from §3.1.1 Typology, where cybercrime was seen as targeting §3.1.1 Cybercrime against Individuals, §3.1.1 Cybercrime against Private institutions and §3.1.1 Cybercrime against Public institutions.

Cybercrime against Individuals: Commencing with a court case of recruitment fraud, several companies that had operations from Scotland into central Europe advertised themselves to Czechs and Slovaks as reliable employment agencies (Lady Paton, Lady Clark of Calton, and Lorde Clarke 2014). The modus operandi required the Czech and Slovakian victims to en-

gage with the websites, sign up and come to Scotland where the criminals collected £400-450 from them at the airport and left them abandoned in an accommodation without any resources. The crimes were carried out between 2009-2011 and point to the complexities of policing internationalised recruitment fraud since the victims were non-UK citizens but have come to Scotland in order to be unwittingly defrauded. Lady Paton, Lady Clark of Calton, and Lorde Clarke 2014's court case is surprisingly current even in the 2020s where the research by Cross, C. and Grant-Smith, D. 2021 found that issues like the COVID-19 pandemic, which gave rise to global unemployment, made people more prone to engage with fraudulent recruitment agencies, thereby creating more cybercrime victims.

Another court case, which pertained to an individual cybercrime victim culminated in murder (Lord Justice Clerk, Lord Brodie, and Lord Drummond Young 2015). This warrants closer attention. Most of the scientific literature pertaining to localised economic cybercrime paints a picture of offenders who conduct the bulk of their nefarious affairs within the digital space as discussed in §3.3.1 Human To Human (H2H) by Bidgoli, M. and Grossklags, J. 2016. From my literature research into §3.2 RQ2.: What is known about cybercrime victims in the UK to date? I formed the impression that the latter are rarely physically attacked as is the case in traditional crime. However, perhaps there is a bias in the literature that puts forward a sanitised version of cybercrime by supplying cases where the offending took places exclusively online and without the use of physical aggression.

This court case by Lord Justice Clerk, Lord Brodie, and Lord Drummond Young 2015 describes the predatory relationship between two middle-aged men suffering from alcohol misuse issues. As a part of his modus operandi, one of the males inserted himself into the life of his friend under the guise of altruism. Instead, he set up various credit cards in the victim's name and caused harm of £32 000. Ultimately, in 2003, the cybercriminal murdered his victim by incapacitating him with drugs before taking his life by smothering. After the victim's death, the now murderer forged an electronic will in the victim's name where he was the beneficiary to the entire estate in addition to £25 000.

In 2022, two UK brothers who are social media personalities with high public profiles. The press reported that: "Two brothers are ranking millions from webcam sites where men hand over a fortune as they fall for models' fake sob stories" (Scully, M. 2022). Scully, M. 2022 asserts that the two brothers have stated that one of the UK victims paid £20 000 to a model whilst others have run up huge debt. In relation to the term "fake sob stories" Scully, M. 2022 indirectly implies that these pertain to stories that attractive Eastern European models tell to their victims to illicit financial compassion. The story themes include: crippling university debt, family member needing private healthcare and the like. The modus operandi described within is that of grooming where each victim is worked upon by a group of offenders whereby the model is the source of visceral input. In the background, offenders fluent in English illicit personal information from the male victim, which they use as a part of the grooming process in the romance scam. Following the news coverage of this particular case brings to the forefront questions regarding the true scale of these brothers' victims. Were all of the cooperating models culprits or were some of them victims too?

The cases by Lord Justice Clerk, Lord Brodie, and Lord Drummond Young 2015 and Scully, M. 2022 highlight that there is a very real possibility that cybercrime escalation does not happen exclusively on the level of IT expertise (Collier, B., Thomas, D.R., Clayton, R., and Hutchings, A. 2019). Instead, it can take place on the level of escalated offending transfer from the digital into the real world setting.

Furthermore, the transnational and complex nature of crime affecting UK nationals was revealed via a BBC investigation, which was conducted alongside German and Georgian police during raids on call centres in Tbilisi (Hudson et al. 2023). Perhaps, most telling are the

predatory notes that the cybercriminals attached to the names of the victims they were planning to scam such as: "Savings less than 10k, very pussy, should scam soon." Hudson et al. 2023 used the case examples of two UK citizens, one male and one female, to illustrate how they have been duped out of £27 000 and £15 000 respectively via investment fraud.

When quantifying financial harm caused by cybercrime, Scottish individuals fare relatively well in the area of cybercrime in comparison to other parts of the UK. According to a Freedom of Information request towards NFIB Fraud and Cybercrime Dashboard cited in Daily Star 2022, Wales is most impacted by cybercrime where victims lost £3 314 per attack. By contrast in the UK's capital, Londoners lost "only" £621 per attack although the intensity of attacks was the highest in their area. However, Scots victimised by cybercrime were recorded as losing on average "a mere" £18. Nevertheless, it is important to interpret this data with caution as reporting practices are likely to vary between the regions and hence what gets reported does not have to reflect the actual extent of cybercrime.

According to a news article by Stewart, S. 2022, the Russian invasion of Ukraine has also played a part in the escalation of cybercrime experienced by the Scots. Among the scams to look out for were: Lottery fraud, which is where the victim is tricked into believing they can claim a win if they pay an advance fee. Racing tip fraud, which is where the victim is made to believe that they can pay for a tip on who will win the races as well as rental fraud where the victim pays upfront for a property they will not gain access to. These scams have been linked with criminal gangs who could be attempting to help the Russian government.

In terms of legislation, the Scottish Conservatives have raised the legal challenges of policing cybercrime, which is currently investigated and prosecuted under "common law fraud" (Percival, R. 2022). Hence, the politicians argue that a new offence of cyber fraud should be put into place to make the processes more effective. In fact, all of the court cases that I reference within were judged as "frauds" or "fraudulent schemes." This is a problem because the ways of reporting and investigating cybercrime will vary from that of the latter, which is why legislating a separate offence would be more helpful.

Cybercrime against Private institutions: A court case pertaining to a series of crimes perpetuated against the Royal Bank of Scotland in 2012 underlines the institution's vulnerability to an antiquated form of cyber-enabled cheque fraud (Lord Justice Clerk, Lady Paton, and Lord Menzies 2015). The modus operandi is that the criminal cashes fake cheques which are paid out by the bank before they had a chance to bounce. Previous research cautioned against this risk citing experiences from USA (Fisher, J. 2008), a point I touched upon in §3.1.1 Cybercrime against Private institutions. The modus operandi required the convicted offender to engage the Royal Bank of Scotland in clearing 23 forged cheques resulting in financial harm of £103 330.

In another court case from 2018 concerning an unnamed bank, the private institution was victimised by one of its employees (Lord Menzies and Lord Turnbull 2018). The modus operandi employed by the cybercriminals was straightforward. Using a member of the group who was an employee of the bank, they managed to extract £51 000 from the customers' accounts over a period of time by stealing their personal details, which was ultimately a source of harm for the bank both in terms of finances but mainly on the level of reputation.

Standing out amid the cybercrime cases affecting predominantly banks, is the court case of Peebles Media Group a company that the court documents describe as "whaling" (Lord Summers 2019; BBC 2019). The modus operandi described within is where the offenders effectively impersonate a manager sending an e-mail asking a subordinate employee to transfer significant amounts of money to a named account. In this case, an employee was deceived into transferring £200 000 to various accounts. Whilst the bank reimbursed the company £85

000, the company pursued the employee for the remaining £107 984. Even though this was overruled by the judge, it remains apparent that the (§2.2) government's responsibilisation strategy manifested as victim-blaming.

Additionally, Lord Summers 2019 and BBC 2019 incorrectly used the term 'whaling' to describe this offence when in fact sources from the NCSC 2020 and FBI n.d. clearly distinguish 'whaling' from 'business e-mail compromise.' In fact, 'business e-mail compromise' is the correct criminological term. The use of incorrect terminology in jurisprudence can cause confusion that further impedes reporting.

As I shifted my attention from court documents towards press-releases, I came across a major attack targeting a Scottish car company that sells used and new cars as well as cars for hire, Arnold Clark (O'Sullivan, K. 2023; Sexton, B. 2023). The latter were attacked on 23-24 December 2022 by a ransomware gang called Play. The company's customers had their details stolen including copies of passports and national insurance numbers alongside other identifiable data, which were leaked online. This is a major source of harm for the company, which has 193 UK dealerships selling more than 250 000 vehicles per annum with a turnaround of £3 000 000, 000. This attack resulted in the risk of data breach for tens of thousands of people across Scotland.

Nevertheless, as O'Sullivan, K. 2023 points out, the ordeal of attacked companies does not end there. In fact, they can be further punished by the Information Commissioner's Office (ICO) for data breaches. For example, the British Airways (ICO 2020b) and the Marriott International hotels (ICO 2020a), both of which have operations in Scotland, were fined £20 000 000 and £18 400 000 respectively for failing to protect customers' data from criminals, which is a form of criminal responsibilisation by the ICO. Yet, this could be seen as a way of motivating well resourced major companies to protect individuals' data a principle which could be considered less ethical if directed against citizens.

Lastly, the privatised Royal Mail suffered significant problems to its international deliveries after it was impacted by ransomware demanding £67 000 000, which it refused to pay (Sweeney, M. 2023). This resulted in major delays which adversely impacted the customers of the mail corporation, specifically 11 500 post branches across the UK were unable to handle international mail or parcels.

Cybercrime against Public institutions: The last of the included court cases features cybercrimes from between 2009-2016, where the victim was Dundee City Council (Lord Justice General, Lord Menzies, and Lord Turnbull 2020). An employee of the local authority with a gambling addiction offended against his employer. The modus operandi required the cybercriminal to make payments on behalf of the council to fictitious suppliers, who were in fact his own bank accounts thereby causing a harm of £1 065 085.32 to the local authority.

Next, press reports informed the reader of how the Scottish Environment and Protection Agency (SEPA) was attacked by the Conti group's ransomware on 24 December 2021 (Stewart, S. 2022; O'Sullivan, K. 2023). Purportedly, the environmental watchdog has spent over £5 000 000 on the recovery of 4 000 lost files. This was the work of a hacker group linked to Russia in 2020.

Lastly, University of the West of Scotland suffered a cybercrime, which caused an online shutdown for several days (Delaney, J. 2023). Even though the actual harm was greater as it had taken six weeks to restore all systems. Crucially, the press report details how the institution addressed the incident in tandem with the Scottish government, the Police as well as the National Cyber Security Centre. This ties closely with the argument we are making when we insist that Individuals and Private institutions should benefit from the same degree of state support as Public institutions. In fact, as we go on to demonstrate, Delaney, J. 2023 report clearly

Table 4.1: Scottish Victims of Cybercrime NVivo Coding: A breakdown of the coding process from the raw interviews via the three stages.

File classification	*Stage 1. Initial c.*	*Stage 2. Focused c.*	*Stage 3. Themes*
1. V. Individuals	74	37	3
2. V. Private inst.	67	34	3
3. V. Public inst.	107	48	3

exemplifies how Public institutions report cybercrime to range of different stakeholders, who in return offer a coordinated response.

Summary: In this introduction I have sought to approximate the subject of SVC by citing real court cases and press reports from credible outlets. In doing so, I have supplied the authentic personal and financial harms surrounding this type of victimisation. Moreover, I have positioned the judicial part of the introduction temporally post 2014 with the bulk of the news cases taken from around the 2020s thereby ensuring a current coverage. In addition, by putting forward the classification of three different types of victims, two of which are institutional, I have resisted the pitfalls of centring victimisation solely on individuals as critiqued by Garland, D. 2002c. In fact, on p200 Garland, D. 2002c states that the suffering of individuals is key because: "Whatever mutuality or solidarity exists is achieved through the direct identification of individuals with one another, not with the polity or the public institutions to which they belong." By identifying institutions are victims too I have exemplified the nuanced landscape of cybercrime victimisation.

What follows now are the §4.2 Results for the empirical study. This empirical study will analyse interviews with real SVC which will follow the established structure of §4.2.2 SVC – Individuals, §4.2.3 SVC – Private institutions, §4.2.4 SVC – Public institutions followed by critical insights regarding §4.2.5 Factors improving cybercrime reporting and §4.2.6 Factors impeding cybercrime reporting. The §4.3 SVC Discussion will highlight what changes need to take place to improve cybercrime reporting. Finally, the §4.5 SVC Conclusion will conclude.

4.2 Results

4.2.1 Analysis

As per Table 4.1, I carried out the analysis of interview data with NVivo 1.3 using the rationale for small sample sizes by Ritchie and Lewis 2003 and methodology that fits closely with how Braun, V. and Clarke, V. 2022 describe "coding reliability thematic analysis (TA)", which is an approach where: "Themes are developed early in the analytic process prior to or following some data familiarisation, and often reflecting data collection questions (p. 6)." Hence, in line with Braun, V. and Clarke, V. 2022's theorising, my themes are best understood as summaries of particular topics, mainly in connection to what improves and impedes reporting. In identifying my TA approach, I have also followed the best practices guidelines by Braun, V. and Clarke, V. 2021 who urged all researchers to "clearly demarcate which TA approach they are using (p.335)."

Firstly, I classified the 10 interview files according to the type of victim. Thus, I created three File classifications: *1. Victims Individuals*, *2. Victims Private institutions* and *3. Victims Public institutions*. Secondly, I coded each File classification in three stages. These stages were: *Stage 1. Initial coding*, *Stage 2. Focused coding* and *Stage 3. Themes*.

Table 4.2: *Stage 2. Focused coding*: Quantifies the number of codes in the File classification.

File classification	*Improves reporting*	*Impedes reporting*	*Other*
1. V. Individuals	20	9	8
2. V. Private inst.	17	11	6
3. V. Public inst.	28	12	8

Table 4.3: *Stage 3. Themes*: Quantifies the number of codes in the File classification.

File classification	*Improves reporting*	*Impedes reporting*	*Case studies*
1. V. Individuals	19	9	9
2. V. Private inst.	14	10	6
3. V. Public inst.	28	12	8

Stage 2. Focused coding during this stage I merged all semantically similar codes, but also various data was uncoded if I thought that the code was erroneous. Lastly, I reorganised the codes into three main groups, which were: *Improves reporting*, *Impedes reporting* and *Other* (quantified in Table 4.2). The first two groups pertained to those codes which could be discussed in terms of improving cybercrime reporting. The category *Other* contained data about criminality that was not otherwise classified.

In *Stage 3. Themes*, depicted in Table 4.3, I further merged the codes from *Improves reporting* and *Impedes reporting* according to their semantic similarities. Lastly, the category *Other* was renamed into *Case studies.* I organised the codes from from *Case studies* in a way that would enable me to tell the story of cybercrime victims most effectively.

In the upcoming section, I will offer a detailed overview of the cybercrime affecting three types of victims (i.e., §4.2.2 SVC – Individuals, §4.2.3 SVC – Private institutions and §4.2.4 SVC – Public institutions. The main contribution of this section is that it supplies information about the modus operandi of cybercriminals contingent on who they are attacking by putting forward case studies and including their outcomes. Furthermore, this part is empirically enriched with direct quotes from the victims to relate specific themes (Lingard 2019) such as their attitudes towards policing. Moreover, I have followed the formal scientific guidance to use quotes that are 40 words long (American Psychological Association 2019) where I have replaced semantically inconsequential quotes' segments with "(...)" to remain within the word limit. I have also provided a short paragraph at the end of each category of case studies that describes victims' attitudes to use of technology. I have done this to find out whether victims may experience psychological obstacles towards technology that may occlude their reporting capabilities.

4.2.2 SVC – Individuals

Case study 1 E-Bay Car Scam

In 2017, the victim was looking to purchase a used vehicle from a seller that was emigrating to Sweden. The victim practised extensive due diligence reconnaissance in order to verify the legitimacy of the advertisement. For example, he identified that the vehicle was in storage with an actual company using the website of the official regulator. The proposed business arrangement was that the victim would transfer the money into escrow whilst he tests the vehicle and if he was happy with it, then the money would be released to the seller. This was followed up by credible and official bureaucracy, which only cemented the victim's confidence. After

the victim transferred the finances (i.e., £5 240), the vehicle never arrived. There was a brief interaction with the seller who apologised for the delay after which the lines of communication went dead. This type of scam is also referred to as advance fee fraud, where the culprit collects an upfront payment for a product they do not deliver (Correia, S.G. 2019; Correia, S.G. 2020).

Outcome: The victim managed to track down the seller to their place of residence and persuaded them to go to the Police under the weight of the collected evidence. He summarised the helpfulness of the English Police in the following way:

> "Ha! Helpful? No! They said absolutely nothing that was helpful. All that they did was to direct me to a phone that was in the corner of the reception area (...) that would put you to 'Action Fraud' (...)."

Furthermore, he interpreted the actions of the Scots Police by saying that:

> "the Fraud Department in Scotland wasn't interested because it was less than seven figures. So, they weren't interested and they didn't want to record it as a fraud, because the fraud technically happened in England according to them."

The victim's assessment of Police Scotland's willingness to investigate only seven figure cyberfraud would have been informal. Nevertheless, I am seeing a connection between some of the criticism leveraged against Action Fraud for the similar reasons in §3.2.1 From elites to the masses by Correia, S.G. 2019. Objectively, the response from the Police Scotland highlights the point I made in §3.2.2 Australia and Canada, where I cited Cross, C. 2018, who found that victims overestimate the Police's competencies in cases where cybercrime crossed different borders. Consequently, despite the victim providing the Police with substantial evidence, no investigation was initiated and he never received his lost finances.

Case study 2 HMRC Scam

In the United Kingdom, Her Majesty's Revenues and Customs (henceforth: HMRC) is a governmental body responsible for tax collection as well as the administration of state social benefits among others. Cybercriminals can impersonate the HMRC as a part of their modus operandi to intimidate victims into divulging personal details. This case study refers to a victim targeted by an *inchoate cybercrime*, which means an instance where a crime had commenced but was not successfully completed. The latter is a phenomenon specifically identified and investigated in the area of cybercrime by Bidgoli, M. and Grossklags, J. 2017 in §3.2.2 International collaboration, where the latter provided cases of undergraduate students targeted by cybercrminals posing as a governmental department. In 2021, the victim was targeted by a phone call claiming to be from the HMRC alleging that she had an outstanding debt. The victim practised due diligence and phoned the HMRC querying the information from the initial phone call. The HMRC confirmed that they had not made the telephone call. Next, the victim received a letter claiming to be from the HMRC in respect to the alleged debt, which was indistinguishable from the organisational one as it also included the victim's national insurance number. The latter is a unique numerical identifier that is used in the United Kingdom for tax and social benefits purposes.

Outcome: The victim was advised by the HMRC to report the *inchoate cybercrime* to the Police because they considered it as sophisticated which carried the risk of catching out many people. In the victim's own words:

> "I was to phone the 'Fraud Squad' and they gave me the number of the 'Fraud Squad.' I called them and I think I waited on the phone for a long time."

'Fraud Squad' advised the victim to hand over the letter as evidence to the local Police. In the end, the victim did not do this which she justified in the following way:

> "the police office wasn't manned and there was no one at the desk. I think I just got fed up parked my car and went home."

This outcome only echoes the concerns raised by Sommer, P. 2017 in §3.1.2 Policing, specifically in §3.1.2 Human resources, who observed that the lack of policing resources are often an obstacle to effective cybercrime policing.

Case study 3 Credit card details theft A

The victim that was interviewed with regards to the *Case study 2 HMRC Scam* also supplied information about her experience of credit card details theft. In 2021, when the victim sought to pay for her shopping in a supermarket, her credit card was declined. She noticed a few missed calls from her bank. Responding to the situation in her own words, the victim made a telephone call using the:

> "number on the back of my card. I just thought that would be the safest way to do it, so instead of Googling the number, I just raised the number on the back of my card and used the steps through that."

The latter confirmed that her bank details were stolen and used in America causing a harm of approximately £20. This resulted in her bank blocking the card and issuing a new one. This ties closely to the information from §4.1 SVC Introduction by Daily Star 2022 who stated that individual Scots were victimised by sums in the region of £18 per scam.

Outcome: The victim was reimbursed the full amount by her bank. As a form of aftercare, her bank sent her e-mail communications about self-protection in the area of cybercrime. The victim's view of the bank is best summarised in her own words:

> "I think the bank dealt with it quite well. Obviously, they're used to these kinds of things."

Case study 4 Credit card details theft B

In 2012, the victim was going over his bank statement and he noticed that it had been debited by £1 000 in order to buy a piece of IT equipment, which was a purchase that he did not recognise. The victim reported the suspicious activity to his bank because he wanted to block his credit card from further usage. The bank had taken the details from the victim in order to carry out a swift investigation.

Outcome: The victim was reimbursed the full amount by his bank. He summarised the financial institution's pro-active approach subsequently:

> "They contacted me and re-credited the account and that was the end of it, yeah. I was satisfied with that at the time, but not satisfied with not hearing anything else. I would like to have heard more."

The bank advised reporting to the Police on a specialised number, which they provided. The victim followed this advice, but did not hear back from the Police afterwards. The victim felt that his bank provided all of the solutions when it came to the reporting and resolution of the offence. Even though it was the bank that advised him to report the cybercrime to the Police, the victim remained sceptical about the Police's response by saying that:

> "I didn't feel I had a great deal of confidence in the Police following it up. But they made all the right noises and said they'd look into it whenever they'd hear again."

Victims' attitudes to use of technology

As a part of this study, I was also interested to analyse how comfortable victims were with the use of technology to see whether they experienced any psychological obstacles that might get in the way of reporting cybercrime. The victims used a range of technology from more mainstream smart devices to advanced and specialised technology. They reported feeling comfortable and very comfortable

4.2.3 SVC – Private institutions

Case study 1 .ru Ransomware A

In 2015, an owner of a Scottish Small-to-medium-sized enterprise (henceforth: SME) was advised by one of his employees that an error message appeared on the computer screen when they started up their systems on a Monday. The error message came from a .ru e-mail address and advised the reader that all of their information was in a data locker and a ransom would have to be paid for its release. The presumed modus operandi was that a legitimate supplier of the SME had been suffered a cyberattack, which caused them to send out a corrupted file to the SME.

The external IT company that was hired by the SME negotiated the ransom at $1 000 through a subsidiary company. As the negotiations were taking place the SME could not conduct its regular business because the customer database had been compromised, which blocked access to between 4 500 contacts. In the words of the SME manager:

> "In those day people relied on a text message to keep them up with appointments, so literally for three days we had maybe one or two people in when we would normally have twenty or thirty in."

Eventually, when the cybercriminals released the data, 95% of it had been corrupted. This shrunk the SME's customer database from 4 500 to between 350-400, which resulted in an indirect harm of £20 000 for lost business revenue.

Outcome: The victim SME had to cut its losses post-attack. The manager reported the cybercrime to the Police and summarised their approach as follow:

> "They had nobody to report it to. The local Police station you would've thought would've been a source of information but they had no information whatsoever on cybercrime. No contact numbers. No departments. No people who knew anything about it."

The victim also failed to get compensation via their insurer as insurance companies did not pay out cyberattack related damages. The SMEs manager felt that he needed to let people know about cybercrime after it had happened to him. He managed to get publicity about their incident via multiple media outlets, which resulted in an unexpectedly helpful dose of PR:

> "(. . .) name a news programme in those days and I think we were probably on it. So, from a PR perspective we got a lot of coverage and that probably made up for that loss of money."

Case study 2 .ru Ransomware B

In the autumn of 2022, the manager of a Scottish SME started noticing abnormalities on the company's reception computer. The manager recalled that he could see this unravelling as a form of activity rather than an event with a sudden short-lived onset post which all files were rendered inaccessible. The manager happened to be standing at reception when he noticed that the computer froze and had been externally accessed. In his own words, he said that:

> "(...) there was coding coming up on the screen and stuff like that. (. . .) our files had been took for ransom and they were demanding to be paid in Bit Coin to retrieve our files back."

The files that became encrypted included various worksheet and organisational administration, but not client files, which allowed the company to remain operable during the period of recovery. The ransom amount was never specified as the message required the manager to follow another link after which he reported the incident to the company's IT specialist. The IT specialist advised closing down all computer and restored the systems although the manager highlighted that:

> "Of course, I'm not too sure what that entails but he's done his work on it and put better security systems on them and has advised that we get some external storage hard drive stuff in case that ever happens again."

Outcome: The SME did not report the incident to the Police at all because a decision was passed that the issue should be resolved via the help of the IT specialist. The manager did not seem to be aware that reporting to the Police was a possibility and did not know that the non-emergency number was designated for this. Whilst the IT specialist appeared to have improved the SME's cybersecurity posture from a technical side, in the words of the manager he did not supply the company with an understanding of what transpired when they were victimised:

> "I'm personally still in the dark because I don't know like how to stop that. Why did it happen to us? (...) Just a bit of a better understanding of it of why it happened. How it happens?"

Victims' attitudes to use of technology

As a part of this study, I was also interested to analyse how comfortable victims were with the use of technology to see whether they experienced any psychological obstacles that might get in the way of reporting cybercrime. The victims used a range of technology where both used designated database systems specifically for their companies, specialised as well as general technology. One victim said that he was very comfortable due to using the software for 25 years, the other felt confident, but also stated that he needed to learn a bit more about the system.

4.2.4 SVC – Public institutions

Case study 1. Educational institution – Poorly designed cybercrime

In 2021, during the night, the Scottish victim got alerted to a cyberattack thanks to anti-virus software. The attacked got picked up 06:30 am by external responders who worked on it until 07:45 am in order to stabilise the network. The attack became uncontrollable and by 08:15 am a decision was passed to shut down the entire network. The access point remains uncertain, but the responder presumed that a student clicked on a phishing link, which caused the contamination to spread. Nevertheless, whilst it was necessary to proceed with extreme caution, the institution's IT specialist started to make some unexpected observations, which he summarised as follows:

> "The thing about it was, it was a badly formulated attack because, we found this out later, but part of the execute support [sic.] they built didn't work so we weren't impacted as much (...)."

The victim institution realised that by taking a zero trust approach and shutting everything down they managed to contain the attack. The actual damage was significantly reduced thanks to this approach. In order to safeguard their systems, they chose to rebuild the entire network from scratch to avoid any possibility of residual malware reinfecting the systems after they were rebooted.

Outcome: In order to restore the network, IT staff had to work 18 hour shifts for a period of 2 to 3 weeks, which was the price the institution and more specifically its specialists paid for restoring their systems. There was a risk of burnout and mental health issues for staff as a result of overworking to ensure that none of the students were affected. Constructively, this victim had cyber-insurance which covered the extent of the damage. There was no financial loss in connection to the ransomware, because the attackers did not attach a request. The victim distinguished his experience of reporting to the local Police versus reporting to Cyber-police:

> "You have to deal with a local Police office, so you report it to your nearest station and they send out a local bobbie and 9 times out of 10 he doesn't have any idea what you're talking about."

In the victim's view contacting local Police as the first port of call is not helpful. Instead, he would like to see a scenario where he could communicate with specialised Cyber-police straight away because like he said:

> "(...) cut out the lower level and say what you should do is report directly to the Cyber-police. It's a centralised organisation, they're the ones that are going to end up doing everything, they're the ones that have got the knowledge (. . .)."

Case study 2. Educational institution – Vendetta cybercrime

In 2021, the institution's manager was preparing to go to work at around 06:30 am. At this point, he was alerted by a member of staff that there had been a data breach. The institution forms a part of a digitalised national network, which was promptly alerted. Subsequently, they were severed from the network and isolated the entire institution in order to contain the cyberattack. Initially, the motivation was unclear and the cybercrime was similar to other attacks on public institutions. However, the attacker started to gradually extract a variety

of personal data of staff and pupils, which he shared with various media outlets, who were reporting on the incident as a data breach. This caused substantial distress to the manager as he was aware that this was a cyberattack. In the manager's own words the attacker even went as far as to:

> "access a member of staff's phone and amongst all of this has sent out porn from this person's personal account. So, it was quite vindictive and quite damaging to a number of folk as well and what was happening."

I can only imagine how distressed the person whose device sent out pornography must have felt as someone in a capacity to care for children and minors. Nevertheless, this is an important case study because it constitutes an instructional outlier. All of cases in this piece of research were financially motivated albeit executed with various degree of aptitude. This case is different because the cybercrime was conducted as vendetta by an ex-pupil, which was a form of malicious insider activity (Martin, P. 2024). In fact, during a period of time prior to the attack, staff have observed the former pupil attaching devices to the backs of physical PCs at the institution with the aim of accessing staff's passwords.

Conclusively, this underlines the importance of closely following the evidence in cybercrime and not making assumptions about whether an incident was a data breach, a cybercrime or a vendetta until all of the evidence is collected and evaluated by specialists.

Outcome: The institution's manager faced a lot of pressure from outside of the local authority to acknowledge that it was a data breach as opposed to a cybercrime. He felt that state officials were looking to place the blame on someone within the institution other than the attacker. More positively, the manager spoke very highly about the Cyber-police's approach highlighting the positive role of the named officer by saying that they:

> "regularly checked-in and checked if I was okay as an individual (...). (...) when they discovered who the attacker was, then they let me know in the morning when they were raiding his house (...)."

This shows the importance victims attach to getting justice and closure for their ordeal after having been put through a crime, followed by a period of victim blaming. These are points that I have discussed in §3.2.2 Victim experiences where I discussed Leukfeldt, E.R., Notte, R.J., and Malsch, M. 2020 who found that victims of cybercrime needed to tell their story to the criminal justice system and feel believed.

Case study 3. Charity for vulnerable people – Fraudulent invoice cybercrime

In 2021, the charity's director commissioned an elevator for a re-use store that provides a source of income for its philanthropic activities. A legitimate company offered to supply this for between £28 000- £29 000 and an agreement was reached. As a part of this agreement, the elevator would be paid for in three separate payments. The first payment was for £11 000 and constituted approximately 40% of the overall price. As a part of the modus operandi, the charity received, what was described, as a legitimately looking invoice with the appropriate features that corresponded to the local company. It was decided that the charity would transfer the money, which was justified in the following way:

> "So, we thought: 'Alright, we're in a bit of a rush here, so let's just agree to pay the 40% to this company."

Hence, a sense of urgency was created by the supplier, which prompted the charity to transfer the finances. Afterwards, the communication from the company became obscure. Suggestions were being made to the charity that the money will be returned to them so that they can wire it through an offshore account. I presume that the fraudsters were merely trying to buy more time to ensure that the money settled in their account irreversibly. However, at this point in time the money had already gone. Next, the local company's director's accent seemed strange and infantile. When the charity's director attempted to call the company, he did not manage to get through. Therefore, he travelled there in person during the weekend to confirm that it existed whilst commenting that:

> "At this point, to my shame, I was wondering around their offices with a golf club in my hand looking for somebody to batter over the head with the golf club."

Luckily, this situation did not result in any actual harm being inflicted to any of the interested parties. Rather, it transpired that the local company was legitimate, but the invoice was fraudulent presumably because they too had been breached. The charity for vulnerable people managed to get the money returned in full because it was caught by their bank in transit thereby making this an *inchoate cybercrime* (Bidgoli, M. and Grossklags, J. 2017).

Outcome: Even though this cybercrime did not result in any financial harm to the charity and the vulnerable people it supports, it did underline several concerning aspects about reporting. Firstly, whilst the bank helped return the finances, it supplied incorrect information about the fraud investigation department, which was only operable in England. This exemplifies that the problems with jurisdiction identified by Cross, C. 2018 in §3.2.2 Victim experiences in §3.2.2 Australia and Canada extend to the private sector. In the director's view this was due to the fact that:

> "whichever department they sent us to said: 'It's got nothing to do with us, we, this process only operates in England."

Secondly, the charity's IT support found out that the fraudulent invoice was sent from USA - Arizona, so they reported it via the FBI's website that was attached to that region. However, they did not hear back from the FBI. Thirdly, the charity reported the cybercrime to the Scottish Police on 101, which resulted in the director being interviewed. The director summarised the response from the local Police as:

> "They were very helpful. They were surprisingly informed. Two beat cops, two basic grade constables, they did seem to get a grasp of it. But they did admit that (...), they hadn't heard of something, they regarded as sophisticated as this."

As I managed to demonstrate, without the director's prompt response to all of the red flags, the charity would have lost its money because the reporting functions of interested agencies proved to be ineffective.

Case study 4. Charity for vulnerable people – Eastern European cybercrime

In 2022, the director identified that the organisation was not capable of accessing its network. Initially, they thought it was a network issue but after three days they realised that this was the modus operandi of a major cyberattack, which disabled their entire system. The access point remains unknown until this day. A ransom note was found advising that if the charity does not pay, then a significant amount of employees' personal data will be released onto the Dark Web. The IT company identified an Eastern European ransomware gang using RansomExx was behind the attack. The charity refused to negotiate and within a matter of days the personal data of its employees were released onto the Dark Web thereby fulfilling the threat.

Outcome: The charity did store third level backups as hard disks off site, which enabled them to recover their entire system within a matter of days. They reported the cybercrime to several agencies starting with the ICO, which I already mentioned in §4.1 SVC Introduction as punishing victimised corporations. The charity was obliged to report to the ICO within 72 hours. The ICO did not follow-up with them substantially. Secondly, they reported the cybercrime to the charity regulator OSCR who likewise did not offer any support. Thirdly, they reported the cybercrime to the Scottish Business Resilience Centre (hence: SBRC), who they found partially helpful but felt overwhelmed by the list of potential responders they were signposted to. Also, they have contacted Police Scotland, whose approach the charity's director described using the following words:

> "The Police said: 'We'll come up.' They came up and interviewed us (...) and, yeah, probably just: 'You'll need expert help to work your way through this.' Probably that was the best thing they said fairly quickly if I'm being honest."

Hence, a picture is starting to emerge whereby, once again, a charity is making an effort to report and resolve the cybercrime, but the help coming from the outside is very limited. In fact, as is the case is responsibilised societies, both Police Scotland and the SBRC restricted their input to advising the victim organisation to seek help from the private sector (Renaud, K., Flowerday, S., et al. 2018).

Case study 5. National governance structure – Christmas midnight cybercrime

In 2020, a member of a team of responders was called to attend the site of a major attack against a Scottish national governance structure. The perpetrators had chosen the time of the attack for Christmas. This modus operandi was suitable because they were assuming that the staffing levels would be low and defences against their attack would be limited. The cybercriminals accessed the structure's network fifteen days prior to launching their full-blown attack in order to tailor the virus to the victim's infrastructure. Then, the attack was launched precisely at one minute past midnight on Christmas Eve, which resulted in it being colloquially referred to as the "One minute past midnight trigger attack."

Outcome: As a result of the attack, the organisation suffered major damage to its systems. In the view of the responder, the staff were negatively affected post-incident. He highlighted that it was good that the staff asked for help and this was something he emphasised. However, he also spoke about the staff showing frustration from being pulled away from trying to recover the systems, which they should not have been doing in the first place. Secondly, staff experienced psychological distress because they were interviewed by Police under caution, which made them feel like they were getting blamed for the cybercrime. I argue that both of the staff's responses point to the government's (§2.2) responsibilisation agenda (Horgan, S. and Collier, B. 2016). Generally, people would not start tidying up a crime scene after a house burglary because they would know that that was the Police's job. However, in cybercrime staff tried to recover the attacked structure because they felt responsible for it and when they were interviewed under caution, they felt blamed.

Victims' attitudes to use of technology

As a part of this study, I was also interested to analyse how comfortable victims were with the use of technology to see whether they experienced any psychological obstacles that might get in the way of reporting cybercrime. All of the victims reported feeling comfortable with

technology and some of them could be described as expert. They generally used Google and Microsoft products in addition to purpose-built custom databases, the latter of which were targeted by cybercrime.

4.2.5 Factors improving cybercrime reporting

The following subsections supply a thematic overview of what is required to improve reporting in Scotland as provided by the three types of victims. The added value of separating by type of victim is that the three types of victims will report via different routes and based on different principles as I will illustrate.

Individuals

If individuals highlighted positive aspects of the reporting process, then it was with respect to the bank whom they found to be helpful because the institution resolved their issue materially speaking, which is in line with Garland, D. 2002a's theorising of how private institutions substitute for the police in responsibilised societies. Speaking from the perspective of what could improve the Police's reporting system the individual victims made various suggestions anchored in their experience. Two of the unrelated victims agreed that a designated case worker would have been helpful in terms of overseeing and following up on their issue. This tied to one of the critiques of the Fraud Squad where the victim highlighted that the service could have accepted at least an e-mail copy of the fraudulent HMRC letter and followed-up on it. It was seen that widely advertising a readily recognisable number would also get more people to dial in. As one victim put it in their own words:

> "I suppose I'm old fashioned. I like talking to people. I don't like things being digital and things getting lost in the mill stream. I'd like to feel like I'm dealing with one person (...)."

Nevertheless, this view was not shared across the board. Another victim did not see the solution in an in-person approach. On the contrary, they stated that an online tool might be preferable because it could send automated confirmations of the query being accepted and would be more reliable than a person who may not even answer the phone.

The Police guaranteeing the dissemination of crime reference numbers could also improve reporting as one of the victims reported to them for that very reason. In terms of the aftercare given by the Police, one victim referenced receiving a leaflet through the door to join a victims' support group. After care should be higher on the list of priorities for the Police if they want to improve cybercrime reporting because people are more likely to come forward when they associate the function with meeting their needs. However, as one victim noticed when they were not able to find an available officer, more manpower is required to resolve under-reporting. The victim observed by their own eyes that the local Police appeared understaffed. On a positive note, none of the victims felt discriminated by the Police during their contacts with the services.

Private institutions

One private institution argued that improved reporting is a question of appropriately marketing a telephone number for reporting cybercrime. Next, the caller would be relayed to an agent who would oversee their particular case until it was successfully resolved:

> "It would passed by the line to a detective or an agent or whatever you want to call it, who would take you on as your agent if you like, go through the whole process, keep you informed as to where they are and what they're doing."

In addition, one of the victims highlighted that they would have welcomed reporting via a link and receiving a series of bullet points of what to do next from the Police's website. Since, the victim recognised that much cybercrime is accessed via social media, they felt that there could be a reporting function connected to the Police there as well.

In terms of reporting to the Police, the victims would prefer to report to specialist Police. Hence, I argue that having confidence in the Police's specialist preparedness would increase reporting. One victim noted that they would report to the Police if they could rely on their support and ability to do something about it. One of the victims reported to the Police because they required a crime reference number for the Police. On a positive note, none of the victims felt discriminated by the Police during their contacts with the services.

Public institutions

There is a stark distinction in the reporting process in the case of public institutions, which follow, what HR terms, "a best practices approach." The latter pertains to managing organisations in accordance with a fixed set of rules which are seen as resulting in the best possible outcomes. Divergence from these rules is usually seen as malpractice, poor practice or even misconduct all of which are sanctioned in prescriptive way. Hence, some of the victims in this category reported cybercrime to the Police because their procedures required them to do so. Therefore, it makes sense to say that following procedures increases reporting to the Police. In the words of one victim:

> "It really was, again, a standard matter of procedure that when a crime happens, we contact the Police, so that it's noted with the Police. And for most things they'll decide to follow it up and they'll contact us for more information or they decide not to."

The same pattern of responses surfaced when another victims was asked the same question. They responded by saying that:

> "Why did I go to them? Because basically that's what our policies and procedures tell us to do, raise a major incident."

Another aspect of the reporting process that is apparent in the public sector is the multi-stakeholder approach. Thus, victims will report across a broad range of interested agencies. In some cases these agencies are helpful, in others they are passive. Whilst this process is not completely unproblematic, it is evident that victims' reporting and support structures are present. In my view, having fixed procedures which activate an entire support network definitely improves reporting. As one victim stated:

> "(...) there were concerns during the incident because of course we were working with the Scottish government, I do believe the Nation Cyber-Security Centre was involved at that stage and the insurance company plus the forensic team. So, we were doing work for the forensic team, not necessarily compliable with what the Police wanted us to do (...)."

Interestingly, public institutions offered significantly more positive feedback on the work of the Police that were involved in responding to the incidents. Again, I would return to the utilisation of the "best practices approach" whereby following a set of procedures instilled a vector into the situation which put everyone else in a better position to respond. Take the complimentary words by one of the victims:

> "I really can't praise them enough for the support they gave us throughout this."

One victim praised the local Police who were sent to his residence to take a statement:

> "They were very helpful. They were surprisingly informed. Two beat cops, two basic grade constables, they did seem to get a grasp of it."

Lastly, another victim highlighted the benefits of the community focus that Police Scotland take when responding to cybercrime by saying that:

> "They kept coming back asking if there was anything that they could do and Police Scotland are great at doing the whole community aspect as well so there was an element there for Police Scotland to learn so they were willing and able to help (...)."

Summary:

The three types of victims faced somewhat different trajectories during their reporting experiences. The Individual victims' experiences were mainly connected to the bank since in two of the cases, it was the latter that resolved their issue. The third victim was less fortunate and lost their money. All victims reported a similar amount of scepticism towards the Police. Next, in the case of Private institutions, both felt that increased awareness raising would improve reporting. The first one had a negative experience with the Police and the second one was not even aware of the option to report to them. Lastly, Public institutions fare the best out of all. Their "best practices approach" to governance results in mandatory reporting of cybercrime. The multi-stakeholder involvement sometimes adds a layer of support. As a result, their view of the Police is least negative out of the three types of victims.

4.2.6 Factors impeding cybercrime reporting

Individuals

The individuals found the Police unhelpful and their approach impeded effective reporting. For example, one victim went to great lengths to supply the Police with all of the relevant evidence for a cybercrime that was perpetuated from England into Scotland. In England, the Police pointed him to Action Fraud and Scotland's Fraud Squad they did not investigate as it was less than a seven figure sum. Another victim that reported the crime found the Police to be courteous but related their feeling that this was insincere and that there was not going to be any outcome to the issue he was faced with. As they said it in their own words:

> "But, yeah, I didn't feel I had a great deal of confidence in the Police following it up. But they made all the right noises and said they'd look into it whenever they'd hear again."

A critique of Fraud Squad was also noted by another victim who found their approach disengaged. They noted that the latter required them to take the physical copy of the fraudulent HMRC letter directly to the Police station, which made the victim feel as if they were just being passed on. In the end, that did not resolve the situation as the station's reception was unstaffed.

