Journal of Economic Criminology 6 (2024) 100103

Contents lists available at ScienceDirect

Journal of Economic Criminology

journal homepage: www.journals.elsevier.com/journal-of-economic-criminology

Investigating what promotes and deters Scottish cybercrime reporting

Juraj Sikra[a,*], Karen V. Renaud[a,b,c,d], Daniel R. Thomas[a,e]

[a] Computer and Information Sciences, University of Strathclyde, Glasgow, United Kingdom
[b] Department of Information Systems, Rhodes University, Grahamstown, South Africa
[c] School of Computing, University of South Africa, Pretoria, South Africa
[d] Division of Cybersecurity, Abertay University, Dundee, United Kingdom
[e] Computer Laboratory, University of Cambridge, Cambridge, United Kingdom

ARTICLE INFO

Keywords:
Cybercrime
Victims
Reporting
Responsibilization
Scotland
MINDSPACE

ABSTRACT

Cybercrime is under-reported in Scotland, with the reasons for this being poorly understood. To investigate underreporting, we commenced with a search of the related research and then carried out a review of actual cases. Next, to uncover Scottish-specific factors, we qualitatively interviewed 10 Scottish cybercrime victims. It emerged that victims blamed themselves for falling prey to cybercrime and were reluctant to report the incident. This is arguably a direct consequence of the UK government's cybersecurity responsibilization strategy. Informed by our findings, we articulated a national strategy for promoting cybercrime reporting using the MINDSPACE behavioral influence model. Subsequently, we verified this model with a survey of 380 Scottish respondents, a representative sample of the general population in terms of age and gender. We report on and discuss our findings. Finally, we recommend two interventions to inform a national strategy for improving cybercrime reporting in Scotland.

1. Introduction

Cybercrime reporting in Scotland is a pertinent issue because of the continuing success enjoyed by cyber criminals. In 2019–2020, there were 8 630 cases, a significant increase over 2019–2020 (Scottish Government, 2022a). This number did not decrease in 2021–22, with almost half of all reported fraud cases being cybercrimes.

While these figures are concerning, the true situation might be even worse because of underreporting (McMurdie, 2016; Whitty and Buchanan, 2012; Protrka, 2021; Buil-Gil et al., 2023). Data from the Scottish Government's (2022b) Scottish Crime and Justice Survey found that only a minority of the victims reported to the Police (6.6 % who experienced bank detail theft, 4.2 % of those whose account was breached for fraud, 3.8 % of those affected by a virus, 2.1 % of victims who received a scam e-mail and 1.8 % of those that were impacted by a phone call scam). Some victims abstained from reporting due to considering the incident trivial whilst others resolved the situation themselves by reporting it to their bank. In these cases, victims often assumed that banks would report the crime themselves after having reimbursed them. Other countries have the same problem: the Netherlands (Van de Weijer et al., 2018), Hong Kong (Cheng et al., 2018), Ireland (Friend et al., 2020) and the USA (Breen et al., 2022), to name but a few.

From Garland's (2002, p. 124) perspective, the UK government's cyber responsibilization strategy makes people feel that it is they rather than the government who should worry about safety. When governments embrace a cybersecurity responsibilization strategy, they issue advice to help citizens to protect themselves when online. If citizens fail to embrace this responsibility and do not follow the advice, they are expected to accept the consequences of falling victim to cybercrime. Renaud et al. (2018) extended this line of argumentation when discussing how neoliberal governments disengage with citizens if they fall victim because they did not follow cyber-security advice. According to Renaud et al. (2018), people may feel that they are to blame. This might well contribute to the underreporting phenomenon.

In essence, the responsibility for preventing cybercrime, as well as recovering from victimhood, is assigned to the responsibilized citizen rather than the state playing a proactive role in providing support, both in terms of prevention and recovery.

In this paper, we reveal factors influencing cybercrime reporting with a particular focus on Scotland. We deliver insights across different victim types: 1) Individuals, 2) Private institutions, and 3) Public institutions, a distinction drawn by Sikra, Renaud and Thomas (2023).

[*] Correspondence to: 26 Richmond Street, Glasgow G1 1XH, United Kingdom.
E-mail addresses: juraj.sikra@strath.ac.uk (J. Sikra), karen.renaud@strath.ac.uk (K.V. Renaud), d.thomas@strath.ac.uk (D.R. Thomas).

https://doi.org/10.1016/j.jeconc.2024.100103
Received 12 June 2024; Received in revised form 20 August 2024; Accepted 9 October 2024

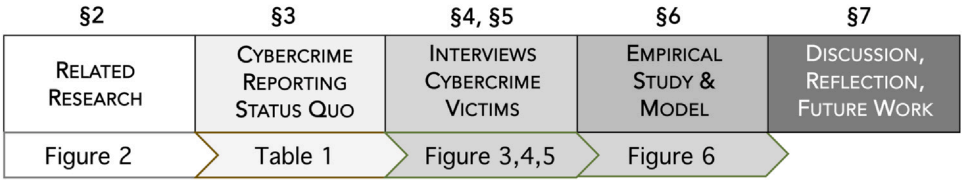
§2
§3
§4, §5
§6
§7
RELATED RESEARCH
CYBERCRIME REPORTING STATUS QUO
INTERVIEWS CYBERCRIME VICTIMS
EMPIRICAL STUDY & MODEL
DISCUSSION, REFLECTION, FUTURE WORK
Figure 2
Table 1
Figure 3,4,5
Figure 6

Fig. 1. Paper Structure.

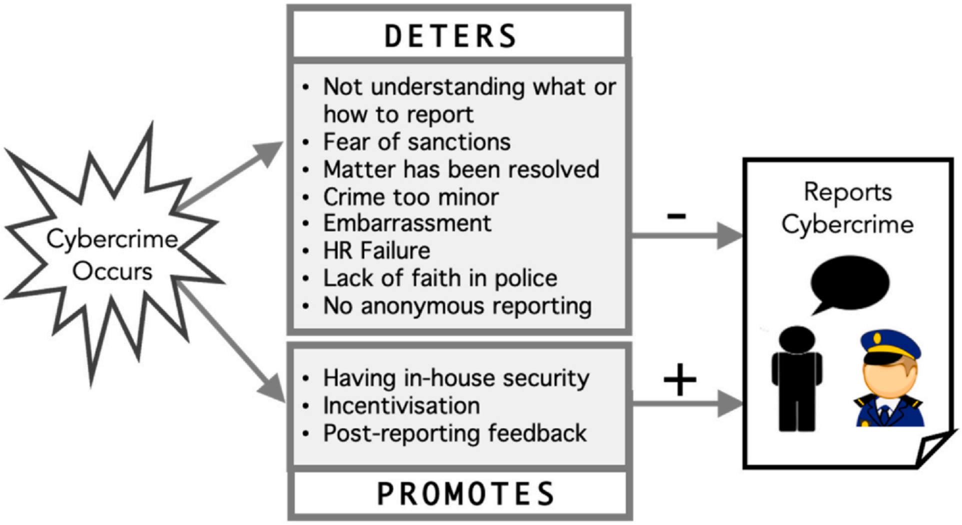

Fig. 2. Model of Factors that promote vs. deter Cybercrime Reporting (from Research Literature).

As shown in Fig. 1, Section 2 reviews the related research and motivates a Scotland-specific investigation. We review court documentation and news articles whilst referring to academic literature in connection to identifying factors that influence cybercrime reporting in Section 3. In Section 4, we describe the interview methodology. We report on the results and enumerate the deterring and promoting factors that interviewees mentioned. Section 5 connects the qualitative results with the MINDSPACE framework of behavioral influencers. Then, Section 6 supplies a quantitative verification approach to factors we uncovered and applied into the MINDSPACE framework. Section 7 discusses and evaluates the findings and Section 8. articulates two key recommendations for improving cybercrime reporting.

2. Related research

The research literature does not deliver many insights into cybercrime underreporting, with some notable exceptions. For example, Ballreich et al. (2023) report that people need to understand what to report and how to report it. People are deterred by the fact that there is no common definition of what security incidents are. This is confirmed by Curtis and Oxburgh (2022) and Bidgoli and Grossklags (2016). Moreover, according to Ballreich et al. (2023), people fear sanctions for falling victim to cybercrime, which deters reporting. In addition, victims try to minimize embarrassment by avoiding reporting, so negative emotions have a deterrent effect (Ballreich et al., 2023). Bidgoli and Grossklags (2016) suggest that a lack of incentivization deters reporting, and that a lack of post-report feedback could also deter future reporting. Baror et al. (2020) suggest that a lack of an anonymous reporting channel deters cybercrime reporting.

From an organizational perspective, there may be a failure of HR to hire someone who is tasked to respond to cybercrime incidents, but also people may be deterred by a lack of faith in the police or feel that the cybercrime is not worth reporting (Ballreich et al., 2023). The deterrent of “lack of faith in the police” is also confirmed by Curtis and Oxburgh (2023) and Graham et al. (2020). Kemp et al. (2023) find that institutions with in-house security teams are more likely to report cybercrimes. Wanamaker (2019) suggests that businesses would not report if they felt the matter had been resolved, perhaps with help from an IT consultant, or if they felt that the incident was too minor. Fig. 2 summarizes this discussion.

The identified factors are not specific to Scotland. Moreover, none of these publications distinguish between the three victim types as proposed by Sikra, Renaud and Thomas (2023) i.e., Individuals, Private institutions and Public institutions. This means that the findings are harder to interpret because the victim experiences are likely to be different. In the case of cybercrime reporting, local context is influential (Popham et al., 2020). We also cannot assume that UK-specific factors will apply equally, given that Scotland underwent a major change in cybercrime reporting when it split from UK’s main cyber fraud reporting mechanism called “Action Fraud” (MacDonald, 2019). Hence a Scottish-specific study is required to deliver insights into Scottish-specific influential reporting factors.