Lastly, there was an important psychological component referenced by two of the victims. Whilst there is no evidence of it impeding reporting, I think the reader can appreciate that a more exacerbated psychological state is likely to increase a victim's isolation. Specifically, one of the victims related feeling very anxious after the cybercrime whilst the other described their psychology as doubting reality. This is why it is important that Police Scotland act as a lighting rod for victim's who can feel so anxious and doubtful of what has played out that otherwise they will feel too vulnerable to come forward.

Private institutions

One of the victims of cybercrime was critical about the local Police whom he perceived as naive of the subject and this is the view that they had taken of the entire Police station at the time. This was an experience that extended to the specialist cyberpolice who, whilst getting in touch, acknowledged that there was nothing that they could do. Victims' experiences of negative outcomes post-reporting are likely to impede reporting.

The other victim did not even report to the Police because they did not have any idea who to report to and were too focused on fixing the problem but also because no sensitive data were leaked. This is a good example of a responsibilised victim (Renaud, K., Flowerday, S., et al. 2018), i.e. a person who sees it as their own responsibility to rectify the situation imposed upon them via cybercrime.

Public institutions

The victims noted more nuanced criticisms of the Police. For example, one victim did not view the response of the local Police as informed but saw their role as formal and spoke highly about the specialised Police. An important observation by another victim was that the Police were required to interview staff of the impacted organisation under caution, which resulted in emotional distress. This is an important point because whilst Police are following procedures, staff who feel responsible for the attack to begin with might experience disproportionate feelings of blame. Such amplified feelings can impede future reporting when staff are victimised as individuals for example. Lastly, a lack of centralisation resulted in the repetitive filling in of forms, which frustrated one victim:

> "The only bit I don't like about this process is the repetitive filling in over and over what's happened. So, I get a local officer to come around and I give them the details of the crime, hear them report it to the cyber-police, who may contact me and I've got to go through the whole process again."

Summary:

Victims agree that there are problems with cybercrime policing. One Individual victim could not activate their case even though they went to extreme lengths to collect the evidence. One Private institution did not receive sufficient support from the Police and the other was too responsibilised to realise that they could contact them. The Police were more involved with the Public institutions.

4.3 SVC Discussion

I have used this research to explore SVC in context with the purpose of improving cybercrime reporting in Scotland. I have compartmentalised SVC according to §4.2.2 SVC – Individuals, §4.2.3 SVC – Private institutions and §4.2.4 SVC – Public institutions.

The court cases and case studies from §4.1 SVC Introduction pertaining to **Cybercrime against individuals** were illustrated on cases of organised crime and a case of cyberfraud, which culminated in murder.

In the case studies of §4.2.2 SVC – Individuals do not show a high degree of harm, yet the data indicates a common denominator in organised crime. Take for example, §4.2.2 Case study 1 E-Bay Car Scam, where the victim exercised extensive due diligence before the purchase of the vehicle. They did not proceed in the heat of the moment when purchasing the vehicle. To the contrary, they gathered sufficient evidence for the credibility of the advert and subsequently sufficient evidence that a crime has taken place. Yet, this was not enough and the offenders managed to evade justice because of ineffective policing. In my opinion, this points to the operation of organised criminals. Similarly in §4.2.2 Case study 2 HMRC Scam, then again there is a pattern where the offenders tailored the scam to the specific victim and even supplied a physical letter, which also points to cybercriminals which have the intelligence, expertise and resources to run a complex operation sitting in between the cyber and real world.

When considering case studies §4.2.2 Case study 3 Credit card details theft A and §4.2.2 Case study 4 Credit card details theft B there is comparably less evidence to draw the conclusion of organised crime involvement. This does not necessarily mean that the latter were targeted by solo offenders, but there is insufficient evidence to hypothesise about their nominal size and organisation.

Yet, as I already highlighted in §3.1.2 Jurisprudence, researchers made a compelling argument that warned against prematurely labelling criminals as "organised crime" because the latter can only be applied to those instances where the offences are punishable by at least seven years in prison. Hence, a group of cybercriminals may be highly organised but in instances where their offences are not punishable by at least seven years in prison, it is better to charge them under different legislation lest the case collapses due to procedural error (Leukfeldt, E.R., Lavorgna, A., and Kleemans, E.R. 2017).

When it came to reporting, I interpret the victims data for what improves versus what impedes reporting via the paradigm of (§2.2) responsibilisation (Renaud, K., Flowerday, S., et al. 2018; Horgan, S. and Collier, B. 2016). Indeed, as demonstrated in §4.2.2 Case study 3 Credit card details theft A and §4.2.2 Case study 4 Credit card details theft B, victims associated the bank with improved reporting as the latter was the source of solutions to their problem since in two of the cases (Garland, D. 2002a), the victims received a refund since the attackers gained access to their banking details. Nevertheless, the bank is not the Police, instead the latter are §2.6.2 RNPAs – Banks, which also offer policing function. Candidly, the victims associated impeded reporting with the Police whose effect was low and symbolic. Once again, this is something I would expect to find in a responsibilised society where the policing functions were delegated away from the state.

Importantly, all victims reported via §3.3.1 Human To Human (H2H) approaches either with the use of mobile phones or alternatively in person. One victim would have preferred a more involved §3.3.1 Human To Human (H2H) approach whereas the other two were exhibiting a shift towards §3.3.1 Human To Machine (H2M) because they associated it with the prospect of receiving closure via a confirmation e-mail for their report.

The court cases and case studies from §4.1 SVC Introduction pertaining to **Cybercrime against Private institutions** are predominantly populated by cases where employees attacked

their employers, who were banks. In addition, two case studies were dedicated to transnational cybercrime against major companies operating in Scotland.

The case studies of §4.2.3 SVC – Private institutions are connected to transnational cybercrime, which originated from a .ru domain. Both victims were Small-to-medium sized enterprises with a localised clientele. §4.2.3 Case study 1 .ru Ransomware A was historic dating back to 2015 and illustrated how the problems with cybercrime reporting have been only mitigated rather than resolved over time. Nevertheless, I thought it was interesting to hear how the victim from this case went to great lengths to report the cybercrime and yet did not arrive at a satisfactory outcome. In §4.2.3 Case study 2 .ru Ransomware B the victim was not even aware that reporting cybercrime was an option and I formed an impression that they compartmentalised their experience differently than they would a physical burglary. This is illustrative of how a responsibilised victim will behave when they will feel that it is their job to resolve the consequences of cybercrime (Sommer, P. 2017). This is a point, which I highlighted in §3.1.2 Human resources by critiquing the research of the latter author.

In relation to reporting, I interpret the victims' data for what improves versus what impedes reporting as a form of movement away from responsibilisation. One victim associated improved reporting with higher degree of hands-on involvement from a dedicated agent ideally connected to the specialist Police. Hence, I am seeing traces of an initiative to put the ball back into the Police's court. The effects of responsibilisation are nevertheless observable. In the first case study, the victim received only symbolic support from the Police and in the second one the victim felt responsible for fixing the situation.

Importantly, the first victim reported via a §3.3.1 Human To Human (H2H) approach either with the use of mobile phones and in person. They would have preferred a more involved §3.3.1 Human To Human (H2H) approach by collaborating with a dedicated agent. The other victim was exhibiting a shift towards §3.3.1 Human To Machine (H2M) by stating that they would like to report via a hyperlink and receive a series of bullet points from the Police on what to do next.

The court cases and case studies from §4.1 SVC Introduction connected to **Cybercrime against Public institutions** are predominantly populated by varied case studies that combine attacks by an employee against the local government, but also transnational cybercrime where SEPA was attacked by Eastern European cybercriminals.

The case studies of §4.2.4 SVC – Public institutions are mainly connected to transnational cybercrime, where the interviewed institutions were infiltrated from abroad. It was evident to me that the level of competence involved in transnational attacks significantly varied whereby some of the attacks such as in §4.2.4 Case study 1. Educational institution – Poorly designed cybercrime and §4.2.4 Case study 3. Charity for vulnerable people – Fraudulent invoice cybercrime seemed as if they were carried out by inexperienced cybercriminals. I postulate this because in the first instance the cybercriminals forgot to attach a ransom note whereas in the second instance their over the phone interactions with the victim set off the alarm bells. To the contrary, attacks such as in the §4.2.4 Case study 4. Charity for vulnerable people – Eastern European cybercrime and §4.2.4 Case study 5. National governance structure – Christmas midnight cybercrime were carried out by highly professional cybercriminals who knew exactly what to do to generate maximum harm.

There is an important outlier, which is §4.2.4 Case study 2. Educational institution – Vendetta cybercrime, which was perpetuated with a very high degree of competence by a former student with a vindictive motive. I have included this case study as a cautionary tale because the victim in this case experienced increased stress due to various agencies engaging in victim blaming and misrepresenting the attack as a data breach. Hence, in this case, the staff of the attacked school were blamed for negligence.

In the context, of the still ongoing War in Ukraine, I cannot exclude the possibility of a moral panic towards cyberattacks perpetuated by Russia. In fact, in the past Lavorgna, A. 2019 from §3.1.2 Jurisprudence warned against a moral panic towards organised cybercrime. Consequently, the times have changed and societal concern has relocated. There is a chance that if the relationship between the West and Russia continues to deteriorate, then a Cold War akin paranoia can set-in in the area of cybercrime and people will follow their assumptions as opposed to the evidence. This could result in seeing Russian attacks behind domestic cybercrime, which would impede effective reporting. Yet, Martin, P. 2019 had warned that if Russia were to escalate its cyber-attacks against the West, then this could result in a conventional retaliation from NATO (p. 161), which is why it important to remain vigilant to the changes in cybercrime trends. Vigilance can play a role in being able to forecast a more substantial cyber-attack on critical infrastructure in the West.

In the arena of reporting, I interpret the victims data for what improves versus what impedes reporting as an analysis of comparably lower responsibilisation in the cases where the state is involved with helping itself. I am seeing how the following of best practices in reporting significantly improves reporting because it is mandated. In addition, the involvement from various stakeholders is substantially higher than in the cases of other types of victims. Like in the other two cases, impeded reporting can be associated with a more nuanced criticism of the Police whereby the victims were complimentary of specialists but critical of the regular Police officers.

Importantly, all victims reported via §3.3.1 Human To Human (H2H) approaches with the use of phone lines. There was no evidence of a shift towards other forms of reporting presumably because the systems that were setup provided them with immediate feedback about what was happening with their case during particular stages of the process. Hence, the victims did not require added closure.

4.4 SVC Limitations

This study used a relatively small sample. We followed the methodology of Ritchie and Lewis 2003 (p.108) who distinguished between non-probability (qualitative) versus probability (quantitative) testing. Non-probability is recommended for use in small-scale in-depth studies where units are deliberately selected to reflect features of the sample Ritchie and Lewis 2003 (p.78). The converse is true for probability testing. Therefore, this limitation is offset by using a qualitative analysis of interview transcripts.

4.5 SVC Conclusion

The purpose of this research was to explore SVC in context in order to improve cybercrime reporting in Scotland. I have started by providing the reader with in indicative introduction of the types of cybercrime perpetuated against the three types of victims with the use of court and newspaper evidence. Then, I have investigated victims' case studies and ways of improving reporting. I was able to draw on victims' experiences to articulate suggestions for improving reporting as well as a critique of policing. Then, I offered a discussion of the research within the broader theoretical frameworks as set out in the systematic literature review. Taken together, the research into SVC expertise highlights that a range of approaches from both human-to-human as well as human-to-machine will be required to improve cybercrime reporting in a way that accounts for victims as individuals. This will only be possible via a collective effort between the victims, academia, policing as well as other interested parties,

which will also reduce responsibilisation.

Chapter 5

Client-centred cybercrime training (CCCT)

The purpose of this work was to position academia as a problem solver in the cybercrime arena as opposed to merely a problem identifier. Most of the scientific literature prioritises cybersecurity training for university educated specialists thereby overlooking the usual victim - the SME (Small-to-medium sized enterprise). I connected with an interviewed victim **Private institution** from the previous chapter. The aim was to collaboratively develop, deliver and evaluate a client-centred cybercrime training as means of achieving closure post-attack, upskilling the workforce and improving cybercrime reporting in Scotland. In practice, 9 staff members engaged with the development of training, 6 staff members attended and 5 supplied feedback. In addition, 2 staff members were qualitatively interviewed. The results showed that the training managed to shift work practices to a limited extent and mainly served to raise staff's awareness of cybercrime, but did not improve cybercrime reporting. The UK government's responsibilisation agenda interfered with staff's ability to see Police Scotland as the go to place for reporting cybercrime. Future work should continue to engage collaboratively with victimised SMEs and create a government funded relationship between the academia and SMEs that will come to be viewed as the norm.

5.1 Introduction

Capitalising on the findings by Bada, M. et al. 2023 I have taken the case study approach (Chetty, S. 1996) to develop a bespoke cybercrime training for an SME that was attacked by ransomware. Even though Bada, M. et al. 2023 were mainly concerned with delivering training on Privacy Enhancing Technologies (PETs) I view their research angle as closely overlapping with cyber-resilience and cybercrime. According to Smith, S. 2023: "Cyber-resilience is the ability of a cyber system to recover from stress that causes a reduction in performance (p.32)." Bada, M. et al. 2023 critique that cyber-resilience frameworks are often aimed at technically minded people (p.278). However, the authors themselves then recruited SME participants from IT, science, technical activities and public administration. In other words, they have fallen into the limitation that they themselves highlighted. I, to the contrary, engaged with an SME from a deprived area in Scotland which employed staff with minimal cyber-resilience understanding thereby addressing a research gap. My approach reflects the assumptions of Chetty, S. 1996, who states that case studies investigate the SME's status quo within a real-life setting, the boundaries between the context and the research question are not clear cut and multiple sources of evidence are used (p.75).

If the reader recalls, in §4.3 SVC Discussion I have spoken about the fact that **Public**

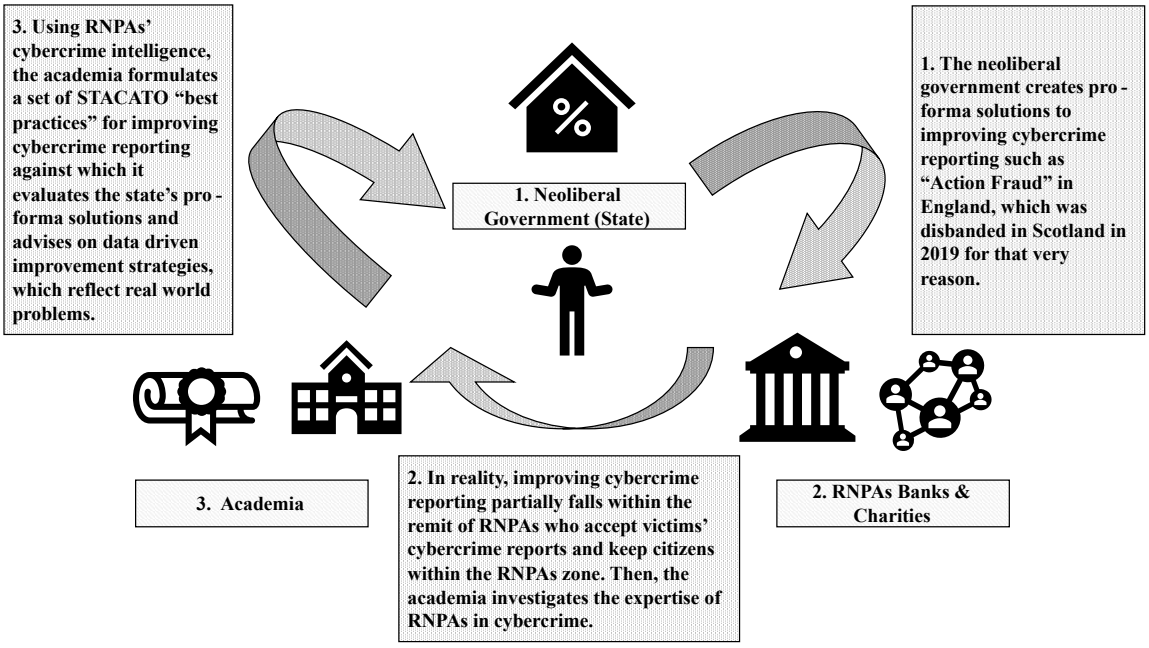


Figure 5.1: The role of academia

institutions have a higher level of protection due to lower (§2.2) responsibilisation and a "best practices" approach to cybercrime safeguarding. I have also connected the training to my main notion of "improving cybercrime reporting in Scotland" because as a part of the study materials the participants and I discussed the most effective ways of reporting to Police Scotland after a cyber-attack, which is a point I will return to throughout, but most specifically in the last paragraph of §5.2.1 Evaluation of training materials.

I theorise academia as an organisation that sits in between the state and other sectors and can play an important role in cybercrime harm reduction. This is because the latter has been responsibilised by the government to substitute some of its policing functions be it in terms of improving cybercrime reporting or victim aftercare. I refer to organisations with this acquired role as Responsibilised Non-Policing Agencies or RNPAs for short. They form an important part of the responsibilised landscape, which was why I have devoted the entire upcoming chapter to them in (§D.3) RNPAs Introduction. At this point it is sufficient to note that academia has simply taken on some of the state's responsibilities in victim aftercare. Hence, it can be a source of solutions in developing and delivering cybercrime training as I explain in Figure §5.1 The role of academia.

In the end only one victim **Private institution** agreed to collaborate with me on this training. The other one felt that it was not worth their time unless they were reimbursed whilst the **Charities** either did not respond to my offer or accepted but later changed their mind. Whilst the reasons for this remain uncertain, it could have partly been because these organisations did not trust that training could improve anything and also because they may not have wanted to discuss their cybersecurity vulnerabilities. Here also the distinction between **Private institution** versus **Charities** is not clear cut. The participating organisation is charity and hence it makes a surplus rather than profit from the collected income. Within, I continue to identify it as a **Private institution** and or SME for simplicity's sake.

Due to participant confidentiality it is not possible to supply details about the participant's business aside from several generic ones. The **Private institution** is an SME operating in the West of Scotland, which is an area that contains some of the nation's most deprived regions (Scottish Government 2020). Thus, SMEs are a vital source of employment and community

life. In addition, this SME is a legacy business, the activity of which spans several decades. Many generations of locals used the services of the SME and it came to be seen as a fixture of community life. A cyberattack on this type of business extends to the community too. Consequently, I felt that it was important to improve the organisation's cyber-resilience posture after it suffered an attack. This means that I wanted them to recover quicker, learn the lessons from past mistakes and display more secure behaviours in the future.

The subsequent section details current cyber-resilience training, which was uncovered via the same systematic method (Pickering, C. et al. 2015) described in §1 Introduction. The ProQuest database was surveyed with the use of Boolean variables "cybersecurity AND curriculum." The reason for selecting these terms stems from the reality that there is no agreed terminology for what Scotland refers to as "cyber-resilience" however the term "cyber-security" resulted in the surfacing of articles, which overlap with the semantic meaning of "cyber-resilience."

Therefore, a simple distinction between cyber-security and cyber-resilience is in place as these terms are both used throughout this chapter. In simple terms, cyber-security is related securing a system from an attack (Yang, S.C. and Wen, B. 2017) whereas cyber-resilience is related to the system's ability to recover from an attack (Smith, S. 2023). In this context, training is a pedagogical methodology that teaches people how to prevent stressors to the cyber system or reduce their effects post-onset. In our case, the stressors are cyber-attacks and cybercrime and the cyber system are the software and hardware components of an SME.

The results of this search are presented both thematically and chronologically. From a thematic perspective they are organised into six subheadings. The first three subheadings are based on the educational level and include: **1. Secondary School**, **2. University** and **3. Industry**. The second three are standalone subheadings: **4. Non-traditional learning**, **5. People with a disability** and **6. A Practical framework**. The contribution of this literature review for the client-centred cybercrime training is that it contextualises my empirical investigation within the global arena of cyber-resilience training. Notably, in my own empirical study I shift from speaking about cyber-resilience training to cybercrime client-centred training, because the attendees of my training were all motivated by having their organisations violated by cybercrime. The reader will notice that much of the cyber-resilience training is aimed at technically proficient people, which underscores the need for my research as it is geared specifically for practical and non-technological people.

5.1.1 Secondary School

Research looked at how to teach cyber-resilience subjects in secondary schools via game design (Kayali, F. et al. 2018). The researchers were interested in examining the effectiveness of games in teaching the pupils a range of IT skills. Overall, they found that games did not enable the students to learn about the subjects in a way that was more effective. Instead, games were useful in terms of raising the students' awareness of the topics under debate. With regards to cyber-resilience in particular, the authors found that games with a multiple-choice component were more effective. I have taken this into consideration when designing the organisation's own client-centred cybercrime training by making the activities as engaging as possible.

Appreciating the role of teachers in the education process of cyber-resilience from the middle and high school contexts, Ivy, J. et al. 2020 examined a program that prepared teachers in this domain. The program concentrated on inquiry-based learning, focused classroom disclosure, and collaborative learning based on the ideas of on GenCyber Cybersecurity First Principles and GenCyber Cybersecurity Concepts. The outcomes of this study showed that teachers were able to apply the principles referred to within to their roles, which improved

their abilities to deliver improved cyber-resilience education to their students. Even though this study was focused on middle and high school teachers, the material that was covered was too specialist for people without prior interest in this domain. I feel that if I used language such as "resource encapsulation", "domain separation" and the like, then this alone could have triggered a mental block in people whose primary interests laid in running an extremely busy SME.

Bolun, I., Bulai, R., and Ciorbă, D. 2021 developed their line of argumentation according to which cyber-resilience should be cultivated at school and throughout the continued phases of the educational journey. Moreover, people should be instructed to see themselves as a part of a whole class, working group or team. Hence, what can be seen within is that the social components are gradually starting to creep into a domain formerly populated exclusively by technological language. As I go on to demonstrate in subsequent sections, socially laden interactive exercise played a crucial role in the delivery of my client-centred cybercrime training, which was positively highlighted by the participants.

5.1.2 University

A study which analysed the learning needs of both teacher and students in higher education examined the vulnerabilities of these institutions (Bjorge, U. J. and Wangen, G. 2021). It found that personally identifiable information was most valuable to the victims and the criminals. This was followed by student grades, and administration data. The most regular attacks were in the areas of intrusion and malware. The sources of these attacks were organised criminals, state espionage and mistakes by other people. This information is useful in designing a client-centred cybercrime training because it mirrors the modus operandi behind the attack on the **Private institution**, which aimed at system's encryption and was operated from a .ru domain.

The lack of cyber-resilience skills is widely recognised by universities and has prompted some changes to existing curricula to cater to this need. In the research by Harris, M.A. and Patten, K.P. 2015 the authors tackled how to include cyber-resilience topics into the curriculum whilst not increasing the overall credit requirements. Harris, M.A. and Patten, K.P. 2015 solved this problem by prioritising cyber-resilience skills over other security skills, which they have moved into the lower levels. Whilst most university cyber-resilience training are likely to significantly exceed the needs and possibilities of SMEs, the authors make a noteworthy observation. They note that if you include this type of training, then you have to reduce the workload elsewhere otherwise people become overwhelmed. I have done my best to account for during my training delivery this by being as flexible as possible and allowing the company as much time as required to schedule a time that was most suitable.

Next, in research by Tagarev, T. 2016 the author examined the creation of a reference curriculum by NATO that should be used as a starting point for universities and training organisations in the field of cyber-resilience. The curriculum has four themes. The first theme serves as an introduction into cybersecurity. The second theme examines risk vectors. The third theme is aimed at good practices derived from international institutions and organisations. The fourth theme is concerned with ground management of cyber-security in the national context. Taken together, the reference curriculum is a useful benchmarking tool for countries interested in cyber-resilience education. Nevertheless, the underlying assumption for this type of research is that the education is for people who will oversee national cybersecurity structures, but that task is too large for any group or organisations. Once again, I am seeing the need for a client-centred cybercrime training specifically aimed at local SMEs.

Vain, J. and Kharchenko, V. 2016 related their findings from the Tempus Serien project, which aims to modernise university studies for MSc and PhD students in the areas of engineer-

ing and management. The MSc students will receive a review in challenges in dependability, cryptography, and risk analysis of security resilience among others. The PhD students will be taught systems security and resilience management as well as cloud management among others. Much like the research by Tagarev, T. 2016, the latter offers highly advanced skills that are unrelatable for people overseeing the running of a legacy SME.

Research has also examined the development of the cyber-resilience curriculum for undergraduate business schools (Yang, S.C. and Wen, B. 2017). They developed a descriptive cyber-resilience curriculum, which commenced with an introduction to information systems and continued with app development, IT infrastructure, data and information management, systems analysis and design, information systems strategy and management and acquisition policy. Yang, S.C. and Wen, B. 2017 also put forward elective courses that can be considered by institutions, which included technical electives such as digital forensics and organizational electives such as legal and ethical subjects. Yet a reader would struggle to find an example of how people with these skills could be paid for by SMEs on a tight budget, which underlines the need for my approach.

As most cyber-resilience university courses tend to aim at people seeking graduate employment as cyber-resilience specialists, Cabaj, K. et al. 2018 analysed the content of curricula in this domain. After examining courses across different universities, they found components such as an emphasis on cryptography, data protection, operating systems security, malicious code, vulnerability analysis and system security evaluation. Furthermore, topics such as defensive programming, secure software engineering, reverse engineering and malware were represented across some masters' programs. Taken together, the evidence suggests that universities across the globe devote significant resources to cyber-resilience education however most of it seems to be highly specialised for people wishing to work in the area.

Based on the findings of Marquardson, J. and Gomillion, D. 2018 hands-on practical exercises are best suited for developing cyber-resilience skills in graduates. Yet, the very exercises that enable effective learning to take place carry most risk to harm the systems on which those skills are practised. According to Marquardson, J. and Gomillion, D. 2018 the educational institution can take steps to manage these risks effectively. This can be done by putting 'preventive controls' in place such as adequate student training before the commencement of exercises. Also 'detective controls' should be in place, which will enable the course supervisor to detect risky activity. Next, 'corrective controls' can help mitigate the effects of an exploited vulnerability such as using effective back-ups. Subsequently, 'deterrent controls' can be used to sanction the students for not following secure behaviours such as expulsion from the course. These types of exercises are important in teaching students how to safeguard organisations, which can be adapted in principle to those working for Small-to-medium sized enterprises (SMEs).

Researchers have also noted problems with the heterogeneity of courses in cyber-resilience. Specifically, Liu, F. and Tu, M. 2020 noted that the differences between various university programs make it difficult to draw effective comparisons. This prompted them to program a database system, which allows for the quick categorisation and comparison of various cyber-resilience qualifications. Scotland faces a similar problem in terms of the cyber-resilience qualifications lacking a unifying framework, hence the implementation of such a framework into a program could support the resolution of this issue. Moreover, Scotland could take things a lot further and become a pioneer in designing training for SMEs, which are most vulnerable to cyberattacks.

In the next research piece, Pike, R.E. et al. 2020 explored a student-lead approach to the cyber-resilience curriculum from middle-school to university. The scientists focused on designing a curriculum that would enable students to organise their studies from complete be-

ginners to entry level professionals. The advantage of their approach is that students played a leading role in identifying their own needs and hence structuring their education through digital badging. Since this study was a pilot, data were not available as to how students structured their learning, but it is assumed that this flexibility would improve both their experience and educational attainment. I have engaged with the principles of this research in collaboratively designing my client-centred cybercrime training, which resulted in higher engagement from my participants.

In Dragoni, N. et al. 2021, the researchers highlighted that software design was extremely important in this respect, the appreciation and evaluation of threats, automated security analysis, and the testing and assessment of newly developed and externally acquired software components. This is an important piece of research that could improve the knowledge of graduates aiming for employment in the SMEs sector tasked with insuring that the cyber-resilience architecture of the company is fit for purpose.

Previous research has also focused on understanding university students' attitudes and behaviours after supplying them with cyber-resilience subjects into the curriculum (Khader, M., Karam, M., and Fares, H. 2021). The latter researchers put forward their own Cybersecurity Awareness Framework, which aims to guide the application of solutions to improve the cyber-resilience awareness of graduates at the university. This is a versatile framework that can be easily adjusted to the varies needs of the implementing university. I have used this approach to inform my flexible use of educational methods, which I have made significantly more accessible to the practice-oriented lay person working in an SME.

Next, Payne, B.K. et al. 2021 designed and delivered an interdisciplinary course on cyber-resilience based on the rationale that cyberspace is not populated by IT professionals alone. Rather it reflects all the diversity that is reflective of the inhabited world. Payne, B.K. et al. 2021 have argued that other professionals that seek to integrate similar courses into their curricula should follow their five recommendations. Firstly, developers should draw on real world examples when developing course materials, which are not contained within disciplinary boundaries. Secondly, the developers should practice what they preach in that the curriculum should be developed by professionals across the disciplines and should not be headed by an individual or a group from the same discipline. Thirdly, developers should think small as opposed to think big. This is because cyber-resilience is a developing and evolving discipline. Materials that are too comprehensive run the risk of becoming outdated very fast, shorter materials on the other hand, can be easily continuously updated. Fourthly, developers should be pro-active in encouraging the university to integrate cyber-resilience education across the board. Fifthly, Payne, B.K. et al. 2021 encourage interested readers to freely use their own downloadable materials from Cybersecurity, Technology and Society. Specifically, Module 4: Business and Cyber Security is extremely useful for students entering the job market, which has units focused on leadership, fundamentals in cyber-security as well as other items relevant for SMEs.

Bearing in mind the challenges brought on by COVID-19 research focused on ways to deliver cyber-resilience curricula online in a way that continued to bring value to university students (Taylor, B., Kaza, S., and Zaleppa, P.A. 2021). The researchers delivered on this aim by creating the CLARK (Cybersecurity Labs And Resource Knowledge base). The main purpose of CLARK is to supply a model for building the curriculum, the digital library system and the curriculum collections. Educators have used the CLARK model to build their curricula, which has aided the process of delivery during COVID-19 pandemic. More information on the CLARK project alongside its practical utilisation can be found at the Clark Center. This project offers a wealth of free information for different educational groups, but none that would be especially accessible for SMEs.

Returning to the subject of evaluating curricula previous research has sought to illuminate the best way to achieve this for cyber-resilience courses at business schools (Yang 2021). Utilising a meta-framework, Yang 2021 examined ten cyber-resilience frameworks and 380 topics and associated areas. Much like the previous research cited within, it was found that most cyber-resilience curricula favour technical topics over cyber-resilience topics. Hence, they neglect the social side of developing cyber-resilience and justify the need for research in the domain of SMEs.

5.1.3 Industry

Educational institutions struggle to integrate cyber-resilience curricula into their syllabus, which results in unprepared job seekers entering the workforce thereby compromising their employers' systems. Take for instance the study by Pusey, P. and Sadera, W.A. 2012, which examined teachers' preparedness to teach cybersecurity subjects to their pupils. It was found that their own skills are inadequate in this area and hence they struggle to impart the knowledge onto their pupils. This points to a systemic problem as it proves that teachers are ill-prepared to teach cyber-security due to their own gaps in knowledge. Consequently, educational systems will fail to prepare the workforce for being cyber-resilient in SMEs making the latter susceptible to cyber-attacks.

In contrast to the theoretical approach set out above, Knapp, K.J., Maurer, C., and Plachkinova, M. 2017 argue for greater links between the academia and the industry that offer cyber-resilience qualifications. In their study they have noted that a substantial amount of people working with cyber-resilience have acquired qualifications via the industry rather than the academia and hence they put forward a model, which derives the cyber-resilience curriculum from the industry qualifications. They have also argued that experiential learning and end of term academic projects should play a more prominent role in teaching cyber-resilience. This reflects the views contained within this research as well as its overarching aim to use academia as a part of the solution in the area of client-centred cybercrime training.

According to previous research even the high end specialised cyber-resilience curricula are struggling to keep up with the industry's requirements (Jones, K.S., Namin, A.S., and Armstrong, M.E. 2018). To identify the knowledge, skills and attributes for performing in this domain, the researchers conducted 44 interviews with cyber-resilience professionals. Based on the acquired data the researchers found that the participants acquired most of their skills in the industry rather than via the formal educational route. Critically, participants viewed topics such as networks, programming vulnerabilities and interpersonal communication as needing to be prioritised in the cyber-resilience curriculum. As a part of my research and client-centred cybercrime training I have placed a high emphasis on communicating with the participants in as accessible and non-judgemental way as possible.

The next research ties closely into the previously discussed topic. Johnson 2019 found that graduates from cyber-resilience courses have acquired theoretical knowledge on the subject but struggled to apply this to their workplace. Hence, she designed a module which would allow students to engage with work placements in the industry. According to preliminary analysis this increased students' preparedness to enter the job market and resolved some of the graduate employers complaints about unprepared graduates. This programme also faced a challenge whereby the internship providers felt challenged by the amount of hand holding that the interns expected them to do. However, it is considered that work placements during a person's degree are good place for students to build their confidence in a place of safety and nurture. I am including this research as it ties closely with the overall aim of my PhD, which is to develop research in close correspondence with industry's needs in Scotland. This

chapter in particular showcases the ability to do outreach work in Scottish communities which are usually forgotten by cybersecurity specialists.

In considering the context of new employees entering the workplace, Blažič, B.J. 2021 identified several areas that are not currently covered in cyber-resilience curricula, but are expected by employers, nevertheless. The areas required by employers are an insight into computer architecture, data, cryptography, networking, secure-coding principles, operating-systems internals, Linux-based systems, low level programming skills. However, it was also argued that people will be better suited for jobs in cyber-resilience if they are from a multidisciplinary background emphasising the need to recruit people with enhanced social skills. Whilst this work highlights the need for social skills in cyber-resilience professionals, it feels that its recommendation is pro-forma as it still heavily relies on technological skills. In this work I go on to demonstrate how I leveraged my social skills when engaging with practice-based professionals in a Scottish SME that lacked a cybersecurity background.

In the next piece by Zuopeng, J.Z. et al. 2021 acknowledged that employees entering into the industry are not adequately prepared in terms of cyber-resilience awareness, which is a source of vulnerability for their employer. Nevertheless, most cyber-resilience awareness training cannot meet this demand due to a lack of focus. To meet this need Zuopeng, J.Z. et al. 2021 have developed a framework that will help organisations develop their training. The framework works on a cost and benefit principle. The costs are specified into three categories: constant, complementary and compensatory. The benefits are specified into four categories: negligible, consistent, increasing and diminishing. The authors argued that this framework will aid companies designing cyber-resilience awareness training that will resolve basic vulnerabilities. From the perspective of client-centred cybercrime training, these types of frameworks are mainly good because they read well on paper. I will discuss this in more depth as I go on because I too have put forward a dichotomous framework believing that it will improve people's learning. However, in the (§5.2.1) evaluation, participants viewed this only as a mental exercise.

Blažič, B.J. 2021 considered the European cyber-resilience curriculum and the extent to which it corresponds to industry's needs. In her analysis she identified five pillar of cyber-resilience education, which are: Device-centric security, Network-centric security, Software System-centric security, Data/Application-centric security and User-centric security. Much like the previous research Blažič, B.J. 2021 suggests that organisational and human-centred aspects of cyber-resilience are neglected in curricula, which are components concretely addressed within.

5.1.4 Non-traditional learning

In a study that concentrated on the techniques of teaching cyber-resilience strategies, Hamman, S.T. et al. 2017 investigated the contribution of game theory to teaching cyber-resilience. Using an empirical set-up, the scientists managed to evidence that a two-hour training course on strategic thinking improves the reasoning of students about cyber-resilience and helps them anticipate the steps taken by the hackers. Whilst this course does seem to be for the more sophisticated pupils, the principles of game theory could be used to help in educating people reflect on suspicious content such as phishing links. I have done this in the current research using more rudimentary principles and approaches from impactful Finney, G. 2020's easily accessible academic literature.

There have also been suggestions in previous research that innovative out-of-class learning experiences are conducive to acquiring cyber-resilience skills (Hwee-Joo, K. and Katerattanakul, P. 2019). Here the authors observed the limited effectiveness of classroom teaching

methods and used empirical methodology to evaluate students' learning in an out of class environment, which entailed experiences such as an internship with the FBI. They found that out-of-class learning did not only improve cyber-resilience skills, but also made the learning process more appealing to the student. Therefore, the future cyber-resilience curriculum would benefit from integrating components that enable students to solve real world problems in a real-world context to improve their learning. The real-world context played an important role in this research too as the participants were keen to learn more about the modus operandi of attacks to make sense of their own experience, which was reflected in the learning materials.

In an article focusing on an evaluation of 'Capture the Flag Challenge (CTFC)', Švábenský, V. et al. 2021 examined the gaps in curricula that the cyber-resilience competitions address as well as those, which they neglect. They found that CTFC addresses skills in relation to technical knowledge such as cryptography and network security. However, it neglects a skills gap in connection to the human components such as social engineering and cyber-resilience awareness. This research lends further support for the current approach where I seek to fill this gap and help my participants understand cybercrime from the perspective of the criminal whilst capitalising on their social skills and critical thinking as important assets.

In addition, Workman, M.D., Luevanos, J.A., and Mai, B. 2022 explored the contribution of educational activities to cyber-resilience behaviours. Their study assumed that whilst traditional modes of classroom learning do not amplify cyber-resilience behaviours, gamified modes of learning do. They have sought to prove this empirically. Based on their results, it was evidenced that simulations of real-world situations improve cyber-resilience behaviours versus classroom taught materials. Nevertheless, the most improved performance was evidenced in the cohort, which received structured cyber-resilience simulations combined with live competitive tasks. The interactive nature of the client-centred cybercrime training complies with these findings and ultimately produces modest results.

5.1.5 People with a disability

When considering the cyber-resilience curriculum, it is crucial to consider research that pertains to individuals living with a disability (Inan, F.A. et al. 2016). Based on the findings from this research, visually impaired people with more cyber-security knowledge were less likely to use the Internet than those with less cyber-security knowledge. This is a good example for the principle that teaching someone cyber-resilience is not enough unless that person is given the tools to apply those principles safely. Hence, the visually impaired participants were disempowered from using the Internet by the very same knowledge that would encourage safe use among the visually healthy population. I was guided by this research when I designed the client-centred cybercrime training because I specifically probed the presence of any disabilities that would impede participation and offered extra assistance to anyone who required it.

5.1.6 A practical framework

In making use of what is already out there, Schaeffer, D.M., Olson, P.C., and Eck, C.K. 2017 applied their understanding of the National Institute of Standards and Technology (NIST) to the subject of cyber-resilience education and related their framework as a way of conceptualising the cyber-resilience curriculum. They suggested that students be developed in the areas of: 1) secure provision, 2) operation and maintenance, 3) protection and defence, 4) investigation, 5) collection and operation, 6) analysis and 7) oversight and development. Whilst the NIST is a highly respected cybersecurity framework, Schaeffer, D.M., Olson, P.C., and Eck, C.K. 2017 did little in terms of explaining to the reader how they would apply the seven areas to the cyber resilience curriculum. Hence, additional effort is required from the reader in terms of

accessing the NIST website and applying the material within onto the subject under review. In this research I aim to avoid this type of complexity by co-designing the client-centred cybercrime training in close collaboration with the attacked company to ensure a close alignment with their needs.

5.2 RESULTS

5.2.1 CCCT for victim Private institution

Development of training materials

Since, the literature review preceding this study revealed only minimally applicable pieces for the purposes of upskilling the staff of an attacked SME, a more individualised approach was required. I commenced by reading *Well Aware* by Finney, G. 2020 as a key piece because I came to see it as a transferable source of knowledge in the context of non-academic communities. It was Finney, G. 2020's theorising about cybercrime education that underlies much of my published training materials (Sikra, J. 2023a) as I have referenced within said publication. The latter is free to download as an A5 pre formatted Microsoft Word booklet entitled Client-centred cybercrime training for Scottish small-to-medium sized enterprises.

As I said in §5.1 Introduction the SME resides in an area with a higher level of deprivation. This meant that staff's level of cybercrime awareness was likely to be even lower than in an SME from an affluent region potentially due to limited resources. Therefore, I sought to ensure a particularly supportive approach, which was informed by psychotherapeutic theory. One might ask: "Why engage with psychotherapeutic theory outside of a clinical setting?" This is based on life experiences within communities faced with deprivation. In my experience, there is a much greater chance of anxiety and suspicion towards people coming from an academic background. People from such communities can often feel talked down to by academics, which may very well be based on prior experiences either from mainstream education or beyond!

Therefore, the training materials and approach were built after sampling people's subjective level of knowledge alongside desired improvement. The chances of increased negative emotions resulted in the need to assess their emotional states (i.e., anxiety, depression and confidence), which were rated using a Likert scale as captured in §C.3 CCCT Pre-training questionnaire.

The latter ties into the §C.4 CCCT Post-training questionnaire which are contrasted against each other as an indicator of progress more broadly discussed in the §5.2.1 Evaluation of training materials. Specific quotes from the forms were used to add detail to the training materials and approaches to delivery. Generally speaking, the staff noted that the need for attending the training emerged as a result of falling victim to an attack, as one staff member explained in their pre-training form:

> "As a team we recently fell victim to a cyber attack on our reception computer. We lost some files and documents unfortunately but this hacking also interfered massively with our membership system. We want to take part in this training to ensure this does not happen in the future. I am confident this training will equip us with the knowledge to identify any suspicious activity."
>
> —Participant 3

In terms of training delivery staff expressed a preference for an interactive mode of delivery, which was accommodated with the use of an interactive flip-chart that utilised sticky

post-it notes and colour pens as a part of group exercises. These approaches alongside the evidence collected from them will be discussed in detail in §5.2.1 Delivery of training materials, which also showcases photographic evidence in the forms of §5.2 Identifying your assets, §5.3 Understanding harm to your assets and §5.4 Safeguarding your assets.

In summary, the systematic literature review was of limited use for developing a training for an attacked Scottish SME that resides in an area of higher deprivation. Hence, additional resources were utilised alongside various sampling techniques to design a bespoke training booklet as well as customised pedagogical approaches.

Delivery of training materials

This section speaks about how the training materials were delivered thereby connecting pedagogical methodology with psychotherapeutic theory as indicated in §5.1 Introduction. When referring to training materials I am speaking about the booklet Client-centred cybercrime training for Scottish small-to-medium sized enterprises and interactive exercises delivered via an in-person session using a flip-chart. As a part of the training I have spoken to staff about the importance for reporting cybercrime to the Police as well as techniques that they could use to maximise the effectiveness of their complaint, which I have specifically described in said booklet on pages 29.-31.

Contracting: This term should be understood as derived from a counselling and psychotherapy contract. This is separate from either the §C.2 CCCT Consent form or the §C.6 CCCT Consent form which were the necessary requisites for the ethical delivery of this study. Rather, psychotherapy contracts, in this sense of the word, pertain to a collaboratively agreed set of expectations about how individual and group interactions shall be conducted to achieve maximum self-actualisation within a safe environment. Self-actualisation signifies the development of skills and talents that increase people's life satisfaction. For example, Hough, M. 2006 states that: "Establishment of a contract ensures that both client and counsellor understand the nature of the commitment between them, and that they work together in harmony (p. 281)." I contracted with the staff team when I presented them with a draft contract at the beginning of their session, which was captured on the flip-chart. I included the following items: 1. Non-judgemental (approach), 2. Honesty, 3. Time keeping (60 minutes), 4. Confidentiality within physical and research limits and left points 5.-10. open for inclusion based on staffs' preferences. I explained to them that in order to learn effectively everyone needed to feel to able to express what they thought or did in with regards to cybersecurity without the fear of being judged, which covered points 1. and 2. Point 3. related to the fact that the session would last for 60 minutes after which it would be completed. Point 4. regarding confidentiality noted that the SME allocated an open physical space for the training which offered some but not complete confidentiality as cleaners and clients were able to pass through now and again. In addition, confidentiality was limited by the fact that the training data would be published in a study. Then, I provided the SME's staff with an opportunity to add five more points to the contracts if it made them feel more comfortable. After a short pause, they stated that they were comfortable with the current contract and did not wish to make further additions.

Self-disclosure: This term should be understood as derived from psychotherapeutic practice, namely as a tool for building connection and increasing transparency (Yalom, I.D. 2011). It has been found that when a psychotherapist is able to become vulnerable by revealing something personal, perhaps embarrassing, it levels the playing field between him and the client in terms of power. As a result of this technique, which must be practised sincerely, the client will become more open and engaged. Nevertheless, Yalom, I.D. and Leszcz, M. 2005 warn that self-disclosure comes at a risk: "Every self-disclosure involves some risk on the part of the disclosurer —how much risk depends in part on the nature of what is disclosed. Disclosing

material that has previously been kept secret or that is highly personal and emotionally charged obviously carries greater risk (p. 343)."

I felt that it would be suitable to proceed with self-disclosure even before the Client-centred cybercrime training for Scottish small-to-medium sized enterprises to show the lay audience the human side of what it means to work in this field. The example I selected also served another important purpose. It was used to illustrate that you must be able to control for the dangers in your immediate environment before you progress to protecting it from "exciting things" like Russian hackers or foreign spies.

I spoke about an incident that happened during a departmental conference during my PhD studies. I was sitting towards the back of the room feeling uninterested which prompted me to use my phone to go through my e-mails. I was on my private account replying to a somewhat sensitive communication with a close friend. Whilst I got a strange sense that one of my PhD colleagues may have been looking over my shoulder, I put this down to suspicion. I resolved to trust him and not my instincts. Shortly after, I heard his voice from the back asking questions closely tied to the contents of my e-mails. He must have been reading them carefully. Shocked I looked back at him: "You've been reading my e-mails?" To which he replied with a couple of more inquisitive questions that only underlined the fact that he built up a half decent understanding of my personal communication. I did not do anything about it, but merely chose to make a point out of avoiding him.

I used self-disclosure as a way of explaining to the SME staff that I can also become careless which results in the leakage of sensitive communication. It was not my colleague's responsibility to safeguard my e-mails, but mine. I also wanted to get them thinking about their physical space and how they were securing it when processing the data of their clients. It was a successful strategy as it prompted them to provide a very honest account of how very cyber insecure their company actually was. This enabled us to formulate ideas for improvement based on the actual situation.

Dialogic approach: This term relates to the general notion that the training was delivered as form of dialogue from start to finish, which enabled staff to step in during any moment of the process and make changes. The dialectic approach was most apparent in the group interactive exercises, which reflected the Finney, G. 2020's applied and extended theory which I captured in Client-centred cybercrime training for Scottish small-to-medium sized enterprises. What follows is a breakdown of the three group exercises alongside my reflective account. In order to mitigate any legibility problems from the original flip-chart photographs, I have transfixed the latter onto a computer generated version for easier reading. In addition, in §5.2 Identifying your assets, bottom left corner, I have redacted the name of the company's operational software as it betrays the subject of its core business.

Exercise 1 Understanding harm to your assets: This interactive exercise was derived from Finney, G. 2020's idea that a company's assets ought to be divided in a way that prioritises the protection of the cardinal ones, which he also likened to the crown jewels. The aim of this exercise was to get staff to analyse which assets are priceless and which was are prized, which would enable them to structure their cyber-resilience.

When looking at §5.2 Identifying your assets the attentive reader will notice my spelling mistake on the flip-chart where I misspelled "priced" as "prized." This was picked-up by a staff member for which I am thankful. The reader can appreciate that the staff tended to view "Members" (i.e., people) alongside more transcendental values such "Our community" and "Reputation" as priceless. Whilst viewing equipment related items such as "IT Equipment" and the like as priced. This speaks to the community orientation of Scottish SMEs in deprived areas and the need for their enhanced protection from the side of the government as they are a source of jobs and services where there is a relative scarcity of both.

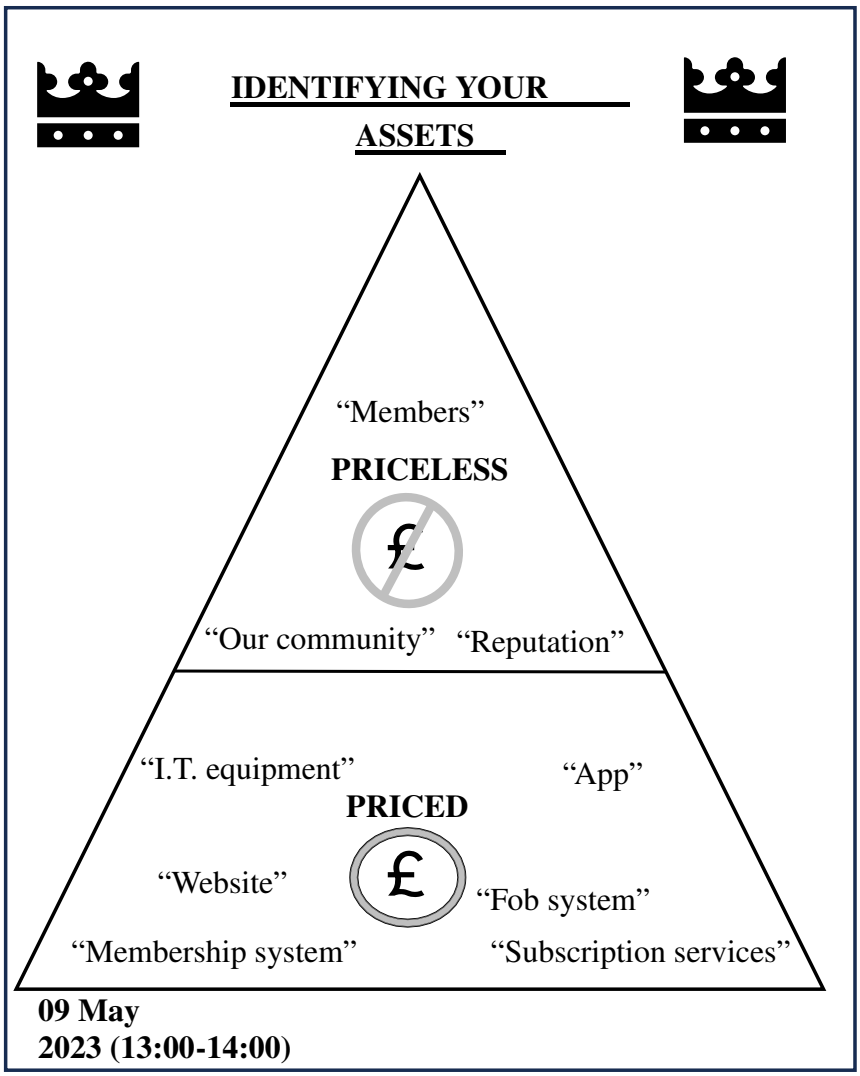


Figure 5.2: Identifying your assets

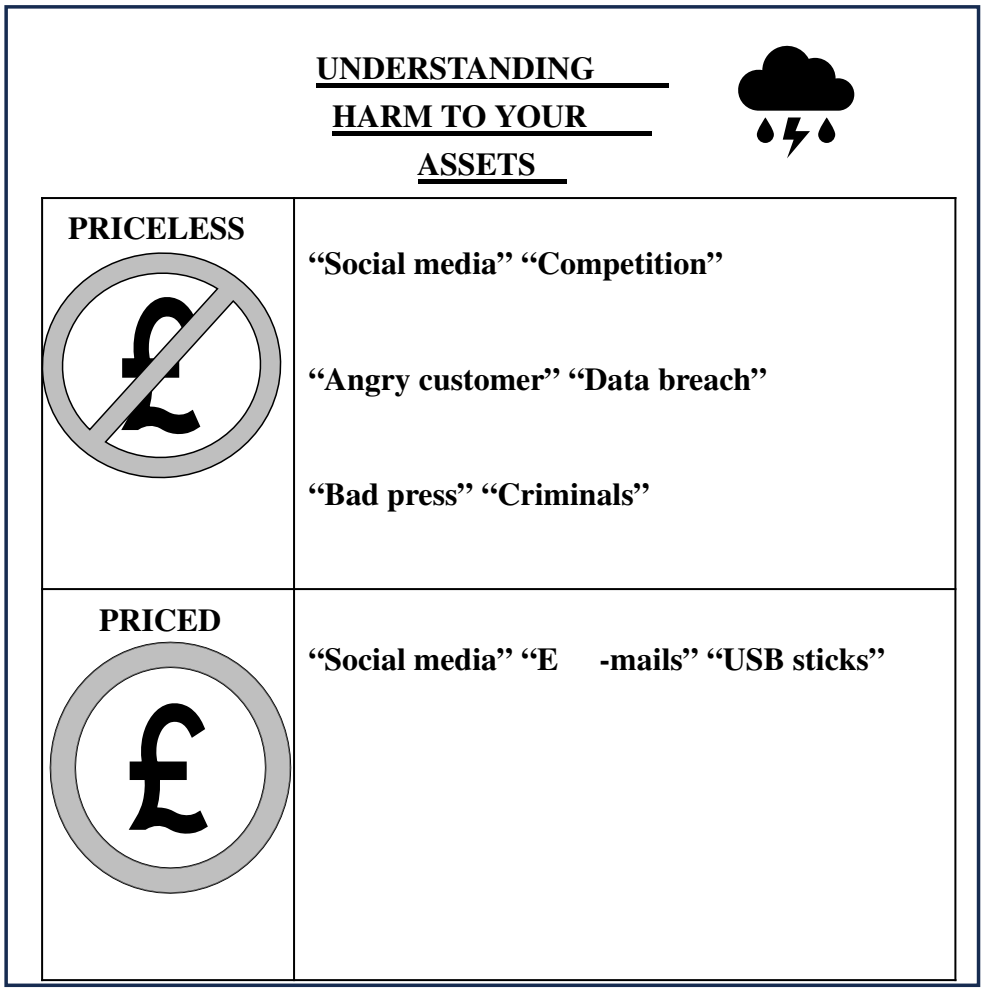


Figure 5.3: Understanding harm to your assets

In hindsight, there could have been more discussion about the connection between the priceless and priced assets because the damage to priced assets (e.g., website defacement) can trigger a negative reaction in the members who will be prompted to unsubscribe. Likewise, the priceless asset of “Reputation” can be connected to how technology is embedded within formal and informal managerial decision-making (Barney 1991).

On pages 8.–10. of Sikra, J. 2023a’s Client-centred cybercrime training for Scottish small-to-medium sized enterprises I present my own ideas and justification for priceless and priced assets. However, in line with the dialogic approach, I have advised staff to adjust these to their situation or simply prioritise the ones from §5.2 Identifying your assets if it suits them.

Exercise 2 Understanding your assets: As before, I used an adapted version of Finney, G. 2020’s theorising about assets in order to invite staff to think about how each could come to harm. Hence, I was aiming to gradually build up their cyber-resilience. Whilst I will not regurgitate the entire discussion, I will note several sources of harm a community based Scottish SME can experience.

As shown in §5.3 Understanding harm to your assets, in the priceless category, staff have identified “social media” and “angry customer” as sources of harm. This was related to their experiences of trolling, which required thoughtful crisis management. This placed the SME in difficult position as it had to retain its social media in order to communicate with its clients,

Figure 5.4: Safeguarding your assets

but also carefully resolve a trolling campaign. In regards to the staff's experience of trolling Barney 1991 draws attention to the social complexity involved in the use of technology in the firms. Barney 1991 describes that even though multiple firms possess the same technology, it will be the social substrate of the company that will engage that technology to gain competitive advantage. Lastly, their experience of "Data breach" was connected to the cyber-attack that prompted the current collaboration on the client-centred cybercrime training. Lastly, their experience of "Data breach" was connected to the cyber-attack that linked me with them to begin with.

On pages 11.–14. of Sikra, J. 2023a's Client-centred cybercrime training for Scottish small-to-medium sized enterprises I present a scientific understanding backed up by referenced terminology that helps people understand harm to their assets. However, in line with the dialogic approach, I have advised staff to adjust these to their situation or simply prioritise the ones from §5.3 Understanding harm to your assets if it suits them.

Exercise 3 Safeguarding your assets: This exercise is a theoretical extension of Finney, G. 2020's cybersecurity concepts. I required the SME's staff to think about cybersecurity as emerging from physical world security. Thus, they put together piles of items that constituted were a "REAL WORLD THREAT" alongside items that were a "REAL WORLD SAFEGUARD."

Then, they repeated the process for the cyber domain which related to activity that takes place online. I exemplified the results in §5.4 Safeguarding your assets. When I facilitated this exercise the staff were divided into small groups, which means that the safeguards do not directly reflect the threats either in numbers or in content. Nevertheless, it was an important exercise to trigger thought on the subject and future replications can consider how to make the process more effective so that, for example, if staff list "Social media" as a "CYBER WORLD THREAT" there is a matching solution "CYBER WORLD SAFEGUARD."

This could also be a derivative of the Concentration card game where the top sides of the cards would be labelled with "CYBER WORLD THREAT" and "CYBER WORLD SAFEGUARD" respectively and people would have to turn them around to find matching pairs, which could also incentivise staff by introducing a competitive component.

On pages 14.–17. of Sikra, J. 2023a's Client-centred cybercrime training for Scottish small-to-medium sized enterprises I present a more technical and analytical synopsis of how to best safeguard and SMEs assets. However, in line with the dialogic approach, I have advised staff to adjust these to their situation or simply prioritise the ones from §5.4 Safeguarding your assets if it suits them.

Evaluation of training materials

Self-evaluation: The ability to be a reflective practitioner in this domain is of the essence as trainees will pick up on implicit emotions and thoughts. In line with Yalom, I.D. 2011's recommendations about self-disclosure I commence with a reflection of my own processes during the training.

Firstly, it is important to note that delivering this training and interacting with the audience was probably the most unnerving part of my PhD to date. I felt very self-conscious about not being perceived as arrogant due to my professional background. This made me quite tense and I could feel myself blushing before I settled into the pace of the training.

Secondly, I should disclose my own experience of responsibilised self-rhetoric. Getting the training up and running proved arduous and despite the manager's best efforts took a lot longer than I felt it should have done. I felt that the SME's staff should take on my advice or face the consequences of another attack if they do not. This is exactly the type of counterproductive attitudes that Renaud, K., Flowerday, S., et al. 2018 and others have warned against in their critique of the (§2.2) responsibilisation agenda. In hindsight, I feel that this responsibilised self-rhetoric may have been a combination of fatigue from having to constantly adjust to the team's availability, but also a lifelong influence of a neoliberal understanding of security.

Quantitative data:

The quantitative data were evaluated based on the criterion that only staff members who submitted both §C.3 CCCT Pre-training questionnaire and §C.4 CCCT Post-training questionnaire were included in the analysis as they were the only attendees where progress could be fully monitored. Thus, 9 participants filled in the §C.3 CCCT Pre-training questionnaire, but only 6 participants attended the training, whilst only 5 participants completed §C.4 CCCT Post-training questionnaires. This brought the overall dropout rate through the process close to 50%. Only the 5 participants that attended the entire process from development, to delivery to evaluation are a part of this study even though the views of those that dropped out are implicitly included.

Their full pre-training and post-training scores are found in the §C CCCT Appendix as Participants 1.–5. Within, I am supplying a short commentary on the progress of individual participants alongside a selection of appropriate quotes from their returned forms. Some participants did not answer all of the questions on one or either forms.

§C.1 Participant 1: In this case, the participant rated their knowledge of cybercrime as 4 pre-training and desired to achieve an 8 post-training. Subsequently, they have rated their knowledge at a 6 post-training, which showed evidence of improvement. In terms of their affective response, their anxiety remained at a 2 before and after, whilst depression increased from 0 to 1 and confidence decreased from 4 to 3. They rated the trainer as 50% supportive. They found group-work helpful, they experienced the training as interactive and easy to understand, they stated that nothing was unhelpful and listed noticing a hacker and a scam as relevant to their personal and professional life respectively.

Here, it is evident that the participant underwent some internal process that they did not feel comfortable in sharing as their negative affectivity increased incrementally and their score for the lecturer's supportiveness was 50%, but they did not specify why.

This could be because, as according to Participant 3., some members of the group preferred to have their questions answered instantly as opposed to being told to wait. Alternatively, the training may have triggered unpleasant feelings connected to the cybercrime, which became transferred onto the trainer (Horwitz, L. 1964).

§C.2 Participant 2: In this case, the participant rated their knowledge of cybercrime as 5 pre-training and desired to achieve an 8 post-training. Subsequently, they have rated their knowledge at a 6 post-training, which showed evidence of improvement. In terms of their affective response, their anxiety increased from 2 to 3 from pre-training to post-training, whilst depression increased from 0 to 1 and confidence from 8 to 9. They rated the lecturer as 100% supportive. They found "discussing areas that could put our business in danger" helpful, they experienced the training as interactive and easy to understand, they stated that nothing was unhelpful and listed most and all of the training as helpful.

Here, it is evident that even though the participant experienced a small increase in negative affect, they also experienced an incremental increase in confidence. These emotional response are important because people may not be comfortable in speaking about their emotions, but they may be willing to disclose them via a survey.

§C.3 Participant 3: In this case, the participant rated their knowledge of cybercrime as 2 pre-training and desired to achieve a 6 post-training. Subsequently, they have rated their knowledge as 5 post-training, which showed improvement. In terms of their affective response, the anxiety increased from 4 to 5, depression remained a 0 and confidence increased from 1 to 5. They rated the lecturer as 80% supportive. In terms of what they found helpful, they stated that: "I enjoyed how engaging the training was as this massively helped keep my focus and not get bored." This participant also offered additional insight into what could be improved by stating that:

> "There were a few occasions where someone would ask a question and they would be told just wait I'm going to cover that later. I think it might have been more useful if the question was answered briefly and then by all means go more in depth later."
>
> —Participant 3

To me this highlights the importance of letting people make their discoveries along the way. The reason why I respectfully asked them to wait was in order to maintain coherence in to the material, but it was perceived as unhelpful. Instead, I could have highlighted that it was a really good point and that they were ahead of the game.

Moreover, the participant was able to connect the training to their workplace practice evidencing a degree of improvement:

> "Moving forward I will be sure to delete all emails which are suspicious or have links attached. In addition, I will be be mindful of data protection and asking

members to confirm their personal details before providing information of their account."

—Participant 3

Here, it is evident that even though the participant experienced a small increase in negative affectivity, they also experienced a 4 point increase in confidence.

§C.4 Participant 4: In this case, the participant rated their knowledge of cybercrime as 5 pre-training and desired to achieve an 8 post-training. Subsequently, they have rated their knowledge as 5 post-training, which showed no improvement. In terms of their affective response, their anxiety decreased from 5 to 0, depression remained a 0 and confidence decreased from 4 to 0. They rated the lecturer as 100% supportive. They found "discussing areas that could put our business in danger" helpful, they experienced the training as interactive and easy to understand, they stated that "learning how we can protect ourselves going forward" was helpful and that the "the exercise with sticky notes" was unhelpful although they did not specify which one as all the interactive exercises used sticky notes. They will change their work practices by "making sure member information isn't accessible to anyone else" and will benefit from the training in their personal life by knowing "how to prevent being scammed on social media."

§C.5 Participant 5: In this case, the participant rated their knowledge of cybercrime as 2 pre-training and desired to achieve a 3 post-training. Subsequently, they have rated their knowledge as 2 post-training, which showed no improvement. In terms of their affective response, their anxiety remained an unchanged 0, depression remained a 0 and confidence increased from 0 to 10. They rated the lecturer as 100% supportive. In terms of what they were able to take away for their job role and personal life, they conjointly listed: "Nothing new after the training." This comment alongside the 0 affective scores and rapid increase in confidence from 0 to 10 is indicative of a break-off pattern in responses Peytchev, A. 2009. According to Peytchev, A. 2009: "those who break off seem to put in effort, and larger or targeted efforts should be made to retain them (p.95)." Given that the questions pertained to emotional insight, they could have also made the participant uncomfortable if they were preparing for a completely theoretical training delivery.

Qualitative data:

As a part of this research, participants 2. and 3. who represented the executive functions were also interviewed as per questions listed in §C.7 CCCT Qualitative interview. Rather than supplying an answer to each question the general theme will be interpreted alongside representative quotes within the context of participants' questionnaire scores. The purpose of the qualitative interview was also to chart the participants' learning and retention over time. Hence, the training had taken place on 09 May 2023, the post-training questionnaires were filled out between 04-10 July 2023 and the qualitative interviews were carried out on the 30 August 2023, which is nearly four months after the training.

The interviewed participants highlighted the importance of training as an awareness raising tool, which has shed light on an important topic. Hence, a training as an awareness raising exercise was the dominant theme in their thinking.

§C.2 Participant 2 The answers of the participant complemented their scores from the post-training questionnaire. Specifically, they have stated that the course resulted in a small improvement in knowledge and awareness of how various assets ought to be safeguarded both in their private and professional life. This is reflective of the participants scores post-training which also marked a small improvement. The training has also helped the participant take an active role in improving the SMEs cybersecurity posture by:

"Simple things like logging out of computers even if only going away for a short

> period, more mindful of data breaches and how they could occur in the organisation and also of not being tempted to click on links that could have serious issues for the organisation's security."
>
> —Participant 2

The training also attempted to help participants formulate a cybercrime resilience strategy by getting to think about prioritising certain assets as priceless versus priced as I have exemplified in §5.2 Identifying your assets. I have specifically probed whether the participant was able to glean any benefit from this exercise to which they responded that:

> "I didn't particularly think of them in this way prior to the course although was aware of them as assets but it is useful to categorise them in this way and how to protect them."
>
> —Participant 2

This response conveys the theme of awareness raising that I have already touched upon, the participant does not go into any detail with regards to what they might do with this categorisation in practice, but they simply note it. Whilst awareness raising was not the goal of the training, the responses highlight the cognitive effects of the experience as opposed to behavioural change.

The participant's responses start to betray the effects of responsibilised thinking when they were asked about how they would report an attack either against themselves or against the company. On the one hand, they state that they would report the attack regardless of how it made them feel whether "silly" or otherwise. But when they were asked about how they would go about it, they stated that if the SME was attacked, then they would report to management and if they were attacked personally, then they would report to their bank. Hence, the participant did not mention the possibility of reporting to Police Scotland at all because they associated reporting with fund reimbursement. Instead, when faced with the same situation in the future, they would conduct themselves in an unchanged way.

§C.3 Participant 3 The answers of the participant complemented their scores from the post-training questionnaire. The participant has described their learning in terms of increased awareness, knowledge attainment as well as an improvement in confidence. With respect to confidence, as stated previously, their score increased from 1 to 5 based on the values listed in the pre- and post-training questionnaires respectively, which they retained until the time of the interview.

Just like their colleague, this participant has found the categorisation from §5.2 Identifying your assets helpful and interesting. Importantly, they stated that it placed them in a better position to protect them: "I didn't think of our assets as two separate entities but with this new perspective, I am more aware of how to protect them."

Interestingly, the participant's view of their own skills development has shifted since the time of the post-training questionnaire, where they explained a change in work practices. At the time of the interview, they provided mixed feedback by initially stating that:

> "While I don't believe this training has improved my skills, it has made me more mindful of the cybercrime that exists today and how often people fall victim to this crime."
>
> —Participant 3

However, then they followed up with showcasing how they engaged in cyber-resilience leadership in their SME by taking up initiative:

> "I would say I have been more cautious when it comes to data security and the protection of our passwords. For example, I find myself making a conscious effort to close down all tabs and membership accounts before I vacate the reception area, even if only for a short time. In addition, I have vocalised in staff meetings the importance of confirming a member's personal details before proceeding with membership updates etc."
>
> —Participant 3

This is interesting because on the one hand, the participant is stating that the training has not improved their skills, but on the other they provide a highly specific example of how their work practices were altered in a positive way. It is difficult to assert a specific reason for this incongruence, but it could be the case that some of the learning integrated on a subconscious level and the participant was not aware that what they were doing was the result of their training.

With regards to reporting cybercrime, much like their colleague, the participant notes that they would have always reported cybercrime. That is if their SME was attacked, they would report to management who would decide what to do next and if their private online banking was attacked they would report to the bank. Once again, there is no mention of Police Scotland. Instead, the responsibilised mindset prevails.

An important finding is that both participants feel that if the SME gets attacked, then it is first and foremost the company's responsibility to fix it. This is a way of saying that the private sector should look after itself. In cases, where people get attacked, it should be the banks (i.e., private sector) who looks after them. On a subconscious level, the state is out of the equation, the training did not alter the responsibilised mindset.

5.3 CCCT Discussion

The purpose of this research was to position academia as a problem solver rather than a problem identifier in the responsibilised landscape of cybercrime reporting in Scotland. This purpose was at least partially accomplished by designing the Client-centred cybercrime training analysed within which also filled a gap in knowledge in upskilling SMEs, but did not result in an improvement to cybercrime reporting in Scotland.

I devoted focused resources into co-designing the training in partnership with the staff of an attacked SME from §4.2.3 SVC – Private institutions. Based on my experiences with online education into the Ukrainian war-zone (Sikra, J. 2022; Sikra, J. 2023b), I felt that I was particularly well suited for this task and that the principles applied formerly would extend to the SME too. This assumption was only partially accurate. In truth, the enthusiasm for this training felt thin from the start and the collaborative nature of co-authorship did not seem to override staff's other priorities. Eventually, 9 members of staff compiled the pre-training questionnaires, which enabled me to design a series of interactive exercises as showcased in §5.2 Results as well as the booklet Client-centred cybercrime training for Scottish small-to-medium sized enterprises, which was distributed among staff in printed and bound format.

When it came to the delivery of the training, finding an appropriate time slot proved once again tricky due to the pressures faced by the business and despite the best efforts of management and staff. Once an appropriate slot was identified and I commenced with training delivery, I significantly drew from my former mental health background. I felt that practising self-disclosure (Yalom, I.D. and Leszcz, M. 2005; Yalom, I.D. 2011) about my own carelessness in data security I would level the power imbalance and enable people to open up. This

was successful and I was able to understand the extent to which the company was truly vulnerable. I tried to work with this knowledge thoughtfully throughout the training by helping people connect the material from the discussions with theory I was presenting. I was curious to see whether my self-disclosure would be reflected in the feedback that was collected after the training, but there was no mention of it. This suggests that it if it affected people's sharing of information, then it did so on a subconscious level.

I could see that the interactive exercises, which I exemplified via Figure §5.2 Identifying your assets, Figure §5.3 Understanding harm to your assets and Figure §5.4 Safeguarding your assets activated the group and even the inactive individuals became more engaged. This manifested as a suggestion from the group that it is is subdivided into "boys versus girls", which to me suggested an unintended competitive element. Future studies that build on my findings can include an element of competitive games since the ones discussed by (Kayali, F. et al. 2018) in §5.1 Introduction were no described as competitive. Whether or not they should contain a gendered element is up to the future authors. If mine were competitive and gender-divided, the women would have overwhelmingly won because of two highly motivated individuals.

I was very interested to see how the subdivision of assets into priced and priceless would help inform the company's defence strategy. Whilst the participants spoke about it in a complimentary way, they did not exemplify how this dichotomy informed their defence strategy. Thereby, making it more of an awareness raising exercise rather than a tool that they could take with them into the field and implement. This makes me think of the various concepts and frameworks discussed in §5.1 Introduction. If such a basic dichotomy is of little use to the hands on person, then more effort is required to translate cybersecurity knowledge into a language that is relatable. That extends to the language that is being used, as I revealed in the aforementioned section, it is far too technical and specialist.

Lastly, in the contexts of countries with a high level of (§2.2) responsibilisation, this requires to be accounted for. SMEs which have had to fend for themselves in the cybersecurity arena have adapted their instincts to this harsh reality. Opening themselves up to formal policing and investigation techniques can seem alien and anxiety provoking. This is why anyone that is interested in building upon my findings needs to do so with the realisation that they will come up against the government's responsibilisation agenda.

5.4 CCCT Conclusion

In conclusion, this chapter went beyond an analysis of the problem poor victim aftercare. Instead, a victim *Private institution* from §4 Scottish victims of cybercrime (SVC) was identified as a suitable candidate for a client-centred cybercrime training which was delivered post-attack. This was developed and delivered in close collaboration with the staff despite temporal constraints and high drop out rates. The main significance of the training was in awareness raising whilst some shift in working practices was evidenced via selected participants' quotes, but the training was not useful in linking the course material with improving cybercrime reporting in Scotland. The status of academia as a credible RNPA substituting the policing function of the state can be upheld alongside evidence of the responsibilisation agenda.

Chapter 6

Responsibilised non-policing agencies (RNPAs)

Responsibilised non-policing agencies (RNPAs) are varied entities within a society which the state uses to externalise cybercrime policing responsibilities. These expertise of these entities can be used to improve cybercrime reporting in Scotland.

My work is stationed within the broader international criminological literature about multi-agency collaboration in community as well as inter-institutional settings.

I have qualitatively interviewed 11 Scottish and 4 Italian RNPAs in order to understand what is needed to improve cybercrime reporting, but also to contrast the level of (§2.2) responsibilisation between the two countries.

The Scottish RNPAs were Banks, State-sponsored charities, Regulators of commerce and Private institutions, although this is not exhaustive. The Italian RNPAs were lawyers. All of these hold invaluable knowledge about victims' needs as well as expertise by experience.

Responsibilisation was nuanced in both countries and some cybercrime interventions are delivered by the state in both countries albeit in a more saturated way in Scotland.

Moreover, the recommendations of Scottish RNPAs were formulated into a "best practices" checklist that is summed up with the mnemonic STACATO. This checklist can be used to guide new state interventions and evaluate existing ones for the purposes of improving cybercrime reporting in Scotland.

The analysis contains an opportunity cost dilemma about the cost-effective way for improving cybercrime reporting. In addition, I justify the role of the academia in filling in the gap created by the drawing back of state interventions.

This work is unique within cyber-criminology due to its fit with existing theories and research on these organisations and its practicality for using their intelligence and expertise for improving reporting.

6.1 Introduction

Overview: This chapter has come about by way of a happy accident. Let me explain exactly how. Originally, I set out to recruit as many victims of cybercrime as possible with the aim of interviewing them about their situation and getting their perspective on what is required to improve reporting. However, as already noted in §4 Scottish victims of cybercrime (SVC) §2.4 Scottish victims of cybercrime (SVC) Methods the ethical process had to be resubmitted multiple times due to problems with victim recruitment. What if, instead, I spoke to organisations that supported victims and interviewed them about the intelligence they received?

Now, I would like to refer to the chapter by Garland, D. 2002a who on pages 121–124 spoke about the already mentioned notion of (§2.2) *responsibilisation*. Within, Garland, D. 2002a explains how, since the 1970s, the state has sought to unload some of its responsibilities for policing crime in general onto the private sector and community organisations.

Thus, I was interviewing non-policing organisations which contained intelligence on cybercrime victims whilst at the same time reading about how the state responsibilises organisations with the same profile to substitute some of its policing functions. I have made the connection and realised that I found myself in the midst of the situation described by Garland, D. 2002a. Hence, I opted for extending his terminology and paying homage to his intellectual legacy by describing these actors as *Responsibilised non-policing agencies*.

Whilst the singular term *RNPA* is an original extension of an existing theoretical concept, the research into organisations substituting policing is not.

Consequently, I commence with a §6.2 Scoping literature review on the subject in the area of criminology from an international perspective. Two types of studies will be discussed using case varied national case studies, the first will concern multi-agency work among actors that substitute the Police and the second will concern multi-agency work among state actors. As a matter of fact, Garland, D. 2002c on p. 202 argued that a comparison comparing countries such Canada, Norway, the Netherlands or Japan would importantly augment how the picture of how neoliberal economic reforms impacted levels of control. Within this short introduction, I managed to look Canada, Norway, the Netherlands in addition to others.

The first type of studies is relevant for understanding (§2.2) responsibilisation and the second for transferring lessons from multi-agency work into a responsibilised environment. Whilst the discourse is predominantly criminological as opposed to cyber-criminological, what ever starts with cyber- grows on the substrate of the real world. This is why any solutions that are effective within the cyber sphere are likely to bear some resemblance to their traditional precursors in the real world from which they are derived.

What follows is the methodological section describing the infrastructure of the study. This will be the first time I will be speaking about Italian RNPAs who I have surveyed as a part of my funded trip to the University of Pisa.

In the §6.3 Results I justify the value of speaking to Italian RNPAs, all of whom were private lawyers. However, it is also important to stress that making comparisons between pairs of nations that are based on convenience is not rare in research (Carla, A. and Nicolson, M. n.d.). The latter serves as a point of contrast for the level of responsibilisation in Italy versus Scotland as I sketch out in §6.3.2 Responsibilisation in Scotland versus Italy. Since the notion of responsibilisation can feel a bit abstract, I hope that by contrasting responsibilisation in different countries, I can illustrate this more concretely.

I will also include general and anonymised information about the content of RNPAs' cybercrime intelligence in §6.4 RNPAs collect and evaluate cyber-intelligence. Then, I present my own paradigm §6.3.3 Propagation of cybercrime explanation of the reporting trajectory from cybercrime perpetuation to reporting via the Scottish RNPAs to the state. The remainder of the chapter will focus on §6.6.1 Factors improving cybercrime reporting: STACATO and §6.6.2 Factors impeding cybercrime reporting as well as §6.6.3 Factors improving cybercrime reporting in Italy and §6.6.4 Factors impeding cybercrime reporting in Italy.

The §6.7 RNPAs Discussion serves to analyse the material in the context of evidence presented in the introduction, but adds further scientific value by arguing that the RNPAs place the state in the midst of an opportunity cost dilemma. The state can either use them to narrate an improving cybercrime reporting strategy, which is cheaper or the state can invest in specialised policing which is more expensive. Both options are viable with specialisation and volume of work bearing the brunt of the opportunity cost. Next, this section will discuss the

justified role of the academia in deriving the "best practices" strategy as an agency, which is well equipped to reduce the RNPAs zone and bring the citizen closer to the state by holding the latter accountable according to set principles.

Lastly, the §6.9 RNPAs Conclusion states that whilst responsibilisation poses problems to cybercrime reporting, the academia, which is closely connected to the state, can reduce responsibilisation by shrinking the gap between victims and the state. The academia can achieve this by effectively operationalising the RNPAs intelligence in the way I have within this chapter.

6.2 SCOPING LITERATURE REVIEW

Netherlands: In an empirical study by Terpstra, J. 2008, the author notes the impact of (§2.2) responsibilisation on Dutch security networks. Building on the work by Garland, D. 2002a he explains how the activities that were formerly monopolised by the Police are being delegated to other agencies as well as citizens as a form of moral duty. Therefore, the role of government is seen as evolving towards managing the activities of varied partners from both private and public sector whilst increasing the distance between the state and the citizens. As I go on to illustrate later on in this chapter, the Scottish state also uses RNPAs as a buffer zone between itself and victims.

Terpstra, J. 2008 set out to investigate a concrete manifestation of this phenomenon on the case of security networks in the Netherlands. The latter are a form of multi-stakeholder initiatives where different agencies join forces to fulfil a common aim. On this occasion, a security network addressing youth disorder in a neighbourhood was formed. The network was composed of citizens, police and local administration staff. The author found that these networks often generate an informal charismatic leader from the Police who takes over the agenda. With respect to the agenda itself, Terpstra, J. 2008 notes that this is usually somewhat vaguely defined in order to appeal to all of the stakeholders whilst acting as veil for the true crime fighting aspiration of the system.

Internally, the security networks are based on informal relationships which enable the smooth exchanging of information and intelligence on the relevant issues. In this particular case, the community police officer was praised for their commitment, drive and goal-directness. The participants viewed the police officer as being personally involved which contrasted with their sceptical view of the police management. This resonates closely with what one of the §4.2.3 SVC – Private institutions spoke about in §4.2.5 Factors improving cybercrime reporting when they voiced that they would like to have seen a designated agent overseeing their case.

United Kingdom: In a piece dedicated to understanding the effectiveness of partnerships in the area of cybercrime fighting, Levi, M. and Williams, M.L 2013 supplied an analysis of how various actors come together to achieve a common aim. Importantly, the researchers note that the majority of data about cybercrime come from the private sector versus the individual citizens, due to banks being incentivized to protect their business.

In fact, as I go on to demonstrate in §2.6.2 RNPAs – Banks this is truly the case whereby banks have a selfish interest in supplying the Police with cybercrime evidence to minimise the requirement to reimburse victimised clients. Levi, M. and Williams, M.L 2013 argues that the (§2.2) responsibilisation of the private sector is technologically motivated as the state does not have the access to the amount of high-tech equipment to address pertinent national needs in the area of cybercrime. As I will go on to demonstrate, the state only partially responsibilises §2.6.2 RNPAs – Banks because whilst they have the technology to compile detailed and robust evidence, the state does not have the staff to drive it towards successful prosecutions and

convictions. Nevertheless, this is not the only problem that faces partnerships where banks play a leading role. As Levi, M. and Williams, M.L 2013 highlight, there is an acute risk that as the number of private actors versus policing actors multiplies, the system will gradually shift from the common good rationale towards the market good rationale. Indeed, the authors found a strong correlation in cooperation between the policing and banking sector (r=0.69) and a weak correlation between the banking and charity sector (r=0.31).

In the light of my §6.3 Results, this does not have to be bad news. This is due to the fact that Scottish §2.6.2 RNPAs – State-sponsored charities are largely funded by the Scots government and occasionally even compete against each other for tenders. This means that the boundary between government and charity is blurred, but also that the charities engage in competitive behaviours akin to that of the private sector. Thus, the Scottish situation may have a more optimistic outlook in terms of partnership collaboration since it can be argued that many RNPAs collaborate with the state for the sake of the common good. On the flip side, this may mean that they are covertly involved in furthering the government's interest.

Sadly, as Levi, M. and Williams, M.L 2013 note, SMEs with poor cybersecurity awareness, may find it challenging to justify a business case for participation in these types of partnerships during times of austerity. This is something I have observed in §5.1 Introduction when the first from two the §4.2.3 SVC – Private institutions did not want to engage in the training unless they received funding for it and the other §5.2.1 CCCT for victim Private institution found it extremely challenging due to demands connected to its core business.

Norway: In a study by Bjelland, H.D. and Vestby, A. 2017 the authors examined the use of a multi-agency approach against an organised crime network, which was allegedly involved in human trafficking for forced labour, illicit work, a range of benefit frauds as well as credit card and identity thefts, which place this case at the intersection between traditional and cyber-enabled crime. The main contribution of this study is organisational in that it analyses the benefits and challenges that are entailed when various agencies come together to meet a common objective, which in this case was to bring down an organised crime network. The limitation of this study is that it captures relationships exclusively between state actors, which diverges from the (§2.2) responsibilisation theme that I pursue within.

In terms of actors involved; the Police were responsible for human trafficking, credit card fraud and money laundering, the Labour & Welfare department oversaw benefit fraud and illicit work and the Tax Authority investigated tax evasion. Multi-agency collaboration required the negotiation across various boundaries. Bjelland, H.D. and Vestby, A. 2017 identify that negotiations take place over the use of limited personnel and equipment, jurisdiction, and the access to common databases. In the Norwegian case, the administrative agencies have some coercive powers to fulfil their aims, which is parallel with the responsibilised role of §2.6.2 RNPAs – Regulators of commerce in Scotland as I go on to discuss later.

Bjelland, H.D. and Vestby, A. 2017's multi-agency approach is inspirational because the state actors coordinated their activities in the spirit of the saying that the goal justifies the means. Thus, they tried to avoid getting too caught up about their different approaches and legislative limitations. Instead, they resolved that it was not important whether the network will be brought down on a criminal or administrative level so long as it was dissolved and its assets were seized.

This meant that the administrative bodies could share intelligence that the Police could use for invasive operations, which in turn generated further evidence for the administrative bodies. Generally, the most intelligence sharing was informal since the agencies shared the same physical space, hence regular coffee meetings as well as overhearing people's conversations in the corridor resulted in a more fluid and cohesive collaboration. Nevertheless, this collaboration

was not unproblematic. For example, the administrative bodies spoke more positively about their work with the financial Police versus other policing functions, whom they felt did not speak the same language. This echoes some of my earlier findings from §4.2.4 Case study 2. Educational institution – Vendetta cybercrime who also found that the specialist Cyber-police were most helpful out of everybody involved in their cybercrime. The authors conclude with a concern that whilst this approach has clear merits, there is a risk of deputisation of partner agencies by the Police due to the latter having the greatest powers.