Case summary	Connection to reporting	Reference	Notes
Individuals			
A trialled case of recruitment fraud where Czech and Slovak citizens were promised employment in the UK in exchange for £400–450 fee.	Language barrier and lack of knowledge of the Scottish legal system impeded reporting.	Lady Paton et al. (2014)	In addition, Cross and Grant-Smith (2019) found that COVID – 19 increased global unemployment, which increased recruitment fraud.
A trialled case of murder revealed how the perpetrator inserted himself into the life of his alcohol-misusing cousin and conducted credit card fraud by siphoning £32.000 prior to killing his victim.	Trust toward the perpetrator and alcohol misuse problems impeded reporting.	Lord Justice Clerk et al. (2015a)	No additional notes.
In a 2022 news story of two brothers, the offenders themselves reported how they engage Eastern-European females to manipulate men into sending finances under the pretext of "fake sob stories".	Trust towards the perpetrator and transnational nature of fraud impeded reporting.	Scully (2022)	No additional notes.
In a 2023 news story of a Tbilisi criminal call centres German and Georgian police conducted raids to disrupt an organised crime network. Back in the UK, examples of a male and female victim were listed as having lost £15.000 and £27.000 respectively.	Assertiveness and need to reclaim lost funds promoted reporting.	Hudson, Weinglass, Turner and Gunter (2023)	No additional notes.
In a 2023 news story, Scottish citizens were targeted by a telephone scam where the criminals advertised a discount on their contract if they read out a text message, which granted access into the victims' phones.	Newspaper was using awareness-raising to promote reporting to Police Scotland and designated charity for further support.	Lyon (2023)	According to Garland (2002, p.124) designated charities substitute some of the policing roles of the state in responsibilised societies.
Private institutions			
In a 2012 case, an insider used cyber-enabled cheque fraud to attack the Royal Bank of Scotland and generate a loss of £103.330 with 23 forged cheques.	Outdated systems impeded reporting.	Lord Justice Clerk et al. (2015a)	No additional notes.
In a 2018 case, an unnamed bank was victimised by an insider who attacked customers' accounts and siphoned £51.000 of clients' money.	Insider threat impeded reporting.	Lord Menzies and Lord Turnbull (2018)	Martin (2024) states that: "an insider is a person who has been trusted with access to an organization's assets, and who betrays that trust by exploiting (or intending to exploit) their access for unauthorized purposes, thereby potentially causing harm (p.7)."
Peebles Group case described as "whaling" where an offender caused the victim to transfer £200.000 by posing as the company's executive. The bank reimbursed the company by £85.000, but the company sued the victimised employee for the remaining £107.984.	Trust towards an offender that impersonated the company's executive, insider risk and incorrect legal terminology in documents deterred reporting.	Lord Summers (2019) and BBC (2019)	Martin (2024) uses the term "insider risk" to describe unsuspecting employees who fall prey to cybercrime. This he distinguishes from "insider threat", which is a premeditated course of harmful action (p. 11–12). Also, 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 (no date) clearly distinguish "whaling" from "business e-mail compromise."
A Scottish car company Arnold Clark was attacked by a ransomware gang called Play in 2024. 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 turnover of £3 billion.	Large scale harm meant it could not be covered up and promoted reporting.	O'Sullivan (2023)	No additional notes.
Royal Mail suffered significant delays to its international deliveries after it was impacted by ransomware demanding £67 million, which it refused to pay. This resulted in major delays that adversely impacted 11.500 post office branches across the UK. They were unable to handle international mail or parcels.	Large scale harm meant it could not be covered up and promoted reporting.	Sweeney (2023)	Royal Mail is private institution according to the UK Government.
Public institutions			
Dundee City Council fell victim to a cybercrime. An employee with a gambling addiction made payments on behalf of the council to fictitious suppliers, with the money going into his own bank account costing the council over a million pounds.	Insider threat and abuse of position of trust of the offender deterred reporting.	Lord Justice General et al. (2020)	No additional notes.
The press reported on the Scottish Environment and Protection Agency (SEPA), which was attacked by the Russian Conti group's ransomware on 24 December 2021. The environmental watchdog has purportedly spent over £5.000,000 on the recovery of 4.000 lost files. The evidence suggests that this offence was reported immediately.	The evidence suggests that this was reported immediately due to the public sector organisations following "best practices." Hence, "best practices" promote reporting.	Stewart (2022) and O'Sullivan (2023).	No additional notes.
According to a news report, the University of the West of Scotland suffered cybercrime, which caused their online service to shut down for several days. 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.	A multi-stakeholders (i.e., Scot Gov, Police and NCSC) support approach promoted reporting.	Delaney (2023)	Individuals and Private institutions do not benefit from the type of multi-stakeholder approach described within.

Based on news from the press, staff at the Sellafield nuclear site regularly covered up cyber incidents due to a toxic workplace culture of bullying and harassment.	Degraded workplace culture deterred staff from reporting.	Lawson and Isaac (2023)	No additional notes.

3. Cybercrime reporting status quo

To reveal influential reporting factors, we reviewed a range of Scottish court documents (Maltz, 1977; Loggen and Leukfeldt, 2022) as well as media reports (Lavorgna, 2019). The court documents were located via the search function of Scottish Courts and Tribunals.[1] The search term “cybercrime” 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 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.

This search aimed to deliver insights into factors that either promoted or deterred cybercrime reporting. However, few cases provided details about how, or to whom, these offences had been reported. Yet, critical analysis of the evidence sometimes made it possible to infer these details, as we will explain in this section.

3.1. Cybercrime against individuals

Commencing with a court case of recruitment fraud, several companies that had operations from Scotland into Europe advertised themselves to Czechs and Slovaks as employment agencies, which collected non-refundable deposits for their services (Lady Paton et al., 2014). The crimes, costing victims between £400-£450, occurred between 2009 and 2011 and point to the complexities of policing transnational fraud since the victims were non-UK citizens but had been defrauded in Scotland. This case is topical because Cross and Grant-Smith (2021) found that the COVID-19 pandemic gave rise to global unemployment, which made job seekers vulnerable to recruitment fraud. The operations of this group spanned several years before they were apprehended. Whilst information on how these offences were initially reporting is lacking, we can infer that language barriers and lack of knowledge of the Scottish legal system deterred the timely reporting of these offences and perpetuated the crimes.

Another court case, which pertained to an individual cybercrime victim, ended in murder (Lord Justice Clerk and Lord Drummond Young, 2015b). The perpetrator inserted himself into the life of his less computer literate cousin with an altruistic pretense. He opened various credit card accounts in the victim’s name and stole £32 000. In 2003, the cybercriminal murdered his victim by smothering for which he was sentenced to prison. Here the cybercrime was fully investigated as result of the murder investigation. Until then it went unreported, possibly due to the high level of trust between the perpetrator and the victim and low psychological astuteness of the victim, who was suffering from alcohol misuse problems. Hence, trust between victim and perpetrator deters reporting.

In 2022, two high profile UK social media personalities reported on their own offending via an interview with a journalist. In the words of the author: “Two brothers are ranking millions from webcam sites where men hand over a fortune as they fall for models’ fake sob stories (Scully, 2022).” In relation to “fake sob stories”, Scully (2022) implies that these pertain to stories that attractive Eastern European models tell their victims to elicit finances. In this case there are two main components that deter the reporting of these offences. Firstly, it is the transnational nature of fraud, which deters effective reporting. Secondly, once again, reporting is deterred by the victims’ trust towards the offenders.

The transnational nature of cybercrime was revealed via a BBC investigation, which was conducted alongside German and Georgian police during raids on call centers in Tbilisi (Hudson et al., 2023). Hudson et al. (2023) used the case examples of two UK citizens, one male and one female, to illustrate how they were duped out of £27 000 and £15 000 respectively via investment fraud. One person did attempt to report being scammed: “*Jane went down various routes, at home and abroad, in pursuit of her lost retirement funds, but got nowhere*.” The UK’s City of London Police took a report from her but “nothing came of it.” In this instance, the innate assertiveness and need to reclaim lost funds promoted Jane’s reporting to the City of London Police and seeking closure. Whilst this case pertains to UK rather than Scotland, its inclusion is logical as it mirrors what Scottish citizens go through as we go on to demonstrate in the first case study in Section 4.4.1.

Lyon (2023) reported that Scottish citizens were being targeted via a telephone scam where the cybercriminals requested the victims to read out a text message to a get 30 % reduction on their telephone contract. Complying resulted in creating access to their devices, which the cybercriminals used to purchase equipment on the victims’ accounts.

Notably, Lyon (2023) prompted readers to report scams both to Police Scotland and to Advice Direct Scotland. The latter is a charity that has taken on some of the policing and reporting functions of the state in line with what we expect to find in responsibilized societies (Garland, 2002, p. 124). This case study is an example of where a newspaper awareness-raising campaign was used to promote reporting both to the Police and a relevant charity.

3.2. Cybercrime against private institutions

A court case pertaining to the Royal Bank of Scotland in 2012 underlines the institution’s vulnerability to an antiquated form of cyber-enabled cheque fraud (Lord Justice Clerk et al., 2015a). The modus operandi is that the criminal cashes fake cheques which are paid out by the bank before the institution has time to authenticate them. The convicted offender cashed 23 forged cheques resulting in financial harm of £103 330. In this case, a lack of modern systems deterred the timely reporting of these offences.

In a case from 2018 concerning an unnamed bank, the private institution was victimized by one of its employees (Lord Menzies and Lord Turnbull, 2015). Using a member of the group who was an employee of the bank, they managed to extract £51 000 from customers’ accounts by stealing personal details, which created financial and reputational harm. In this case, insider threat deterred the immediate reporting of the offence. Defining insider threat, Martin (2024) states that: *“an insider is a person who has been trusted with access to an organization's assets, and who betrays that trust by exploiting (or intending to exploit) their access for unauthorized purposes, thereby potentially causing harm (p.7).*”

Cybercrimes against banks highlight the limitations of the government’s responsibilization strategy because the institutions that are meant to substitute the policing function (Garland, 2002, p. 124) fail to police themselves due to insider threat.

Standing out amid the cybercrime cases mostly affecting banks, is the court case of Peebles Media Group, a case that the court documents as “whaling” (Lord Summers, 2019; BBC, 2019). The modus operandi

[1] https://www.scotcourts.gov.uk/search-judgments/about-judgments

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. In reference to these cases, Martin (2024) uses the term "insider risk" to describe unsuspecting employees who fall prey to cybercrime. This he distinguishes from "insider threat", which is a premeditated course of harmful action (p. 11–12). This is a meaningful distinction because we use the term "insider threat" throughout to refer to malicious actors. In this case, 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 government's responsibilization strategy manifested as victim-blaming. In this instance, the reporting of the offence was deterred by the impersonation strategy of the offenders. However, victim blaming can also deter victims from reporting and promote cover-ups.

Moreover, 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 (no date) clearly distinguish "whaling" from "business e-mail compromise." In fact, "business e-mail compromise" is the correct criminological term in this case. The use of incorrect terminology in jurisprudence can cause confusion that further deters reporting.

A major attack targeting a Scottish car company Arnold Clark caught the public eye (O'Sullivan, 2023). They were attacked on 23–24 December 2022 by a ransomware gang called Play. The company's customers and employees had their details stolen and leaked online, including copies of passports and national insurance numbers. 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 turnover of £3 billion. In this case, the large scale of the attack meant that it could not be covered up and this promoted reporting. Hence, the scale of the harm positively promotes reporting.

Lastly, the privatized Royal Mail[2] suffered significant delays to its international deliveries after it was impacted by ransomware demanding £67 million, which it refused to pay (Sweeney, 2023). This resulted in major delays that adversely impacted 11 500 post office branches across the UK. They were unable to handle international mail or parcels. It can be inferred that the scale of harm promoted the reporting of the offence both to the Police and customers.

3.3. *Cybercrime against public institutions*

Dundee City Council fell victim to a cybercrime (Lord Justice General et al., 2020). An employee with a gambling addiction made payments on behalf of the council to fictitious suppliers, with the money going into his own bank account costing the council over a million pounds. In this case, insider threat and position of trust of the offender (Martin, 2024) deterred immediate reporting.

In addition, the press reported on the Scottish Environment and Protection Agency (SEPA), which was attacked by the Russian Conti group's ransomware on 24 December 2021 (Stewart, 2022; O'Sullivan, 2023). The environmental watchdog has purportedly spent over £5 000 000 on the recovery of 4 000 lost files. The evidence suggests that this offence was reported immediately.

Moreover, the University of the West of Scotland suffered cybercrime, which caused their online service to shut down for several days (Delaney, 2023). 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 gives strength to our argument that individuals and private institutions should benefit from the same degree of state support as public institutions. In fact, as we will show, Delaney's (2023) report clearly exemplifies how public institutions report cybercrime to a range of different stakeholders, who in return offer a coordinated response, which promotes reporting. This is not the case for Individuals and Private institutions.

Finally, in the case brought forward by Lawson and Isaac (2023) revelations were made surrounding the Sellafield nuclear site, where staff have routinely covered up cyber incidents whilst tolerating a toxic work culture of bullying and harassment. Whilst this case took place in England, it does provide insights into the hazards of non-reporting. It also exemplifies how a degraded workplace culture reduces transparency across the board. Hence, the latter will deter reporting as people will be reluctant to come forward on other matters too.

3.4. *Summary*

The literature review reveals the complexity of the cybercrime reporting phenomenon. What is 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 cases explicitly gave details related to reporting, a curious omission. See Table 1 for a summary of our findings.

4. Interviews

4.1. *Design*

We carried out semi-structured interviews which elicited information about victims' experiences reporting cybercrimes (Individuals, Private institutions, and Public institutions). The qualitative interviews (see APPENDIX A) lasted between 20 and 45 minutes with the questions being informed by the findings of Sikra, Renaud and Thomas (2023). We received ethical approval from the University of Strathclyde's Computer & Information Sciences Ethics Committee, for the interviews from 22 April 2022–09 January 2023, with application ID 2090.

4.2. *Participants*

In the terminology of Braun and Clarke (2021), the principles underlying our 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. We recruited who was available and in accordance with the victim typology of Individuals, Private institutions and Public institutions (Sikra, Renaud and Thomas, 2023). In addition, in line with Richie and Lewis (2003, p. 284–285), we recognize that the generalizability of our findings does not conform to the same principles as quantitative research. Instead, generalization in qualitative research has diverse meanings. The meaning we ascribe to generalization is most closely aligned with inferential generalization, because we use our findings to infer to other scientific contexts (Ritchie and Lewis, 2003, p. 267–298). We use our qualitative findings to infer our quantitative methodology as seen in Fig. 4., which contains all the items used to create the quantitative questionnaire.

Individual interviewees consisted of 2 males and 1 female who were victimized 2012–2022. The first participant suffered harm of £1 000, the second £5 240 and the third lost £20.

Two private institutions were represented by their managers, both of whom were male and in charge of a Small-to-Medium-sized Enterprises (SMEs). The first SME had been victimized in 2015. The requested ransom was £1 000. The loss to business was estimated at £20 000. The second SME was victimized in September-October 2022. The ransom was an unspecified number of Bitcoins. The loss to business was a non-financial cost of the human resources required to recover the corrupted systems.

Five public institutions were interviewed (5 males): 2 educational institutions, 2 charities for vulnerable people and 1 national governance

[2] https://www.gov.uk/government/news/government-completes-final-sale-of-its-stake-in-royal-mail-at-455p-per-share

Table 1
Influential Cybercrime Reporting Factors (from Case Studies).

	Cases where Reporting Mentioned	Promoting Factor	Deterring Factor	Confirmation of Factors from Research Literature
Individuals	2	assertiveness[1], need to reclaim lost funds[1]	language barrier[2], limited legal knowledge[2], trust towards offender[3,4], substance abuse[3], transnational nature of cybercrime[1,4]	[1]Hudson et al. (2023) [2]Lady Paton et al., (2014) [3]Lord Justice Clerk et al. (2015b) [4]Scully (2022)
Private institutions	0	large scale harm[1]	dated systems[2], insider threat[3], impersonation[4], victim blaming[4], incorrect legal terminology[4,5]	[1]Sweeney (2023) [2]Lord Justice Clerk et al., (2015a) [3]Lord Menzies and Lord Turnbull, (2015) [4]Lord Summers (2019); BBC (2019) [5]NCSC (2020); FBI (no date)
Public Institutions	1	best practices[1], multi-agency support[2]	insider threat[3], degraded workplace culture[4]	[1]Stewart (2022); O'Sullivan (2023) [2]Delaney (2023) [3]Lord Justice General et al. (2020) [4]Lawson and Isaac (2023)

To reveal the factors that are specific to Scotland, we proceeded to interview Scottish victims.

structure represented by their managerial and IT functions, and, in one case, a person involved in incident response post-victimization.

4.3. Analysis

We carried out a thematic analysis (TA) of interview data with NVivo 1.3 using the rationale for small sample sizes by Ritchie and Lewis (2003, p. 108), which is explained in detail in Section 5.1. In addition, in line with Braun and Clarke (2022)'s theorizing, our themes are best understood as summaries of topics, mainly in connection to what promotes and deters reporting. Firstly, we classified the 10 interview files according to the type of victim. Thus, we created three file classifications: 1. Individuals, 2. Private institutions and 3. Public institutions. Secondly, we coded each file during three stages: Stage 1. Initial coding during where we sieved through relevant information, Stage 2. Focused coding after which the general themes were identified and during Stage 3. Thematic coding was used to derive coherent stories. Table 2 summarizes the coding process which culminated in main themes: (1) promoting factors and (2) deterring factors whereas the third theme pertained to the actual case studies.

4.4. Results

Here, we discuss how the three categories of victims were affected by cybercrime based on the typology from prior research (Sikra, Renaud and Thomas, 2023). We accomplish this via specific case studies including direct quotes from the participants (Lingard, 2019) evidencing their perceptions and experiences. We have replaced semantically inconsequential quote segments with "(…)". Here, we move towards analyzing the victims' reporting trajectories.

4.4.1. Individuals

Case study 1: E-Bay Car Scam: In 2017, the victim was looking to purchase a used vehicle. The victim practiced extensive due diligence reconnaissance to verify the legitimacy of an advertisement. After that, the victim transferred the funds (£5 240), but the vehicle never arrived. There was a brief interaction with the seller who apologized for the delay after which the lines of communication went dead. The victim managed to track down the seller to their place of residence and persuaded the seller to go to the police under the weight of the collected evidence. He summarized the helpfulness of the English police in the following way:

Table 2
The thematic coding process depicting the gradual merging of codes via the three stages.

	Initial Coding	Focused Coding	Themes
1. Individuals	74	37	3
2. Priv. institutions	67	34	3
3. Pub. institutions	107	48	3

> 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 (…).
>
> (Participant no.:2)

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.
>
> (Participant no.:2)

The victim's assessment of Police Scotland's willingness to investigate only seven figure cyber-fraud would have been informal. Nevertheless, we are seeing a connection between some of the criticism leveraged against Action Fraud for similar reasons (Hunter, 2008; Correia, 2019). Objectively, the response from Police Scotland highlights that victims overestimate the police's competence in cases where cybercrime crossed jurisdictional boundaries (Cross, 2020).

Case study 2 HMRC Scam: In the United Kingdom, Her Majesty's Revenues and Customs (HMRC) is a governmental body responsible for tax collection as well as the administration of state social benefits among others. Its powers extend to Scotland too. Cybercriminals can impersonate HMRC to intimidate victims into divulging personal details. In 2021, the victim was targeted by a phone call claiming to be from HMRC alleging that she had an outstanding debt. The victim practiced due diligence and phoned HMRC querying the information from the initial phone call. HMRC confirmed that they had not made the telephone call. Next, the victim received a letter claiming to be from HMRC in respect to the alleged debt, which was indistinguishable from the organizational one. The victim was advised by the HMRC to report to the police because they considered it 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.

> (Participant no.:1)

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.
>
> (Participant no.:1)

Case study 3 Credit card details theft A: 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. The latter confirmed that her bank details were stolen and used in America causing a harm of £20. This resulted in her bank blocking the card and issuing a new one. The victim was reimbursed the full amount by her bank.