USA: In an important piece by Lum, C., Koper, C.S., and Willis, J. 2017 the authors explored the impact of technological improvement in the area of information and crime analysis (i.e., a shared website) on a multi-agency approach to improved crime responding and community relations. Specifically, I am interested in how technology could enter the RNPAs arena and improve reporting. The authors found that the Police valued the efficiency that was technology carried which they described as the "maximising of outputs with the fewest resources or costs possible (p. 148)." To the contrary, some officers felt burdened by the need to acquire new skills to navigate the automated systems, highlighting that learning new codes made their job more difficult. Moreover, specialised Police valued and capitalised on the data analytics that could be gleaned from the new system whereby regular patrol officers found it problematic. This connects to my argument in §4.3 SVC Discussion, where I highlighted that SVCs provided more positive feedback on the specialist versus regular Police. Lastly, Lum, C., Koper, C.S., and Willis, J. 2017 found that the Police saw value in technology's ability to improve their chances of catching offenders and closing cases rather than in preventative work. Therefore, if any system or approach were to emerge from the RNPAs intelligence, then this would have to be based on dishing out justice if it were to appeal to the Police's mentality as the ones catching the bad guys.

Canada: A cautionary case study by Sanders, C.B. and Langan, D. 2019 speaks about the pitfalls within a responsibilised society where the helping professions work alongside the Police as a part of a multi-agency approach. Whilst the described actors could be seen as belonging to the government, in Scotland some of these agencies would in fact be charity organisations sponsored by the government. The working model referred within is that of "Situation tables" which are frequent in-person meetings among multi-agency professionals to quickly identify a client's needs and deploy rapid interventions to meet those needs. The clients that are referred to Situation tables must be identified as being at high risk of victimisation or offending.

Members of Situation Tables that are from the helping professions have raised the critique that it is the Police that is determining what the most suitable interventions from mental health ought to be. The problem with this is the fact that the role of mental health is a non-judgemental approach to those in suffering, but the role of police is more focused on controlling and charging anti-social behaviour, which can lead to a conflict in organisational values. In fact, 85% of cases referred to Situation tables come from the Police who are scarcely involved in the evaluation or implementation.

This rings all too familiar with some of the work that is being done in Scotland as a part of the National MAPPA Team HM Prison and Probation Services Public Protection Group HMP 2023 which instils the collaboration between the Police and various agencies, including social care, in the management of sexual offenders in the community setting. In fact, often the social care agencies and other charities simply substitute the police by effectively supervising the offenders in the community. In practice, the charity organisations are made to feel responsible for the offenders behaviour as they have spend the most time with them whilst at the same

time not receiving any accredited training (or appropriate pay!) for dealing with manipulative and calculating behaviours that occasionally surface. This is also relevant for the study of §2.6.2 RNPAs – State-sponsored charities who are also responsibilised to operate within highly sensitive contexts whilst lacking the effective training and remuneration that the work requires.

Australia: Exploring multi-agency work on the case of governmental fusion centres, Bright, D. and Whelan, C. 2019 analysed this approach across participating organisations. Fusion centres are physical places which house representatives from various agencies with the aim of collecting and analysing information from a range of different sources. The main insight for my purposes concerns the trade-off between incorporating a range of different agencies versus a more selective approach to the inclusion criteria.

Namely, it was found that fusion centres that included a range of agencies increased the scope with which they could address various criminal issues, but had to dilute their goals to cater to the varied needs of all those involved. On the contrary, fusion centres that implemented selective inclusion criteria were able to retain a close goal-oriented focus and the expense of reduced scope.

This is relevant for the study of both §2.6.2 RNPAs – Banks and §2.6.2 RNPAs – State-sponsored charities because their mission statements are unconnected to improving cybercrime reporting. Rather it was the (§2.2) responsibilisation agenda of the Scots neoliberal government that placed cybercrime into their agendas. Thus, it is important to remain thoughtful about how to operationalise organisations with varied missions effectively in the domain of improving cybercrime reporting.

South Korea: In their work with the Police, Paek, S.Y., Nalla, M.K., and Lee, J. 2020 focus on the perceptions of the latter towards public-private partnerships, which is a form of multi-agency collaboration in the area of cybercrime. These partnerships are reminiscent of the role §2.6.2 RNPAs – Banks play in responsibilised Scotland as I go on to illustrate in Factors impeding cybercrime reporting. Paek, S.Y., Nalla, M.K., and Lee, J. 2020 found that as police officers gained more traditional work experience they were less likely to support innovative types of partnerships, which is suggestive of structural indoctrination. In addition, officers tended to be more sympathetic towards the partnerships in cases where they perceived the cybercrimes to be frequent and serious. Lastly, Police officers with a positive outlook on their own IT proficiency and cybercrime training needs were more likely to support this work model.

Conclusion: The Police appear to exert power over contexts where they have the upper hand from a legislative perspective but not so much in contexts of economic disadvantage i.e., towards banks. This means that when Police are faced with under-funded charities they may seek to operationally dominate the collaboration. On the other hand, when the Police are faced with a bank that has substantially more resources for tackling cybercrime than they do, then they will behave or equitably. This is an important insight as to what future interventions should account for in a responsibilised multi-agency environment. Thus, future interventions should commence with a formal written agreement about the distribution of power in multi-agency partnership, which will take priority over legislative or competitive advantage.

Table 6.1: Scottish and Italian RNPAs NVivo Coding

File classification	*Stage 1. Initial c.*	*Stage 2. Focused c.*	*Stage 3. Themes*
1. Scottish RNPAs	256	239	4
2. Italian RNPAs.	25	25	3

Table 6.2: Stage 2. Focused coding

File classification	*Improves reporting*	*Impedes reporting*	*Other*
1. Scottish RNPAs	127	21	91
2. Italian RNPAs.	11	6	8

6.3 RESULTS

6.3.1 Analysis

Firstly, the 15 interview files were classified according to the nationality of the RNPA. Thus, two File classifications were created: *01. Scottish RNPAs*, *02. Italian RNPAs*. Secondly, the File classifications were each coded in three stages. These stages were: *Stage 1. Initial coding*, *Stage 2. Focused coding* and *Stage 3. Themes*.

As I demonstrate with the use of Table 6.1 the raw interviews underwent three stages of coding. The numbers in each column represent the number of codes during each stage. As is evident, the numbers reduce significantly during each stage as a result of merging conceptually similar phrases.

During *Stage 2. Focused coding* shown in Table 6.2 I merged all semantically similar codes, but also various data was uncoded if I thought that the code was erroneous. Lastly, I re-organised the data into three main groups, which were: *Improves reporting*, *Impedes reporting* and *Other*. The first two groups pertained to those codes which could be discussed in terms of improving cybercrime reporting. The category *Other* contained data about criminality that was not otherwise classified.

In *Stage 3. Themes* shown in Table 6.3, the codes from the *Improves reporting* and *Impedes reporting* categories were further merged and reorganised according to their semantic similarities. Lastly, in the case of Scottish RNPAs a category *Case studies* was extracted from the category *Other* although the latter was preserved. *Other* contained very varied pieces of information from autobiographical commentaries to information of how RNPAs report cybercrime within their own infrastructure. In the case of Italian RNPAs the category *Other* was entirely replaced by *Case studies*. The codes from *Case studies* were organised in a way that would enable me to tell the story of cybercrime victims most effectively. One could question why I did not separate RNPAs according to their various types during coding. That is why did I not create a detailed File classification for 01. Scottish RNPAs based on them being: RNPAs – Banks, RNPAs – State-sponsored charities, RNPAs – Regulators of commerce and RNPAs –

Table 6.3: Stage 3. Themes

File classification	*Improves rep.*	*Impedes rep.*	*Case stud.*	*Other*
1. Scottish RNPAs	43	23	40	103
2. Italian RNPAs.	7	6	8	0

Private institutions. This is due to the fact that the RNPAs play a different role in the research of improving cybercrime reporting in Scotland versus that played by the cybercrime victims. Whilst it is important to know a little bit about RNPAs original vocation, their role for my research is for victim expertise, intelligence purposes and understanding the responsibilisation landscape. It is with respect to those roles that my research will analyse their data as opposed to picking them apart as research subjects.

6.3.2 Responsibilisation in Scotland versus Italy

As mentioned in §2.2 Theoretical framework: Responsibilisation, responsibilisation occurs when the state educates the citizens about the risks of cybercrime but does not engage with the victims if they fail to follow that advice through (Renaud, K., Flowerday, S., et al. 2018). Renaud, K., Flowerday, S., et al. 2018 criticised this approach because they argued that most people lack the skills to behave safely online, but also because an attack can spread from one person onto many computers, which is something illustrated by the cases of §4.2.3 SVC – Private institutions and §4.2.4 SVC – Public institutions who suffered various problems as a result of a single point of entry attack.

The purpose of this subsection is, to describe the responsibilised cybercrime landscape in Scotland. Using the data from Scottish RNPAs a nuanced picture of responsibilisation in Scotland has emerged. Namely, the Scots state goes somewhat beyond merely educating its citizens and disengaging thereafter. In fact, RNPAs – State-sponsored charities are funded via the state and some of these impart both education, but also signpost victims to the Police or other useful agencies after they have been attacked. In addition, as I have illustrated in §4.2.5 Factors improving cybercrime reporting victims spoke highly of the Scottish specialised Cyber-police, which shows that the state invests in robust policing interventions even though these are much scarcer than victims desire. Therefore, the Scots state somewhat responsibilises its citizens as opposed to completely responsibilising them.

This is the comparative difference between Scotland and the Tuscan region in which Pisa resides. At the time of my research (June - July 2022), the Italian RNPAs stated that cyber-security education was only available to the "younger generation", which were people under the age of twenty five. Hence, there is a risk that an unspecified portion of the workforce does not receive any cybersecurity training either via the state or state-sponsored charities as is the case in Scotland. Moreover, whilst reporting could be done both online and in-person, the on-line platform was undergoing maintenance at the time for an unspecified period and the office was scarcely manned, the latter of which sounds like a familiar complaint made by one of the §4.2.2 SVC – Individuals, who also could not report cybercrime to the local station as nobody was there. In addition, victims seek out the help of the lawyers because they fear legal con-sequences for cybercrimes that have impacted their companies, which effectively means that victims will go out of their way to pay a private lawyer to protect them from their employers after they were victimised. My research on victims thus far implies that this rarer in Scotland, but as shown in §4.1 SVC Introduction using the case of the Peebles Group (Lord Summers 2019), Scottish victims can also find themselves sued by their own employers.

To summarise, neoliberal governments such as the Scottish and Italian ones responsibilise citizens in the area of cybercrime, which means that victims have to bear the brunt of the consequences themselves. Responsibilisation in both nations is nuanced as are the comparative differences. Nevertheless, it suffices to say that the Scots state responsibilises its citizens to a somewhat lesser degree than the Italian state because of its distributed funding across a range of RNPAs – State-sponsored charities, which substitute some of its policing roles. This is not a phenomenon that was touched upon by the Italian RNPAs during data collection which, in

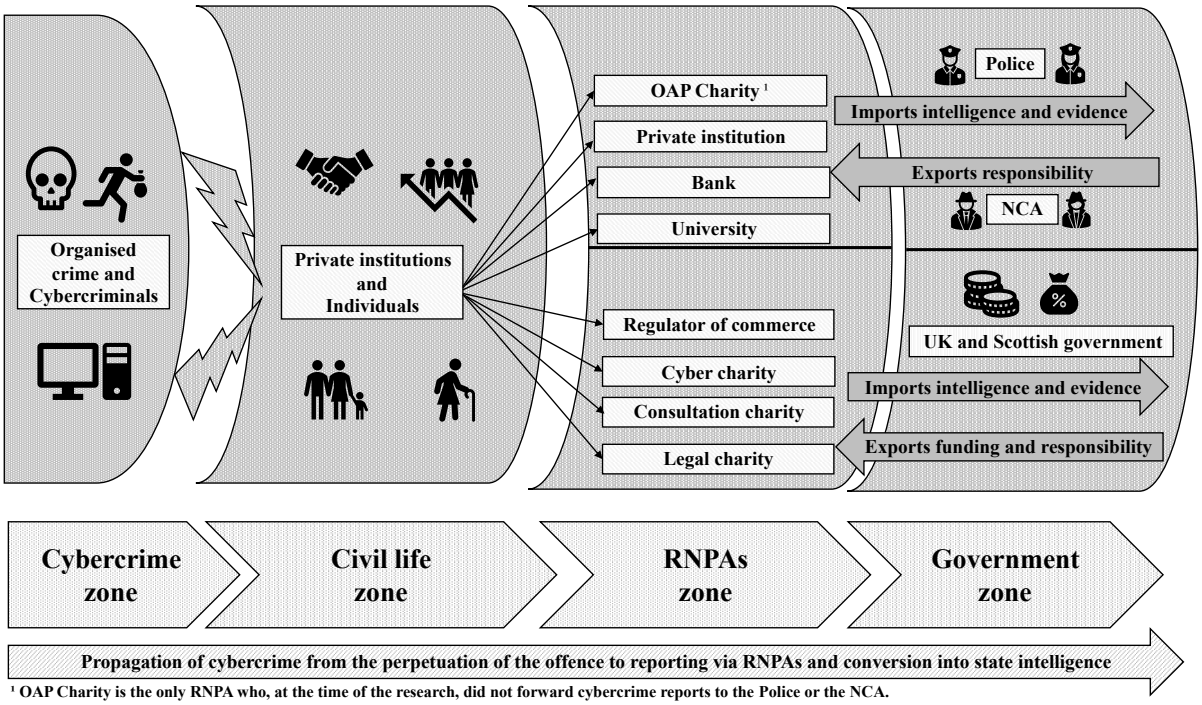


Figure 6.1: Propagation of cybercrime explanation

conjunction with other data, allows me to presume that it simply does not exist.

6.3.3 Propagation of cybercrime explanation

To better understand the responsibilised cybercrime landscape, I have developed Figure 6.1 to visually explain what goes on during the propagation of cybercrime. The term "propagation" is borrowed from neuroscience where it is used to describe the movement of electricity in between neurons during brain activity. Much like neurons communicate via electricity to operationalise behaviour, crime also travels via the fabric of society which becomes activated in particular ways.

Hence, starting from left to right, cybercrime originates from the Cybercrime zone, where Organised crime and Cybercriminals reside. These attack SVC – Private institutions and SVC – Individuals. Naturally, they also attack SVC – Public institutions, but these do not form a part of the argument concerning RNPAs because they report cybercrime according to a set of "best practices" as I explained in §4.3 SVC Discussion.

After the cybercrime was perpetuated in the Cybercrime zone, it propagates into the Civil life zone, where it impacts §4.2.3 SVC – Private institutions and §4.2.2 SVC – Individuals, which may or may not report the incident to other organisations including the Police. In line with the prediction of Garland, D. 2002a, some victims will report to private institutions and community organisations, which I have referred to as RNPAs and which are depicted in Figure 6.1.

Hence, based on the victim profile, the latter will transmit their reports into the RNPAs zone, which houses various RNPAs. Generally speaking, RNPAs respond to the victims by offering advice on how to resolve their situation and encouraging them to report the cybercrime to the Police as well. Under certain circumstances, RNPAs, which are banks will reimburse victims for the amount of money lost, which is generally well received as I have already illustrated in §4.2.5 Factors improving cybercrime reporting. However, as a rule of thumb, RNPAs will impart some form of post-victimisation education and care whilst compiling the

details of the cybercrime as a part of their own intelligence picture. As I have already noted on multiple occasions, the imparting of education is a fixture of neoliberal policies (Renaud, K., Flowerday, S., et al. 2018) and this principle extends to the activities of the RNPAs.

As I have shown in Figure 6.1 there is a black dividing line that splits the segments of RNPAs zone and Government zone. After the RNPAs have compiled the victim data into an intelligence picture, they then pass this to the government, which is where the meaning of the dividing line comes into play.

RNPAs that sit above the black dividing line (Private institution, Bank and University, but not OAP Charity) report to the Police and the National Crime Agency (NCA). Specifically, the Private institution, which is a first responder post-attack, reports to the Police via a back door in a way that passes on intelligence about cybercrime trends, but does not identify the clients. The Bank passes very detailed information about the cybercrimes against its clients to the Police and the University predominantly reports to the NCA in cases where it suspects that money laundering is occurring. The OAP Charity, which supports the elderly, does not report to anybody but instead advises its clients to report to the Police. This is a missed opportunity from the side of the Police to engage with an RNPA who could supply insight into the cyber-victimisation of this specific population.

RNPAs that sit below the black dividing line (Regulators of commerce, Cyber charity, Consultation charity and Legal charity) report to the UK and Scottish government directly although some of them also cooperate with the Police to a lesser degree. Specifically, the Regulator of commerce reports to the UK government because that is where it receives its funding from. The remaining RNPAs report to the Scottish government for the same reason. All of these charities apart from the Cyber charity have taken up cybercrime reporting over and above their mission, which is cyber unrelated, usually via a combination of pressing societal need and available government tenders.

As I have demonstrated, by the time the cybercrime moves from the RNPAs zone into the Government zone, it has been repackaged as intelligence about current trends. The state, along with its subsidiaries the Police and NCA, imports this intelligence and exports funding to all RNPAs apart from RNPAs that are banks.

One limitation of Figure 6.1 is that it paints an incomplete picture of what goes on in a responsibilised society where RNPAs substitute some of the functions of the Police. Hence, I did not interview all RNPAs that there are in Scotland and my sample is purely based on convenience.

This is especially true because RNPAs are a theoretical concept and, strictly speaking, a charity that rehouses stray dogs could be an RNPA if it found itself in a position where it was repeatedly receiving relevant intelligence on pet related cybercrimes (Levi, M. and Smith, R.G. 2021). Whilst this example is theoretical, the idea that any organisation in a neoliberal society can substitute the Police is not.

In conclusion, the propagation of cybercrime via the responsibilised neoliberal society is reminiscent of neuronal firing that activates a broad set of actors many of whom are not naturally disposed to deal with cybercrime. The RNPAs zone in particular acts as a buffer zone that protects the state from the concerns of the citizens and ensures that any information that passes through is sufficiently sanitised from the individual humanity of the complainants.

6.4 RNPAs COLLECT AND EVALUATE CYBER-INTELLIGENCE

I use this section to build a malleable picture of the cybercrime environment impacting SVC – Individuals and SVC – Private institutions using the intelligence gleaned from the RNPA Participants.

6.4.1 Changing cybercrime landscape

The representatives of RNPAs which I interviewed have been associated either with their specific organisations or a relevant industry for at least several years, therefore they were in a position to comment on how the cybercrime landscape has changed over time.

There was a consensus that cybercrime was more obvious in the past and has become more sophisticated in the present. It is important to question the impact of people's memory on this assessment. Whilst cybercrime would have certainly been less sophisticated in the past so was people's understanding of computers. Thus, it would be more precise to say that as computers evolve so does cybercrime, but it should not be inferred that people were less likely to get duped in the past.

With the evolution of computers, fraud migrated from postal to telephones to e-mails to social media accounts. This is in line with how people's use of technology changed with fake social media accounts being exploited for a range of nefarious cybercrime activities.

Back in the 1990s to 2000s, when cybercrime was in its infancy the RNPAs – Private institutions believed it to be more of an annoyance as opposed to a full-blown criminal industry. In those days it was mostly about hackers testing their abilities against a range of different users without causing the extent of harm which is commonplace today.

Time has also seen a shift in the victim profiles, which I will touch upon in more detail later. According to one of the RNPAs – State-sponsored charities past victims were often people suffering from some type of vulnerability whether it was mental or age related. Currently, highly educated and successful people are falling victims to cybercrime and everyone is seen as being at risk.

As I will go on to explain international university students, who form an especially vulnerable category, were reporting only one type of scam back in the 2000s. This was by criminals claiming to be from the UK Visas and Immigration requesting that the students transfer £700 as a landing fee in order to avoid negative consequences. Currently, students are targeted by a couple of scams both of which are more sophisticated and tailored.

6.5 Trending cybercrimes in Scotland

What follows is a sample of cybercrimes that have impacted mainly §4.2.2 SVC – Individuals and to a lesser extent §4.2.3 SVC – Private institutions. This is especially the case because §4.2.3 SVC – Private institutions are populated by §4.2.2 SVC – Individuals and the former will be affected by what affects the latter.

1. HMRC cybercrimes: As I already demonstrated in §4.2.2 Case study 2 HMRC Scam, cybercriminals commonly impersonate the institution to illicit compliance from SVC – Individuals. Nevertheless, a university, which I interviewed has noted how the HMRC pretext is used to target specifically Indian international students. In this case, the cybercriminals possess knowledge of which university accommodation is commonly occupied by students from India and they use this knowledge to send them threatening letters, which contain a sufficient amount of tailored information to appear credible.

2. Chinese government impersonation cybercrimes: The interviewed university has also noted a rise in scams targeting Chinese nationals. These are more detailed than the former HMRC Cybercrimes. In these cases, cybercriminals possess very detailed biographical data of the students in terms of which village they came from and who their family are. They use this knowledge to frighten students into transferring large sums of money.

3. Localised social media cybercrimes: What makes these cybercrimes stand out from other social media cybercrimes is that they appeared to be localised whereby the cybercriminals were using the social media to target people within one particular region. This is not a completely new trend as Collier, B., Horgan, S., et al. 2020 noted the localisation of most cybercrime. Whilst most cybercrimes can be perpetuated via the social media, the first real surge was noted during the COVID-19 pandemic when cybercriminals were advertising fake testing kits.

4. COVID-19 cybercrimes: The pandemic in general created an environment where cybercriminals flourished, because the unpredictable and frightening nature of the health emergency enabled them to target people with urgent and creative messages. Thus, governmental interventions were often mimicked to attract new victims. For example, victims fell for various bounce back loans scams, but also pet scams where they transferred a £200 deposit for a pet online, which they never got to buy.

5. Cost-of-Living cybercrimes: Once again, as the Cost-of-Living crisis continues to batter the UK citizens, cybercriminals have found ample opportunities to turn this adversity into a profit. Namely, criminals will roll out phishing campaigns requesting that citizens apply for the Cost-of-Living payments from the government, which is a benefit that does not require an online application. As a consequence, individuals will have their details stolen by the cybercriminals.

6. E-Bay cybercrimes: E-Bay is an online marketplace that allows various sellers from around the world to advertise and auction their goods. Cybercriminals go out of their way to learn E-Bay's terms and conditions to pull-off effective cybercrimes against their victims. For example, one victim ended up transferring regular payments to an E-Bay scammer over a period of four months because E-Bay's payback policy expires after that period, which means that the victim lost his money and never received an item. Luckily, one of the §2.6.2 RNPAs – State-sponsored charities pressured the bank to the point that they had reimbursed the victim after taking into account their vulnerability. Banks reimbursing victims is something I touched upon already in §4.2.2 Case study 3 Credit card details theft A and §4.2.2 Case study 4 Credit card details theft B where the bank both carried out the investigation and supplied the solution in line with its responsibilised role.

7. Energy Efficiency cybercrimes: In line with the Scottish government's net zero commitment the cybercriminals will exploit current ecological priorities to exploit citizens and undermine their impact. For example, individuals will get targeted via social media advertising claiming to offer window scrappage schemes as a part of an insulation deal. The individual is tricked into believing that if they apply to the scheme, they will receive window scrappage for free. In fact, there is no government window scrappage scheme and they are likely to have their details sold on and receive a set of windows at a price that is inflated by the hidden cost of the scrappage.

8. Crypto cybercrimes: Returning to social media again, these cybercrimes are promoted by influencers who claim to be making significant amounts of money from investing in crypto-currency. The latter will use social media to exhibit various luxury items to evidence the lifestyle that they were able to acquire via the investment in a crypto-currency scheme, which will serve the purpose of luring unsuspecting victims. The losses victims acquire range from

£500 to £100 000 with victim willing to pay over a protracted period of time as they slide into denial of the fact that they are being scammed.

9. Glaswegian cybercrime gang: Between 2015-2017, Glasgow based cybercriminals attacked predominantly people in England by impersonating banks and requiring victims to reveal their logon details. This case was curious because the cybercriminals' first language was not English although they were fluent in it. This meant that if they wanted to scam people in Scotland, there is a greater chance that their Scottish accent would be seen as insufficiently authentic, which would raise suspicion. But because they were attacking people in England, the victims were insufficiently tuned in to pick up that their Scottish accent was acquired.

10. Glaswegian COP-26 cybercrimes: During the 2021, the United Nations Climate Change Conference, which is more commonly referred to as the Conference of the Parties (COP-26) was held in Glasgow. This resulted in COP-26 impersonation cybercrimes being perpetuated on a localised level. Namely, there was a flurry of phishing e-mails sent around to people purporting to be from organisations associated with COP-26 requiring them to supply their details as a part of competition for a prize. This is a good example of how any event with a bit of emotional salience can be impersonated to trick victims into revealing their details.

11. Initial Access Brokers (IABs) cybercrimes: The IABs affect financial institutions in Scotland, their role is to penetrate and organisations network, i.e. gain access, which they then sell on to ransomware gangs, who will encrypt the victims' systems. Hence, the main purpose of IABs is to reduce the workload of ransomware gangs for which they are financially rewarded.

6.5.1 Insightful attacks on victims

Based on the intelligence gleaned from RNPAs, it is safe to say that cybercriminals are very apt at collecting intelligence on victims too and using it to tailor very insightful attacks against the systems they wish to harm.

Attacks on §4.2.2 SVC – Individuals: Increasingly, young people in their late teens and early twenties are getting caught out by cybercrime, which could be because they are overconfident in their use of technology (Collier, B., Thomas, D.R., Clayton, R., and Hutchings, A. 2019). I postulate that this is due to the fact that younger people confuse their ability to use technology, which is very high, with their ability to understand the broader ramifications of their online behaviour, which could be lower.

Cybercriminals are also psychologically in sync with people's spending and reporting behaviour. For example, they know that people will be reluctant to report a cybercrime with a value of £100 out of embarrassment, but will report a cybercrime of £100 000 due to having their existence threatened. People are also likely to report scams which they have identified before being exploited by them. In my case studies of §4.2.2 Case study 3 Credit card details theft A, §4.2.2 Case study 2 HMRC Scam and §4.2.4 Case study 3. Charity for vulnerable people – Fraudulent invoice cybercrime, I certainly formed the impression that people who managed to defy the criminals exhibited a degree of pride in speaking about their experiences. Cybercriminals will leverage this knowledge for low value high volume cybercrime. In addition, the latter also possess an understanding of how much money people are prepared to spend without going to see a car, which is the region of £5 000. This is shown in §4.2.2 Case study 1 E-Bay Car Scam where the victim paid £5 240 for a vehicle that he never saw and even though he engaged in robust due diligence processes, he was still scammed.

Cybercriminals have also found innovative ways to bypass some the banks' systems when misappropriating a client's finances. This is because banks have become more able at blocking payments that are done from unusual destinations. Consequently, cybercriminals use social engineering techniques to get victims to key in the details themselves and make transfers whilst they have the fraudster on the phone giving them instructions.

Attacks on §4.2.3 SVC – Private institutions: Cybercriminals are aware of when finances get transferred as a part of business and they use this knowledge to create normative attacks on companies. For example, organised crime will know that law firms usually transfer large amounts of finances on Fridays, which is due to house sales usually happening towards the end of the week. Hence, cybercriminals will use combined knowledge of the housing market and the behaviour of law firms to con companies out of sums in the region of £1 000 000.

Attacks on §4.2.4 SVC – Public institutions: Educational institutions and charities are increasingly coming under attack. Whilst the intelligence from the §2.6.2 RNPAs – Banks suggests that this is due to lower technical astuteness of staff employed at these institutions, the data I analysed earlier speaks a slightly different story. For example, §4.2.4 Case study 2. Educational institution – Vendetta cybercrime was carried out by a technically gifted and vindictive student against an institution, which prided itself in having the most modern IT systems. Hence, the assessment supplied by the banking interviewee may not universally hold.

Conclusively, cybercriminals and RNPAs are involved in, what could be called, a game of hide and seek whereby each collect highly specific information about victims whilst the first seeks to exploit it and the second use it altruistically.

6.6 RNPAs' CYBERCRIME REPORTING EXPERTISE

The purpose of this section is the utilisation of RNPAs expertise for improving cybercrime reporting to the Police predominantly in Scotland, but I have also included the data from the Italian study as a point of comparison. To increase the memorability of the factors that improve cybercrime reporting I have arranged them in a mnemonic **"STACATO"**, which is an abbreviation of each factors, but also a precursor for an assessment checklist for the effectiveness of reporting systems based on RNPAs intelligence.

The STACATO factors are a natural extension of the responsibilisation theory (§2.2) because they reflect an effort to introduce the "best practices" (Pfeffer, J. 1998) approach into a domain that is unregulated – namely the reactive multi-agency collaboration. As was already discussed in the §4.2.4 SVC – Public institutions, these are governed by fixed "best practices", which also improves reporting and state support. It is believed that the RNPAs can ultimately become more aligned with the state by the adoption of this approach as it reflects a policy-friendly framework that can be integrated within government research, policy and ultimately the law. Moreover, it is interesting how the expertise of RNPAs produced factors that are typically associated with the state, which further lends itself to the argument that they are unconsciously aware of their substitutional role in the cybercrime reporting domain.

Moreover, the STACATO factors are closely aligned with answering the research question because they clearly demonstrate how improved reporting can be achieved by effectively engaging with the responsibilised landscape, where multi-agency work substitutes the police with the resources that are readily available. Another benefit of this approach is that it was developed by agencies that have significant contact with cybercrime victims, which increases the credibility of their expertise. For example, RNPAs which are banks reimburse victims' funds, which enables them to form trusting relationships and gain greater insights into victims' needs.

6.6.1 Factors improving cybercrime reporting: STACATO

Sharing:

RNPAs have converged on the notion of creating a shared system that will be accessible to all RNPAs and the Police in a way that can triage the relevant intelligence and enables the development of a holistic picture. In the words of one RNPAS:

> "And I think on the other side of the reporting system it would need to be an accessible central repository that is accessible to all agencies who can perhaps act on the information within it whereas at the moment information does sit in silos in organisations and isn't shared to the best effect. We might hold information. The Police might hold information. The HMRC might hold information and in isolation it doesn't really look significant, but when it's all put together you get a better sense of what the problem is."
>
> —RNPAs – Regulators of commerce

Realistically, what I am seeing here is a drive towards centralisation of cybercriminal intelligence sharing. This can receive some support from Police Scotland due to the reforms, which favour centralisation (Jones, T., Newburn, T., and Smith, D.J. 1996). Let me return to the argument from §1.3 Police Scotland, where I compared and contrasted research favouring the municipal policing that was decentralised and community oriented (Wooff, A. 2015; Wooff, A. 2016) with research that favoured a centralised model of policing which is easier to scrutinise (Murray, K. and Harkin, D. 2017). In fact, a shared and centralised repository, which would allow access to RNPAs and the Police is both a centralist and democratic instrument as the different actors come together around the same table. An analogical version of this has already been developed by the NCSC and is available to interested professionals at Connect, Inform, Share, Protect, which is a portal that could be used to integrate the needs of RNPAs.

Transparency:

There was a sense that greater transparency is required in order to improve reporting, which would require the simplification and streamlining of processes in a way that is clear to everyone as currently different organisations report according to different principles, which is something I have sought to visually depict in §6.1 Propagation of cybercrime explanation. As summarised by one RNPA:

> "One that is transparent as to what you have to do in any point in time and who's doing what. (...) So, yeah just understanding, training, understanding and clarity. And simplicity as well I think there's a danger of making things over-complicated which would put people off from reporting so it has to be something that is easy to use and I suppose relatively quick to populate."
>
> —RNPAs – State-sponsored charities

Hence, what I am reading is based on an understanding that current reporting approaches are frankly a bit erratic with too many actors involved, which is a phenomenon that originates from the deputisation of the private and community sector organisations in cybercrime policing (Garland, D. 2002a) and results in the arena being defined by cybercriminals.

Advertisement:

There was a consensus across multiple RNPAs that any interventions that are to be carried out will only succeed if they are accompanied by a nationwide advertisement campaign. In fact, one RNPA event went as far as to design its own awareness-raising campaign based on the intelligence it collected from the victims that were reaching out:

> "One of the things we've done over the last four years since starting to deliver this service is using the data that we collect to inform the campaigns that we put out. So, in order to stay concurrent with the recently trending types of scams and cybercrime we use the information the consumers provide us to then disseminate that information to different stakeholders who we work with to make sure the information can go out there as quickly as possible."
>
> —RNPAs – State-sponsored charities

This denotes an important shift away from the more traditional conceptions of (§2.2) responsibilisation in cybercrime (Renaud, K., Flowerday, S., et al. 2018) because the RNPA is going further than merely educating the population about cybercrime. Rather, the RNPA is working in close collaboration with the victims and other stakeholders to tailor awareness-raising campaigns to reflect the fluid trends in cybercrime. This sounds like the responsibilised body is moving towards a more interventionist model of operation.

Another RNPA recognised that SVC – Private institutions do not associate cyber-victimisation with the same type of harm that they would incur during a traditional burglary. The interviewed professional made this problem clear in the following quote and argued that advertisement could lift some of the psychological obstacles victims face and improve reporting:

> "I think that if I break into an office and steal their laptops and a load of money out of the safe, they'd phone right away. However, if I scam them out of £2 000 and they recover their computers quite quickly or manage to stop it. Most businesses probably wouldn't even phone the Police for that. It's bizarre how they seem to think, I don't know, they don't think they can help, or they think it's cybercrime so it's someone that's in Russia or China or something like this, so let's not bother."
>
> —RNPAs – State-sponsored charities

In fact, as I have already exemplified in §4.2.3 Case study 2 .ru Ransomware B, the victim did not even know who to report the cybercrime to and was overwhelmed with trying to resolve the situation caused by attack via the use of a private IT specialist, who offered a degree of practical support, but did not advise about the details of the cyber-attack or why it happened and how it can be prevented in the future. This is why my approach to offering practical and tailored training to this as described in §5.2.1 CCCT for victim Private institution can be seen as an important step in terms of bringing these types of victims back into the picture by giving them the education and tools to defend themselves to a higher level in the future.

Centralisation:

As I have already noted when speaking about the need for a shared access to cybercrime intelligence, the RNPAs converged on the fact a centralised system is what is required. They hope to use this to marry the different loose pieces of data into one coherent national picture:

> "I think a centralised reporting system for Scotland as a whole. So, currently what you have is disparate sets of data from different organisations, so certainly we will receive scam reports but different people will go to Police Scotland to report a scam on 101."
>
> —RNPAs – State-sponsored charities

The world has experienced centralised cybercrime reporting systems. Namely, as I already highlighted on the case of UK's Action Fraud in §3.2.1 From elites to the masses, the system was critiqued for a tendency to prioritise high value and low volume cybercrimes (Hunter, P. 2008; Correia, S.G. 2019). Likewise, as I have demonstrated on the case of Australia's ACORN in §3.3.1 Human To Human (H2H), the system ended up posing various jurisdictional and transparency challenges (Cross, C. 2020a). Some of these problems could potentially be mitigated by Scotland being a much smaller country than the UK as a whole or Australia. This could hypothetically allow for a more fine-tuned instrument if the overall volume of incoming data is going to be comparatively smaller.

Automation:

RNPAs with a greater technological prowess have argued that improved cybercrime reporting could benefit from increasing the automation of the processes, which would in turn reduce the strain on human resources and enable a more accurate collection of data:

> "I think it would be great if it was automated, so I think the difficulty is the sheer volume of information that's being passed on to criminal investigations and the Police just means that the Police are swamped, they have way too much to do and they can't easily match cases together because they don't have the capability to do so."
>
> —RNPAs – Banks

Indeed, insufficient §3.1.2 Human resources to Police both traditional and cybercrime is something that was already discussed throughout this work. As Sommer, P. 2017 noted the lack of specialised cybercrime policing staff impedes their ability to effectively carry out their work with some forces needing to resort to up-skilling regular officers to become effective in cybercrime (Wilson-Kovacs, D. 2021). As one individual noted in §4.2.2 Case study 2 HMRC Scam, the Police station was not even manned when they came to submit their cybercrime report, which only further amplifies the human resources problems that Police Scotland faces during austerity.

Another RNPA saw the benefits of automation in ensuring a non-judgemental approach towards the victim:

> "It's been because in the US when you report things, you can report via websites as well, and people are becoming less and less used to using a phone for actually making phone calls and they are getting more and more used to engaging with bots. And what's been interesting in the states people have been starting to use the bots more because the bots have been non-judgemental and they've not had to deal with the human."
>
> —RNPAs – Private institutions

The importance of ensuring that victims are not judged is something that I discussed in the context of §3.4 SLR Discussion where I argued that one of the effects of the neoliberal governments' (§2.2) responsibilisation agenda can be that people are afraid to come forward and report cybercrime out of a fear of being judged.

Training:

A couple of RNPAs converged on the point that various forms of training especially towards §4.2.3 SVC – Private institutions would improve cybercrime reporting as well as improve the security posture of companies. In the words of one of them:

> "But education is a huge piece for the public at large and I think once you educate people about what they should look out for, then that should see a huge improvement in the types of, I suppose the scale of reporting in Scotland but also the quality of reporting in Scotland as well."
>
> —RNPAs – State-sponsored charities

This refers to the tailored type of awareness-raising already discussed earlier, which would enable the reduction of the gap between the state and the victims. One RNPA specifically saw this as connected to keeping up to date with the latest requirements to update passwords:

> "I suppose more education and training always helps. Having the time to keep up with the latest trends and emerging threats. Just today I was looking at, I was at a session for security of passwords, um, and I realised that the passwords I was using weren't as safe as they could be and made changes just today."
>
> —RNPAs – State-sponsored charities

I have fully acted upon this piece of intelligence within my dissertation by supplying a victim the victim from §4.2.3 SVC – Private institutions with a §5.2.1 CCCT for victim Private institution whilst also offering the same tailored training to the other interviewed victims.

Online:

Lastly, RNPAs shared the view that reporting via an online portal would improve public engagement. This was summarised must succinctly by the following RNPA:

> "An ideal reporting system for the public would be without a doubt online- a contact form. The last thing someone wants to do is be sitting on their phone on whatever social media platform and something happens or whatever and then have to come off that, find the number on a Police Scotland website and then have to. I'm off the website, why not just stay where you are and be able to just report something you know? The Police Scotland need to move with the time in terms of reporting mechanisms."
>
> —RNPAs – State-sponsored charities

This piece of expertise from the interviewed RNPA is corroborated by the view of one of the interviewed victims from §4.2.2 SVC – Individuals, who stated that an online contact form would be an improvement because they would have then received a confirmation that their complaint has been processed, therefore it is fair to say that this recommendation is victim-driven.

Summary: The RNPAs have put forward and justified what is required to improve cybercrime reporting to the Police in Scotland. Their intelligence and expertise was arranged into **"STACATO"** which is a mnemonic for a checklist, which can serve to assess state's interventions in this arena. The latter denotes a strategy which would enable shared access to information, transparent intelligence sharing, national advertisement, centralisation of systems, automation of high volume reports, cybercrime awareness-raising training as well as the possibility to report online.

6.6.2 Factors impeding cybercrime reporting

The following subsection offers an overview of factors that are impeding the reporting of cybercrime to the Police according to the RNPAs. Unlike the previous subsection, this one does not provide the reader with a mnemonic because I think that it is not possible to create a "best practices" checklist from what an improving cybercrime reporting strategy should not possess. Thus, this section serves as a warning rather than an assessment tool. The intelligence within is organised according to its originators.

RNPAs – Regulators of commerce: When victims reach out to the RNPA, they often do not know that they have fallen for a scam and are seeking clarifications. From the perspectives of emotions, the interviewees identified that victims experience embarrassment, which makes it difficult for them to file a report to the Police. In the words of one of the interviewees:

> "And there are certain sections of society that are reluctant to report probably because they're feeling embarrassed for falling victim and I think we need to work to remove that stigma so that people feel more comfortable coming forward and don't feel that because they've fallen victim of a scam, they're somehow not representative of their cross-section of society."
>
> -RNPAs – Regulators of commerce

Concerns were also raised about the resourcing of Police Scotland and the extent to which the non-emergency 101 and emergency 999 numbers cater effectively to the needs of the population under the effects of austerity. It is interesting how a responsibilised organisation is observing the tendencies that give rise to its own activities.

RNPAs – State-sponsored charities: Charity workers believe that the Police's unwillingness to take cybercrime reports seriously can result in under-reporting. For example, one worker mused how they were trying to report a scam on behalf of the client using the 101 number because the bank required a crime reference in order to reimburse the victim:

> "Now, when we speak to 101 and we speak to the advisers, if they don't think it's enough to send to an officer, that means that we then don't get an incident number. So that's what I mean about taking it seriously. (...) A lot of the times even an incident number won't be provided."
>
> -RNPAs – State-sponsored charities

This piece of intelligence fits very nicely with the points that I already raised in §4.2.5 Factors improving cybercrime reporting where I uncovered the connection between victims requiring a crime reference number in order to process a refund from their bank. Thus, this point is corroborated on the level of empirical evidence.

The system on which the 101 number operates was analysed by another interviewee who highlighted its limitations for cybercrime reporting. They stated that victims often make erroneous assumptions about reporting cybercrime, namely that the Police which will attend the incident will wipe all of their data during the course of their investigations. Callers can also have an expectation that if they call the 101 number a specialised Police officer will attend the incident and may be surprised to find a regular uniformed officer. Lastly, in their own words:

> "That said, it can be difficult for someone to get through the 101 system. They're often held for 10-20 minutes and frustration sets in and they don't bother."
>
> -RNPAs – State-sponsored charities

Moreover, one charity worker found themselves in a revolving door situation with the Police when they tried to support a client to report a cybercrime. As they tried to explain:

> "I don't want to speak ill of the police. However, how helpful were they, is a double loaded question. The police have a very kind of stance of speak to your local *[name redacted]*. So, even though we had reported it, nothing normally happens and if a client does report it to the police without going directly to us and they will normally be told speak to your local *[name redacted]*."
>
> -RNPAs – State-sponsored charities

This is a good example of how the state keeps the citizen at arm's length as I have already demonstrated with the use of §6.1 Propagation of cybercrime explanation where we are seeing the Police refusing to accept a cybercrime report and instead insist on keeping the victimised citizen within the RNPA buffer zone. Here they cannot threaten the state with their needs.

Furthermore, an interviewee referenced varying legal opinions on whether a case falls under civil or criminal law as impeding reporting to the Police. Namely, they found that when they support a victim to make a report about cyber-enabled fraud, the Police take the view that this is a commercial dispute rather than a criminal matter, which both impedes reporting, but also gives an opportunity to the offender to get away and carry on with their nefarious activities.