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 to buy a piece of IT equipment, which was a purchase that he did not recognize. The victim reported the suspicious activity to his bank because he wanted to block his credit card from further usage. The victim was reimbursed the full amount by his bank:

> 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.
>
> (Participant no.:3)

The bank advised reporting to the police on a specialized number, which they provided. The victim followed this advice but did not hear back from the police afterwards. The victim remained skeptical 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.
>
> (Participant no.: 3)

4.4.2. 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 (where.ru is a country code for a Russian online domain) and advised the reader that all 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 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 days 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.
>
> (Participant no.: 4)

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 and 400, which resulted in an indirect harm of £20 000 for lost business revenue. The victim SME had to cut its losses post-attack. The manager reported the cybercrime to the police and summarized 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.
>
> (Participant no.: 4)

Hence, the manager would have preferred to report to specialists who could have taken the case over in a more constructive way because the ones at the time did not manage to supply him with a satisfactory response.

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.
>
> (Participant no.: 5)

The files that became encrypted included various worksheet and organizational 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 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, but the manager continues to wonder what transpired:

> 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?
>
> (Participant no.: 5)

4.4.3. Public institutions

There is a stark distinction in the reporting process in the case of public institutions, which follow, what HR terms, "best practices" (Pfeffer, 1998). The latter pertains to managing organizations in accordance with a fixed set of rules which are seen as resulting in the best possible outcomes.

Case study 1. Educational institution - Poorly designed cybercrime: In 2021, during the night, the Scottish victim got alerted to a cyber-attack thanks to anti-virus software. The attack got picked up at 06:30 am by external responders who worked on it until 07:45 am to stabilize 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 summarized 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 (…).
>
> (Participant no.: 10)

To restore the network, IT staff had to work 18-hour shifts for 2–3 weeks, which was the price the institution and specifically its specialists paid for restoring their systems. There was a risk of burnout and mental health issues for staff because of overworking to ensure that none of the students were affected. 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 vs. 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.
>
> (Participant no.: 10)

Case study 2. Educational institution – Grudge 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, which resulted in victim blaming. Initially, the motivation was unclear, but it surfaced that the attacker was a vindictive ex-pupil. 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.
>
> (Participant no.: 6)

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 (…).
>
> (Participant no.: 6)

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 (Leukfeldt et al., 2020). It also exemplifies the importance of not making assumptions about the origins and motivations behind a cybercrime when receiving reports. This is especially true during a time when laymen and experts alike might be tempted to misattribute cyber-attacks to hostile state actors as has happened before in the case of the Mirai malware (Greenberg, 2023).

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 attack, the charity received a legitimate-looking invoice 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."
>
> (Participant no.: 7)

Hence, a sense of urgency was created by the supplier, which prompted the charity to transfer the finances. 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.
>
> (Participant no.: 7)

Luckily, this situation did not result in any actual harm being inflicted on 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 and Grossklags, 2017).

Case study 4. Charity for vulnerable people - Eastern European cybercrime: In 2022, the director identified that the organization was not capable of accessing its network. Initially, they thought it was a network issue but after three days they realized that this was 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 number 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 did not negotiate so the cybercriminals leaked the private details online. The charity reported to several agencies. Also, they have contacted Police Scotland, who were described in this way:

> 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.
>
> (Participant no.: 8)

Case study 5. National governance structure - Christmas midnight cybercrime: In 2020, cybercriminals chose to attack over Christmas. They were assuming that the staffing levels would be low and limiting organizational defenses. The cybercriminals accessed the structure's network fifteen days prior to launching their full-blown attack 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". Post-attack, staff showed 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. We argue that both staff's responses point to the government's responsibilization agenda (Horgan and Collier, 2016). Generally, people would not start tidying up a crime scene after a house burglary because they would know that the police would need to collect evidence. However, IT staff tried to recover the attacked structure because they felt responsible and when they were interviewed under caution, they felt scapegoated.

Fig. 3 summarizes the factors promoting or deterring cybercrime reporting that emerged from the interviews.

5. MINDSPACE: Towards a national strategy

The effects of responsibilization emerge from this investigation. In particular, victims felt unsupported, which might well be due to reduced UK police numbers (Travis, 2017). This state of affairs is confirmed by a recent report (Hymas and Butcher, 2023). There is the sense that many policemen and women are poorly prepared to deal with cybercrimes, confirming what was reported by Jayanetti and Townsend (2022). There is a worrying tendency towards victim blaming, as reported by Tims (2022). On the contrary, it is apparent from the factors that promote cybercrime reporting that the victims are seeking financial restoration but also want a force that is prepared to resolve their concerns and spread out a protective umbrella Fig. 4.

While responsibilization seems to deter reporting by individuals and private institutions, public institutions are legally required to report cybercrimes against them. The government's strategy thus impacts those who are least able to embrace responsibilization.

The impact of the UK's responsibilization strategy is clear. The deterring factors are related to a lack of direct support in the aftermath of

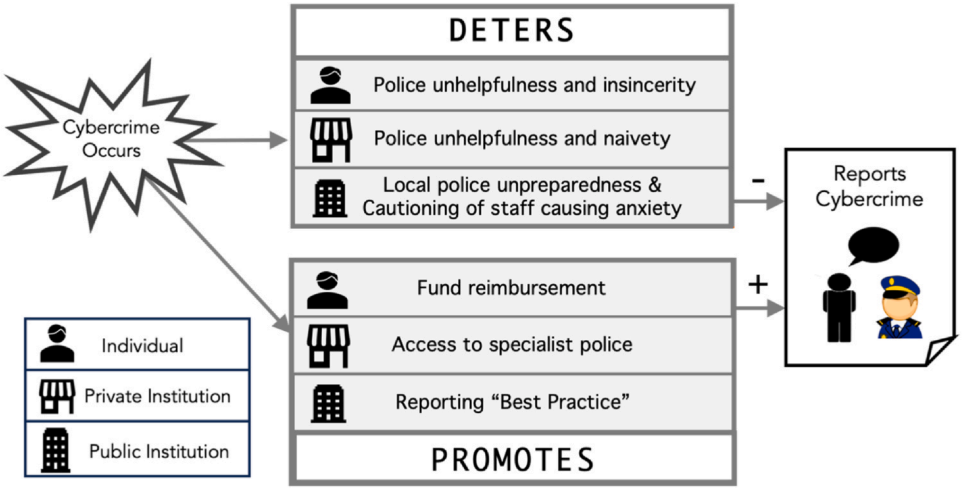
DETERS
Police unhelpfulness and insincerity
Police unhelpfulness and naivety
Local police unpreparedness &
Cautioning of staff causing anxiety
Cybercrime
Occurs
-
Reports
Cybercrime
+
Fund reimbursement
Access to specialist police
Reporting "Best Practice"
PROMOTES
Individual
Private Institution
Public Institution

Fig. 3. Model of Factors that Deter or Promote Scottish Cybercrime Reporting for the three Victim Types.

cybercrime. Individuals and private institutions point to police unhelpfulness, and public institutions point to the lack of assistance in terms of cautioning staff who might have been involved in facilitating cybercrime via insider risk (Martin, 2024, p. 11–12).

Individuals talk about wanting reassurance in terms of getting their money back. Private institutions want access to specialist police who can support them during the recovery process, and public institutions suggest that they could use assistance in formulating best practice guidelines to ease reporting. While Public institutions reside within the protective layer of the state, this also means that they are legally required to report falling victim to cybercrimes. Whilst criticism of the police emerged in our interviews in cases of public institutions, specifically police involvement during the cautioning staff tending to raise anxiety, one starts to appreciate the complexity of the cybercrime underreporting issue and of the ways in which it can be improved.

Fig. 4 maps the deterring and promoting factors that emerged from: (left) the related research, (middle) our scoping of court and news coverage and (right) interviews with cybercrime victims. The contribution of Fig. 4 for this research is that it serves to chart out how our research progressed from a more sterile environment (i.e., Related Research), closer to the actual victims (i.e., Court & News Coverage) until the ultimate proximity with the victim via the Scottish Victim Interviews. Hence, our theorizing follows a logical progression rather than being the result of ad hoc processes. This is most apparent through Section 5.1., where we transfer the factors from Fig. 4. into a usable governmental framework.

Many deterring factors are cognitive or emotional. For example, “lack of faith in police” led to negative affect. Indeed, according to Hymas and Butcher (2023), 22 out of 43 police forces of England and Wales were failing to investigate reported crime properly. Whilst our work is focused on Scotland, these failures serve as a stark reminder of what deters cybercrime reporting in the United Kingdom if victims feel their reports will not be investigated thoroughly, they are unlikely to report. Over the years, the need for police to provide specific support to other victims has been widely accepted. That is why, for example, reporting rape in Scotland can provide inspiration given that both cybercrime and rape are subject to victim blaming and shame (Renaud et al., 2021a; Renaud et al., 2021b; Van der Bruggen and Grubb, 2014). Consider, for example, Brooks-Hay (2019), who examined the Scottish victims’ perspective for reporting rape. The author found that rape victims occasionally found the police supportive, but at other times victims felt coerced into reporting to protect future possible victims. They also experienced police turning up unexpectedly in the early morning hours post reporting as anxiety provoking. This highlights the

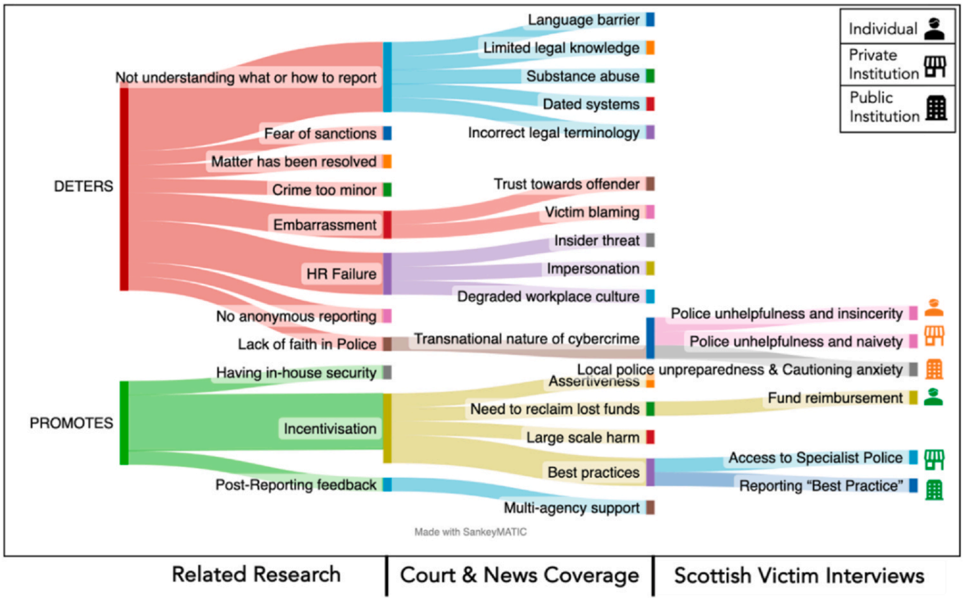

Fig. 4. Sankey Diagram Mapping of Factors that Emerged from (left) the Related Research, (middle) the Court &News Coverage and (right) Scottish Victim Interviews.

tension between low involvement and victim blaming, on the one hand, and high involvement and victim coercion on the other. It is challenging for the police to get the balance right, which will be partly related to the highly individualized phenomenology of victimhood. Our evidence is helpful in terms of hearing victims' voices and underlining research assumptions about how aspirations of high police engagement can play out in real life.

It is interesting to note that far fewer factors promote reporting. Some, such as "incentivization" suggest a focus for interventions. Judging by the mapping shown in Fig. 4, improved reporting might require addressing deterring factors, more so than merely focusing on maximizing promoting factors. Addressing the former is likely to require provision of victim support from the police. It would be beneficial if cybercrime responses matured to the point which would allow nuanced support for individuals and private institutions. This would constitute a welcome and much-needed relaxation of the UK's current responsibilization strategy and might encourage cybercrime reporting. This, in turn, would give the country more accurate data about levels of cybercrime in the country, and a sense of who the most targeted populations are, which could inform interventions particularly for more vulnerable population groups. As a result, this would contribute to the UK's policy objectives to make the country "*the safest place in the world to live and work online* (GOV, 2023)."

Levi and Burrows (2008) suggest that a responsibilization strategy is counterproductive because it makes the responsibilized do their own policing. This means law enforcement does not have an accurate idea of the extent of cybercrime in Scotland and the UK. Cobb (2020) also points out that without law enforcement policing cybercrime, businesses will factor it into their prices. This will fuel inflation and hit the most vulnerable in society the hardest, once again. We hope that this paper will help the government to understand the unintended consequences of this strategy.

5.1. MINDSPACE: encouraging reporting

We built on our insights to formulate an intervention that can improve a national strategy for cybercrime reporting. Here, we benefit from the MINDSPACE framework of behavioral influencers (Dolan et al., 2012): M = Messenger, I = Incentives, N = Norms, D = Defaults, S = Salience, P = Priming, A = Affect, C = Commitment, E = Ego. We map the influential reporting factors that emerged from our investigation (both deterring and promoting) to the MINDSPACE framework in Fig. 5 (details in Table A.1) to demonstrate why cybercrime is underreported.

Table A.1
Mapping of Factors to MINDSPACE Framework

MINDSPACE	*Related Research*	*Cases*	*Interviews*
Messenger	× Lack of faith in police	× language barrier × limited legal knowledge × trust towards offender	√ Access to Specialist Police
Incentivisation	× Matter has been resolved × Crime too minor	√ large scale harm	√ Wanting reimbursement × Police unpreparedness
Norms	√ Having in-house security	√ best practices √ multi-agency support × insider threat × incorrect legal terminology × degraded workplace culture	√ Reporting Best Practices
Defaults	× Not understanding what to report, or how to report	√ best practices √ multi-agency support × transnational nature of cybercrime	√ Reporting Best Practices
Salience	√ Post reporting feedback	× dated systems	√ Access to Specialist Police
Priming	× Fear of Sanctions		
Affect	× Embarrassment × Fear of Sanctions		× Cautioning staff causing anxiety
Commitment	× HR Failure	√ need to reclaim lost funds	√ Fund reimbursement
Ego	× Embarrassment	√ assertiveness × substance abuse × victim blaming	× Police Unhelpfulness, Insincerity and Naivety

× Deters Reporting. √Promotes Reporting.

The current responsibilization strategy focuses primarily on the messenger (M) influence but does not seem to utilize any of the other MINDSPACE influencers to encourage reporting. In fact, the strategy appears to subdue and suppress reporting by neglecting the impact of other influences such as affect and ego (see R in Fig. 5). What is clear is that our study revealed far more deterring than promoting factors, and it is thus unsurprising that cybercrime is underreported in Scotland and the UK. Finding ways to deploy all the potential influencers in the MINDSPACE framework so that cybercrime reporting is encouraged is a fruitful avenue for future research.

6. MINDSPACE: empirical survey

Since the MINDSPACE influencers were derived from a small sample of interviews, a quantitative verification approach was carried out to confirm factors. We designed a survey that tested these influencers on the general population focusing on victims that were typologically classed as individuals by prior research (Sikra et al., 2023). This is because under reporting is particularly poor in this demographic (Leukfeldt et al., 2020), unlike in organisations "who are inclined to report to public authorities" (Kemp et al., 2023).

6.1. Survey development

To test the influencers that promote and deter reporting, identified in the prior analysis and shown in Fig. 5 we conducted a survey using Prolific and Qualtrics. Each influencer was turned into a question as shown in tables A.2 and A. 3 (see: APPENDIX C & D). We also collected demographic information on gender and age range to evidence a representative sample of the general population. The survey was piloted on multiple occasions by the researchers before it went live to refine questions and assess completion time.

The full survey is attached in the APPENDIX B. The survey was launched via Prolific, and participants were paid the living wage equivalent for their efforts, which was at the time £10.42 per hour. This amounted to £2.00 for the ten-minute survey.

6.2. Participant demographics

We surveyed 407 Scottish participants via Prolific out of which 27 were excluded for failing the attention test. Our final sample contained

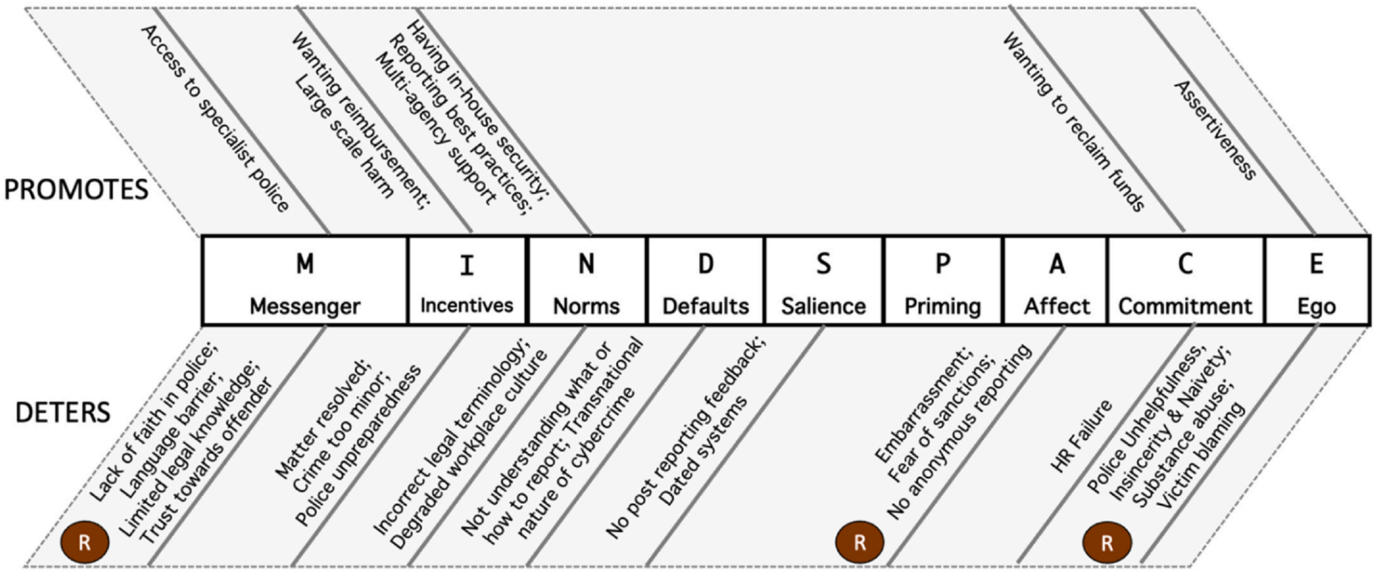
PROMOTES
Access to specialist police
Wanting reimbursement; Large scale harm
Having in-house security; Reporting best practices; Multi-agency support
Wanting to reclaim funds
Assertiveness
M Messenger
I Incentives
N Norms
D Defaults
S Salience
P Priming
A Affect
C Commitment
E Ego
DETERS
Lack of faith in police; Language barrier; Limited legal knowledge; Trust towards offender
Matter resolved; Crime too minor; Police unpreparedness
Incorrect legal terminology; Degraded workplace culture
Not understanding what or how to report; Transnational nature of cybercrime
No post reporting feedback; Dated systems
Embarrassment; Fear of sanctions; No anonymous reporting
HR Failure
Police Unhelpfulness, Insincerity & Naivety; Substance abuse; Victim blaming
R
R
R

Fig. 5. Fishbone Diagram Mapping Deterring and Promoting Cybercrime Reporting Factors to Dolan et al.'s (2012) MINDSPACE Framework (R = Responsibilisation Consequence).

203 females, 177 males, 6 non-binary/ third gender and 1 that preferred not to say. These participants were surveyed across age ranges. Subsequently, in the range 18–30 (64 males, 36 females, 3 non-binary/ third gender), 31–40 (57 males, 66 females, 1 non-binary/ third gender), 41–50 (50 males, 43 females, 1 non-binary/ third gender), 51–60 (24 males, 22 females, 1 non-binary/ third gender), Over 60 (8 males, 7 females) and 1 preferred not to disclose gender or age range. Of these participants 235 did not report cybercrime and 151 participants did. We did not test for gender effects as this was not included in our research questions or ethics approval application. 6.3. MINDSPACE: Results

The results are shown on tables A.4 – A.9. Tables A.4 and A.5 pertain to information that was extracted from two of the three qualitative open-ended questions, which are marked by capitalized letters B. and C. in APPENDIX B. The results from question A. were not included in this study. The "COUNT" column relates to the number of times participants supplied responses that align with the MINDSPACE factors.