Legal challenges can also be connected to the fact that whilst the selling of counterfeit goods via social media is a form of cyber-enabled crime, the purchase of these goods is not illegal. This is unlike the case of drugs where both the sale and purchase of narcotics is illegal. Therefore, the consumer, who may or may not be aware of the fact that they are enabling a cybercriminal, can end up using goods, which are faulty and dangerous.

RNPAs – Private institutions: The interviewee from this category merely corroborated the intelligence from the other RNPAs. They stated the reporting is firstly impeded by people not knowing that they have been victimised. Secondly, people do not want to make an effort to report the cybercrime and thirdly the feelings of embarrassment pose an obstacle to reporting. The company also found that time-lining can pose challenges for effective reporting. This happens when reports come from different parts of the world and the evidence needs to be consolidated so that it can be further processed. There are particular legal and technical challenges to collecting evidence from the same time across different time zones, which can pose obstacles to reporting in cases where access to relevant software is not available.

RNPAs – Banks: According to the interviewed bank, fraudsters are very quick to adapt their technology in order to come up with new attacks. This poses challenges for both reporting and Policing because the Police will not have the financial resources to purchase the technology that is required to keep up with the cybercriminals' constantly evolving modus operandi. The bank also found that the Police will not investigate fraud that is under a certain financial amount because they do not have the resources to do it. This frustrated the bank because they handed over all of the evidence required to catch the offenders, but due to austerity the Police would not deal with smaller cases. This is a frustration that was already echoed within the §4.2.2 Case study 1 E-Bay Car Scam where the victim supplied the Police with the required evidence but jurisdiction issues coupled with the relatively small loss resulted in no action being taken.

Summary: As I have demonstrated, victims often do not know that they have been attacked and even if they possess this knowledge they experience embarrassment and stigma. RNPAs showed insight into the effects of austerity on cybercrime policing highlighting the scarcity of resources during 101 calls. The acquisition of a crime reference number is influential in cybercrime reporting and when victims feel turned down, their trust in Police's ability to solve their

problems can be impacted. From the perspective of jurisprudence, conflicts between professionals about the type of applicable law (i.e., civil versus criminal) as well as the time-lining of international offences further exacerbates existing problems. Lastly, the cost of technology required to keep up with the fraudsters can be unachievable for the Police. In summary, these are the factors likely to impede reporting of cybercrime based on RNPAs' intelligence.

6.6.3 Factors improving cybercrime reporting in Italy

The cybercrime reporting system in Italy is comparably less equipped to accept complaints of cybercrime. Therefore, it is a bit trickier to make the argument regarding what precisely improves reporting in Italy. It is meaningful to think of the situation in terms of "what work is currently in progress" and see it as pre-cursor to the argument of what improves reporting. Nevertheless, the Postal office plays in important role in informing citizens about cybercrime with the use of their websites, which is especially useful for those that want to make a report post-attack. However, it is not geared towards awareness-raising and protection. People in Italy are inclined to report in person via the Police station, which is their chosen access point. In the view of one RNPA an online system could better the situation:

> "The hope is that the online reporting system will be improved in order to achieve a simpler submission of relevant information and a faster response capacity of the postal police."
>
> -RNPAs – Italian lawyers

It is important to see the limitations of the Italian system in context. One could argue that the main difference between the Italian and Scottish situation is that Italy's cybercrime policing landscape is saturated by state interventions to a far lesser degree. However, of those interventions that are present, Italy's have similar pros and cons to Scotland's albeit in a far more streamlined form.

Reporting is improved in cases where the victims seek to minimise economic damage by being able to prove that they have done the maximum to formally resolve the situation. Much like in the case of §4.2.2 Case study 3 Credit card details theft A and §4.2.2 Case study 4 Credit card details theft B victims are motivated to report to the bank to reinstate lost funds:

> "For example, in the case of credit card cloning and online purchases, the complaint against unknown persons allows the victim to go to his or her bank to claim compensation for unlawful charges (in this case, the bank carries out a subsequent verification step to assess possible negligence or misconduct)."
>
> -RNPAs – Italian lawyers

Victims prefer to report in-person versus online suggesting a social proclivity. Training was seen as an important contributor to both increased reporting and prevention, which is a point already alluded to.

6.6.4 Factors impeding cybercrime reporting in Italy

Lack of cybersecurity training was seen as the dominant factor in impeding cybercrime reporting. This is important because it showcases the higher level of (§2.2) responsibilisation in Italy since in most Western countries a certain degree of state-sponsored cybersecurity awareness training is considered the norm (Renaud, K., Flowerday, S., et al. 2018). In a similar vein to what Scottish RNPAs said, Italians perceived the ignorance of ones own victimisation as

another impediment. Equally, the Police's prey drive towards catching prominent criminals might mean that they neglect high volume low value crimes, as one RNPA observed:

> "(...) the interest of those who directed the investigations was motivated more by the desire to get to the so-called 'big fish', i.e. those who had engineered the fraud from above, than to take into account who had or had not filed the complaint."
>
> -RNPAs – Italian lawyers

Finally, vulnerability does not appear to be accounted for by the Italian legal system, which is centred around the particularities of the crime rather than the person who was impacted. Therefore, under-reporting can also be the result of the system not being setup to accept complaints from people deemed as vulnerable due to possessing a protected characteristic.

Summary: Italy's cybercrime reporting system has similar strengths and weaknesses to the Scottish one, but is comparably less saturated by state interventions. Italians, much like the Scots, report to their banks to reinstate lost funds. Police reporting is motivated by a fear of criminalisation. A lack of awareness raising campaigns impedes reporting and prevention, but a desire to have it as a key intervention shows high citizen (§2.2) responsibilisation. The latter could be devised as victim-centred both for the vulnerable and the general population to detract from a purely prey-driven crime fighting mentality towards a more caring approach.

6.7 RNPAs Discussion

This section contextualises the results of the study within the existing scientific landscape and adds further value to the debate by presenting an original opportunity cost dilemma, which surfaced during analysis. In addition, this section justifies the role of the academia as central in improving cybercrime reporting because it is an agency, which can shrink the RNPAs buffer zone and bring the citizens closer to the state by formulating a set of "best practices" from the RNPAs intelligence. The academia will use these "best practices" to hold the state accountable for producing practicable solutions to counteract the under-reporting of cybercrime.

Netherlands versus Scotland: To recapitulate, the Dutch piece by Terpstra, J. 2008 is useful for the current research because it allows me to strategise about interactions between RNPAs and the Police in the domain of improving cybercrime reporting. In this research the Police that took control of the Dutch security network were praised if they exhibited a high level of involvement, which is helpful for understanding what behaviours are potentially cohesive from the Police.

Currently, Police Scotland are not involved with operationalising RNPAs in a networked way. Rather, they accept their intelligence, which is further analysed. There is clear potential for greater involvement from the Police especially in terms of using RNPAs' as an evidence gathering mechanism, which could facilitate arrests against on a national level or contribute to a greater understanding of prolific offenders on an international level. As exemplified in Figure 6.1, Police Scotland and the NCA by and large appear to be a recipients of information.

UK versus Scotland: According to Levi, M. and Williams, M.L 2013 caution needs to be paid that RNPAs – Banks do not exert undue influence over the multi-agency environment, which would result in the Police protecting the business interests of the RNPAs – Banks as opposed to the vulnerable citizens. I agree that this can pose a risk in cases where RNPAs – Banks and RNPAs – State-sponsored charities sit at one table with the Police, because banks by their very nature will adopt and extremely structured and managerial attitude to the problem, which

will fit well with the Police's managerial approach. As a consequence, the comparatively more improvised nature of charities might convert them from partners into followers.

Yet, the situation in Scotland seems to be still some way away from even this risk manifesting as my interviewee, who was an employee of a bank, alleged that Police Scotland lack the capacity to process the detailed evidence supplied by the bank in a way that would facilitate arrests. On the other hand, Police Scotland can assert itself pro-actively within this environment and propose that if the bank wants to see offenders taken of the street, then it must accept a position of partnership with the other RNPAs before any collaboration commences.

Norway versus Scotland: The Norwegian research by Bjelland, H.D. and Vestby, A. 2017 is beneficial for improving cybercrime reporting because it allows me to predict how RNPAs – Regulators of commerce could be deputised by the Police in the area of cybercrime, which would shift the focus of collaboration from a partnership model towards a hierarchical model. This is something I am keen to avoid as I believe that a levelled playing field based on principles of partnership is the best operational model.

In fact, I have already exemplified some evidence of the risk manifesting in interactions between RNPAs and Police Scotland, where the latter showed a propensity towards arguing that cases that were forwarded by the RNPAs were in fact matters for civil law as opposed to criminal law, thereby deputising RNPAs to address cases that would have been originally dealt with by the Police.

US versus Scotland: The US article by Lum, C., Koper, C.S., and Willis, J. 2017 explains how technological advancements are perceived differently based on the policing role within a hierarchical structure, whereby those at the lower end are likely to view the latter as a hindrance and those from the upper ranks will view it more favourably. This is useful for improving cybercrime reporting because it suggests that if Police Scotland's management are content with my solutions, then the people actually tasked with carrying them out might perceive them as a hindrance. Hence, any solutions that are produced as a part of this work need to take into account the entire hierarchy and not just management.

This is especially true in cases where the current work would lead towards formulating a set of "best practices" principles which would be rolled out across the organisations. Something can only be called "best practices" if it is practicable for the entire organisation rather then merely a managerially appealing set of goals on paper, which will get archived as soon as they encounter the first signs of resistance to change.

Canada versus Scotland: The Canadian work by Sanders, C.B. and Langan, D. 2019 is useful in understanding how the managerial approach of the Police can result in the (§2.2) responsibilisation of agencies whose primary role is to offer a person-centred service to an individual facing acute risk. This is important to bear in mind when thinking about how to best operationalise the relationships between RNPAs – State-sponsored charities and the Police as the latter may exert their own philosophy over the processes of RNPAs in the area of improving cybercrime reporting. This would turn the RNPAs into followers as opposed to partners in communication.

I have already demonstrated in subsection 6.6.2 there were some signs of inter-agency awkwardness when a worker from an RNPAs – State-sponsored charities spoke about how the Scottish Police have a tendency to re-refer cases back to the charity in order to avoid issuing a crime reference number, thereby creating a circular situation. As a part of this approach, it is remains important to be assertive and insist that Police Scotland understand the importance

Using RNPAs for policing:

a) RNPAs are experts by experience.
b) RNPAs can function within a "flexible practices" approach.
c) RNPAs are cheaper.
d) "Higher volume of lower quality work will be completed."

Using specialised policing:

a) Victims favour specialised policing.
b) Specialists are embedded within a "best practices" approach.
c) Specialists are more expensive.
d) "Lower volume of higher quality work will be completed."

Figure 6.2: The opportunity cost dilemma

of crime reference numbers for victims in order to get the most out of charities whose primary role is unconnected to cybercrime reporting.

Australia versus Scotland: The Australian article by Bright, D. and Whelan, C. 2019 is aligned with my research into RNPAs because the latter operate in an unsystematic environment with other RNPAs, the Police and the government. Thus, it is important to remember that their interests will be broad, which is why I will have to develop the strategy very pedantically if encouraging the collaboration on something as narrow as improving cybercrime reporting in Scotland. It is likely that this will not be possible without increasing the funding for selected RNPAs so that they can increase their resources to work alongside Police Scotland.

South Korea versus Scotland: The South Korean research by Paek, S.Y., Nalla, M.K., and Lee, J. 2020 is useful as it illuminates how the Police in other countries perceived the prospects of this collaboration in addition to shedding light on what career profiles are likely to find this type of partnership meaningful.

This means that officers from Police Scotland may be less likely to engage in collaboration with RNPAs the longer they have been with the force. This could be due to the hierarchical structure of policing, which can be resistant to more flexible ways of working. However, Paek, S.Y., Nalla, M.K., and Lee, J. 2020 also state that the police would be more likely to engage with this type of collaboration if the cybercrimes were perceived as serious, which ought to be evident from the scale of evidence supplied by various RNPAs. However, as the researchers caution, the first steps towards these new forms of working should seek to include officers with a high degree of IT proficiency.

The opportunity cost dilemma of Scottish RNPAs: To add analytical value to the work a theoretical argument is being put forward that places the state in the midst of an opportunity cost dilemma. This argument is derived from the data collected throughout this study and rests on the assumption that RNPAs' cybercrime reporting know-how can be operationalised without further increasing the costs to the state. As I demonstrate on Figure 6.2 the state has to weigh up the opportunity cost dilemma created by the responsibilised environment.

Specifically, in Figure 6.2, in the column on the left the state can choose to use RNPAs for cybercrime reporting which is being done to some extent anyway. If the state does this, then it will gain experts by experience as RNPAs have constant exposure to the fluid national trends in cybercrime. Furthermore, the state can flexibly adjust its approach to this collaboration as it would not be bound by current laws. This approach is cheaper because the state is already

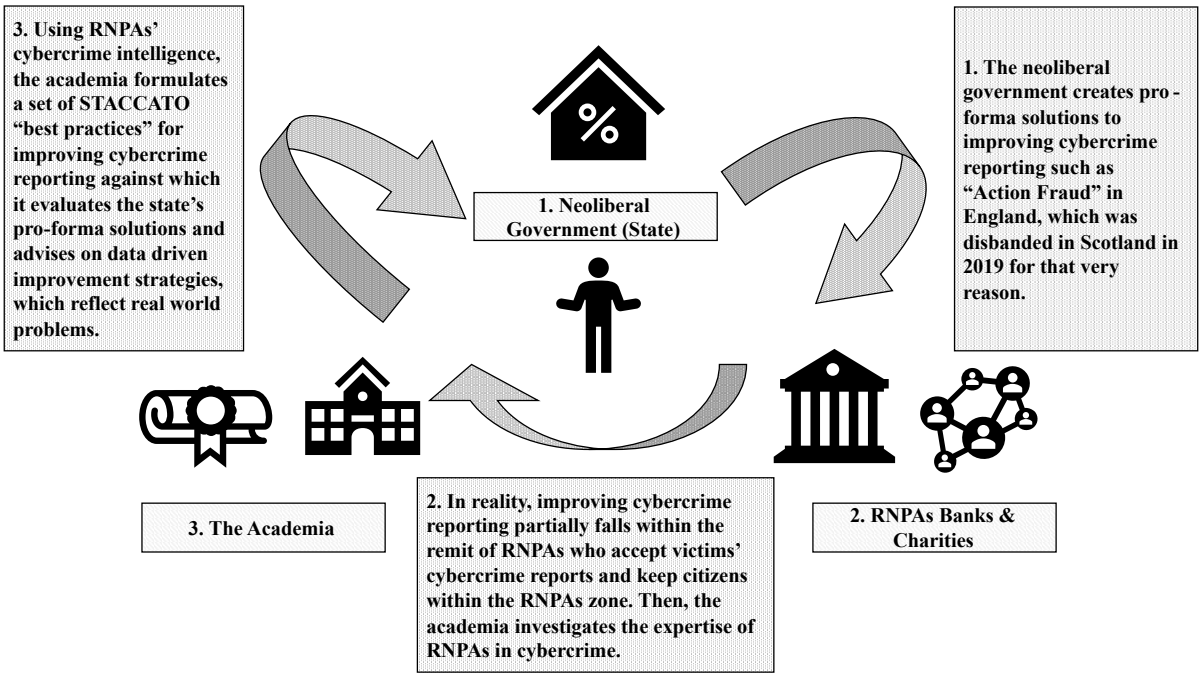


Figure 6.3: The role of the academia

either funding RNPAs in most cases with the exception of banks, which make their own profit. Thus, minimal additional funding would be required to operationalise this structure as it is already in existence. An outcome of this collaboration would be that a higher amount of lower quality work would get completed. This is due to the fact that RNPAs are not setup for cybercrime reporting so the rigour of their output is likely to be variable on the whole, but their bandwidth is such that a lot of evidence is likely to get collected.

Moreover, in Figure 6.2 in the column on the right, the state can instead invest in specialised policing by operationalising RNPAs for cybercrime policing. As I have demonstrated in §4.3 SVC Discussion, victims prefer specialised policing. The benefits of this include the embodiment of the "best practices" approach which is characteristic for public sector organisations. This would mean that the state would be in a better position to monitor the effectiveness of its strategies than in the case of RNPAs which would present it with high volume variable quality evidence. In the same vein, specialised policing would have to operate within a legislative framework which would further increase the accountability towards the victims. On the downside, specialists are more expensive and therefore a smaller amount of staff would be hired in comparison to the amount involved in precarious work within RNPAs. Thus, from a theoretical standpoint, specialised policing staff would carry out a lower volume of higher quality work.

Justification for the role of academia: Throughout this work, I have engaged in a sociological analysis of the role of RNPAs for improving cybercrime reporting in Scotland. Entire sections were dedicated to making recommendations for the improvement of reporting as well as cautioning against what might impede it.

The aspiration of this work is to evidence its ability to improve the situation rather than just make recommendations hoping that someone will pick them up and do something useful with them. If anything, this research provides justification for the role of academia in the responsibilised environment where the state has created the RNPAs buffer zone to protect itself from the needy citizens.

As I demonstrate in Figure 6.3 the academia is justified in its role to improve cybercrime

reporting as the one, which is able to effectively analyse RNPAs intelligence and transform it into expertise as has been done in this work by putting forward my own "best practices" checklist referred to as "STACATO." This checklist can be used to evaluate existing pro-forma solutions to cybercrime reporting whether they are online computer interfaces or reporting via the local police stations or designated phone numbers. In addition, since "STACATO" is data driven it can be used as guidance for creating new cybercrime improvement strategies from scratch, because it already contains the vital expertise required to successfully pilot the task.

6.8 RNPAs Limitations

This study used a relatively small sample. We followed the methodology of Ritchie and Lewis 2003 (p.108) who distinguished between non-probability (qualitative) versus probability (quantitative) testing. Non-probability is recommended for use in small-scale in-depth studies where units are deliberately selected to reflect features of the sample Ritchie and Lewis 2003 (p.78). The converse is true for probability testing. Therefore, this limitation is offset by using a qualitative analysis of interview transcripts.

6.9 RNPAs Conclusion

In conclusion, (§2.2) responsibilisation characterises the cybercrime landscape within which the RNPAs operate as was demonstrated throughout this work. This is especially true because RNPAs create a buffer zone which protects the state from needs of the citizens and sanitises their concerns so that they are forwarded as intelligence rather than complaints, which should be urgently resolved.

I have finalised this undertaking by an impartial proposition towards the state whereby I suggested the operationalisation of RNPAs for improving cybercrime reporting versus an increase into specialised policing. I have justified this proposition on the level of cost-effectiveness as well as victim preferences.

Academia can play a vital role in shrinking the RNPAs buffer zone between the state and the citizens by analysing the intelligence of the former in order to articulate suggestions for the improvement of improving cybercrime reporting. The academia is strategically positioned for this task because it receives some funding from the state, but also other sources whilst aspiring to conduct research that is independent. In this chapter, I have accomplished this task by extracting RNPAs intelligence and expertise to improve cybercrime reporting in Scotland.

Chapter 7

Overall Discussion

The overall discussion will be structured in a way that ties together the theory I have developed via the §3 Systematic literature review (SLR) with the empirical work I carried out by researching victims, devising (§5) bespoke client-centred cybercrime training as well theorising about Responsibilised Non-Policing Agencies (RNPAs). The purpose of this exercise is to test the theoretical foundation on which my dissertation is built on and see how it answers the cardinal research question of what is required for improving cybercrime reporting in Scotland. It is neither possible nor desirable to contrast every reference from my systematic literature review with an iteration from subsequent qualitative interviews. I will not be looking to secure a perfect fit but points of overlap between my systematic literature review (SLR) theory versus results.

7.1 Introduction

I have commenced this dissertation by acknowledging that I have used UK-wide cybercrime research to make extrapolations to Scotland. Even though Scotland is a part of the UK, due to the devolution of policing, I hoped draw out major contrasts. Looking back at this approach, it was helpful at teasing out some of the nuances concerning the the views of victims and responsibilised non-policing agencies. These subtleties can be compared with future researchers against the situation in England and Wales for example to see whether people's views of Action Fraud have evolved. The notion of responsibilisation helped with answering the main research question regarding what is required to improve cybercrime reporting in Scotland. Mainly, it was apparent across all studies that cybercrime victims blamed themselves for falling prey to cybercrime. Yet, this was mainly inferrable based on their at times frantic attempts to resolve the situation themselves. It is interesting that in some respect, the victims did not "play the victim." To the contrary, they entered into a high agency problem solver mode, which was left unrequited by the system.

I have then proceeded to discuss the processes and perspectives on the unification of (§1.3) Police Scotland to supply the reader with an understanding of how the reshaping of the force may contribute to a strategy that seeks to improve cybercrime reporting. What stands out in the Scottish situation is the interconnectedness between the police and the community whereby officers practice discretion to remedy antisocial behaviour (Wooff, A. 2015; Wooff, A. 2016). During my own PhD I have been able to uncover the importance of fostering close bonds with the local community when it comes to improving cybercrime reporting. For example, my work into providing an attacked SME with a (§5) bespoke cybercrime training would not have been possible unless I had built pre-existing bonds based on trust. Likewise, a victim from the (§4.2.2) Individuals specifically complained about the fact that they were not capable of

reporting cybercrime to their local police station because the desk was left unstaffed. Hence, in my view prior research (Wooff, A. 2015; Wooff, A. 2016) is correct about emphasising the community context of crime control and remediation.

Some of the analysis of the status quo in §1.3 Police Scotland was also dedicated to the shift in strategic organisation, which occurred when Police Scotland became centralised in 2013 (Henry, A., Malik, A., and Aydin-Aitchison, A. 2019; Murray, K. and Harkin, D. 2017) as well as when it separated from UK's main cybercrime reporting mechanism Action Fraud (Dyson, I. 2019; MacDonald, K. 2019). Based on my research findings, I have not uncovered compelling evidence that these major changes filtered through into the cybercrime arena in a way that could be retraced back to them. This means that my approach of making extrapolations from the whole of the UK onto Scotland was likely unproblematic the policing of cybercrime faces similar challenges across the board.

None of the interviewed (§4.2.2) Individuals made reference to Action Fraud and most associated the bank with solving their problem rather than the Police. Even the (§4.2.3) Private institution, which reported cybercrime prior to Scotland's disengagement from Action Fraud, reported via the local police who, in tandem with his insurer, did not offer any help. In addition to that, the rest of my research into (§4.2.4) Public institutions shows a completely different, multi-stakeholder approach, to reporting. Whilst my research into §6.6 RNPAs' cybercrime reporting expertise uncovers the complex and changeable system of reporting via a multitude of agencies. Hence, these apparently tectonic shifts in the reorganisation of policing systems display only little bearing on the day to day lived realities of the cybercrime victims. It is worth mentioning that a more nuanced picture emerged when these interview findings were augmented with a survey on 380 Scottish victims of cybercrime as mentioned in Table 1.1. However, the findings from the co-authored article do not tell an entirely different story. Rather, some historical victims of cybercrime mentioned reporting to Action Fraud prior to the separation, but aside from that they converged on finding Police Scotland mostly unhelpful.

Guided by prior research I had followed the criminological trend of researching cybercrime as close to the victim as possible (Maltz, M.D. 1977). In fact, in my research on §4 Scottish victims of cybercrime (SVC) I have analogically followed the historical evolution of crime counting by commencing from the reading of court documents (as well as news articles) before gradually working my way towards actual victims. I believe that this approach allowed me to sample a greater part of the cybercrime situation in Scotland and UK more generally. Looking back at my results from the (§4.1) introduction section of Individual victims, I realise that much of the court documents and news coverage does not cover how these offences were reported, which further highlights the importance of the research I conducted on victims.

Lastly, it pays to contrast the findings from Hall, M. 2021 who suggested that the enforcement of strict best practices guidelines for crime reporting would reduce police autonomy. Once again, these research concerns simply do not tie with current cybercrime reporting situation in Scotland. In terms of the interviewed Individuals and Private institutions the connection between cybercrime reporting and the police was weak. The only cybercrime victims, which followed a set of best practices when reporting were the Public institutions, who are a part of the state anyway. This is the pattern of cybercrime reporting reality, which is characteristic of responsibilised neoliberal societies (Garland, D. 2002a; Garland, D. 2002b) where Individuals and Private institutions are imparted hardly any advice on cybersecurity. In cases where victims fail to follow the advice, they are made to feel like it is their fault (Renaud, K., Flowerday, S., et al. 2018; Renaud, K., Orgeron, C., et al. 2020). I feel that the current situation is better reflected in the concerns of the ACPO 2005, which highlighted that the most difficult area to "manage" between the police, who accept crime reports, and the general public was

that of soft skills. The police's problem with social skills can also tie into the lack of support they receive in their role when accepting reports of cybercrime (HMICFRS 2020). Therefore, the improvement of cybercrime reporting may be connected to a greater amount of support of the police from their superiors, which would enable them to develop a softer approach to the cybercrime complainant.

7.2 SLR - Theory versus Results

Due to the scarcity of data on Scotland much of my (§3) Systematic literature review (SLR for short) was conducted on cybercrime research on all of the UK and further afield. This section brings together the theory from the SLR and compares it against my collected findings in a way that draws out the differences between theory and reality, but also advances new lessons for improving cybercrime reporting in Scotland. Its subdivision mirrors the Research Questions (RQs) of the original SLR whilst the subsections reflect the insights drawn out from data collection for improving cybercrime reporting in Scotland.

7.2.1 RQ1.: What is known about cybercrime research in the UK to date?

Insights for typology

A contribution of the SLR to my research into improving cybercrime reporting is the postulation of the victim taxonomy: Individuals (Collier, B., Thomas, D.R., Clayton, R., and Hutchings, A. 2019), Private institutions (Lavorgna, A. 2019) and Public institutions (Hutchings, A. and Collier, B. 2019), which provided the necessary foundation to proceed with interviewing these victim types to use their experience for improving cybercrime reporting.

In the SLR I have uncovered that (§4.2.2) Individuals in the UK were most likely to experience bank card fraud accounting for 66% of all incidents (Levi, M. 2017). I have found points of correspondence with my data, whereby two victim Individuals reported bank card fraud (recall for example: (§4.2.2) this credit card fraud). Moreover, whilst Correia, S.G. 2019 found that females were more likely to fall for advance fee fraud (i.e., where people pay upfront for products they do not receive), my research on individual victims revealed that males can be victim too (as described in: (§4.2.2) E-Bay car scam). This case study in particular served as a poignant example for responsibilisation. The victim exercised extensive due diligence prior to the product purchase and also collected evidence after of the crime. Yet, the policing system completely shook of the responsibility for investigating the crime, which demonstrates the real perils of getting justice.

At the time of my writing, my SLR revealed Business E-Mail Compromise (BEC) (i.e., criminals posing as the company's executives requesting a transfer of fund) as a frequent crime affecting (§4.2.3) Private institutions (Fisher, J. 2008). Whilst my qualitative interviews did not find a correspondence with BEC, I have uncovered two cases of ransomware (i.e., the locking down of systems in exchange for a ransom) as the affliction affecting the interviewed victims (recall: (§4.2.3) Russian ransomware). I think that this can potentially be due to the fact that, in the cases of concrete Scottish SMEs, the impersonation of an executive can be tricky as people have a deeper an awareness of each other's interpersonal styles. BEC can be easier to carry out in larger Private institutions where there is greater anonymity between the executives and lower rank staff. From the criminal's mind, the use of ransomware "is more suitable" for a small SME as people are more likely open links and download malware.

Thirdly, during my SLR, I uncovered evidence that ransomware (Wirth, A. 2018) exerted a major effect on UK's Public institutions (e.g. NHS) as well as insiders (Martin, P. 2024) from within organisations who with a weak or non-existential financial motive (Cross, C. 2019; Hutchings, A. and Collier, B. 2019). My own research into cybercrime affecting Public institutions uncovered a more nuanced picture. For instance, there were multiple instances of ransomware (e.g., as described in the case of a (§4.2.4) charity and (§4.2.4) government structure), but there was also a (§4.2.4) fraudulent invoice case that sat in between advance fee fraud and BEC. Lastly, insider risk (Martin, P. 2024) was responsible for a (§4.2.4) crippling cybercrime that was initially attributed to external malicious actors.

Insights for policing

A research gap that I left unaddressed from the SLR connected to §3.1.2 Policing. The SLR served to uncover a significant amount of information about the organisation of policing and cybercrime. For example, in the (§3.1.2) Models section, I uncovered literature that encouraged a structured approach to cybercrime investigation (Hunton, P. 2011; Hunton, P. 2012). Sadly, the research that I had planned with Police Scotland did not come to fruition due to internal structural reorganisation. Nevertheless, my observations from the regional call centre, which collected cybercrime reports from the general public, was that their approach was less structured. During our informal conversations, we discussed the reporting of financial sextortion, which was conflated on the reporting system's drop-down menu with kidnappings due to high suicide risk. Whilst financial sextortion was not the subject of my dissertation, I am left wondering whether the integration of cybercrime into regular policing practices is effective. This is an important concern because regular "bread and butter" policing is the first port of call for most cybercrime from the general public even before the specialist cyber units get involved. Therefore, it remains important that there is clarity in procedure.

In the (§3.1.2) Organisation section that followed, I extracted information on the delegation of policing responsibilities onto the private sector (Wall, D.S. 2013; Johnson, D. et al. 2020). Whilst the section itself went beyond the responsibilisation of the private sector, highlighting also the positive work that the police are doing (Collier, B., Thomas, D.R., Clayton, R., Hutchings, A., and Chua, Y.-T. 2021), my own empirical research corroborated the existence of the merger between the police and private institutions. In fact, I brought forward a compelling thread of evidence that highlighted how Individuals associated banks with fund reimbursement more so than the police, which is characteristic of responsibilisation. In actual fact, my interviewees even spoke of the banks playing a pro-active role when contacting them about credit card fraud. However, when considering the role (§2.6.2) of RNPAs- Banks in cybercrime reporting, I have also revealed the expansive criminalistic process that these institutions possess for tackling cybercrime. The effectiveness of these processes at times exceed those of the police. So, it could be said, that my own results tie closely to some research points uncovered via the SLR.

Subsequently, the (§3.1.2) Human resources (HR) section detailed a range of research that could be conceived as HR approaches to improving cybercrime reporting. Within this discussion, I will touch upon the research by Sommer, P. 2017 who stated that it was the companies' role to collect evidence for the police if they expect a thorough investigation. In fact, these responsibilised assumptions have resulted in a disconnect between victimised companies and the police, whereby one of my interviewed Private institutions related feeling displeased with the lack of support from the police in response to the ransomware attack. The second interviewed private institution did not even contact the police, but rather instantly outsourced a private responder.

As a part of the HR, Forouzan, H., Jahankhani, H., and McCarthy, J. 2018 discussed the

unfortunate fact that the London Met had rolled out training package (i.e., NCalt) to upskill officers in tackling cybercrime, however this was done at the very best pro-forma and the uptake was left unmonitored. In my own research, I have collected data connected from the (§5) client-centred cybercrime training with qualitative and quantitative methodologies. I did this as a form of aftercare of an attacked Private institution. My training was bespoke, which allowed me to connect with the specific mentalities of attacked staff from a Scottish SME combining what they wanted to learn with what they should be learning. The result was some improvement in practices, raised awareness but no connection to improved cybercrime reporting outside of the organisation, which I ascribed to the responsibilised mindset. It is possible that a more personalised approach to training the police which engages members of the force interactively could be more successful. In addition, during my (§6) RNPAs research, I have uncovered an emphasis on training being a part of the STACATO best practices, where the Scottish RNPAs have specifically suggested this as a way of (§6.6.1) improving cybercrime reporting in Scotland.

An HR piece worth mentioning was that by Bossler, A.M. et al. 2020, who identified the need to form a set of best practices when responding to cybercrime. As was uncovered via (§4.2.5) factors that improve reporting, it is only victimised Public institutions (i.e., the state itself) that stands to benefit from a best practices and multi-stakeholder approach to cybercrime victimisation. The remaining victims (i.e., Individuals and Private institutions) have to look for the solutions themselves in the responsibilised cybersecurity arena. I have argued in the previous sections that this should change so that the best practices approach is not only reserved for the governmental bodies.

The last piece of research from HR that is useful for reinforcing a case in point is that of Johnson, D. et al. 2020 who polemised about the effects of decentralisation on the English policing of cybercrime. As I have tried to demonstrate via this discussion, cybercrime reporting in Scotland does, at least in part, have a life of its own within the broader organisational structure of the police force. As such, it appears to be only minimally affected by these tectonic changes within the upper echelons that oscillate between centralisation and decentralisation. Nevertheless, my data did uncover one partial exception to this rule whereby it was suggested, as a part of STACATO best practices, that a centralised repository of cybercrime intelligence accessible to all agencies might improve reporting. However, this is not the same as saying that a centrally managed police force would be helpful in this regard. Yet, it is interesting from the perspective of responsibilisation that the STACATO best practices mirror a component of the Scottish policing system because it shows how responsibility was delegated outside of the state.

The HR section was followed by (§3.1.2) Jurisprudence, which considered the legal challenges of policing cybercrime under closer observation. Sampson, F. 2014 considered introducing the use of dedicated police constables, which would frequent the cyber arena in a similar fashion as they do in the physical spaces. My data uncovered similar theorising among the interviewed victims. The victims in particular spoke highly of specialist police, whom they negatively contrasted to regular police during cybercrime reporting.

7.2.2 RQ2.: What is known about cybercrime victims in the UK to date?

Insights for victim profiles

A case in point from the SLR is the victimisation of former shadow home secretary David Davis, who started criticising the UK government's approach to cybercrime after his own victimisation in 2008 (Hunter, P. 2008). Based on a reflection of my own findings this is a case where a person who is a member of a responsibilising government comes to realise the pitfalls

of the neoliberal government's own agenda. Yet, as an individual he is in a weak position to deliver that point in a compelling way. This is because, in practice, the likelihood of a successful cybercrime investigation has dropped since the forces will only investigate offences above £100 000 (Correia, S.G. 2019). This was corroborated by one of my interviewed individual victims from the already mentioned (§4.2.2) advance fee fraud or E-Bay case study. This victim applied significant due diligence before making a purchase and invested considerable resources into collecting evidence of the fraud after he lost £5 240 for a car he never received. His own subjective conclusion was that the police would investigate only seven figure sums. This can be seen as indicative of a worsening situation if neither powerful politicians nor astute victims can expect a successful outcome after a submitted cybercrime report. Additionally, it slightly brings into question the Routine Activity Theory (RAT) discussed next.

A section of the SLR was dedicated to (§3.2.1) RAT (Nasi, M. et al. 2015), which found that individuals from marginalised populations were more likely to fall victim due to, among other factors, spending more time online. The core assumption of RAT was that some people tend to behave in ways that puts them more in harm's way than others. Whilst the data from my interviews are qualitative, they draw attention to the incongruence with RAT. For example all of my individual victims behaved typically when they were attacked whilst one practised extensive due diligence. In fact, in the case of one of the (§4.2.2) HMRC scam, the offenders were extremely sophisticated even going to the lengths of posting compelling fake letters purporting to be from the HMRC. In fact, the categories put forward by Nasi, M. et al. 2015 simply did not reflect any of the characteristics of the interviewed victims. Yet, when it came to Private institution victims, my collected results displayed a better fit with the theory.

Subsequent pieces of the SLR shifted from victims that were Individuals to victims that were Private institutions - SMEs (CFS 2018; Donegan, M. 2019). According to the CFS 2018, SMEs that invested in cybersecurity reduced the chances of falling victim to an attack. This corresponds to the findings from my interviews. For example, the SME that was attacked by (§4.2.3) Russian ransomware updated its systems post-attack by moving its data into the cloud but also investing in more effective cyber-insurance policies. According to the owner, they have not suffered a cybercrime since. Conversely, the second SME, which was also attacked by (§4.2.3) had a very vulnerable cybersecurity posture prior to the attack (Donegan, M. 2019). In my own research, I have sought to understand the vulnerability of this particular SME, which is why I devised a (§5.2.1) bespoke psychology-informed training to upskill its staff post-attack whilst summarising the (§5.2) results and (§5.3) discussion of my findings within this dissertation.

In returning to the (§3.2.1) psychological perspective in my SLR, I have uncovered research by Connolly, A.Y. and Borrison, H. 2020 which identified victims' varied approaches to paying off ransomware attackers. Broadly speaking, the authors subdivided victims into two types. Firstly, those that paid the ransom due to ineffective backups and advice from their IT consultant. Only one of my interviewed victims from the (§4.2.3) first Russian ransomware case attempted to pay off the attackers and this was unsuccessful in terms of protecting their data as it was returned corrupted. Secondly, Connolly, A.Y. and Borrison, H. 2020 spoke of victims that do not pay the ransom due to having effective back-ups and following the advice from the police. The remaining victims of ransomware that I interviewed did not neatly fall into either category. Instead, they sat somewhere in between. For example, the victim from the (§4.2.3) second Russian ransomware case study was reluctant to contact Police Scotland, but followed the advice of a private IT consultant that stated he should not pay the ransom and instead focus on restoring the systems. As a part of the SLR, I critiqued Connolly, A.Y., Wall, D.S., et al. 2020's viewpoint whereby the authors emphasised the systems resilience of Public institutions but overlooked the impact of attacks on the working staff. Indeed, the (§4.2.4)

Public institution which I interviewed mentioned that the cautioning of staff by the police as a standard matter of procedure was anxiety-provoking, which could (§4.2.6) impede reporting. Lastly, Buil-Gil, D. and Zeng, Y. 2021 and Correia, S.G. 2020 found varied correlations between age and people's susceptibility to romance fraud during the COVID-19 pandemic. Whilst, romance fraud was not represented in my findings, (§6.1) RNPAs reported on a (§6.5) trend during COVID-19 whereby people fell for fake government loans causing them to loose money. Thereby, this can be considered an addendum to the types of cybercrimes people became vulnerable to during COVID-19.

Insights for victim experiences

Prior research on victims' experiences found the deterring effects of cybercrime on Internet usage in those that were attacked on heard about the threats (Bohme, R. and Moore, T. 2012). My sample of interviewees did not corroborate these findings for multiple reasons. For example, all of the victimised Individuals were either attacked by the cybercrime coming to them via credit card fraud or despite extensive due diligence. Therefore, it was not their casual Internet usage that mediated their victimisation. In terms of the Private institutions, the first one increased its Internet usage post-victimisation by storing data on the cloud and the second one did not show any apprehension to its use either. Rather, they stood to benefit from the bespoke training I delivered for them as a way of meeting their needs.

Victims' psychological needs was also a domain examined by Leukfeldt, E.R., Notte, R.J., and Malsch, M. 2020, who found that victims sought a recognition for their ordeal as well as the need to remain informed on the development of the court proceedings. My results from (§4.2.5) factors that improve reporting specifically touched upon the need to appoint a designated agent or case worker to oversee the investigative process from reporting until resolution. I am seeing this as overlapping with the findings of Leukfeldt, E.R., Notte, R.J., and Malsch, M. 2020 who identified victims' need to remain informed about case development. It should be also noted that Van de Weijer, S., Leukfeldt, R., and Van der Zee, S. 2020b discovered that victims are internally motivated to report cybercrime to the police if they incurred a financial loss. This broadly reflects my findings although Individuals generally reported the offences because they were prompted by the bank. However, one victim Individual reported the advance fee fraud due to losing a considerable amount of money. With regard to the Private institutions, in fact, one of the victims reported the offence due to having lost money, whereby the other one specified that they refrained from reporting due to not incurring financial losses.

The effects of educating on cybercrime prevention also came up during the SLR whereby Cross, C. and Kelly, M. 2016 found that people disassociate between what they learned and the situation with the cybercriminal - particularly if they have invested emotions into the scammers trap. Cross, C. and Kelly, M. 2016 advises that this situation can be improved if people are imparted only very basic guidance on cybersecurity. The authors could be correct, but I have taken a different approach. Rather than assuming that victims' capacity to absorb information is limited, I assumed that what they were lacking was a sense of connection during cybersecurity education. This is why, as a part of my bespoke (§5) client-centred cybercrime training, I invested in self-disclosure (Yalom, I.D. 2011; Yalom, I.D. and Leszcz, M. 2005) as a way of building that connection and levelling the playing field in terms of power.

In the next piece, Cross, C. 2018 identified that victims' experiences were often influenced by unrealistic expectations. If the reader recalls, this was in connection to the fact that, in Australia, victims get frequently passed on in between agencies. In addition, victims, inspired by crime series overestimate the police's capabilities in investigating cybercrime. In the case of Scotland, I have found a very fragmented cybercrime reporting arena, which is heavily subsidised by (§6) RNPAs whereby (§2.6.2) banks and (§2.6.2) charities substitute the policing

functions of the state to a significant degree. Whilst the effects of this on victims' experiences remains an avenue for future research, it suffices to assume that victims will find this terrain hard to navigate. I have specifically illustrated how this complexity plays out via (§6.3.3) propagation of cybercrime, where the states utilises RNPAs to maintain victims at arm's length.

The former article was followed by Abdulai, M.A. 2020 who examined students' fear of credit card fraud in comparison to demographics and found that demographics did not exert an effect over people's fear. Taking into consideration my research, the Individual victims of cybercrime varied in terms of demographics, but none of them were particularly fearful of cybercrime. Fear started to become a salient factor in my research on victims that were representing either Private or Public institutions and I feel that this was connected to people's sense of responsibility for the greater whole. Multiple interviewees that represented institutional victims also corroborated the findings of prior research in the sense that they felt immune to cybercrime before it happened to them (Cross, C. 2021).

An important component of victims' experiences can be that of marginalisation due to immigration status (Bidgoli, M. and Grossklags, J. 2017). If victims feel marginalised even before they are targeted by cybercriminals, then it makes that much harder to report. I addressed the problem of marginalisation of victims in multiple ways. For example, in the case (§5) client-centred cybercrime training, I conducted a training for an SME that operates in an area with high deprivation, which can create a sense of marginalisation among the predominantly all-white working class Scottish community. Moreover, thanks to my work on (§6) RNPAs, I was able to uncover very similar scams plaguing the international student community in Glasgow to that described by Bidgoli, M. and Grossklags, J. 2017. Recall, that in the case of Bidgoli, M. and Grossklags, J. 2017's research they uncovered evidence of cybercrminals impersonating US governmental institutions to threaten migrant victims. According to an RNPA which was a university (§6.5) Indian and (§6.5) Chinese students are targeted by cybercriminals whilst on campus in Glasgow. Namely, Indian students receive threatening correspondence purporting to be from the HMRC whilst Chinese students receive threatening correspondence purporting to be from the Chinese government.

From the perspective of international collaboration, Monteith, S. et al. 2021 conducted a study between U.S.A., Germany, Canada and UK to examine the interaction between the COVID-19 pandemic and the risk of developing a mental illness post-cybercrime victimisation. It was found that COVID-19 significantly worsened the pre-existing mental health problem of cybercrime victims as well as predisposing otherwise healthy people to developing them. The subject of COVID-19 came up in my data as well. Namely, RNPAs reported on (§6.5) COVID-19 cybercrimes where victims were tricked into sending money to cybercriminals posing as the government. It is logical that these people would have experienced increased psychological stress as a result.

7.2.3 RQ3.: What is known about cybercrime reporting to date?

Insights for cybercrime reporting approaches

Human To Human (H2H) In the SLR, I uncovered research by Bidgoli, M., Knijnenburg, B.P., and Grossklags, J. 2016 which highlighted how victims preferred reporting to other people by contacting their bank as well as the retailer. Using the data from victims as well as RNPAs I am seeing a complex picture emerge. For example both (§4.2.5) Individuals and (§4.2.5) Private institutions related that cybercrime reporting would improve if people could report via H2H approaches. Yet, when I consulted the RNPAs, who have been responsiblised by the state to collect cybercrime reports, a different picture emerges. As a part of their STACATO best practices to improving cybercrime reporting, they are indirectly suggesting a

reduction in the H2H approach. Rather, they would want to see a strategy that contains (§6.6.1) automation and is (§6.6.1) online. This is unsurprising because as the abbreviation "RNPAs" suggests, these organisations were (usually) not setup for cybercrime reporting and hence they are converging on an approach that would protect human resources rather than further deplete them.

Further research by Cross, C. and Kelly, M. 2016 touched upon the problem of jurisdiction in cybercrime reporting. This problem occurs when cybercrime crosses many geographical and legal jurisdictions before it reaches the end victim. Due to this re-wiring, victims usually do not get justice when they report via H2H because it is hard to establish where cybercrime originated from. Also, it is tricky to establish which country's legislation should be applied to the investigation. In general, the (§6.5) trending data from RNPAs supports these sceptical conclusions about the reporting of transnational cybercrime. Nevertheless, the data from RNPAs also warns against blanket scepticism. Take the example of the (§6.5) Glaswegian cybercrime gang reported by one of the RNPAs. In this instance, criminals operating from Glasgow managed to impersonate a Scottish accent to the point that they managed trick English victims into sending them money, which they otherwise may not have done. In this case, it would have been premature to abandon an investigation only due to an assumption that jurisdiction poses a challenge to cybercrime reporting and investigation. Therefore, all H2H reports of cybercrime must be judged on an individual basis.

In addition, Popham, J. et al. 2020 critiqued the effects of dated legislation on poor cybercrime reporting in Canada. The authors have argued that cyber-law is merely traditional law that is polished by cyber jargon but overall unsuitable for receiving reports of an investigating cybercrime. From a legal standpoint, this dissertation has uncovered an overlap with the situation in Canada. For example, when I conducted the search of Scot Courts as a part of the (§4.1) introduction into the study of victims, the term "cybercrime" was used exclusively in connection to child abuse imagery. Economic cybercrimes of dishonesty were only revealed using the more antiquated phrases such as "fraud" and "fraudulent scheme." It is possible that there are even more cybercrimes captured within the judgements of Scot Courts using other antiquated terminology, which further complicates research into understanding reporting. On the flip side, due to the fact that many court judgements are oral rather than written, perhaps the use of correct terminology has become more prevalent.

As already noted, (§2.2) responsibilisation exerts a significant effect on H2H reporting. As Van de Weijer, S., Leukfeldt, R., and Van der Zee, S. 2020b noted on a hypothetical study of 595 participants; most people would simply prefer to report economic cybercrime to an organisation other than the police. This corresponds to the indicative data that I have accumulated from the RNPAs, who were able to supply me with a precise snapshot of what (§6.5) cybercrime trends are impacting the Scottish population. Victims simply associated RNPAs with H2H forms of reporting, which allowed the organisations to gradually build-up an intelligence pictures as I depicted via the (§6.3.3) propagation of cybercrime figure.

Unlike the hypothetical setup put forward by Van de Weijer, S., Leukfeldt, R., and Van der Zee, S. 2020b, I also discussed a real study of a cyberstalker (Yadav, H. et al. 2021) who was an art gallery owner, but also a cyberstalker who managed to extort over $3 000 000 from his victims. I used the SLR to highlight that despite the offender's prolific nature, there was actually no information about how these offences were reported. This type of omission was obvious also from the court cases and news stories, which I described in the (§4.1) introduction to the study of victims. In that instance, I have uncovered that only 3 out of the 14 cases contained information about how cybercrime was reported. I think that if H2H cybercrime reporting is to improve, then court cases and news stories must detail the reporting trajectories so that the reader is able to form that connection in their mind.

The last piece from the SLR H2H section referenced research by Alzubaidi, A. 2021 who measured the levels of cybercrime reporting in Saudi Arabia. In his research, the author found that people were confused about who to report to often preferring to confide in their friends, which is an H2H pathway. Much like in the case of Scotland, Saudi Arabian citizens were unlikely to associate cybercrime reporting with the police. In response to Alzubaidi, A. 2021's findings, I have reached out to the author and commenced a dialogue about collaborating on the shared interest of improving cybercrime reporting. Towards the end of my PhD, the fruits of this gradual dialogue manifested when Dr Alzubaidi joined us at the 7th Strathclyde International Perspectives on Cybercrime Summer School, where he presented his research (Sikra, J. et al. 2024). As a part of this dialogue, we have envisaged a joint collaboration, which would draw out comparisons between cybercrime reporting in Scotland and Saudi Arabia.

Human To Machine (H2M) As a part of research into H2M approaches, I used the SLR to discuss the piece by Heinonen, J.A., Holt, T.J., and Wilson, J.M. 2012 who evaluated the U.S. Internet Crime Complaint Center (IC3). The IC3 receives complaints via its online interface from the public, but also private sector. Also, it is interconnected with the websites of the FBI and and National White Collar Crime Center (NW3C). Up until this point, the ICR corresponds to the RNPAs' best practices for improving cybercrime strategy - STACATO. Recall that the RNPAs suggested a strategy that would be (§6.6.1) advertised, (§6.6.1) centralised and (§6.6.1) online. Moreover, when evaluating the IC3, Bidgoli, M. and Grossklags, J. 2016 stated that its main strength resides in the system being able to advise people on how to stay safe online, which corresponds with the STACATO best practices factor of (§6.6.1) training provision. A weakness of the IC3 according to Bidgoli, M. and Grossklags, J. 2016 was that it was insufficiently advertised. Intriguingly, the STACATO best practices for improving cybercrime reporting contains recommendations for the (§6.6.1) advertisement of the approach. In other words, the RNPAs intelligence was useful in compiling an approach to improve cybercrime reporting, which reflects the strengths of the IC3 and addresses its weaknesses too.

Moreover, in a paper by Bidgoli, M., Knijnenburg, B.P., Grossklags, J., and Wardman, B. 2019 the researchers streamlined a procedure for reporting cybercrime in the PayPal service. The main strengths of this procedure were that it effectively connected reports within and outwith PayPal as well raising awareness of cybercrime with the customers. Once again, this corresponds to factors that improve reporting within the STACATO strategy, namely the factor of (§6.6.1) sharing and triaging information behind the scenes as well as (§6.6.1) advertisement of the system and (§6.6.1) training provided by the system. Therefore, this is further evidence that the RNPAs' access to the grass roots of cybercrime lends effective insights into what is required to improve reporting.

The STACATO best practices approach also ties closely with the recommendations by Baror, S.O., Ikuesan, R.A., and Venter, H.S. 2020 who highlighted that the problem of under-reporting was connected to a lack of clear criteria that victims could follow on what to report. The STACATO approach accounts for this as the RNPAs have advised that greater (§6.6.1) transparency is required to improve cybercrime reporting. Hence, once again I am able to highlight how the know-how from RNPAs ties into the existing literature.

A possible caveat for using the STACATO best practices for improving cybercrime reporting is that they do not address some of the limitations highlighted by previous research (Cross, C. 2020b). Namely, Cross, C. 2020b identified that complaints were unhappy with ACORN, which was Australia's centralised cybercrime reporting mechanism. The data on ACORN was of poor quality whilst capturing not completed scams. People also inflated losses to trigger a response and reported sexual abuse crimes, which the system was not designated to deal with. The STACATO best practices strategy does little in terms of addressing these concerns, which

might be also due to the fact that RNPAs are not setup for cybercrime reporting. Therefore, they will struggle to predict the intricate challenges that may follow when their strategy in engineered into a technological platform.

Yet, the research by Das, A. et al. 2021 is aligned with the STACATO best practices because it suggests that improved reporting is also about accounting for how information is stored as often these are disorganised. This ties into the STACATO criterion of (§6.6.1) sharing and (§6.6.1) transparency, which are both concerned with how the cybercrime reports are stored and organised.

To finish off, the research by Mackey, T.K. et al. 2020 sat in between H2M and M2M as the authors first scraped social media posts to code for the sale of fake COVID-19 remedies and tests. During the second stage, the data was analysed with the use of Natural language processing. This is a piece, which ties mostly to the (§6.6.1) automation factor of STACATO best practices for improved cybercrime reporting.

Machine To Machine (M2M) The summary of the M2M approaches from the SLR contained three articles in total. From the perspective of the STACATO best practices they all tie in to the principle of (§6.6.1) automation as a way forward to improved reporting. The first by paper Carpineto, C. and Romano, G. 2020 was most closely tied to designing a machine learning pipeline, which could identify counterfeit goods. This is something that (§2.6.2) RNPAs - Regulators of commerce would find especially relevant as it is their role to ensure that the market is not contaminated by counterfeits. The other two papers were concerned with the classification of spam e-mails (Sheikhalishahi, M. et al. 2020) and phishing e-mails (Singh, S. et al. 2020) however neither of those were touched on by RNPAs. Fortunately, in the UK this function is still catered to by the state albeit to a limited degree via the NCSC's Phishing: Spot and report scam emails, texts, websites and calls.

Chapter 8

Future Work

8.1 Direct Extensions

There are multiple promising research avenues that could expanded in relation to the results and discussions presented within this dissertation.

The Small Business Survey Scotland 2022-23 (SBSS 2022-23) identified that 75% SMEs used external finance with many accessing multiple methods simultaneously such as credit cards (37%), leasing or hire purchases (30%) and bank overdrafts (28%). Yet, when it comes to reporting on the obstacles the SMEs face, the SBSS 2022-23 does not mention cybersecurity risks. I interpret the evidence from the SBSS 2022-23 as an example of responsibilisation by omission whereby cybersecurity expenses simply are not reflected in the obstacles to business, whereas in fact they will form an important obstacle. These types of omissions deepen the responsibilised mindset of the population and directly impede reporting.

Hence, there is substantial work required to understand the effect of cybercrime on SMEs. This is because SMEs form an important part of the national economy and hence the harm they suffer as a result of cybercrime will impact the amount of taxes they can pay. My results have also shown that Scottish SMEs feel solely responsible for their cybersecurity, which will reduce the chances of reporting. This is why I believe that future PhDs could be dedicated to the impact of cybercrime on SMEs alone since they, unlike Individuals or Public institutions, are less represented in the cybercrime literature.

In addition, work on RNPAs could be directly extended too. Due to various confidentiality requirements, I was not able to fully showcase the interconnectedness of these organisations in Scotland. In fact, several of them closely collaborate between each other or are at least known to one another as competitors for governmental grants. There would be value in seeking to formalise this network in the arena of cybercrime reporting and beyond. The STACATO (§6.6.1) best practices for cybercrime reporting, that have been co-authored by the RNPAs, could serve as a preliminary guideline as far the common approach to his collaboration would be concerned.

Lastly, there was planned work to be conducted with Police Scotland on understanding how cybercrime offences are reported via their call-centres, which did not take place due to structural reorganisation. Future work could also build on this collaboration and seek to understand the levels of support that police staff receive for accepting reports of cybercrime. Future researchers can utilise the instruments, which I have developed, but not used for this purpose.

8.2 NEW APPROACHES

Even though this dissertation was centred around crime that happens in and around computers, it lacked a technical component. However, when considering the STACATO best practices approach to improving cybercrime reporting, there is potential for a technical project. For example, the STACATO best practices approach could be used to design a reporting interface for victims of cybercrime. Alternatively, the STACATO best practices could be used to design a system within which RNPAs could input and share intelligence, in other words, it could be a purpose-built database.

Chapter 9

Overall Conclusion

This dissertation has set out to investigate ways of improving reporting in Scotland. The core assumptions underlying this approach were anchored in the devolved landscape of Scottish policing which has separated itself from Action Fraud. The systematic literature review (SLR) served as the conceptual foundation for the understanding of victimilogy (i.e., framing the victim types as Individuals, Private and Public institutions) and cybercrime reporting approaches (i.e., Human to Human, Human to Machine, Machine To Machine). The insights (i.e., victim types and reporting approaches) from the SLR can be used to inform strategies for research into victim needs – for instance the needs of neglected SMEs. The results of these insights were interwoven in between chapters alongside the recurring theme of (§2.2) responsibilisation - i.e., the shifting of responsibility and blame for cybercrime victimisation from the state onto the victim.

I conducted three major studies to understand reporting and victims to draw out lessons for improving cybercrime reporting in Scotland. In the first study of victims, I was able to derive factors that improve (e.g., fund reimbursement) and impede cybercrime reporting (e.g., lack of faith in the police). In the second study, I offered a bespoke client-centred cybercrime training to a victimised private institution as a form of aftercare. As a result of this training, I observed a slight improvement in work practices alongside a prevailing effect of responsibilisation. The need for fund reimbursement and lack of faith in the police will also be useful in researching the unspoken costs of protecting SMEs from cybercrime, who's implicit responsibilisation is fuelled by these two factors.

In the last study, I investigated how the multi-agency approach could be used for improving cybercrime reporting. I achieved this by engaging with Responsibilised Non-Policing Agencies (RNPAs) – a novel term which I pioneered in the cybercrime reporting arena as a way of referring to multi-agency cybercrime quasi-policing work. Intriguingly, the insights that RNPAs supplied into what is required to improve cybercrime reporting (e.g., the STACATO best practices approach) corresponded to some of the literature uncovered via the SLR. The insights I extracted can be used to facilitate in-person collaborations between the heads and staff of RNPAs, but also to design a technological interface for cybercrime reporting and tactical information sharing.

Therefore, I conclude that research into improving cybercrime reporting should continue because, at least in Scotland, it displays promise for addressing the major economical and psychological costs of cybercrime victimisation. However, to achieve necessary success, policy initiatives must address the effects of responsibilisation by reducing the blame and shame placed upon the victims. This PhD dissertation is a source of direction for future scientists because it has managed to showcase how responsibilisation supplies the key assumptions for an accurate understanding of cybercrime under-reporting. Lastly, this research should continue because the deteriorating geopolitical landscape marked by Russia's hybrid war against

the UK and the increasing threat posed by China mean that cybercrime will only significantly increase in the future.

Bibliography

Abdulai, M.A. (2020). "Examining the effect of victimization experience on fear of cybercrime: University students' experience of credit/debit card fraud". In: *International Journal of Cyber Criminology* 14.1, pp. 157–174 (cit. on pp. 43, 134).

ACPO (2005). *National Call Handling Standards*. United Kingdom: Association of Chief Police Officers, p. 278 (cit. on p. 128).

Akdemir, N. and Lawless, C.J. (2020). "Exploring the human factor in cyber-enabled and cyberdependent crime victimisation: a lifestyle routine activities approach". In: *Human Factor In Cybercrime Victimisation* 30.6, pp. 1665–1687 (cit. on p. 39).

Alzubaidi, A. (2021). "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia". In: *Heliyon* 7.1 (cit. on pp. 46, 55, 136).

American Psychological Association (2019). *Quotations From Research Participants*. URL: https://apastyle.apa.org/style-grammar-guidelines/citations/quoting-participants (cit. on p. 63).

Bada, M., Furnell, S., Nurse, J.R.C., and Dymydiuk, J. (2023). "Supporting Small and Medium-Sized Enterprises in using Privacy Enhancing Technologies". In: *HCI for Cybersecurity, Privacy and Trust*. 5th International Conference, HCI-CPT 2023 Held as Part of the 25th HCI International Conference, HCII 2023 Copenhagen, Denmark, July 23–28, 2023 Proceedings. Denmark: Springer, pp. 274–289 (cit. on p. 80).

Bana, A. and Hertzberg, D. (2015). "Data Security and the Legal Profession: Risks, Unique Challenges and Practical Considerations". In: *Business International Law* 16.3, pp. 247–264 (cit. on p. 37).

Barney, J. (1991). "Firm Resources and Sustained Competitive Advantage". In: *Journal of Management* 17.1, pp. 99–120 (cit. on pp. 93, 94).

Baror, S.O., Ikuesan, R.A., and Venter, H.S. (2020). "A defined digital forensic criteria for cybercrime reporting". In: Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020, pp. 617–626 (cit. on pp. 47, 56, 136).

BBC (Nov. 15, 2019). "Employee who fell for £200k email scam feared she would lose her home". In: *BBC UK*. URL: https://www.bbc.co.uk/news/uk-scotland-glasgow-west-50432294 (cit. on pp. 60, 61).

Bennett, R.R. and Wiegand, R.B. (1994). "Observations on crime reporting in a developing nation". In: *Criminology* 32.1, pp. 135–148 (cit. on p. 11).

Bidgoli, M. and Grossklags, J. (2016). "End user cybercrime reporting: What we know and what we can do to improve it". In: 2016 IEEE International Conference on Cybercrime and Computer Forensic, ICCCF 2016 (cit. on pp. 46, 55, 59, 136).

— (2017). "'Hello. This is the IRS calling.': A case study on scams, extortion, impersonation, and phone spoofing". In: eCrime Researchers Summit, eCrime, pp. 57–69 (cit. on pp. 43, 54, 64, 70, 134).

Bidgoli, M., Knijnenburg, B.P., and Grossklags, J. (2016). "When cybercrimes strike undergraduates". In: eCrime Researchers Summit, eCrime. Vol. 2016, pp. 42–51 (cit. on pp. 45, 55, 134).

Bidgoli, M., Knijnenburg, B.P., Grossklags, J., and Wardman, B. (2019). "Report Now. Report Effectively. Conceptualizing the Industry Practice for Cybercrime Reporting". In: eCrime Researchers Summit, eCrime. Vol. 2019 (cit. on pp. 2, 46, 56, 136).

Bjelland, H.D. and Vestby, A. (2017). "'It's about using the full sanction catalogue': on boundary negotiations in a multi-agency organised crime investigation". In: *Policing & Society* 27.6, pp. 655–670 (cit. on pp. 104, 123).
Bjorge, U. J. and Wangen, G. (2021). "A Systematic Review of Cybersecurity Risks in Higher Education". In: *Future Internet* 13.2, p. 39 (cit. on p. 83).
Blažič, B.J. (2021). "The cybersecurity labour shortage in Europe: Moving to a new concept for education and training". In: *Technology in Society* 67, p. 1 (cit. on p. 87).
Bohme, R. (2013). *The Economics of Information Security and Privacy*. Springer Heidelberg New York Dordrecht London: Springer (cit. on pp. 37, 40, 53).
Bohme, R. and Moore, T. (2012). "How do consumers react to cybercrime?" In: eCrime Researchers Summit, eCrime (cit. on pp. 41, 54, 133).
Bolun, I., Bulai, R., and Ciorbă, D. (2021). "Support of education in cybersecurity". In: *Pro Publico Bono - Magyar Kozigazgatas* 1, pp. 128–147 (cit. on p. 83).
Bossler, A.M., Holt, T.J., Cross, C., and Burruss, G.W. (2020). "Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness". In: *Security Journal* 33, pp. 311–328 (cit. on pp. 35, 52, 131).
Braun, V. and Clarke, V. (2021). "One size fits all? What counts as quality practice in (reflexive) thematic analysis?" In: *Qualitative Research in Psychology* 18.3. Publisher: Routledge, pp. 328–352 (cit. on pp. 13, 25, 28, 62).
— (2022). "Conceptual and design thinking for thematic analysis." In: *Qualitative Psychology* 9.1, pp. 3–26 (cit. on pp. 13, 20, 24, 26, 28, 62).
Bright, D. and Whelan, C. (2019). "On the relationship between goals, membership and network design in multi-agency "fusion" centres". In: *Policing* 42.3, pp. 441–454 (cit. on pp. 106, 124).
Brown, R.C.H., Malsen, H., and Savulescu, J. (2019). "Against Moral Responsibilisation of Health: Prudential Responsibility and Health Promotion". In: *Public Health Ethics* 25.12, pp. 114–129. DOI: 10.1093/phe/phz006 (cit. on pp. 14, 15).
Buil-Gil, D., Miro-Llinares, F., Moneva, A., Kemp, S., and Diaz-Castano, N. (2021). "Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK". In: *European Societies* 23 (S1), pp. 47–49 (cit. on pp. 33, 39, 53).
Buil-Gil, D. and Saldana-Taboada, P. (2021). "Offending Concentration on the Internet: An Exploratory Analysis of Bitcoin-related Cybercrime". In: *Deviant Behavior* (cit. on pp. 50, 51).
Buil-Gil, D. and Zeng, Y. (2021). "Meeting you was a fake: investigating the increase in romance fraud during COVID-19". In: *Journal of Financial Crime* (cit. on pp. 30, 35, 40, 53, 133).
Bunge, E.L., Williamson, R.E., Cano, M., Leykin, Y., and Muñoz, R.F. (2016). "Mood management effects of brief unsupported internet interventions". In: *Internet Interventions* 5, pp. 36–43 (cit. on pp. 13, 24).
Burns, J. and Crawford, A. (Feb. 15, 2024). "Brianna Ghey's mother and Molly Russell's father join forces to combat online harm". In: *BBC News*. URL: https://www.bbc.co.uk/news/uk-68309102 (visited on Jan. 12, 2025) (cit. on p. 14).
Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., and Wang, V. (2021). "From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom". In: *Telematics and Informatics* 64, pp. 1–11 (cit. on p. 40).
Button, M. and Whittaker, J. (2021). "Exploring the voluntary response to cyber-fraud: From vigilantism to responsibilisation". In: *International Journal of Law, Crime and Justice* 66 (cit. on pp. 35, 53).
Cabaj, K., Domingos, D., Kotulski, Z., and Respício, A. (2018). "Cybersecurity education: Evolution of the discipline and analysis of master programs". In: *Computers & Security* 75, p. 24 (cit. on p. 84).
Carla, A. and Nicolson, M. (n.d.). "Negotiated belonging in sub-state nationalist contexts: young adult migrant narratives in Scotland and South Tyrol". In: *Comparative Migration Studies* 11.1 (), pp. 1–21 (cit. on p. 102).
Carpineto, C. and Romano, G. (2020). "An Experimental Study of Automatic Detection and Measurement of Counterfeit in Brand Search Results". In: *ACM Transactions On The Web* 14.2 (cit. on pp. 48, 137).

CFS (2018). “Number of cybercrime victims falls”. In: *Computer Fraud & Security*, p. 20 (cit. on pp. 38, 132).

Chetty, S. (1996). “The Case Study Method for Research in Small-and Medium-Sized Firms”. In: *International Small Business Journal* 15.1, pp. 73–85 (cit. on p. 80).

Cockroft, T., Shan-A-Khuda, M., Schreuders, Z.C., and Trevorrow, P. (2021). “Police Cybercrime Training: Perceptions, Pedagogy, and Policy”. In: *Policing-A Journal Of Policy And Practice* 15.1, pp. 15–33 (cit. on pp. 35, 52).

Collier, B., Horgan, S., Jones, R., and Shepherd, L. (2020). “The implications of the COVID-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations”. In: *Research Evidence in Policing: Pandemics* 1 (cit. on p. 112).

Collier, B., Thomas, D.R., Clayton, R., and Hutchings, A. (2019). “Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks”. In: *Internet Measurement Conference (IMC ’19)*. IMC’19. Amsterdam, New York, p. 15 (cit. on pp. 1, 30, 59, 113, 129).

Collier, B., Thomas, D.R., Clayton, R., Hutchings, A., and Chua, Y.-T. (2021). “Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market of cybercrime services”. In: *Policing & Society An International Journal of Research and Policy* (cit. on pp. 33, 130).

Connolly, A.Y. and Borrison, H. (2020). *Your Money or Your Business* (cit. on pp. 39, 132).

Connolly, A.Y., Wall, D.S., Lang, M., and Oddson, B. (2020). “An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability”. In: *Journal of Cybersecurity*, pp. 1–18 (cit. on pp. 39, 40, 132).

Correia, S.G. (2019). “Responding to victimisation in a digital world: a case study of fraud and computer misuse reported in Wales”. In: *Crime Science* 8.4, pp. 1–12 (cit. on pp. 30, 37, 64, 117, 129, 132).

— (2020). “Patterns of online repeat victimisation and implications for crime prevention”. In: *2020 APWG Symposium on Electronic Crime Research (eCrime)*. Boston, MA, USA: IEEE (cit. on pp. 30, 40, 53, 64, 133).

Cox, A. (Sept. 8, 2023). “Sextortion on Snapchat is not the end of my world, says victim”. In: *BBC News*, online. URL: https://www.bbc.co.uk/news/uk-northern-ireland-66736462 (visited on Jan. 12, 2025) (cit. on p. 14).

Cross, C. (2018). “Expectations vs reality: Responding to online fraud across the fraud justice network”. In: *International Journal of Law, Crime and Justice* 55, pp. 1–12 (cit. on pp. 43, 55, 64, 70, 133).

— (2019). “Is online fraud just fraud? Examining the efficacy of the digital divide”. In: *Journal of Criminological Research, Policy and Practice* 5.2, pp. 120–131 (cit. on pp. 31, 130).

— (2020a). “‘Oh we can’t actually do anything about that’: The problematic nature of jurisdiction for online fraud victims”. In: *Criminology and Criminal Justice* 20.3, pp. 358–375 (cit. on pp. 45, 47, 55, 117).

— (2020b). “Reflections on the reporting of fraud in Australia”. In: *Policing* 43.1, pp. 49–61 (cit. on pp. 47, 136).

— (2021). “Theorising the impact of COVID-19 on the fraud victimisation of older persons”. In: *The Journal of Adult Protection* 23.2, pp. 98–109 (cit. on pp. 30, 51, 134).

Cross, C. and Grant-Smith, D. (2021). “Recruitment fraud: Increased opportunities for exploitation in times of uncertainty?” In: *Social Alternatives* 40.4, pp. 9–14 (cit. on p. 59).

Cross, C., Holt, T., Powell, A., and Wilson, M. (2021). “Responding to cybercrime: Results of a comparison between community members and police personnel”. In: *Trends And Issues In Crime And Criminal Justice* 635, pp. 1–20 (cit. on pp. 43, 54).

Cross, C. and Kelly, M. (2016). “The problem of "white noise": Examining current prevention approaches to online fraud”. In: *Journal of Financial Crime* 23.4, pp. 806–818 (cit. on pp. 42, 43, 54, 133, 135).

Daily Star (May 20, 2022). “Are you being scammed? Worst regions for cybercrime and how to avoid being a victim”. In: *Daily Star (Online)*. URL: https://www.dailystar.co.uk/tech/you-being-scammed-worst-regions-27019667 (cit. on pp. 60, 65).

Das, A., Nayak, J., Naik, B., and Ghosh, U. (2021). "Generation of overlapping clusters constructing suitable graph for crime report analysis". In: *Future Generation Computer Systems-The International Journal Of Escience* 118, pp. 339–357 (cit. on pp. 48, 137).

De Kimpe, L., Walrave, M., Snaphaan, T., Pauwels, L., Hardyns, W., and Ponnet, K. (2021). "Research Note: An investigation of cybercrime victims' reporting behavior". In: *European Journal of Crime, Criminal Law and Criminal Justice* 29.1, pp. 66–78 (cit. on p. 50).

Delaney, J. (2023). "University working with police and government after cyber". In: *STV News. Glasgow & West.* URL: https://news.stv.tv/west-central/university-of-west-of-scotland-working-with-police-and-government-after-cyber-attack (cit. on p. 61).

Doig, A. (2018). "Implementing national policing agendas and strategies for fraud at local level". In: *Journal of Financial Crime* 25.4, pp. 984–996 (cit. on p. 33).

Done, E.J. and Murphy, M. (2016). "The responsibilisation of teachers: a neoliberal solution to the problem of inclusion". In: *Discourse: Studies in the Cultural Politics of Education* 39.1, pp. 142–155 (cit. on p. 14).

Donegan, M. (2019). "Crime script for mandate fraud". In: *Journal of Money Laundering* 22.4, pp. 770–781 (cit. on pp. 38, 132).

Dragoni, N., Alberto, L.L., Massacci, F., and Schlichtkrull, A. (2021). "Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs [Education]". In: *IEEE Security & Privacy* 19.1, pp. 81–88 (cit. on p. 85).

Dyson, I. (2019). *Chief Constables/PCCs* (cit. on pp. 9, 128).

Enang, I., Murray, J., Dougall, N., Wooff, A., Heyman, I., and Aston, E. (2019). "Defining and Assessing vulnerability within law enforcement and public health organisations: A scoping review." In: *Health and Justice* 7.2 (cit. on p. 10).

FBI (n.d.). *Business E-mail Compromise*. How can we help you. Scams and Safety. URL: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise#Overview (cit. on p. 61).

Finney, G. (2020). *Well Aware - Master the nine cybersecurity habits to protect your future*. 1st. United States of America: Greenleaf Book Group. 216 pp. ISBN: 978-1-62634-737-3 (cit. on pp. 87, 89, 91, 93, 94).

Fisher, J. (2008). "The UK's faster payment project: avoiding a bonanza for cybercrime fraudsters". In: *Journal of Financial Crime* 15.2, pp. 155–164 (cit. on pp. 30, 60, 129).

Forouzan, H., Jahankhani, H., and McCarthy, J. (2018). "An examination into the level of training, education and awareness among frontline police officers in tackling cybercrime within the metropolitan police service". In: *Advanced Sciences and Technologies for Security Applications*, pp. 307–323 (cit. on pp. 34, 52, 130).

Garland, D. (2002a). "103Policy Predicament: Adaptation, Denial, and Acting Out". In: *The Culture of Control: Crime and Social Order in Contemporary Society*. Oxford University Press, pp. 103–138 (cit. on pp. 10, 14, 15, 58, 72, 76, 102, 103, 109, 115, 128).

— (2002b). "167The New Culture of Crime Control". In: *The Culture of Control: Crime and Social Order in Contemporary Society*. Oxford University Press (cit. on pp. 10, 14, 27, 57, 128).

— (2002c). "193Crime Control and Social Order". In: *The Culture of Control: Crime and Social Order in Contemporary Society*. Oxford University Press (cit. on pp. 14, 62, 102).

Hadlington, L., Lumsden, K., Black, A., and Ferra, F. (2021). "A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime". In: *Policing-A Journal Of Policy And Practice* 15.1, pp. 34–43 (cit. on p. 50).

Hall, M. (2021). "Counting crime: Discounting victims?" In: *International Review of Victimology*, p. 0269758021995909 (cit. on pp. 11, 52, 128).

Hamman, S.T., Hopkinson, K.M., Markham, R.L., Chaplik, A.M., and Metzler, G.E. (2017). "Teaching Game Theory to Improve Adversarial Thinking in Cybersecurity Students". In: *IEEE Transactions on Education* 60.3, pp. 205–211 (cit. on p. 87).

Harris, M.A. and Patten, K.P. (2015). "Using Bloom's and Webb's Taxonomies to Integrate Emerging Cybersecurity Topics into a Computing Curriculum". In: *Journal of Information Systems Education* 26.3, pp. 219–234 (cit. on p. 83).

Heinonen, J.A., Holt, T.J., and Wilson, J.M. (2012). "Product Counterfeits in the Online Environment: An Empirical Assessment of Victimization and Reporting Characteristics". In: *International Criminal Justice Review* 22.4, pp. 353–371 (cit. on pp. 46, 55, 136).

Henry, A., Malik, A., and Aydin-Aitchison, A. (2019). "Local governance in the new Police Scotland: Renegotiating power, recognition and responsiveness". In: *European Journal of Criminology* 16.5, pp. 573–591 (cit. on pp. 8, 128).

HMICFRS (2020). *A call for help Police contact management through call handling and control rooms in 2018/19*. United Kingdom: Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, p. 21 (cit. on p. 129).

Horgan, S. (2021). *The reality of 'cyber security awareness': findings and policy implications for Scotland*, pp. 1–12 (cit. on p. 10).

Horgan, S. and Collier, B. (2016). "Barriers to a Cyberaware Scotland". In: *Scottish Justice Matters* 4.3, pp. 19–20 (cit. on pp. 10, 14, 58, 71, 76).

Horgan, S., Collier, B., Jones, R., and Shepherd, L. (2021). "Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing". In: *Journal of Criminal Psychology* 11.3, pp. 222–239 (cit. on pp. 33, 52).

Horwitz, L. (1964). "Transference in Training Groups and Therapy Groups". In: *International Journal of Group Psychotherapy* 14.2, pp. 202–213 (cit. on p. 96).

Hough, M. (2006). *Counselling Skills & Theory*. 2nd. Hodder Arnold. 352 pp. (cit. on p. 90).

Huaman, N., von Skarczinski, B., Stransky, C., Wermke, D., Acar, Y., Dreißigacker, A., and Fahl, S. (2021). "A large-scale interview study on information security in and attacks against small and medium-sized enterprises". In: Proceedings of the 30th USENIX Security Symposium, pp. 1235–1252 (cit. on p. 41).

Huang, R.-T. (2015). "Overcoming invisible obstacles in organizational learning: The moderating effect of employee resistance to change". In: *Journal of Organizational Change Management* 28, pp. 356–368 (cit. on p. 23).

Hudson, M., S. Weinglass, M. Turner, and J. Gunter (2023). "On the hunt for the businessmen behind a billion-dollar scam". In: *BBC Eye Investigations*. URL: https://www.bbc.co.uk/news/world-65038949 (cit. on pp. 59, 60).

Hunter, P. (2008). "UK shadow home secretary victim of online card fraud". In: *Computer Fraud & Security*, p. 4 (cit. on pp. 37, 53, 117, 131).

Hunton, P. (2011). "A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment". In: *Digital Investigation* 7.3, pp. 105–113 (cit. on pp. 32, 130).

— (2012). "Managing the technical resource capability of cybercrime investigation: A UK law enforcement perspective". In: *Public Money and Management* 32.3, pp. 225–232 (cit. on pp. 32, 51, 130).

Hutchings, A. and Collier, B. (2019). "Inside out: Characterising cybercrimes committed inside and outside the workplace". In: *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. Stockholm, Sweden: IEEE (cit. on pp. 31, 129, 130).

Hutchings, A. and Pastrana, S. (2019). "Understanding eWhoring". In: *2019 4th IEEE European Symposium On Security And Privacy (EUROS&P)*. Stockholm, Sweden: IEEE, pp. 201–214 (cit. on pp. 30, 51).

Hwee-Joo, K. and Katerattanakul, P. (2019). "Enhancing Student Learning in Cybersecurity Education using an Out-of-class Learning Approach". In: *Journal of Information Technology Education. Innovations in Practice* 18, pp. 29–47 (cit. on p. 87).

ICO URL: https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf (cit. on p. 61).

ICO URL: https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf (cit. on p. 61).

Inan, F.A., Namin, A.S., Pogrund, R.L., and Jones, K.S. (2016). "Internet Use and Cybersecurity Concerns of Individuals with Visual Impairments". In: *Educational Technology & Society* 19.1, pp. 28–40 (cit. on p. 88).

Ivy, J., Kelley, R., Cook, K., and Thomas, K. (2020). "Incorporating Cyber Principles into Middle and High School Curriculum". In: *International Journal of Computer Science Education in Schools* 4.2 (cit. on p. 82).

Jarvie, C. and Renaud, K.V. (2024). "Online Age Verification: Government Legislation, Supplier Responsibilization, and Public Perceptions". In: *Children* 11.9, p. 1068 (cit. on p. 14).

Jhaveri, M.H., Cetin, O., Gañán, C., Moore, T., and Van Eeten, M. (2017). "Abuse reporting and the fight against cybercrime". In: *ACM Computing Surveys* 49.4 (cit. on pp. 45, 55).

Johnson, C. (2019). "University of South Wales National Cyber Security Academy – Creating Cyber Graduates Who Can 'Hit the Ground Running': An Innovative Project Based Approach". In: *Higher Education Pedagogies* 4.1, pp. 300–303 (cit. on p. 86).

Johnson, D., Faulkner, E., Meredith, G., and Wilson, T.J. (2020). "Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts". In: *Journal of Criminal Law* 84.5, pp. 427–450 (cit. on pp. 32, 33, 35, 51, 52, 130, 131).

Jones, H.S., Towse, J.N., Race, N., and Harrison, T. (2019). "Email fraud: The search for psychological predictors of susceptibility". In: *Plos One* 14.1, e0209684 (cit. on pp. 39, 53).

Jones, K.S., Namin, A.S., and Armstrong, M.E. (2018). "The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals". In: *ACM Transactions on Computing Education* 18.3, pp. 1–12 (cit. on p. 86).

Jones, T., Newburn, T., and Smith, D.J. (1996). "Policing and the idea of democracy". In: *British Journal Of Criminology* 36.2, pp. 182–198 (cit. on pp. 8, 115).

Karagiannopoulos, V., Sugiura, L., and Kirby, A. (Oct. 2019). *The Portsmouth Cybercrime Awareness Clinic Project: Key Findings and Recommendations*. University of Portsmouth. 26 pp. (cit. on pp. 11, 51).

Kayali, F., Schwarz, V., Purgathofer, P., and Götzenbrucker, G. (2018). "Using Game Design to Teach Informatics and Society Topics in Secondary Schools". In: *Multimodal Technologies and Interaction* 2.4, p. 77 (cit. on pp. 82, 100).

Kemp, S., Buil-Gil, D., Moneva, A., Miro-Llinares, F., and Diaz-Castano, N. (2021). "Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19". In: *Journal Of Contemporary Criminal Justice* (cit. on p. 50).

Khader, M., Karam, M., and Fares, H. (2021). "Cybersecurity Awareness Framework for Academia". In: *Information* 12.10, p. 417 (cit. on p. 85).

Knapp, K.J., Maurer, C., and Plachkinova, M. (2017). "Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance". In: *Journal of Information Systems Education* 28.2, pp. 101–113 (cit. on p. 86).

Kuenssberg, L. (Jan. 11, 2025). "Molly Russell's dad warns UK 'going backwards' on online safety and urges PM to act". In: *BBC News*, Online. URL: https://www.bbc.co.uk/news/articles/cp3j5kp8501o (visited on Jan. 12, 2025) (cit. on p. 14).

Lacey, D., Salmon, P., and Glancy, P. (2015). "Taking the Bait: A Systems Analysis of Phishing Attacks". In: *Procedia Manufacturing* 3, pp. 1109–1116 (cit. on pp. 42, 54).

Lady Paton, Lady Clark of Calton, and Lorde Clarke URL: https://www.scotcourts.gov.uk/search-judgments/judgment?id=a2af8aa6-8980-69d2-b500-ff0000d74aa7 (cit. on pp. 58, 59).

Lavorgna, A. (2019). "Cyber-organised crime. A case of moral panic?" In: *Trends in Organized Crime* 22, pp. 357–374 (cit. on pp. 31, 36, 58, 78, 129).

Leukfeldt, E.R., Kleemans, E.R., and Stol, W.P. (2017). "Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis". In: *Crime, Law and Social Change* 67, pp. 39–53 (cit. on p. 31).

Leukfeldt, E.R., Lavorgna, A., and Kleemans, E.R. (2017). "Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime". In: *European Journal on Criminal Policy and Research* 23.33, pp. 287–300 (cit. on pp. 36, 76).

Leukfeldt, E.R., Notte, R.J., and Malsch, M. (2020). "Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes". In: *Victims & Offenders* 15.1, pp. 60–77 (cit. on pp. 1, 41, 42, 54, 69, 133).

Levi, M. (2017). "Assessing the trends, scale and nature of economic cybercrimes: overview and Issues In Cybercrimes, Cybercriminals and Their Policing, in Crime, Law and Social Change". In: *Crime, Law and Social Change* 67, pp. 3–20 (cit. on pp. 30, 51, 129).

Levi, M., Doig, A., Gundur, R., Wall, D., and Williams, M. (2017). "Cyberfraud and the Implications for Effective Risk-Based Responses: Themes from UK Research". In: *Crime, Law and Social Change* 67.1, pp. 77–96 (cit. on p. 31).

Levi, M. and Smith, R.G. (2021). "Fraud and pandemics". In: *Journal of Financial Crime* (cit. on pp. 30, 51, 110).

Levi, M. and Williams, M.L (2013). "Multi-agency partnerships in cybercrime reduction: Mapping the UK information assurance network cooperation space". In: *Information Management & Computer Security* 21.5, pp. 420–443 (cit. on pp. 30, 103, 104, 122).

Lingard, L. (2019). "Beyond the default colon: Effective use of quotes in qualitative research". In: *Perspec. Med. Edu.* 8.6, pp. 360–364 (cit. on p. 63).

Liu, F. and Tu, M. (2020). "An Analysis Framework of Portable and Measurable Higher Education for Future Cybersecurity Workforce Development". In: *Journal of Education and Learning (EduLearn)* 14.3, pp. 322–330 (cit. on p. 84).

Loggen, J. and Leukfeldt, E.R. (2022). "Unraveling the crime scripts of phishing networks: an analysis of 45 court cases in the Netherlands". In: *Trends in Organized Crime* 25.2, pp. 205–225 (cit. on p. 58).

Lord Justice Clerk, Lady Paton, and Lord Menzies URL: https://www.scotcourts.gov.uk/search-judgments/judgment?id=1c68e6a6-8980-69d2-b500-ff0000d74aa7 (cit. on p. 60).

Lord Justice Clerk, Lord Brodie, and Lord Drummond Young URL: https://www.scotcourts.gov.uk/search-judgments/judgment?id=5db2c7a6-8980-69d2-b500-ff0000d74aa7 (cit. on p. 59).