6.2.1. *Results: tables A.4- A.5*

Table A. 4 depicts the spontaneous responses of participants to qualitative question B related to why they did *not* report the cybercrime. Their answers are thematically organized according to the MINDSPACE framework. Also, we have employed a discretionary criterion where only those factors connected with ten or more responses were identified as critical and highlighted in grey. As is obvious from our findings, most people did not report cybercrime because of a lack of faith in the police (87). The other dominant factors were the crime being too minor (56), the matter being resolved (54), not understanding what to report (25), embarrassment (41) and victim-blaming (10). Hence, we confirm that there is a breakdown in trust between the general public and the police, which contributes to under-reporting. Participants felt it was their role to rectify the situation or alternatively their fault if they could not.

Table A. 5 depicts responses to qualitative question C related to why they reported the cybercrimes. We have employed a discretionary criterion where only those factors connected with ten or more responses were identified as critical (highlighted in grey). According to our discretionary criterion 33 % of deterring factors crossed the critical threshold and 33 % of the promoting factors crossed the critical threshold. It emerges that wanting to reclaim lost funds (85) was the highest promoting factor for cybercrime reporting. In addition, large-scale harm (17) and assertiveness (altruism) (55) were other major promoting factors. Moreover, upon inspecting our data, we realized that the more assertive often reported cybercrime to protect others from the same ordeal.

If tables A.4 and A.5 (see: APPENDIX E & F) are analysed conjointly, we can conclude that cybercrime reporting can be improved if Police Scotland repair the relationship with the victimised public by playing a more active role in fund recovery. At present, reclaiming lost funds is mainly the remit of banks, with Police Scotland supplying the crime reference number. Moreover, Police Scotland could tap into a sense of altruism and conduct awareness-raising campaigns encouraging the public to protect others from falling victim to cybercrime.

6.2.2. *Results: tables A.6- A.7*

Tables A.6 and A.7 map the quantitative responses onto the MINDSPACE factors. The qualitative information from the tables A.4 and A.5 (see: APPENDIX G & H) is organized in column "(Qual.) COUNT." In our analysis, we emphasize comparison between the critical qualitative factors (highlighted in grey) and their quantitative counterparts.

In Table A.6, the general trend in the data is that factors that scored critically high in the qualitative domain also scored high on the quantitative survey. Nevertheless, there are some instances of noteworthy incongruence. In particular, the factors "Police unpreparedness" and "Police unhelpfulness, insincerity, and naivety" did not cross the ten-response threshold in the qualitative analysis, which was our discretionary critical cut-off as already discussed in Tables 4 and 5. Nevertheless, as we can see from table A.6 that people have scored these factors higher than the more connected qualitative factors. This is perhaps because both "Police unpreparedness" and "Police unhelpfulness, insincerity, and naivety" are manifestations of "Lack of faith in police" since the victims can only objectively judge their own lack of faith in police but cannot objectively assess how prepared the force actually is.

In table A.7, the general trend in the data is that factors that scored critically high in the qualitative domain also scored high on the quantitative survey. Here, there is also a noteworthy incongruence. In particular, the factor "Assertiveness (altruism)", which featured prominently in the qualitative responses scored the lowest out of all factors in the quantitative responses. This could be because the more salient theme in the victims' minds is wanting to reclaim lost funds and they may not realize that to meet that need they must become more assertive.

6.2.3. Results: Tables A.8- A.9

Tables 8 and 9 (see: APPENDIX I & J) are tabular representations of people's extreme scores calculated as percentages of responses. Consulting the percentage of extreme scores is useful for bringing out how strongly people felt about particular statements.

In table A.8, the general trend in the data is that deterring factors that scored critically high in the qualitative domain were also skewed towards more extreme scores in the quantitative domain. This means that victims showed a strongly skewed pattern of responses that corresponded with the factor whereas only a small percentage of them showed a strong pattern of skewed responses away from the factor. Nevertheless, there is noteworthy incongruence in the data. Namely, the factors "Police unpreparedness" and "Police unhelpfulness, insincerity, and naivety" did not cross the ten-response threshold in the qualitative analysis. Nevertheless, as we can see from table A.8 people's pattern of responses was strongly skewed towards these factors. This is perhaps because both "Police unpreparedness" and "Police unhelpfulness, insincerity, and naivety" are in fact instances of "Lack of faith in police" since the victims can only objectively judge their own lack of faith in police but cannot objectively assess how prepared the force is.

In table A.9, the general trend in the data is that promoting factors that scored critically high in the qualitative domain were also skewed towards more extreme scores in the quantitative domain. This means that victims showed a strongly skewed pattern of responses that corresponded with the factor whereas only a small percentage of them showed a strong pattern of skewed responses away from the factor. Nevertheless, there are multiple noteworthy incongruences in the data that merit further discussion. Namely, the factor "Assertiveness (altruism)", which featured prominently in the qualitative responses scored the lowest out of all the factors in the quantitative section. This could be because the more salient theme in the victims' minds is that of wanting to reclaim lost funds and they might not appreciate the need for assertiveness. Even so, some factors scored minimally or not at all in the qualitative responses but displayed a strongly skewed pattern of scores in the current quantitative section. This is likely related to the composition of our sample and how our victims were likely to view themselves. Respondents were victims-individuals (Sikra, Renaud and Thomas, 2023) so they might not provide spontaneous qualitative responses related to factors that emerged from interviewees representing institutions (e.g., best practices and multi-agency support to name just a couple). This might be why they exhibited a stronger pattern of agreement only once they were primed to do so by the survey questions.

7. Discussion

The approach within this study was to break down the problem of cybercrime under-reporting into more manageable components and decide which ones are most critical for promoting reporting. Governmental statistics were used to lend credence to our concerns and served as an introduction into the current study (e.g., Scottish Government, 2022a, 2022b). We based our approach on the underlying assumption that under-reporting will be the result of the UK government's neoliberal responsibilisation approach (Garland, 2002; Renaud et al., 2018).

We first reviewed prior research findings, which led to a parsimonious two-factor model of factors influencing cybercrime reporting (see: Fig. 2). This model served as a basic prism, which was useful in breaking down the first dataset- the analysis of Scottish court documents and news coverage.

Next, we combined our basic two factor cybercrime reporting model from Fig. 2. with the framework by Sikra et al. (2023) to organize the promoting and deterring factors according to the three victim types (i.e., Individuals, Private institutions and Public institutions). This provided a more nuanced picture of the cybercrime reporting landscape. Our Table 1. supplies insights for policy makers and legal analysists, who want to understand the problem at hand

Armed with our simple two-factor model from Fig. 2. and findings from the Scots courts and news in Table 1., as well as qualitative interviews of 10 cybercrime victims, we were able to derive a fuller set of influential factors, as depicted in Fig. 3. The theme of "Lack of faith in police" emerged as a strong cybercrime reporting deterrent and "Fund reimbursement" took center stage as a promoting factor.

The MINDSPACE framework of behavioral influencers by Dolan et al. (2012) proved to be particularly useful in terms of organizing our findings for what deters and promotes reporting in a way that exhaustively encapsulated our data and is in line with the approach taken by UK policy makers (see: Table A.1 and Fig. 5.) Some behavioral influencers contain multiple factors (e.g., in Deters, Messenger is connected to three factors) whereas others have not been uncovered via our data gathering and analysis (e.g., in Promotes, Salience). To preserve the Dolan et al. (2012) framework and remain true to our data, we have left some behavioral influencers empty.

To empirically confirm these factors, we posed a survey solely to individual cybercrime victims as they were seen as the most vulnerable out of the three since, unlike public institutions they lacked government support,

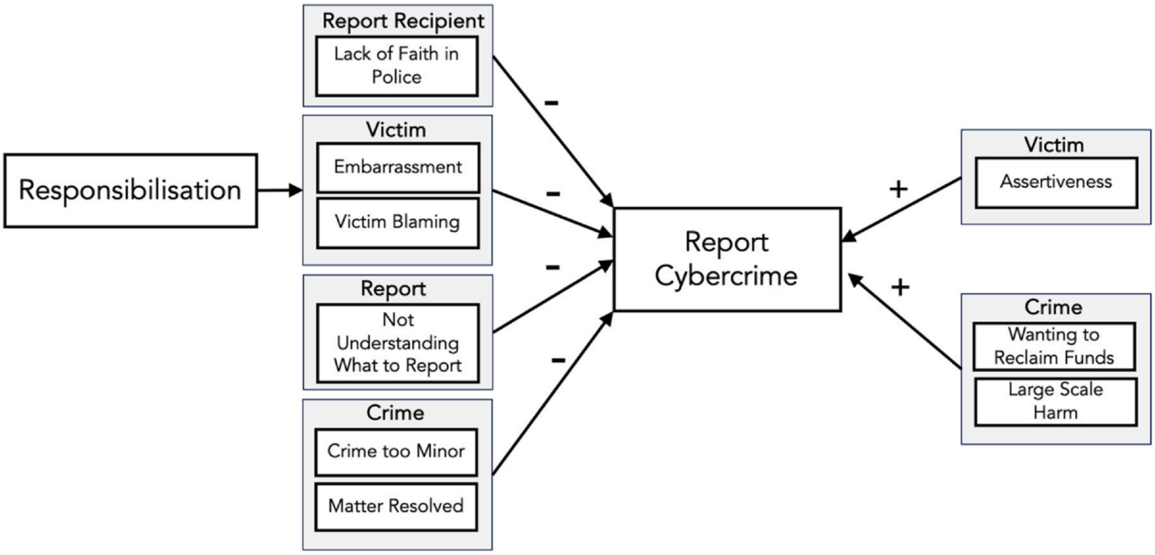

Fig. 6. Final Model of Factors that Deter and Promote Cybercrime Reporting.

and unlike private institutions bore the entire loss themselves. The survey questions were fitted tightly around MINDSPACE model, its influencers and factors that were connected to them (see: Table A.2 and A.3).