Lord Justice General, Lord Menzies, and Lord Turnbull URL: https://www.scotcourts.gov.uk/docs/default-source/cos-general-docs/pdf-docs-for-opinions/2020hcjac48.pdf?sfvrsn=a4d223dd_0 (cit. on p. 61).

Lord Menzies and Lord Turnbull URL: https://www.scotcourts.gov.uk/docs/default-source/default-document-library/2019hcjac16.pdf?sfvrsn=d7240bd2_0 (cit. on p. 60).

Lord Summers (cit. on pp. 60, 61, 108).

Lord, J. (2016). "Fifty Shades of Fraud". In: *Computer Fraud & Security* Volume 2016.6, pp. 14–16 (cit. on pp. 30, 31).

Loveday, B. (2018). "The Shape of Things to Come. Reflections on the potential implications of the 2016 Office of National Statistics Crime Survey for the police service of England and Wales". In: *Policing-A Journal Of Policy And Practice* 12.4, pp. 398–409 (cit. on p. 35).

Lum, C., Koper, C.S., and Willis, J. (2017). "Understanding the Limits of Technology's Impact on Police Effectiveness." In: *Police Quarterly* 20.2, pp. 135–163 (cit. on pp. 105, 123).

Lyle, A. (2016). "Chapter 17 Legal Considerations for Using Open Source Intelligence in the Context of Cybercrime and Cyberterrorism". In: *Open Source Intelligence Investigation. Advanced Sciences and Technologies for Security Applications*, pp. 277–294 (cit. on p. 36).

MacDonald, K. (June 12, 2019). *Action Fraud*. V3-A0718. SPC, Tulliallan (cit. on pp. 2, 9, 53, 55, 128).

Mackey, T.K., Li, J., Purushothaman, V., Nali, M., Shah, N., Bardier, C., Cai, M., and Liang, B. (2020). "Big data, natural language processing, and deep learning to detect and characterize illicit COVID-19 product sales: Infoveillance study on Twitter and Instagram". In: *JMIR Public Health and Surveillance* 6.3 (cit. on pp. 48, 137).

Maltz, M.D. (1977). "Crime Statistics: A Historical Perspective". In: *Crime & Delinquency* 23.1, pp. 32–40 (cit. on pp. 11, 52, 55, 56, 58, 128).

Mapimele, F. and Mangoale, B. (2019). "The cybercrime combating platform". In: 14th International Conference on Cyber Warfare and Security, ICCWS 2019, pp. 237–242 (cit. on p. 47).
Marquardson, J. and Gomillion, D. (2018). "Cyber Security Curriculum Development: Protecting Students and Institutions While Providing Hands-On Experience". In: *Information Systems Education Journal* 16.5, pp. 12–21 (cit. on p. 84).
Martin, P. (2019). *The Rules of Security: Staying Safe in a Risky World*. Oxford University Press (cit. on p. 78).
— (2024). *Insider Risk and Personnel Security: An Introduction*. 1st ed. Routledge (cit. on pp. 69, 130).
Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P.C., and Glenn, T. (2021). "Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry". In: *Current Psychiatry Reports* 23.4 (cit. on pp. 44, 134).
Murray, K. and Harkin, D. (2017). "Policing in cool and hot climates: Legitimacy, power and the rise and fall of mass stop and search in Scotland". In: *British Journal Of Criminology* 57.4, pp. 885–905 (cit. on pp. 9, 52, 115, 128).
Naimark, N.M. (2008). *Political violence*. Palgrave Macmillan New York. 39-47. ISBN: 978-0-230-61624-0 (cit. on p. 15).
Nappa, A., Rafique, M.Z., and Caballero, J. (2015). "The MALICIA dataset: identification and analysis of drive-by download operations". In: *International Journal of Information Security* 14.1, pp. 15–33 (cit. on p. 49).
Nasi, M., Oksanen, A., Keipi, T., and Rasanen, P. (2015). "Cybercrime victimization among young people: a multi-nation study". In: *Journal of Scandinavian Studies in Criminology and Crime Prevention* 16.2, pp. 203–210 (cit. on pp. 38, 53, 132).
National MAPPA Team HM Prison and Probation Services Public Protection Group HMP (2023). *MAPPA Guidance Updated March 2023*. Guidance. United Kingdom: Ministry of Justice, p. 178. URL: https://www.gov.uk/government/publications/multi-agency-public-protection-arrangements-mappa-guidance (cit. on p. 105).
NCSC (2020). *Whaling: How it works, and what your organisation can do about it*. URL: https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it (cit. on p. 61).
O'Sullivan, K. (2023). "Cyber raid on scots drivers: Car giant Arnold Clark faces multi-million pound ransom demand after hacking gang puts personal details of customers up for sale on the 'dark web' 'Thousands of people are at risk of having personal details used by criminals' [Scot Region]". In: *Mail on Sunday* (cit. on p. 61).
Paek, S.Y., Nalla, M.K., and Lee, J. (2020). "Determinants of police officers' support for the public-private partnerships (PPPs) in policing cyberspace". In: *Policing* 43.5, pp. 877–892 (cit. on pp. 106, 124).
Pastrana, S., Hutchings, A., Thomas, D.R., and Tapiador, J. (2019). "Measuring eWhoring". In: *IMC '19: Proceedings of the Internet Measurement Conference*, pp. 463–477 (cit. on pp. 30, 51).
Payne, B.K., He, W., Wang, C., Wittkower, D. E., and Wu, H. (2021). "Cybersecurity, Technology, and Society: Developing an Interdisciplinary, Open, General Education Cybersecurity Course". In: *Journal of Information Systems Education* 32.2, pp. 134–149 (cit. on pp. 23, 85).
Peeters, R. (2019). "Manufacturing Responsibility: The Governmentality of Behavioural Power in Social Policies". In: *Social Policy and Society* 18.1, pp. 51–65. DOI: 10.1017/S147474641700046X. URL: https://www.cambridge.org/core/product/08CA658F1AFF68236C063E75FC0D8C49 (cit. on p. 14).
Percival, R. (2022). "Cyber cons crackdown scheme for Scotland [Scot Region]". In: *Daily Star*, p. 4 (cit. on p. 60).
Peytchev, A. (2009). "Survey Breakoff". In: *Public Opinion Quarterly* 73.1, pp. 74–97 (cit. on p. 97).
Pfeffer, J. (1998). *The Human Equation: Building Profits By Putting People First*. Boston: MA: Harvard Business School Press (cit. on p. 114).

Pickering, C., Grignon, J., Steven, R., Guitart, D., and Byrne, J. (2015). "Publishing not perishing: how research students transition from novice to knowledgeable using systematic quantitative literature reviews". In: *Studies in Higher Education* 40.10, pp. 1756–1769 (cit. on pp. 13, 16, 82).

Pike, R.E., Blažič, B.J., West, T., and Zentner, A. (2020). "Digital Badges and E-Portfolios in Cybersecurity Education". In: *Information Systems Education Journal* 18.5, pp. 16–24 (cit. on pp. 23, 84).

Police Scotland (n.d.[a]). *About Us*. URL: https://www.scotland.police.uk/about-us/ (cit. on p. 8).

— (n.d.[b]). *Call handling When you call 999 or 101*. URL: https://www.scotland.police.uk/about-us/how-we-do-it/call-handling/ (cit. on p. 8).

Police Scotland and Scottish Police Authority (2020). *Cyber Strategy 2020*. (Visited on Oct. 8, 2021) (cit. on pp. 1, 9, 10, 51, 53).

Popham, J., McCluskey, M., Ouellet, M., and Gallupe, O. (2020). "Exploring police-reported cybercrime in Canada: variation and correlates". In: *Policing* 43.1, pp. 35–48 (cit. on pp. 45, 135).

Pretorius, L. (2024). "Demystifying Research Paradigms: Navigating Ontology, Epistemology, and Axiology in Research". In: *The Qualitative Report* 29.10, pp. 2698–2715 (cit. on p. 13).

Prior, S. and Renaud, K. (2023). "Who Is Best Placed to Support Cyber Responsibilized UK Parents?" In: *Children* 10.7, p. 1130 (cit. on p. 14).

Prislan, K., Bernik, I., Mesko, G., Hacin, R., Markelj, B., Vrhovec, S.L.R., and ACM (2019). "Cybercrime victimization and seeking help: A survey of students in Slovenia". In: Third Central European Cybersecurity Conference (CECC 2019) (cit. on p. 49).

Privacy Notice for Participants in Research Projects (2025). *Privacy Notice for Participants in Research Projects*. URL: https://www.strath.ac.uk/whystrathclyde/universitygovernance/accesstoinformation/dataprotection/privacynotices/ (cit. on pp. 20, 24, 25, 192).

Pusey, P. and Sadera, W.A. (2012). "Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference". In: *Journal of Digital Learning in Teacher Education* 28.2, pp. 82–88 (cit. on p. 86).

Reep-van den Bergh, C.M.M. and Junger, M. (2018). "Victims of cybercrime in Europe: a review of victim surveys". In: *Crime Science* 7.1 (cit. on p. 41).

Reinsberg, B., Kentikelenis, A., and Stubbs, T. (2021). "Creating crony capitalism: neoliberal globalization and the fueling of corruption". In: *Socio-Economic Review* 19.2, pp. 607–634 (cit. on p. 15).

Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., and Orgeron, C. (2018). "Is the responsibilization of the cyber security risk reasonable and judicious?" In: *Computers & Security* 78, pp. 198–211. ISSN: . (Cit. on pp. 10, 14, 54, 58, 71, 75, 76, 95, 108, 110, 116, 121, 128).

Renaud, K., Orgeron, C., Warkentin, M., and French, P.E. (2020). "Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China". In: *Public Administration Review* 80.4, pp. 577–589 (cit. on pp. 10, 54, 128).

Ritchie, J. and J. Lewis (2003). *Qualitative research practice: A guide for social science students and researchers*. SAGE Publications Ltd. London (cit. on pp. 13, 28, 62, 78, 126).

Sampson, F. (2014). "Cyberspace: The new frontier for policing?" In: *Cyber Crime and Cyber Terrorism Investigator's Handbook*, pp. 1–10 (cit. on pp. 35, 131).

Sanders, C.B. and Langan, D. (2019). "New public management and the extension of police control: community safety and security networks in Canada". In: *Policing & Society* 29.5. Place: Abingdon Publisher: Taylor & Francis Ltd., pp. 566–578 (cit. on pp. 105, 123).

Schaeffer, D.M., Olson, P.C., and Eck, C.K. (2017). "An Interdisciplinary Approch to Cybersecurity Curriculum". In: *Journal of Higher Education Theory and Practice* 17.9, pp. 36–40 (cit. on p. 88).

Schreuders, Z.C., Cockroft, T., Elliott, J., Butterfield, E., Soobhany, A.R., and Shan-A-Khuda, M. (2020). "Needs Assessment of Cybercrime and Digital Evidence in a UK Police Force". In: *International Journal of Cyber Criminology* 14.1, pp. 316–340 (cit. on pp. 35, 52).

Scottish Government (Jan. 28, 2020). *Scottish Index of Multiple Deprivation 2020*. URL: https://www.gov.scot/news/scottish-index-of-multiple-deprivation-2020/ (cit. on p. 81).

Scottish Government (2022). *Recorded Crime in Scotland, 2021-2022*. Publication- Statistics, p. 15. URL: https://www.gov.scot/publications/recorded-crime-scotland-2021-2022/pages/15/ (cit. on p. 57).
— (2024). *Recorded Crime in Scotland, 2023-24*. URL: https://www.gov.scot/publications/recorded-crime-scotland-year-ending-june-2024/ (cit. on pp. 4, 1).
Scully, M. (2022). "Exclusive: Brothers make millions using webcam girls to sell 'sob' stories to desperate men". In: *Mirror*. URL: https://www.mirror.co.uk/news/uk-news/brothers-make-millions-using-webcam-26508739 (cit. on p. 59).
Sexton, B. (2023). "Arnold Clark contacts 1,000s of customers over fears hackers stole their personal data [Scot Region]". In: *Daily Mail*, p. 11 (cit. on p. 61).
Shan-A-Khuda, M. and Schreuders, Z.C. (2019). "Understanding Cybercrime Victimisation: Modelling the Local Area Variations in Routinely Collected Cybercrime Police Data Using Latent Class Analysis". In: *International Journal of Cyber Criminology* 13.2, pp. 493–510 (cit. on p. 33).
Sheikhalishahi, M., Saracino, A., Martinelli, F., La Marra, A., Mejri, M., and Tawbi, N. (2020). "Digital Waste Disposal: an automated framework for analysis of spam emails". In: *International Journal Of Information Security* 19.5, pp. 499–522 (cit. on pp. 48, 137).
Sikra, J. (2021). "The connection between leadership and low training uptake: The case of RAMH". Integrated dissertation. Department of Work, Employment and Organisation: University of Strathclyde Glasgow. 78 pp. (cit. on p. 23).
— (2022). "Delivering an interactive university curriculum during Russia's invasion of Ukraine". In: VII International Scientific Conference Military Psychology in the Dimensions of War and Peace. Kyiv- Ukraine (Online): Taras Shevchenko Kyiv National University, pp. 13–16 (cit. on pp. 13, 23, 99).
— (May 9, 2023a). *Client-centred cybercrime training for Scottish Small-to-Medium Sized Enterprises (SMEs) [Delivered as part of PhD research]*. URL: https://pureportal.strath.ac.uk/en/publications/client-centred-cybercrime-training-for-scottish-small-to-medium-s (cit. on pp. 89, 93–95).
— (2023b). "Evaluating a university curriculum delivered during Russia's invasion of Ukraine". In: *The Bulletin of Taras Shevchenko University of Kyiv Social Work* 8.1, pp. 78–80 (cit. on pp. 13, 23, 99).
Sikra, J., Renaud, K., Aßmuth, A., and Frank, R. (2024). "7th Strathclyde International Perspectives on Cybercrime Summer School". In: *7th Strathclyde International Perspectives on Cybercrime Summer School*. University of Strathclyde (cit. on p. 136).
Singh, S., Singh, M. P., Pandey, R., and IEEE (2020). "Phishing Detection from URLs Using Deep Learning Approach". In: Proceedings Of The 2020 5th International Conference On Computing, Communication And Security (ICCCS-2020) (cit. on pp. 48, 137).
Skidmore, M., Goldstraw-White, J., and Gill, M. (2020). "Understanding the Police Response to Fraud: The Challenges in Configuring a Response to a Low-Priority Crime on the Rise". In: *Public Money & Management* 40.5, pp. 369–379 (cit. on p. 9).
Smith, S. (2023). "Towards a Scientific Definition of Cyber Resilience". In: *Proceedings of the 18th International Conference on Cyber Warfare and Security*. Vol. 18. TowsonUniversity (cit. on pp. 80, 82).
Sommer, P. (2017). "The future for the policing of cybercrime". In: *Crime and Deviance in Cyberspace*, pp. 541–546 (cit. on pp. 34, 65, 77, 117, 130).
Stevens, T. and O'Brein, K. (2019). "Brexit and Cyber Security". In: *The RUSI Journal* 164.3, pp. 22–30. ISSN: 1744-0378 (cit. on p. 36).
Stewart, S. (2022). "Experts fear Kremlin cyber attacks: Security analysts warn of imminent assaults by Russian hacker gangs". In: *Sunday Post*, p. 17 (cit. on pp. 60, 61).
Švábenský, V., Čeleda, P., Vykopal, J., and Brišáková, S. (2021). "Cybersecurity knowledge and skills taught in capture the flag challenges". In: *Computers & Security* 102, p. 1 (cit. on p. 88).
Sweeney, M. (2023). "Royal Mail resumes overseas deliveries via post offices after cyber-attack". In: *The Guardian*. URL: https://www.theguardian.com/business/2023/feb/21/royal-mail-international-deliveries-cyber-attack-ransom-strikes (cit. on p. 61).

Tagarev, T. (2016). "A generic reference curriculum on cybersecurity". In: *Information & Security* 35.1, pp. 181–184. ISSN: 1311-1493 (cit. on pp. 83, 84).
Tarling, R. and Morris, K. (2010). "Reporting Crime to the Police". In: *British Journal Of Criminology* 50.3, pp. 474–490 (cit. on p. 11).
Taylor, B., Kaza, S., and Zaleppa, P.A. (2021). "CLARK: A Design Science Research Project for Building and Sharing High-Quality Cybersecurity Curricula". In: *IEEE Security & Privacy* 19.5, pp. 72–76 (cit. on p. 85).
Terpstra, J. (2008). "Research Article: Police, local government, and citizens as participants in local security networks". In: *Police Practice and Research* 9.3, pp. 213–225 (cit. on pp. 103, 122).
Thatcher, J.B. and Perrewé, P.L. (2002). "An Empirical Examination of Individual Traits as Antecedents to Computer Anxiety and Computer Self-Efficacy". In: *MIS Quarterly* 26.4, pp. 381–396 (cit. on p. 23).
Thomas, D.R., Collier, B., and Renaud, K.V. (2019). *SIPR PhD Studentships Proposal - 50/50 Matched funded* (cit. on pp. 4, 1).
Vain, J. and Kharchenko, V. (2016). "Enhanced education for cybersecurity and resilience". In: *Information & Security* 35.1, pp. 5–8 (cit. on p. 83).
Van de Weijer, S., Leukfeldt, R., and Van der Zee, S. (2020a). "Reporting cybercrime victimization: determinants, motives, and previous experiences". In: *Policing* 43.1, pp. 17–34 (cit. on pp. 2, 42).
— (2020b). "Reporting cybercrime victimization: determinants, motives, and previous experiences". In: *Policing* 43.1, pp. 17–34 (cit. on pp. 45, 46, 55, 133, 135).
Van De Weijer, S.G.A. and Leukfeldt, E.R. (2017). "Big Five Personality Traits of Cybercrime Victims". In: *Cyberpsychology, Behavior, and Social Networking* 20.7, pp. 407–412 (cit. on p. 41).
Van de Weijer, S.G.A., Leukfeldt, R., and Bernasco, W. (2019). "Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking". In: *European Journal of Criminology* 16.4, pp. 486–508 (cit. on p. 49).
Waldrop, M.M. (2016). "The Human Side of Cybercrime". In: *Nature* 533, pp. 164–167 (cit. on p. 38).
Wall, D.S. (2013). "Policing identity crimes". In: *Policing and Society* 23.4, pp. 437–460 (cit. on pp. 32, 130).
Whitty, M.T. (2018). "Do You Love Me? Psychological Characteristics of Romance Scam Victims". In: *Cyberpsychology, Behavior, And Social Networking* 21.2, pp. 105–109 (cit. on pp. 30, 51).
Wilson-Kovacs, D. (2021). "Digital media investigators: challenges and opportunities in the use of digital forensics in police investigations in England and Wales". In: *Policing: An International Journal* 44.4, pp. 669–682 (cit. on pp. 35, 117).
Winder, D. and Trump, I. (2015). "Mitigating Cybercrime Through Meaningful Measurement Methodologies". In: *The EDP Audit, Control, and Security Newsletter* 52.5, pp. 1–8 (cit. on p. 49).
Wirth, A. (2018). "The Times They Are a-Changin': Part Two". In: *Biomedical Instrumentation & Technology*, pp. 236–240 (cit. on pp. 31, 130).
Wooff, A. (2015). "Relationships and responses: Policing anti-social behaviour in rural Scotland". In: *Journal of Rural Studies* 39, pp. 287–295 (cit. on pp. 8, 9, 51, 52, 115, 127, 128).
— (2016). "'Soft' Policing in Rural Scotland". In: *Policing* 11.2, pp. 123–131 (cit. on pp. 8, 9, 51, 52, 115, 127, 128).
Workman, M.D., Luevanos, J.A., and Mai, B. (2022). "A Study of Cybersecurity Education Using a Present-Test-Practice-Assess Model". In: *IEEE Transactions on Education* 65.1, pp. 40–45 (cit. on p. 88).
Wyatt, G. (2003). "Corruption, Productivity and Socialism". In: *Kyklos, the International Review for Social Sciences* 56.2, pp. 223–244 (cit. on p. 15).
Yadav, H., Gautam, S., Rana, A., Bhardwaj, J., and Tyagi, N. (2021). *Various Types of Cybercrime and Its Affected Area*. Vol. 164. Lecture Notes in Networks and Systems. 305 pp. (cit. on pp. 46, 135).
Yalom, I.D. (2011). *Staring at the sun - Overcoming the dread of death*. Great Britain: Clays Ltd, St Ives plc. 306 pp. (cit. on pp. 90, 95, 99, 133).
Yalom, I.D. and Leszcz, M. (2005). *The theory and practice of group psychotherapy*. 5th. Basic Books. 679 pp. (cit. on pp. 90, 99, 133).

Yang, S.C. (2021). “A Meta-Model of Cybersecurity Curriculums: Assessing Cybersecurity Curricular Frameworks for Business Schools”. In: *Journal of Education for Business* 96.2, pp. 99–110 (cit. on p. 86).

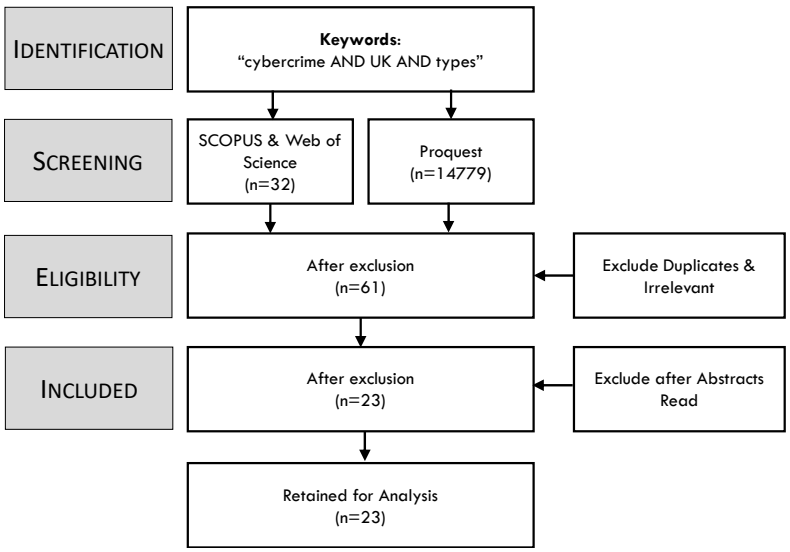
Yang, S.C. and Wen, B. (2017). “Toward a cybersecurity curriculum model for undergraduate business schools: A survey of AACSB-accredited institutions in the United States”. In: *Journal of Education for Business* 92.1, pp. 1–8 (cit. on pp. 82, 84).

Zuopeng, J.Z., Wu, H., Li, W., and Abdous, M.H. (2021). “Cybersecurity awareness training programs: a cost–benefit analysis framework”. In: *Industrial Management & Data Systems* 121.3, pp. 613–636 (cit. on p. 87).

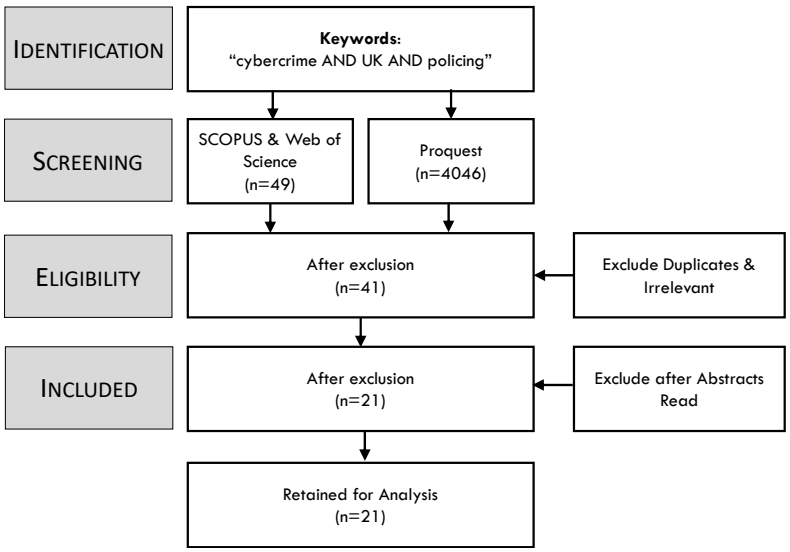
Appendix A

PRISMA Appendix

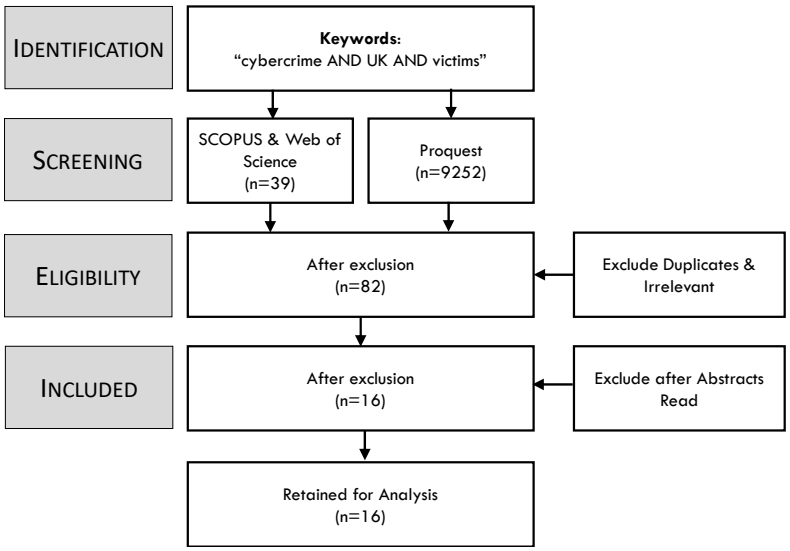
A.1 PRISMA 1



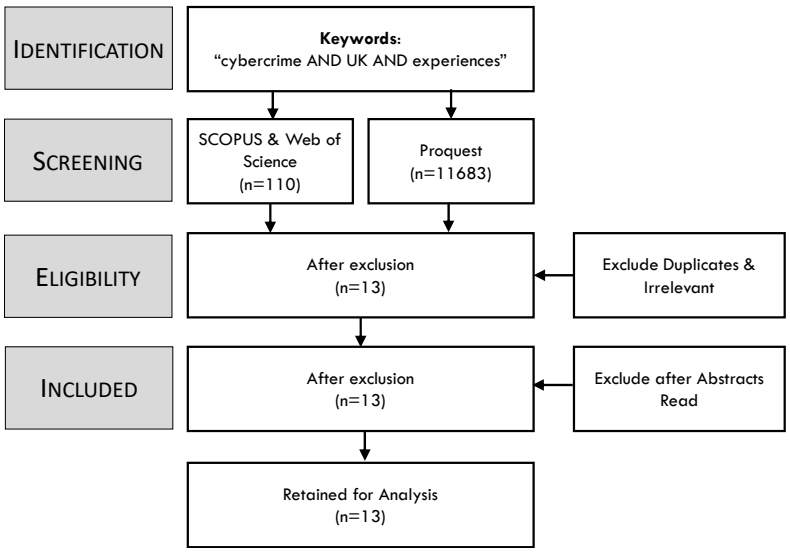
A.2 PRISMA 2



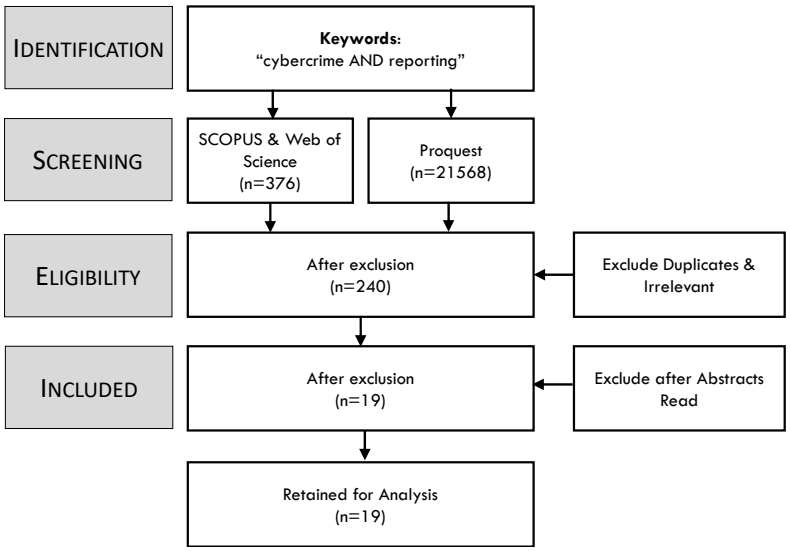
A.3 PRISMA 3



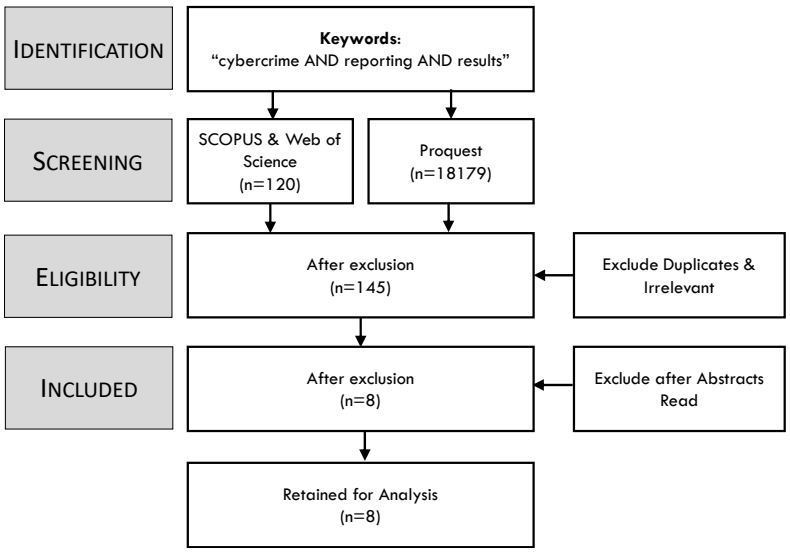
A.4 PRISMA 4



A.5 PRISMA 5



A.6 PRISMA 6


IDENTIFICATION
Keywords:
"cybercrime AND reporting AND results"
SCREENING
SCOPUS & Web of Science
(n=120)
Proquest
(n=18179)
ELIGIBILITY
After exclusion
(n=145)
Exclude Duplicates & Irrelevant
INCLUDED
After exclusion
(n=8)
Exclude after Abstracts Read
Retained for Analysis
(n=8)

Appendix B

SVC Appendix

B.1 SVC PARTICIPANT INFORMATION SHEET

Participant Information Sheet for Study Participants

Name of department: Computer and Information Sciences

Title of the study: Improving cybercrime reporting in Scotland: The victims' perspective

Introduction
My name is Juraj Sikra (e-mail: juraj.sikra@strath.ac.uk) and I am a first year PhD student at the University of Strathclyde (Glasgow) at the Department of Computer and Information Sciences with a professional background in the Scottish mental health system.

My supervisor is Dr Daniel R Thomas (e-mail: d.thomas@strath.ac.uk) – Chancellor's Fellow at the University of Strathclyde.

This study was designed in response to the fact that an increasing number of people are victimised by online scams, which they are reluctant to report for various reasons. I'm doing this study to understand what gets in the way of reporting this type of crime so that the approaches can be adjusted to serve victims' needs. To achieve this, I need to collect data via interviews with people and organizations that have lived experience of this type of crime. Whilst revisiting these experiences can bring about negative emotions, it can also help protect other people from being victimised in the future. The interviews will collect mainly information around your experiences and reasons around reporting the crime. However, there will be other questions as well, which will help me understand you as a person. This information is vital for improving reporting as it provides a fuller picture of the victims' situation.

What is the purpose of this research?
The aim of this research is to understand what gets in the way of people reporting cybercrime to the police and using those findings to adjust the systems in place for reporting cybercrime so that more people are willing to come forward.

Do you have to take part?
Your participation in this interview is entirely voluntary and you may withdraw during any time. If you consent, then I would like to use Microsoft Teams, Zoom or Skype online or an Olympus WS-853 Voice recordings either in person or over the phone to record our interview as this will help me capture verbatim what your thoughts are. All information that you provide me with will kept confidential in terms of being untraceable to you as an individual. The information, which you provide, including some of your anonymised quotes may be used in published versions of this research to support any common trends that may emerge. You may refuse to answer any of the questions or discontinue the interview during at any time and without providing a reason. Would you like to take a moment to see whether you have any questions about what you have just read?

What will you do in the project?
You will be asked to answer 10 interview questions (and some sub-questions) about your experience of cybercrime as well as about you as a person. Try to think of it as an informal conversation rather than an interview if you can. The questions will be asked by the researcher Juraj Sikra.

Why have you been invited to take part?
You have been invited to take part because you are a victim of cybercrime and potential user of the police's reporting systems.

What are the potential risks to you in taking part?
There are no risks to taking part, but you may experience some negative emotions when remembering how you were victimised by cybercrime. Alternatively, you may find that talking over your experience has helped. If you experience any negative emotions, you are encouraged to reach out to a support agency such as **Victim Support Scotland** https://victimsupport.scot/ or using their telephone number on 0800 160 1985.

What information is being collected in the project?
The main information that is of interest is people's experience of cybercrime reporting. All other data such as gender and age range are merely indicators that allow the researchers to make inferences about the population. This research does not collect and analyse data that pertains to the specific identity of victims.

Where will the information be stored and how long will it be kept for?
The Microsoft Teams, Zoom or Skype online or an Olympus WS-853 Voice recordings either in person or over the phone recordings shall be safely downloaded on the University of Strathclyde's One Drive until being destroyed no later than December 2022. The full length transcribed and anonymised interviews will be stored for no longer than October 2024 by which time it is expected that selected anonymised quotes from them will be integrated into a publicly available study. The researcher will carry out the transcriptions.

Thank you for reading this information – please ask any questions if you are unsure about what is written here.

All personal data will be processed in accordance with data protection legislation. Please read our Privacy Notice for Research Participants for more information about your rights under the legislation.

What happens next?
You'll now be asked whether you want to participate. Then, the interview will commence. If you want to know more about the project then feel free to speak to the researcher at the end of the session. Also, if you would like access to work once it has been published, then please indicate that now. Is there any other information that you require to provide your informed consent?

Researchers' contact details:
Dr Juraj Sikra

E-mail: juraj.sikra@strath.ac.uk
Chief Investigator details:
Dr Daniel R Thomas
Computer and Information Sciences
Livingstone Tower
University of Strathclyde (Glasgow-UK)
Tel.no.: + 44 141 548 3524
E-mail: d.thomas@strath.ac.uk

This research was granted ethical approval by the Departmental Ethics Committee.

If you have any questions/concerns, during or after the research, or wish to contact an independent person to whom any questions may be directed or further information may be sought from, please contact:

Department of Computer & Information Sciences Ethics Committee
email: ethics@cis.strath.ac.uk

B.2 SVC CONSENT FORM

Consent Form for Study Participants

Name of department: Computer and Information Sciences
Title of the study: Improving cybercrime reporting in Scotland: The victims' perspective

- I confirm that I have read and understood the Participant Information Sheet for the above project and the researcher has answered any queries to my satisfaction.
- I confirm that I have read and understood the Privacy Notice for Participants in Research Projects and understand how my personal information will be used and what will happen to it (i.e. how it will be stored and for how long).
- I understand that my participation is voluntary and that I am free to withdraw from the project at any time, up to the point of completion, without having to give a reason and without any consequences.
- I understand that I can request the withdrawal from the study of some personal information and that whenever possible researchers will comply with my request. This includes the following personal data:
    - Microsoft Teams, Zoom or Skype online or an Olympus WS-853 Voice recordings either in person or over the phone that identify me;
    - My personal information from transcripts.
- I understand that anonymised data (i.e. data that do not identify me personally) cannot be withdrawn once they have been included in the study.
- I understand that any information recorded in the research will remain confidential and no information that identifies me will be made publicly available.
- I consent to being a participant in the project.
- I consent to being recorded with Microsoft Teams, Zoom or Skype online or an Olympus WS-853 Voice recordings either in person or over the phone and will turn on my camera only if I consent to do so.

(PRINT NAME)	
Signature of Participant:	Date:

B.3 SVC INTERVIEW QUESTIONS

Juraj Sikra

01 December 2022

Improving cybercrime reporting in Scotland: The victims' perspective

Note: Victims

Demographics:

(i) What is your gender?
(ii) What is your age range: 18-24; 25-34; 35-44; 45-54; 55-64; 64+

0. What was your understanding of scams and cybercrime before it happened to you?
1. What kind of IT technology do you use in your everyday life?
>How comfortable are with using this technology?
2. Please walk me through what happened to you when you were victimised. Please include as much factual detail as possible including, for example, date and time, but also your surroundings and anything else that comes to mind.
3. Who did you contact to report the experience to initially?
>Why did you go to them?
>Can you please provide an example of something they said or did that was helpful?
> Can you please provide an example of something they said or did that was unhelpful?
4. If you did not initially report to the police, when have you decided to report to them and how helpful were they?
>Why did you go to them?
>Was there anything they said or did that was unhelpful?
5. Please walk me through your experience of reporting? What steps did you follow?
6. When you reported the cybercrime to the police, did you feel that you were treated differently based on your religion, gender, ethnicity, disability, age, gender-reassignment status or any other aspect of who you are that was separate from the fact that you were victimised?
7. Based on how you were treated by the police, how likely are you to report similar instances of cybercrime in the future?
>What could the police improve about their approach to encourage you to report even more?
>In your opinion, whose responsibility is it to report this cybercrime?
8. What kind of aftercare did you receive from the police?
> Did you receive after care from any other agency?
9. Please describe whether you encountered any obstacles in terms of your ability or accessibility to technology when reporting the cybercrime?
10. What would an ideal reporting system look like?

Appendix C

CCCT Appendix

C.1 CCCT Participant information sheet

Participant Information Sheet for Study Participants

Name of department: Computer and Information Sciences

Title of the study: Cybercrime client-centred training

Introduction
My name is Dr Juraj Sikra (e-mail: juraj.sikra@strath.ac.uk) and I am a second year PhD student at the University of Strathclyde (Glasgow) at the Department of Computer and Information Sciences with the majority of my background in clinical and criminal mental health. More topically, I have experience in evaluating the reasons for low training uptake in Scottish regional mental health charity as well as delivering an online curriculum into a warzone in Ukraine during the Russian invasion. You can find out more about me by copy pasting this link into your browser: https://pureportal.strath.ac.uk/en/persons/juraj-sikra.

My supervisor is Dr Daniel R Thomas (e-mail: d.thomas@strath.ac.uk) – Chancellor's Fellow at the University of Strathclyde. You can find out more about Daniel by copy pasting this link into your browser: https://personal.cis.strath.ac.uk/d.thomas/.

What is the purpose of this research?
The purpose of this research is to evaluate a cybercrime client-centred training for your company after it had been attacked by cybercrime/ ransomware. Following discussions with your manager it was agreed that a tailored training would be delivered to your company free of charge. In return, the researchers would be allowed to use the data from the pre-training and post-training questionnaires as a part of their research. During this research you will be required to complete a short-pre training questionnaire where you will speak about what you need to learn. The data from this questionnaire will be used to develop a tailored training for you and your colleagues. Subsequently, you will receive the training in the premises of your company. Afterwards, you will be asked to fill out a post-training questionnaire. The latter will measure the effectiveness of the training. The researcher will then compare the pre-training questionnaire with the post-training questionnaire to evaluate the effectiveness of the cybercrime client-centred training.

Do you have to take part?
Your participation in this research is entirely voluntary and you can withdraw at any time.

What will you do in the project?
1. You will fill out an online pre-training questionnaire consisting of 10 questions, which should take approximately 5 minutes to fill in. This questionnaire collects information that is required to

understand your training needs in addition to your age range, gender, position. Your responses will be anonymised and not traceable back to you. The management of your company will not have access to your answers from the questionnaire.
2. Subsequently, you will complete the in-person training within the premises of the company on an agreed date.
3. After the in-person training, you will be sent a link to a post-training questionnaire which will contain 10 questions. These should take approximately 5 minutes to fill in. This questionnaire collects information about your age, gender, position. Your responses will be anonymised and not traceable back to you. The management of your company will not have access to your answers from the questionnaire.

Why have you been invited to take part?
You have been invited to take part because your organisation was a victim of a ransomware attack. As a person who is professionally associated with the organisation, you play a vital role in supporting its cyber-resilience. Hence, the purpose of this training is to put you in a position of power when safeguarding your organisation's cyber-resilience.

What are the potential risks to you in taking part?
There are no risks to taking part, but you may experience some negative emotions when remembering how your company was victimised. Alternatively, you may find that undergoing this training will make you feel empowered. If you experience any negative emotions, you are encouraged to reach out to a support agency such as Victim
Support Scotland https://victimsupport.scot/ or using their telephone number on 0800 160 1985.

What information is being collected in the project?
In addition to the information supplied in the pre- and post-training questionnaires, this project collects information about the number of attendees, their gender, age and position within the company. Moreover, this project will collect your name and surname on the consent form solely for the purpose of connecting the results from your pre-training questionnaire to your post-training questionnaire to measure the effectiveness of the training. The collected information will be carefully anonymised before being published in an open-access academic journal.

Where will the information be stored and how long will it be kept for?
The pre- and post-training questionnaires will be stored on the University of Strathclyde's One Drive from the time they are completed until no later than October 2024 after which all of the data will be destroyed. Please read our **Privacy Notice for Research Participants** on the upcoming page for more information about your rights under the legislation. You can also download a copy from
here: University Ethics Committee

What happens next?

Next you will be asked to complete the pre-training questionnaire in this online form.

Researchers' contact details:
Dr Juraj Sikra
E-mail: juraj.sikra@strath.ac.uk
Chief Investigator details:
Dr Daniel R Thomas
Computer and Information Sciences
Livingstone Tower
University of Strathclyde (Glasgow-UK)
Tel.no.: + 44 141 548 3524
E-mail: d.thomas@strath.ac.uk

This research was granted ethical approval by the Departmental Ethics Committee.
If you have any questions/concerns, during or after the research, or wish to contact an independent person to whom any questions may be directed or further information may be sought from, please contact:
Department of Computer & Information Sciences Ethics Committee
email: ethics@cis.strath.ac.uk

C.2 CCCT CONSENT FORM

Consent Form for Study Participants

Name of department: Computer and Information Sciences

Title of the study: Cybercrime client-centred training

* I confirm that I have read and understood the Participant Information Sheet for the above project and the
researcher has answered any queries to my satisfaction.

* I confirm that I have read and understood the Privacy Notice for Participants in Research Projects and
understand how my personal information will be used and what will happen to it (i.e. how it will be stored
and for how long).

* I understand that my participation is voluntary and that I am free to withdraw from the project at any time,
up to the point of completion, without having to give a reason and without any consequences.

* I understand that I can request the withdrawal from the study of some personal information and that
whenever possible researchers will comply with my request. This includes the following my personal information from questionnaires

* I understand that anonymised data (i.e. data that do not identify me personally) cannot be withdrawn once
they have been included in the study.

* I understand that any information recorded in the research will remain confidential and no information that
identifies me will be made publicly available.

* I consent to being a participant in the project.

C.3 CCCT PRE-TRAINING QUESTIONNAIRE

Juraj Sikra via Qualtrics, 24 March 2023
Age:
Gender:
Date:
Position:

Cybercrime client-centred pre-training questionnaire
1. How would you rate your current understanding of cybercrime on a scale of 1-10, where 1 is “no understanding” and 10 is “cybercrime expert.”
2. What kind of improvement are you hoping to achieve at the end of this training on a scale of 1-10, where 1 is “no understanding” and 10 is “cybercrime expert.”
3. What do you want to learn about that will be useful for your role in the company?
4. What do you want to learn about that will be useful for your personal life?
5. What made you choose this training?
6. Tell me about what kind of learning is most enjoyable to you.
7. Is there anything that you’re looking especially forward to about this training?
8. Is there anything that makes you apprehensive about this training?
9. Please rate how you feel about preventing cybercrime before completing this training where 0 is no emotion and 10 is extreme emotion.
10. Do you have a disability that may impact your learning? If so, what supports do you require to make your learning effective?

C.4 CCCT POST-TRAINING QUESTIONNAIRE

Juraj Sikra via Qualtrics, 24 March 2023
Age:
Gender:
Date:
Position:

Cybercrime client-centred post-training questionnaire
1. How would you rate your cybercrime knowledge after the training on a scale of 1-10, where 1 is “no understanding” and 10 is “cybercrime expert.
2. Was the training material and content helpful for you? (Yes/ No)
3. What was a helpful aspect of the training?
4. What was an unhelpful aspect of the training?
5. Was the training programme interactive and engaging? (Yes/ No)
6. What part of the training will you apply into your job role?
7. What part of the training will you apply into your personal life?
8. Was the training easy to understand?
9. Please rate the supportiveness of the course leader during your learning, where 0 is "completely unsupportive" and 10 is "extremely supportive."
10. Please rate how you feel about preventing cybercrime after completing this training where 0 is no emotion and 10 is extreme emotion.

C.5 CCCT PARTICIPANT INFORMATION SHEET

Participant Information Sheet for Study Participants

Name of department: Computer and Information Sciences

Title of the study: Cybercrime client-centred training – Qualitative interviews

Introduction

My name is Dr Juraj Sikra (e-mail: juraj.sikra@strath.ac.uk) and I am a second year PhD student at the University of Strathclyde (Glasgow) at the faculty of Computer and Information Sciences with the majority of my background in clinical and criminal mental health. More topically, I have experience in evaluating the reasons for low training uptake in Scottish regional mental health charity as well as delivering an online curriculum into a warzone in Ukraine during the Russian invasion. You can find out more about me by following this link: https://pureportal.strath.ac.uk/en/persons/juraj-sikra.

My supervisor is Dr Daniel R Thomas (e-mail: d.thomas@strath.ac.uk) – Chancellor's Fellow at the University of Strathclyde. You can find out more about Daniel by following this link: https://personal.cis.strath.ac.uk/d.thomas/.

What is the purpose of this research?

The purpose of this research is to augment the research on Cybercrime-client centred training, which you have recently attended. This was the training where you were required to complete a pre-training questionnaire based on which a bespoke training was developed for your company. After you completed the training, you completed a post-training questionnaire about your experience. This study is connected to but separate from the previous one.

Organisations, which have agreed to participate in the former research will be invited to participate in its current extension, which aims to evaluate how people's views and practices in cybersecurity have evolved since they have received the training after a period of at least three weeks or more. This will enrich the research into cybercrime client-centred training as currently it is merely based on quantitative surveys, hence introducing the qualitative interviews will aid a more holistic evaluation of this approach.

Do you have to take part?

Your participation in this research is entirely voluntary.

What will you do in the project?

You will be expected to answer 10 interview questions, which you will receive in advance your arranged date. We do not expect this to exceed 30 minutes of your time. This is not a test, but merely a detailed exploration of how useful the training was after a period of time has passed. If you find that the training has not helped you as much as you hoped, then please inform us of this during the interview. Everything you have to say is invaluable to us, so please do not feel that you must prepare for this in any way. There are no right or wrong answers. These interviews will be recorded by either online Zoom, Skype, Teams where you can opt for having your camera switched on or off. Alternatively, if you wish these interviews can be recorded in-person with the use of an Olympus WS-853 voice recorder.

Why have you been invited to take part?

You have been invited to take part because you have completed the Cybercrime client-centred training and this is a follow-up to explore how much of what you learned remained meaningful for you in everyday life be it at the workplace and/or privately.

What are the potential risks to you in taking part?
There are no risks to taking part, but you may experience some negative emotions when remembering certain parts of the training such as for example discussions about how your company was victimised or learning about different types of risks. Alternatively, you may find that undergoing these interviews will make you feel empowered and help consolidate your learning. If you experience any negative emotions, you are encouraged to reach out to a support agency such as Victim Support Scotland https://victimsupport.scot/ or using their telephone number on 0800 160 1985.

What information is being collected in the project?
The information that will be collected will be Age Range, Gender, Date, Position, and Educational attainment. We collect this information to get a better idea of what the people who received this training look like from a human resources perspective. Hence, we will use this information to make inferences about how much of Scotland's employed population might benefit from this training. In addition, we will use this information to make inferences about the suitability of current Scottish cyber-trainings for people with your professional profile.

Where will the information be stored and how long will it be kept for?
The recordings will be stored on the University of Strathclyde's One Drive from the time they are completed until no later than October 2024 after which all the data will be destroyed. Please read our **Privacy Notice for Research Participants** for more information about your rights under the legislation.

What happens next?

Next you will be interviewed.

Researchers' contact details:
Dr Juraj Sikra

E-mail: juraj.sikra@strath.ac.uk
Chief Investigator details:
Dr Daniel R. Thomas
Computer and Information Sciences
Livingstone Tower
University of Strathclyde (Glasgow-UK)
Tel.no.: + 44 141 548 3524
E-mail: d.thomas@strath.ac.uk

This research was granted ethical approval by the Departmental Ethics Committee.

If you have any questions/concerns, during or after the research, or wish to contact an independent person to whom any questions may be directed or further information may be sought from, please contact:

Department of Computer & Information Sciences Ethics Committee
email: ethics@cis.strath.ac.uk

C.6 CCCT CONSENT FORM

Consent Form for Study Participants

Name of department: Computer and Information Sciences
Title of the study: Cybercrime client-centred training – Qualitative interviews

- I confirm that I have read and understood the **Participant Information Sheet** for the above project and the researcher has answered any queries to my satisfaction.
- I confirm that I have read and understood the **Privacy Notice for Participants in Research Projects** and understand how my personal information will be used and what will happen to it (i.e., how it will be stored and for how long).
- I understand that my participation is voluntary and that I am free to withdraw from the project at any time, up to the point of completion, without having to give a reason and without any consequences.
- I understand that I can request the withdrawal from the study of some personal information and that whenever possible researchers will comply with my request. This includes the following personal data:
    - video or audio recordings of interviews that identify me.
    - my personal information from transcripts.
- I understand that anonymised data (i.e., data that do not identify me personally) cannot be withdrawn once they have been included in the study.
- I understand that any information recorded in the research will remain confidential and no information that identifies me will be made publicly available.
- I consent to being a participant in the project.
- I consent to being audio and/or video recorded as part of the project.

(PRINT NAME)	
Signature of Participant:	Date:

C.7 CCCT Qualitative interview

Demographics
Age Range (18-24; 25-34; 35-44; 45-54; 55-64; 64+):
Gender:
Date:
Position:
Educational attainment (Select the highest applicable):
a) Certificate of Higher Education – Advanced Higher/ Higher National Certificate
b) Diploma of Higher Education – Higher National Diploma
c) Bachelors Degrees – Graduate Diplomas and Certificates
d) Bachelors Degrees with Honours – Graduate Diplomas and Certificates
e) Masters Degrees (including all Postgraduate Degrees)
f) None apply, please specify in your own words your level of educational attainment.

Cybercrime client-centred post-training qualitative interview

1. Looking back at the time you spent at the client-centred cybercrime training, how helpful was it for your role in the company and why?
2. Looking back at the time you spent at the client-centred cybercrime training, how helpful was it for your personal life and why?
3. Has the client-centred cybercrime training affected your confidence in the realm of cybersecurity? If so, how, what changes to your confidence have you observed?
4. Has the client-centred cybercrime training affected your skills in the realm of cybersecurity? If so, how, what changes to your skills have you observed?
5. Since the time you have attended the client-centred cybercrime training, have you shown leadership/initiative in making your company more cybersecure? If so, what have you done that was an act of leadership/ initiative?
6. Since the time you have attended the client-centred cybercrime training, have you shown leadership/ initiative in making your personal life more cybersecure? If so, what have you done that was an act of leadership/ initiative?
7. Since the time you have attended the client-centred cybercrime training, how has your perception of the company's priceless assets evolved in cybersecurity?
8. Since the time you have attended the client-centred cybercrime training, how has your perception of the company's prized assets evolved in cybersecurity?
9. Since the time you have attended the client-centred cybercrime training, how has your understanding of the need to report cybercrime evolved?
10. If you or your company became a victim of a cyberattack how would you proceed with reporting this offence? Please supply a real or theoretical example for each.

C.8 CCCT Quantitative comparisons

Participant.: 01 (Age range: 18-24, female)			
Knowledge			
Pre-training		**Post-training**	
Current	**Desired**	**Achieved**	**Improvement**
4	8	6	Yes.
Emotions			
	Pre-training	**Post-training**	
Anxious	2	2	
Depressed	0	1	
Confident	4	3	
Rated lecturer supportiveness			
50%			

Figure C.1: Participant 1

Participant no.: 02 (Age range: 55-64, female)			
Knowledge			
Pre-training		**Post-training**	
Current	**Desired**	**Achieved**	**Improvement**
5	8	6	Yes.
Emotions			
	Pre-training	**Post-training**	
Anxious	2	3	
Depressed	0	1	
Confident	8	9	
Rated lecturer supportiveness			
100%			

Figure C.2: Participant 2

Participant no.: 03 (Age range: 18-24, female)			
Knowledge			
Pre-training		**Post-training**	
Current	**Desired**	**Achieved**	**Improvement**
2	6	5	YES.
Emotions			
	Pre-training	**Post-training**	
Anxious	4	5	
Depressed	0	0	
Confident	1	5	
Rated lecturer supportiveness			
80%			

Figure C.3: Participant 3

Participant no.: 04 (Age range: 18-24, male)			
Knowledge			
Pre-training		**Post-training**	
Current	**Desired**	**Achieved**	**Improvement**
5	8	5	-
Emotions			
	Pre-training	**Post-training**	
Anxious	5	0	
Depressed	0	0	
Confident	4	0	
Rated lecturer supportiveness			
100%			

Figure C.4: Participant 4

Participant no.: 05 (Age range: 25-34, male)			
Knowledge			
Pre-training		**Post-training**	
Current	Desired	Achieved	Improvement
2	3	2	-
Emotions			
	Pre-training	**Post-training**	
Anxious	0	0	
Depressed	0	0	
Confident	0	10	
Rated lecturer supportiveness			
100%			

Figure C.5: Participant 5

Appendix D

RNPAs Appendix

D.1 RNPAS PARTICIPANT INFORMATION SHEET

Participant Information Sheet for Study Participants

Name of department: Computer and Information Sciences

Title of the study: Improving cybercrime reporting in Scotland: The victims' perspective

Introduction

My name is Juraj Sikra (e-mail: juraj.sikra@strath.ac.uk) and I am a second year PhD student at the University of Strathclyde (Glasgow) at the faculty of Computer and Information Sciences with a professional background in the Scottish mental health system.

My supervisor is Dr Daniel R Thomas (e-mail: d.thomas@strath.ac.uk) – Chancellor's Fellow at the University of Strathclyde.

This study was designed in response to the fact that an increasing number of people are victimised by online scams, which they are reluctant to report for various reasons. I'm doing this study to understand what gets in the way of reporting this type of crime so that the approaches can be adjusted to serve victims' needs. To achieve this, I need to collect data via interviews with people and organizations that have lived experience of this type of crime. Whilst revisiting these experiences can bring about negative emotions, it can also help protect other people from being victimised in the future. The interviews will collect mainly information around your experiences and reasons around reporting the crime. However, there will be other questions as well, which will help me understand you as a person. This information is vital for improving reporting as it provides a fuller picture of the reporting situation.

What is the purpose of this research?

The aim of this research is to understand what gets in the way of people reporting cybercrime to the police and using those findings to adjust the systems in place for reporting cybercrime so that more people are willing to come forward.

Do you have to take part?

Your participation in this interview is entirely voluntary and you may withdraw during any time. If you consent, then I would like to use Microsoft Teams, Zoom or Skype online or an Olympus WS-853 Voice recordings either in person or over the phone to record our interview as this will help me capture verbatim what your thoughts are. All information that you provide me with will kept confidential in terms of being untraceable to you as an individual. The information, which you provide, including some of your quotes may be used in published versions of this research to support any common trends that may emerge. You may refuse to answer any of the questions or discontinue the interview during at any time and without providing a reason. Would you like to take a moment to see whether you have any questions about what you have just read?

What will you do in the project?

You will be asked to answer 10 interview questions (and some sub-questions) about your experience of cybercrime as well as about you as a person. Try to think of it as an informal conversation rather than an interview if you can. The questions will be asked by the researcher Juraj Sikra.

Why have you been invited to take part?
You have been invited to take part because you are a victim of cybercrime and potential user of the police's reporting systems.

What are the potential risks to you in taking part?
There are no risks to taking part, but you may experience some negative emotions when remembering how you were victimised by cybercrime. Alternatively, you may find that talking over your experience has helped. If you experience any negative emotions, you are encouraged to reach out to a support agency such as Victim Support Scotland https://victimsupport.scot/ or using their telephone number on 0800 160 1985.

What information is being collected in the project?
The main information that is of interest is people's experience of cybercrime reporting. All other data such as gender and age range are merely indicators that allow the researchers to make inferences about the population. This research does not collect and analyse data that pertains to the specific identity of victims.

Where will the information be stored and how long will it be kept for?
The Microsoft Teams, Zoom or Skype online or an Olympus WS-853 Voice recordings either in person or over the phone recordings shall be safely downloaded on the University of Strathclyde's One Drive until being destroyed no later than August 2023. The full length transcribed and anonymised interviews will be stored for no longer than October 2024 by which time it is expected that selected anonymised quotes from them will be integrated into a publicly available study. The researcher will carry out the transcriptions.
Thank you for reading this information – please ask any questions if you are unsure about what is written here. All personal data will be processed in accordance with data protection legislation. Please read our Privacy Notice for Research Participants for more information about your rights under the legislation.

What happens next?
You'll now be asked whether you want to participate. Then, the interview will commence. If you want to know more about the project then feel free to speak to the researcher at the end of the session. Also, if you would like access to work once it has been published, then please indicate that now. Is there any other information that you require to provide your informed consent?

Researchers' contact details:
Dr Juraj Sikra

E-mail: juraj.sikra@strath.ac.uk
Chief Investigator details:
Dr Daniel R Thomas
Computer and Information Sciences
Livingstone Tower
University of Strathclyde (Glasgow-UK)
Tel.no.: + 44 141 548 3524
E-mail: d.thomas@strath.ac.uk

This research was granted ethical approval by the Departmental Ethics Committee.

If you have any questions/concerns, during or after the research, or wish to contact an independent person to whom any questions may be directed or further information may be sought from, please contact:

Department of Computer & Information Sciences Ethics Committee
email: ethics@cis.strath.ac.uk

D.2 RNPAs Consent form

Consent Form for Study Participants

Name of department: Computer and Information Sciences
Title of the study: Improving cybercrime reporting in Scotland: The victims' perspective

- I confirm that I have read and understood the Participant Information Sheet for the above project and the researcher has answered any queries to my satisfaction.
- I confirm that I have read and understood the Privacy Notice for Participants in Research Projects and understand how my personal information will be used and what will happen to it (i.e. how it will be stored and for how long).
- I understand that my participation is voluntary and that I am free to withdraw from the project at any time, up to the point of completion, without having to give a reason and without any consequences.
- I understand that I can request the withdrawal from the study of some personal information and that whenever possible researchers will comply with my request. This includes the following personal data:
    - Microsoft Teams, Zoom or Skype online or an Olympus WS-853 Voice recordings either in person or over the phone that identify me;
    - My personal information from transcripts.
- I understand that anonymised data (i.e. data that do not identify me personally) cannot be withdrawn once they have been included in the study.
- I understand that any information recorded in the research will remain confidential and no information that identifies me will be made publicly available.
- I consent to being a participant in the project.
- I consent to being recorded with Microsoft Teams, Zoom or Skype online or an Olympus WS-853 Voice recordings either in person or over the phone and will turn on my camera only if I consent to do so.

(PRINT NAME)	
Signature of Participant:	Date:

D.3 RNPAs Interview questions

Juraj Sikra

01 December 2022

Improving cybercrime reporting in Scotland: The victims' perspective

Note: Victims

Demographics:

(i) What is your gender?
(ii) What is your age range: 18-24; 25-34; 35-44; 45-54; 55-64; 64+

0. What was your understanding of scams and cybercrime before you started this job?
1. How did reporting cybercrime become a part of your agenda?
> Did you notice any trends in cybercrime in Scotland whilst you've been addressing it?
2. What kind of IT technology do you use in your everyday life?
>How comfortable are with using this technology?
3. Please walk me through how you receive reports of cybercrime. Please include as much factual detail as possible about what is reportable including, for example, date and time, but also your surroundings and anything else that comes to mind.
4. Who do you report your findings to?
>Why did you go to them?
>Can you please provide an example of something they said or did that was helpful?
> Can you please provide an example of something they said or did that was unhelpful?
5. If you did not initially report to the police, when have you decided to report to them and how helpful were they?
>Why did you go to them?
>Was there anything they said or did that was unhelpful?
6. When you reported the cybercrime to the police, did you feel that you were treated differently based on your religion, gender, ethnicity, disability, age, gender-reassignment status or any other aspect of who you are that was separate from the fact that you were reporting victimisation?
7. Based on how you were treated by the police, how likely are you to report similar instances of cybercrime in the future?
>What could the police improve about their approach to encourage you to report even more?
>In your opinion, whose responsibility is it to report this cybercrime?
8. Please describe whether you encountered any obstacles in terms of your ability or accessibility to technology when reporting the cybercrime?
9. What would an ideal reporting system look like?
10. What else is needed to improve cybercrime reporting in Scotland?

Appendix E

Italian RNPAs Appendix

E.1 RNPAS- ITALIAN LAWYERS PIS AND CONSENT FORM

Participant Information Sheet for Study Participants

Name of department: Computer and Information Sciences
Title of the study: Improving cybercrime reporting in Italy: The experts' perspective

Introduction
My name is Juraj Sikra (e-mail: juraj.sikra@strath.ac.uk) and I am a first year PhD student at the University of Strathclyde (Glasgow) at the faculty of Computer and Information Science with a professional background in the Scottish mental health system.

My supervisor is Dr Daniel R Thomas (e-mail: d.thomas@strath.ac.uk) – Chancellor's Fellow at the University of Strathclyde.

Department of Computer & Information Sciences Ethics Committee
email: ethics@cis.strath.ac.uk

This study was designed in response to the fact that an increasing number of people are victimised by online scams, which they are reluctant to report for various reasons. I'm doing this study to understand what gets in the way of reporting this type of crime so that the approaches can be adjusted to serve victims' needs. To achieve this, I need to collect data via a focus group with people that have worked with cybercrime victims. The focus group will function as an informal discussion between you as experts, who have received the topic areas in advance via e-mail.

What is the purpose of this research?
The aim of this research is to understand what gets in the way of people reporting cybercrime to the police and using those findings to adjust the systems in place for reporting cybercrime so that more people are willing to come forward.

Do you have to take part?
Your participation in this focus group is entirely voluntary and you may withdraw during any time. If you consent, then I would like to video record our interview as this will help me capture verbatim what your thoughts are. All information that you provide me with will kept confidential in terms of being untraceable to you as an individual. The information, which you provide, including your job title and some of your quotes may be used in published versions of this research to support any common trends that may emerge. You may refuse to engage with any subject area or leave the focus group during any time and without providing a reason. Would you like to take a moment to see whether you have any questions about what you have just read?

What will you do in the project?
You will be presented with five subject areas which you had a chance to view in advance of the meeting. These will serve to facilitate an effective debate between the experts taking part. The subject areas will be put forward

by the researcher Juraj Sikra in English and will be translated by Prof Stefano Chessa and Dr Federica Casarosa into Italian. Prof Stefano Chessa and Dr Casarosa will also assist with the transcription of the focus group.

Why have you been invited to take part?
You have been invited to take part because you play an active role as an expert in enabling the reporting process of cybercrime.

What are the potential risks to you in taking part?
There are significant no risks to taking part.

What information is being collected in the project?
The main information that is of interest are the expert opinions of the participants which emerge thanks to the presentation of shared as well as contrasting views. Apart from the latter, this research will collect the age range, gender, and job role (e.g., a legal representative) of the participants.

Who will have access to the information?
This information from the audio/video recording will be accessible to the researcher (Juraj Sikra) and his supervisor (Dr Daniel Thomas) as well as his secondary supervisors (Dr Ben Collier & Dr Karen Renaud) and Italian collaborators from the University of Pisa, who are Prof Stefano Chessa and Dr Federica Casarosa until the end of December 2022 when it will be destroyed. Anonymised quotes (including job role) from the focus group are likely to be published and disseminated among scientists and practitioners, but any traceable information will be carefully excluded.

Where will the information be stored and how long will it be kept for?
The Microsoft Teams recordings shall be safely downloaded on the University of Strathclyde's One Drive until being destroyed no later than December 2022. The full length transcribed and anonymised focus group will be stored for no longer than October 2024 by which time it is expected that selected anonymised quotes from them will be integrated into a publicly available study. The researcher will carry out the transcriptions with the help of Dr Stefano Chessa and Dr Federica Casarosa who will assist with translation as well.

Thank you for reading this information – please ask any questions if you are unsure about what is written here.

All personal data will be processed in accordance with data protection legislation. Please read our Privacy Notice for Research Participants in English for more information about your rights under the legislation.

What happens next?
You'll now be asked whether you want to participate. Then, the focus group will commence for the duration of 1.5 hours. The focus group shall run as a single isolated meeting. If you want to know more about the project then feel free to speak to the researcher at the end of the session. Also, if you would like access to work once it has been published, then please indicate that now. Is there any other information that you require to provide your informed consent?

Researcher contact details:
Dr Juraj Sikra

E-mail: juraj.sikra@strath.ac.uk
Chief Investigator details:
Dr Daniel R Thomas
Computer and Information Sciences
Livingstone Tower
University of Strathclyde (Glasgow-UK)
Tel.no.: 00 44 548 3524
E-mail: d.thomas@strath.ac.uk

This research was granted ethical approval by the Departmental Ethics Committee.

If you have any questions/concerns, during or after the research, or wish to contact an independent person to whom any questions may be directed or further information may be sought from, please contact:

Department of Computer & Information Sciences Ethics Committee
email: ethics@cis.strath.ac.uk

Consent Form for Study Participants

Name of department: Computer and Information Sciences
Title of the study: Improving cybercrime reporting in Italy: The victims' perspective

- I confirm that I have read and understood the Participant Information Sheet for the above project and the researcher has answered any queries to my satisfaction.
- I confirm that I have read and understood the Privacy Notice for Participants in Research Projects and understand how my personal information will be used and what will happen to it (i.e. how it will be stored and for how long).
- I understand that my participation is voluntary and that I am free to withdraw from the project at any time, up to the point of completion, without having to give a reason and without any consequences.
- I understand that I can request the withdrawal from the study of some personal information and that whenever possible researchers will comply with my request. This includes the following personal data:
    - Microsoft Teams recordings of interviews that identify me;
    - My personal information from transcripts.
- I understand that anonymised data (i.e. data that do not identify me personally) cannot be withdrawn once they have been included in the study.
- I understand that any information recorded in the research will remain confidential and no information that identifies me will be made publicly available.
- I consent to being a participant in the project.
- I consent to being recorded with Microsoft Teams and will turn on my camera only if I consent to do so.

(PRINT NAME)	
Signature of Participant:	Date:

Foglio informativo per i partecipanti allo studio

Nome del dipartimento: Computer and Information Science
Oggetto dello studio: Migliorare le segnalazioni relative ai crimini informatici in Italia: la prospettiva delle vittime

Introduzione
Sono Juraj Sikra, studente al primo anno del Dottorato di Ricerca in Informatica presso l'Università di Strathclyde (Glasgow, U.K.), e ho precedenti esperienze professionali allo "Scottish mental health system".
Il supervisore della mia di tesi di dottorato è il Dr. Daniel R Thomas – Chancellor's Fellow presso l'Università di Strathclyde

Department of Computer & Information Sciences Ethics Committee
email: ethics@cis.strath.ac.uk

Questo studio è stato progettato in risposta al fatto che un numero crescente di persone è vittima di truffe online, che sono riluttanti a denunciare per vari motivi. Sto conducendo questo studio per capire cosa ostacola la denuncia di questo tipo di reato, in modo da poter adattare gli approcci alle esigenze delle vittime. A tal fine, devo raccogliere dati attraverso un focus group con persone che hanno lavorato con le vittime di reati informatici. Il focus group funzionerà come una discussione informale tra esperti, che hanno ricevuto le aree tematiche in anticipo via e-mail.

Qual è lo scopo di questa ricerca?
L'obiettivo di questa ricerca è capire cosa ostacola le persone che denunciano i crimini informatici alla polizia e utilizzare questi risultati per adeguare i sistemi di denuncia dei crimini informatici in modo che più persone siano disposte a farsi avanti.

Siete obbligati a partecipare?
La sua partecipazione a questo focus group è del tutto volontaria e può ritirarsi in qualsiasi momento. Se lei è d'accordo, vorrei videoregistrare la nostra intervista per aiutarmi a cogliere testualmente i suoi pensieri. Tutte le informazioni che mi fornirete saranno mantenute riservate e non riconducibili a voi come individui. Le informazioni da lei fornite, compreso il suo titolo di lavoro e alcune delle sue citazioni, potranno essere utilizzate nelle versioni pubblicate di questa ricerca per sostenere eventuali tendenze comuni che potrebbero emergere. Potete rifiutarvi di rispondere a qualsiasi quesito delle area tematiche e potete lasciare il focus group in qualsiasi momento e senza fornire alcuna motivazione. Vuole prendersi un momento per vedere se ha delle domande su ciò che ha appena letto?

Cosa farete nel progetto?

Vi verranno presentate cinque aree tematiche che avete avuto modo di visionare prima dell'incontro. Queste serviranno a facilitare un dibattito efficace tra gli esperti partecipanti. Le aree tematiche saranno presentate dal ricercatore Juraj Sikra in inglese e saranno tradotte in italiano dal Prof. Stefano Chessa e dalla Dott.ssa Federica Casarosa. Il Prof. Stefano Chessa e la Dott.ssa Casarosa assisteranno anche nella trascrizione dei contenuti del focus group.

Perché siete stati invitati a partecipare?
Siete stati invitati a partecipare perché svolgete un ruolo attivo come esperti nel processo di denuncia dei crimini informatici.

Quali sono i rischi potenziali che correte partecipando?
Non ci sono rischi significativi nel partecipare.

Quali informazioni vengono raccolte nel progetto?
Le principali informazioni di interesse sono le opinioni degli esperti dei partecipanti che emergono grazie alla presentazione di punti di vista condivisi e/o contrastanti. Oltre a queste ultime, la ricerca raccoglierà la fascia d'età, il sesso e il ruolo lavorativo (ad esempio, rappresentante legale) dei partecipanti.

Chi avrà accesso alle informazioni?
Le informazioni ricavate dalla registrazione audio/video saranno accessibili al ricercatore (Juraj Sikra) e al suo supervisore (dottor Daniel Thomas), nonché ai suoi supervisori secondari (dottor Ben Collier e dottoressa Karen Renaud) e ai collaboratori italiani dell'Università di Pisa, che sono il professor Stefano Chessa e la dottoressa Federica Casarosa, fino alla fine di dicembre 2022, quando saranno distrutte. Le citazioni anonime (compreso il ruolo lavorativo) del focus group saranno probabilmente pubblicate e diffuse tra gli scienziati e gli operatori del settore, ma ogni informazione rintracciabile sarà accuratamente esclusa.

Dove saranno conservate le informazioni e per quanto tempo?
Le registrazioni svolte attraverso la piattaforma Microsoft Teams saranno scaricate in modo sicuro su One Drive dell'Università di Strathclyde fino a quando non saranno distrutte entro dicembre 2022. Le trascrizioni integrali e anonimizzate dei focus group saranno conservate per un periodo non superiore a ottobre 2024, quando si prevede che le citazioni anonime selezionate saranno integrate in uno studio disponibile al pubblico. Il ricercatore effettuerà le trascrizioni con l'aiuto del dottor Stefano Chessa e della dottoressa Federica Casarosa, che lo assisteranno anche nella traduzione.

Vi ringraziamo per aver letto queste informazioni - vi preghiamo di porre qualsiasi domanda se non siete sicuri di ciò che è scritto qui.

Tutti i dati personali saranno trattati in conformità alla legislazione sulla protezione dei dati. Per ulteriori informazioni sui vostri diritti in base alla legislazione, leggete la nostra Informativa sulla privacy per i partecipanti alla ricerca in inglese.

Cosa succede ora?
Vi verrà chiesto se volete partecipare. Poi inizierà il focus group della durata massima di 1,5 ore. Il focus group si svolgerà come un unico incontro isolato. Se volete saperne di più sul progetto, potete parlare con il ricercatore alla fine della sessione. Inoltre, se desiderate avere accesso al lavoro una volta pubblicato, vi preghiamo di indicarlo subito. Ci sono altre informazioni di cui ha bisogno per fornire il suo consenso informato?

Dati di contatto del ricercatore:
Dr Juraj Sikra
E-mail: juraj.sikra@strath.ac.uk

Dati del ricercatore capo:
Dr Daniel R Thomas
Computer and Information Sciences
Livingstone Tower
University of Strathclyde (Glasgow-UK)
Tel.no.: 00 44 548 3524
E-mail: d.thomas@strath.ac.uk

Questa ricerca è stata approvata dal Comitato etico del Dipartimento.

In caso di domande/dubbi, durante o dopo la ricerca, o se si desidera contattare una persona indipendente a cui rivolgere le domande o chiedere ulteriori informazioni, si prega di contattare:
Comitato etico del Dipartimento di Informatica e Scienze dell'Informazione
e-mail: ethics@cis.strath.ac.uk

Consenso Informato per i partecipanti allo studio

Nome del dipartimento: Computer and Information Sciences

Title of the study: Migliorare le segnalazioni relative ai crimini informatici in Italia: la prospettiva delle vittime

- Confermo di aver letto e compreso la scheda informativa dei partecipanti per il progetto di cui sopra e di aver ricevuto dal ricercatore risposte soddisfacenti a qualsiasi mia domanda.
- Confermo di aver letto e compreso l'Informativa sulla privacy per i partecipanti al progetto di ricerca e di aver compreso come verranno utilizzate le mie informazioni personali e cosa accadrà ad esse (cioè come saranno conservate e per quanto tempo).
- Comprendo che la mia partecipazione è volontaria e che sono libero di ritirarmi dal progetto in qualsiasi momento, fino al punto di completamento, senza dover dare una motivazione e senza alcuna conseguenza.
- Comprendo che posso richiedere il ritiro dallo studio di alcune informazioni personali e che ogni volta che sarà possibile i ricercatori soddisferanno la mia richiesta. Ciò include i seguenti dati personali:
  - Registrazioni di Microsoft Teams di interviste che mi identificano;
  - Le mie informazioni personali dalle trascrizioni.
- Comprendo che i dati anonimizzati (cioè i dati che non mi identificano personalmente) non possono essere ritirati una volta che sono stati inclusi nello studio.
- Comprendo che tutte le informazioni registrate nella ricerca rimarranno riservate e che nessuna informazione che mi identifica sarà resa pubblicamente disponibile.
- Do il mio consenso a partecipare al progetto.
- Do il mio consenso alla registrazione con Microsoft Teams e attiverò la mia fotocamera solo se acconsentirò a farlo.

(NOME IN STAMPATO)	
Firma del partecipante:	Date:

E.2 RNPAS- ITALIAN LAWYERS PRIVACY NOTICE FOR RESEARCH PARTICIPANTS

Italian translation of the University's Privacy Notice for Research Participants Privacy Notice for Participants in Research Projects 2025 follows.

Informativa sulla privacy per i partecipanti a progetti di ricerca

Introduzione
La presente informativa sulla privacy si riferisce alle persone che partecipano a progetti di ricerca condotti dall'Università di Strathclyde. Spiega come l'Università di Strathclyde utilizzerà le sue informazioni personali e i suoi diritti ai sensi della legislazione sulla protezione dei dati. È importante leggere questo avviso prima di fornire le proprie informazioni. Si prega di notare che queste informazioni standard dovrebbero essere considerate insieme alle informazioni fornite dal ricercatore per ciascun progetto, che di solito è sotto forma di una scheda informativa del partecipante (PIS). Il PIS include ulteriori dettagli su come le informazioni personali vengono elaborate nel particolare progetto, tra cui: quali dati vengono elaborati; come vengono memorizzati; per quanto tempo saranno conservati e qualsiasi altro soggetto che avrà accesso ad informazioni personali. Di solito il PIS viene fornito ai partecipanti prima che decidano se vogliono o meno partecipare alla ricerca.
Responsabile per il trattamento e per la protezione dei dati
L'Università di Strathclyde è il responsabile del trattamento dei dati ai sensi della legislazione sulla protezione dei dati. Ciò significa che l'Università è responsabile di come vengono utilizzati i suoi dati personali e di rispondere a qualsiasi richiesta da parte sua in relazione ai suoi dati personali. Eventuali richieste relative alla protezione dei dati devono essere indirizzate al responsabile della protezione dei dati dell'Università presso dataprotection@strath.ac.uk.
Basi giuridiche per il trattamento dei dati personali
Se sta partecipando a un progetto di ricerca, potremmo raccogliere le sue informazioni personali. Il tipo di informazioni che raccogliamo varierà a seconda del progetto. La nostra base per la raccolta di queste informazioni è descritta di seguito:

Tipo di informazione	**Basi per il trattamento**
Informazioni personali e dati di ricerca associati raccolti allo scopo di condurre ricerche.	Sono necessari per l'esecuzione di un compito svolto nell'interesse pubblico.
Alcuni tipi di informazioni personali come informazioni sulla razza, l'origine etnica, la politica, la religione, l'appartenenza sindacale, la genetica, la biometria (se utilizzate per scopi di identificazione), la salute, la vita sessuale o l'orientamento sessuale di un individuo sono definite come dati di "categoria speciale" ai sensi della legislazione.	È necessario per l'esecuzione di un compito svolto nell'interesse pubblico e È necessario per scopi di ricerca scientifica o storica in conformità con la legislazione pertinente (Legge sulla protezione dei dati 2018, Allegato 1, Parte 1, Paragrafo 4).

Dati relativi a condanne penali/reati	È necessario per l'esecuzione di un compito svolto nell'interesse pubblico ed è trattato in conformità con l'articolo 10 del regolamento generale sulla protezione dei dati e la legge sulla protezione dei dati 2018, Allegato 1, Parte 1, paragrafo 4.

Dettagli dei trasferimenti verso paesi terzi e garanzie

Per alcuni progetti, le informazioni personali possono essere trasferite al di fuori del Regno Unito. Questo sarà normalmente fatto solo quando la ricerca si svolge in luoghi al di fuori del Regno Unito. Se ciò accade, l'Università garantirà che siano in atto adeguate salvaguardie. Sarà pienamente informato su qualsiasi trasferimento di dati al di fuori del Regno Unito e sulle relative garanzie, di solito nella Scheda informativa del partecipante.

Condivisione dei dati

Se i dati saranno condivisi con altri individui o organizzazioni, sarete informati di questo nel PIS.

Conservazione dei moduli di consenso

Se partecipa a un progetto di ricerca, le potrebbe essere chiesto di firmare un modulo di consenso dei partecipanti. I moduli di consenso saranno in genere conservati dall'Università almeno per il tempo in cui i dati di ricerca identificabili vengono conservati. Nella maggior parte dei casi saranno conservati più a lungo, il periodo di tempo esatto sarà determinato dalla necessità di accedere a queste informazioni nel malaugurato caso di un problema imprevisto o di un reclamo.

Per molti progetti questo tempo sarà di cinque anni dopo il completamento della ricerca, ma per qualsiasi studio longitudinale o "ad alto rischio" che coinvolga bambini, i soggetti giuridicamente incapaci o un risultato di ricerca controverso questi saranno conservati fino a venti anni.

Diritti dell'interessato

Ha il diritto di: essere informato sulla raccolta e l'utilizzo dei suoi dati personali; richiedere l'accesso ai dati personali che deteniamo su di lei; richiedere la rettifica dei dati personali se inesatti o incompleti; opporsi al trattamento dei suoi dati; richiedere di limitare il trattamento delle sue informazioni personali; e i diritti connessi al processo decisionale automatizzato e alla profilazione. Per esercitare tali diritti si prega di contattare: dataprotection@strath.ac.uk.

Si prega di notare che molti di questi diritti **non si applicano** quando i dati vengono utilizzati per scopi di ricerca. Tuttavia, cercheremo sempre di conformarci laddove ciò non impedisca o comprometta seriamente il raggiungimento dello scopo della ricerca.

Diritto di reclamo all'autorità di controllo

In caso di dubbi / problemi con il modo in cui l'Università ha elaborato i suoi dati personali, può contattare il responsabile della protezione dei dati presso dataprotection@strath.ac.uk. Ha anche il

diritto di presentare un reclamo contro l'Università in merito a questioni di protezione dei dati con l'Ufficio del Commissario per le informazioni (https://ico.org.uk/concerns/).

E.3 RNPAs- Italian lawyers Focus group

Juraj Sikra

22 May 2022

Improving cybercrime reporting in Italy: The experts' perspective

Focus group subject areas

1. If an Italian citizen falls victim to an online scam, phishing, or malware attack, who do they usually report this too? Please elaborate on the benefits and disadvantages of the usual reporting pathway in Italy.

2. There are different obstacles because people are reluctant to report being victimised by cybercrime. An internal obstacle might be shame and an external obstacle might not know who to report the crime to. Please elaborate on what you see as the common obstacles to cybercrime reporting in Italy considering both the internal motivations of victims as well as structural challenges.

3. Vulnerability to cybercrime does not have a universal definition, however it is commonly viewed in connection to living with a disability (both physical and mental) as well as being an elderly person or a child. Does the usual cybercrime reporting pathway in Italy take vulnerability into consideration when working with victims of cybercrime? Please elaborate on the benefits and disadvantages that may arise for a vulnerable Italian cybercrime victim during the reporting process.

4. Responsibilisation in cybercrime is when the criminal justice system educates citizens about the risks of cybercrime but does not designate resources for effective reporting and response. This is due to the assumption that if the citizen was educated about internet safety and still became victimised, then it is their fault. How would you describe the Italian criminal justice system in connection to responsibilisation? Please elaborate on the benefits and disadvantages of the Italian criminal justice system with respect to responsibilisation in cybercrime.

5. What kind of changes should take place in Italy to improve the reporting of cybercrime to the police? Please elaborate on a realistic as well as an ideal scenario.

Juraj Sikra

22 May 2022

Migliorare la segnalazione dei crimini informatici in Italia: Il punto di vista degli esperti

Aree tematiche del focus group

1. Se un cittadino italiano è vittima di una truffa online, di un attacco di phishing o di un malware, chi lo denuncia di solito? Si prega di elaborare i vantaggi e gli svantaggi dell'attuale iter di denuncia in Italia.

2. Esistono diversi ostacoli che portano le persone ad essere riluttanti nel denunciare di essere state vittime di crimini informatici. Un ostacolo interno potrebbe essere la vergogna mentre un ostacolo esterno potrebbe essere il non sapere a chi denunciare il reato. La preghiamo di approfondire quali sono, a suo avviso, gli ostacoli comuni relativi alla denuncia dei crimini informatici in Italia, considerando sia le motivazioni interne delle vittime sia le sfide strutturali.

3. Il concetto di vulnerabilità rispetto alla criminalità informatica non ha una definizione universale, ma è comunemente considerato in relazione alla disabilità (sia fisica che mentale), all'essere anziani o bambini. Il consueto percorso di denuncia dei crimini informatici in Italia prende in considerazione la vulnerabilità quando si lavora con le vittime di crimini informatici? Si prega di approfondire i vantaggi e gli svantaggi che possono emergere per una vittima di cybercrime italiana vulnerabile durante il processo di denuncia.

4. La responsabilizzazione nella criminalità informatica si ha quando il sistema di giustizia penale istruisce i cittadini sui rischi della criminalità informatica, ma non destina risorse per una denuncia e una risposta efficaci. Ciò è dovuto al presupposto che se il cittadino è stato istruito sulla sicurezza di Internet ed è stato comunque vittimizzato, allora è colpa sua. Come descriverebbe il sistema penale italiano in relazione alla responsabilizzazione? La preghiamo di approfondire i vantaggi e gli svantaggi del sistema penale italiano rispetto alla responsabilizzazione nei crimini informatici.

5. Che tipo di cambiamenti dovrebbero avvenire in Italia per migliorare la segnalazione dei crimini informatici alle autorità? Si prega di elaborare uno scenario realistico e uno ideale.