Analysis revealed that factors generated a far greater response rate both in terms of the free text responses as well as the quantitative survey rankings.

8. Recommendations

Recommendation 1: Based on our analysis "Lack of faith in Police" is a critical theme that deters cybercrime reporting. This theme signals a breakdown in the relationship between victims of economic cybercrime and Police Scotland. We recommend that Police Scotland makes it their priority to inform communities across the country that they can rely on them in cases of economic cybercrime just as they could in the case of a stolen bike, physical assault or an illicit cannabis farm in a seemingly dilapidated property. Police Scotland should raise awareness so that people know that economic cybercrime is common and that they should not feel embarrassed for falling prey to offenders. Rather, victims should be made to feel that they are playing a part in protecting others from the same ordeal if they report to the police.

Recommendation 2: Based on our analysis "Wanting to reclaim lost funds" is a critical theme that promotes cybercrime reporting. To improve cybercrime reporting, the police must become more involved in fund reimbursement and victims must see evidence that the police are taking their situation seriously. Therefore, the police must stop playing second fiddle to the bank. A way forward could be for the police to enter a thought-out alliance with the bank where their respective responsibilities would be clearly divided based on their capabilities, which would be transparently communicated to the public. Communications with the public must acknowledge the limitations of what can be achieved to avoid a dip in the faith towards the police. This initiative should not be centralized, but rather individual bank branches should collaborate with local police stations in designing campaigns that fit with the diverse communities that compose Scotland. A centralized one-size fits all approach must be avoided.

9. Conclusion

Our investigation sought to identify cybercrime reporting promoting and deterring factors. In this paper we report on our findings, informed by prior research, news and court reports, interviews and a final survey. The final model that captures the relationship between the collaboration of police and banks on the vertical axis versus improved reporting on the horizontal axis is depicted in Fig. 6.

The take home message is that Police Scotland should improve its relationship with the cybercrime victimized public and the most effective strategy is likely to reside in awareness raising and embarrassment reduction community campaigns alongside facilitating the reimbursement of lost funds. The only way to achieve this is if the police forge a deeper and more strategic alliance with the banks, which will be decentralized and appropriated to unique community contexts (i.e., different tools and techniques will be used to engage citizens from deprived communities vs. affluent communities). This will, in turn, reduce the responsibilization of cybercrime victims but also the responsibilization of banks, who are augmenting the police's role in fund reimbursement. Finally, the reduction of responsibilization will steadily improve reporting.

CRediT authorship contribution statement

Juraj Sikra: Writing – review & editing, Writing – original draft, Investigation, Formal analysis, Data curation, Conceptualization. **Karen Renaud**: Writing – review & editing, Visualization, Supervision, Methodology, Funding acquisition, Conceptualization. **Daniel Thomas**: Writing – review & editing, Supervision, Methodology, Funding acquisition, Conceptualization.

Funding statement

This research was funded by the Scottish Institute for Policing Research (SIPR) (SIPR21MFS_003) and the University of Strathclyde in Glasgow.

Declaration of Competing Interest

The authors report there are no competing interests to declare.

Acknowledgements

The authors would like to acknowledge and thank the Scottish Institute for Policing Research (SIPR) and the University of Strathclyde in Glasgow for their support of this research. In addition, the authors are extremely grateful to all the victims that agreed to get interviewed and thereby relive their ordeal in the interest of advancing scientific know how and improving cybercrime reporting in Scotland and beyond.

Declaration of interest

The authors report there are no competing interests to declare.

APPENDIX A

QUALITATIVE INTERVIEW

Demographics

a) What is your gender?
b) What is your age range: 18–24; 25–34; 35–44; 45–54; 55–64; 64+

1. What was your understanding of scams and cybercrime before it happened to you?
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 what happened to you when you were victimized. 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.
4. 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?
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. Please walk me through your experience of reporting. What steps did you follow?

7. 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 victimized?
8. 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?
9. What kind of aftercare did you receive from the police? Did you receive after care from any other agency?
10. Please describe whether you encountered any obstacles in terms of your ability or accessibility to technology when reporting cybercrime?
11. What would an ideal reporting system look like?

APPENDIX B

QUANTITATIVE SURVEY

Please confirm that you have previously fallen victim to a cybercrime?

o Yes, I have.
o No, I have not.
Gender?
o Male
o Female
o Non-binary / third gender
o Prefer not to say.
Age Range?
o 18–30
o 31–40
o 41–50
o 51–60
o Over 60
o Prefer not to say.
Recall when you fell victim to a cybercrime. Did you report the crime?
o Yes
o No

A. **Who did you report it to?**

____
____

Why didn’t you report it?

____
____

Why did you report it?

____
____

Imagine that you fall victim to a cybercrime sometime in the future. The following questions will ask you to say whether you agree or disagree with different factors that can influence your decisions to **report, or not to report**, falling victim to a cybercrime.

1. In deciding whether to report a cybercrime, faith in the Police would encourage reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

2. In deciding whether to report a cybercrime, being able to report to someone who speaks your mother tongue would encourage reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

3. In deciding whether to report a cybercrime, having legal knowledge would encourage reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

4. In deciding whether to report a cybercrime, having trusted a person who deceived you to commit a crime would deter me from reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

5. In deciding whether to report a cybercrime, the amount of money lost would be influential

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

6. In deciding whether to report a cybercrime, how well the police are prepared to deal with the report is important in encouraging reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

7. In deciding whether to report a cybercrime, whether you already received a refund from your bank might deter reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

8. In deciding whether to report a cybercrime, if it occurred at work, a toxic workplace culture would deter reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

9. In deciding whether to report a cybercrime, not understanding what or how to report might deter reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

10. In deciding whether to report a cybercrime, the global nature of cybercrime might deter reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

11. In deciding whether to report a cybercrime, whether you will receive post reporting feedback would encourage reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

12. In deciding whether to report a cybercrime, outdated reporting systems would deter reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

13.In deciding whether to report a cybercrime, embarrassment would deter reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

14. In deciding whether to report a cybercrime, fear of sanctions would deter reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

15. In deciding whether to report a cybercrime, being able to report anonymously would encourage reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

16. In deciding whether to report a cybercrime, if it happened at work, HR failures would deter reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

17. In deciding whether to report a cybercrime, police helpfulness would encourage reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

18. In deciding whether to report a cybercrime, police unhelpfulness and insincerity would deter reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

19. In deciding whether to report a cybercrime, fear of being blamed would deter reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

20. In deciding whether to report a cybercrime, if substance abuse was involved, this would deter reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

21. In deciding whether to report a cybercrime, access to specialist police would encourage reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

22. In deciding whether to report a cybercrime, wanting to be reimbursed would encourage reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

23. In deciding whether to report a cybercrime, the scale of the harm being large would encourage reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

24. If at work, in deciding whether to report a cybercrime, the existence of a dedicated cybersecurity unit would encourage reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

25. If at work, in deciding whether to report a cybercrime, reporting being "required by company policy” is important in encouraging reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

26. In deciding whether to report a cybercrime, receiving support from different organizations might encourage reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

27. In deciding whether to report a cybercrime, being an assertive person is important in encouraging reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

28. In a work context, in deciding whether to report a cybercrime, the use of the incorrect term by the organization to describe the attack might deter reporting

	1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree

29. In deciding whether to report a cybercrime, attention test, check the middle option

		1	2	3	4	5	6	7	
Strongly Disagree	o	o	o	o	o	o	o	Strongly Agree	Strongly Disagree

APPENDIX C

Table A. 2
- Victims study factors that were used to construct survey questions about what DETERS reporting.

MINDSPACE	FACTORS	SURVEY QUESTIONS (Strongly disagree 1 - Strongly agree 7) In deciding whether to report a cybercrime, … ◊
Messenger	Lack of faith in police	faith in the Police would encourage reporting.
	Limited legal knowledge	having legal knowledge would encourage reporting.
	Language barrier	being able to report to someone who speaks your mother tongue would encourage reporting.
	Trust towards offender	having trusted a person who deceived you to commit a crime would deter me from reporting.
Incentivization	Crime too minor	the amount of money lost would be influential.
	Matter has been resolved	whether you already received a refund from your bank might deter reporting.
	Police unpreparedness	how well the police are prepared to deal with the report is important in encouraging reporting.
Norms	Degraded workplace culture	if it occurred at work, a toxic workplace culture would deter reporting.
	Insider threat	being able to report anonymously would encourage reporting.
	Incorrect legal terminology	In a work context, (…), the use of the incorrect term by the organization to describe the attack might deter reporting.
Defaults	Not understanding what to report	not understanding what or how to report might deter reporting.
	Trans-national nature of cybercrime	the global nature of cybercrime might deter reporting.

(*continued on next page*)

Table A. 2 (*continued*)

MINDSPACE	FACTORS	SURVEY QUESTIONS (Strongly disagree 1 - Strongly agree 7) In deciding whether to report a cybercrime, … ◊
Salience	Dated systems	outdated reporting systems would deter reporting.
Priming	Fear of sanctions	fear of sanctions would deter reporting.
Affect	Embarrassment	embarrassment would deter reporting.
	Fear of sanctions	fear of sanctions would deter reporting.
Commitments	HR failure	if it happened at work, HR failures would deter reporting.
Ego	Embarrassment	embarrassment would deter reporting.
	Victim blaming	fear of being blamed would deter reporting.
	Police unhelpfulness, insincerity and naivety	police unhelpfulness and insincerity would deter reporting. *
	Substance abuse	if substance abuse was involved, this would deter reporting.

◊The three dots indicate the continuation of all questions in the "SURVEY QUESTIONS." There is an exception to this rule where it is indicated "(…)." In this instance, the beginning of the question is different and the space in brackets is filled with "in deciding whether to report a cybercrime."

* In addition, we have made a clerical error, which is apparent from viewing the APPENDIX B questions 16 and 17 which pertain to police (un)helpfulness and are semantically similar. In our tabular analysis we have included question 17 due to its tighter correspondence with the factor. Question 16 has been completely excluded.

APPENDIX D

Table A. 3

-Victims study factors that were used to construct survey questions about what PROMOTES reporting:

MINDSPACE	FACTORS	SURVEY QUESTIONS (Strongly disagree 1 - Strongly agree 7) In deciding whether to report a cybercrime, …◊
Messenger	Access to specialist police	access to specialist police would encourage reporting.
Incentivization	Wanting to reclaim lost funds	wanting to be reimbursed would encourage reporting.
	Large scale harm	the scale of the harm being large would encourage reporting.
Norms	Best practices	reporting being "required by company policy" is important in encouraging reporting.
	Having in-house security	If at work, (…), the existence of a dedicated cybersecurity unit would encourage reporting.
	Multi-agency support	receiving support from different organizations might encourage reporting
Defaults	Best practices	reporting being "required by company policy" is important in encouraging reporting.
	Multi-agency support	receiving support from different organizations might encourage reporting.
Salience	Post reporting feedback	whether you will receive post reporting feedback would encourage reporting.
	Access to specialist police	access to specialist police would encourage reporting.
Priming	0*	N/A
Affect	0*	N/A
Commitments	Wanting to reclaim lost funds	wanting to be reimbursed would encourage reporting.
Ego	Assertiveness	being an assertive person is important in encouraging reporting.

* Since these MINDSPACE factors were not revealed via our research that informed the survey questions a discretionary exclusion criterion was applied to them.

◊The three dots indicate the continuation of all questions in the "SURVEY QUESTIONS." There is an exception to this rule where it is indicated "(…)." In this instance, the beginning of the question is different and the space in brackets is filled with "in deciding whether to report a cybercrime."

APPENDIX E

Table A. 4

- Victims study survey qualitative analysis of DETERRING FACTORS.

MINDSPACE	FACTORS	COUNT	EXAMPLE QUOTES FROM SURVEY
Messenger	Lack of faith in police	87	"Police wouldn't do anything."
	Limited legal knowledge	5	"(…) I was also worried about possible interrogation (…)"
	Language barrier	2	"I was in a foreign country and didn't know how to."
	Trust towards offender	2	"I didn't report it to the police but did report it to the company they were pretending to be."
Incentivization	Crime too minor	56	"It was something I could handle and didn't cost me money."
	Matter has been resolved	54	"I managed to retrieve the funds and change my passwords."
	Police unpreparedness	14	"I didn't think anything could be done about it and the police are busy."
Norms	Degraded workplace culture	1	"When I was in school if I had reported cyber bullying (cybercrime) to anyone it would have made the situation worse (…)"
	Insider threat	0	N/A
	Incorrect legal terminology	0	N/A
Defaults	Not understanding what to report	25	"I didn't know how to go about reporting it."
	Trans-national nature of cybercrime	6	"The attack originated from a country different to my own and I figured that it would not be something taken seriously or just ignored."
Salience	Dated systems	1	"No easy way to do it."
Priming	Fear of sanctions	6	"I was worried I'd get in trouble as I was downloading a TV show when it happened."
Affect	Embarrassment	41	"I felt very silly for falling victim to it and did not want to be judged as I felt it would have been very obvious to someone else that it was a scam."
	Fear of sanctions	6	"It is a bit embarrassing, and threats were made if I went to the police."
Commitments	HR failure	0	N/A
Ego	Embarrassment	43	"I was embarrassed and concerned about suffering retribution (…)."
	Victim blaming	10	"It is a bit embarrassing, and threats were made if I went to the police."

(*continued on next page*)

Table A. 4 (*continued*)

MINDSPACE	FACTORS	COUNT	EXAMPLE QUOTES FROM SURVEY
	Police unhelpfulness, insincerity, and naivety	6	“I have absolutely no confidence Police Scotland even understanding the scam let alone being able to recover my loss, so what good would it do? (…)”
	Substance abuse	0	N/A

We have employed grey highlighting for factors that surfaced on 10 or more occasions as a part of the spontaneous qualitative text box questions. The 10-response cut off was employed as a discretionary criterion.

APPENDIX F

Table A. 5
- Victims study survey qualitative analysis of PROMOTING FACTORS:

MINDSPACE	FACTORS	COUNT	EXAMPLE QUOTES FROM SURVEY
Messenger	Access to specialist police	1	“The bank contacted us initially, told us to contact the police and then because of that, we were contacted by, as I said, I think it was the cyberfraud unit in London. (…)”
Incentivization	Wanting to reclaim lost funds	85	“So, it was on record and so I could get a crime reference number for the bank.”
	Large scale harm	17	“As they wiped out my bank account, I felt like I had no other option.”
Norms	Best practices	5	“It was company policy to report anything that was a security risk for our clients and fellow colleagues.”
	Having in-house security	0	N/A
	Multi-agency support	0	N/A
Defaults	Best practices	5	“I didn’t report it, I just complied with the procedure, they carried out the investigation on my behalf.”
	Multi-agency support	0	N/A
Salience	Post reporting feedback	1	“The bank contacted us initially, told us to contact the police and then because of that, we were contacted by, as I said, I think it was the cyberfraud unit in London. (…)”
	Access to specialist police	1	“The bank contacted us initially, told us to contact the police and then because of that, we were contacted by, as I said, I think it was the cyberfraud unit in London. (…)”
Priming	0*	0	N/A
Affect	0*	0	N/A
Commitments	Wanting to reclaim lost funds	85	“It was a requirement of my bank in order to be reimbursed the money that I was robbed.”
Ego	Assertiveness (altruism Δ)	55	“I didn’t want anyone else to suffer. We need to support each other against cybercrime. It could happen to anyone.”

□We have employed grey highlighting for factors that surfaced on more than 10 occasions as a part of the spontaneous qualitative text box questions. The 10-response cut off was employed as a discretionary criterion.
Δ 18 out of the 55 responses were driven by an explicit need to protect others and or a strong sense of right and wrong, which is why it is meaningful to draw out “altruism” as a specific sub-component of Assertiveness.
* Since these MINDSPACE factors were not revealed via our research that informed the survey questions a discretionary exclusion criterion was applied to them.

APPENDIX G

Table A. 6
- Victims study survey comparison of qualitative vs. quantitative survey data on DETERRING FACTORS:

MINDSPACE	FACTORS	(Qual.) COUNT	(Quan.) MEAN & [ST. DEV.]	(Quan.) MEDIAN & [RANGE]	(Quan.) REPORTED MEAN & [UNREPORTED MEAN]
Messenger	Lack of faith in police	87	5.87[1.25]	6[1–7]	5.75[5.94]
	Limited legal knowledge	5	5.24[1.56]	6[1–7]	5.17[5.29]
	Language barrier	2	5.90[1.40]	6[1–7]	5.91[5.89]
	Trust towards offender	2	4.26[1.85]	5[1–7]	3.79[4.57]
Incentivization	Crime too minor	56	6.13[1.34]	7[1–7]	5.78[6.35]
	Matter has been resolved	54	5.23[1.75]	6[1–7]	4.77[5.51]
	Police unpreparedness	14	6.04[1.12]	6[1–7]	5.99[6.08]
Norms	Degraded workplace culture	1	5.11[1.77]	6[1–7]	4.75[5.35]
	Insider threat	0	5.83[1.37]	6[1–7]	5.70[5.92]
	Incorrect legal terminology	0	4.41[1.61]	5[1–7]	4.11[4.61]
Defaults	Not understanding what to report	25	5.79[1.36]	6[1–7]	5.54[5.94]
	Trans-national nature of cybercrime	6	4.38[1.77]	5[1–7]	3.72[4.80]
Salience	Dated systems	1	5.25[1.51]	5.5[1–7]	4.97[5.43]
Priming	Fear of sanctions	6	4.61[1.86]	5[1–7]	4.23[4.85]
Affect	Embarrassment	41	5.01[1.84]	5[1–7]	4.36[5.42]
	Fear of sanctions	6	4.61[1.86]	5[1–7]	4.23[4.85]
Commitments	HR failure	0	4.55[1.75]	5[1–7]	4.22[4.77]

(*continued on next page*)

Table A. 6 (*continued*)

MINDSPACE	FACTORS	(Qual.)	(Quan.)	(Quan.)	(Quan.)
		COUNT	MEAN	MEDIAN	REPORTED MEAN &
			& [ST. DEV.]	& [RANGE]	[UNREPORTED MEAN]
Ego	Embarrassment	43	5.01[1.84]	5[1–7]	4.36[5.42]
	Victim blaming	10	5.18[1.75]	6[1–7]	4.73[5.48]
	Police unhelpfulness, insincerity, and naivety	6	6.12[1.18]	6.5[1–7]	5.85[6.29]
	Substance abuse	0	4.53[1.79]	5[1–7]	4.27[4.70]

□We have employed grey highlighting for factors that surfaced on 10 or more occasions as a part of the spontaneous qualitative text box questions. The 10-response cut off was employed as a discretionary criterion.

APPENDIX H

Table A. 7
- Victims study survey comparison of qualitative vs. quantitative survey data on PROMOTING FACTORS:

MINDSPACE	FACTORS	COUNT	(Quan.)	(Quan.)	(Quan.)
			MEAN	MEDIAN	REPORTED MEAN & [UNREPORTED MEAN]
			& [ST. DEV.]	& [RANGE]	
Messenger	Access to specialist police	1	5.76[1.23]	6[1–7]	5.87[5.69]
Incentivization	Wanting to reclaim lost funds	85	6.16[1.24]	7[1–7]	6.18[6.14]
	Large scale harm	17	6.06[1.23]	6[1–7]	5.93[6.14]
Norms	Best practices	5	5.57[1.39]	6[1–7]	5.48[5.63]
	Having in-house security	0	5.93[1.20]	6[1–7]	6.01[5.88]
	Multi-agency support	0	5.54[1.18]	6[1–7]	5.64[5.48]
Defaults	Best practices	5	5.57[1.39]	6[1–7]	5.48[5.63]
	Multi-agency support	0	5.54[1.18]	6[1–7]	5.64[5.48]
Salience	Post reporting feedback	1	5.15[1.52]	5[1–7]	5.10[5.18]
	Access to specialist police	1	5.76[1.23]	6[1–7]	5.87[5.69]
Priming	0*	0	N/A	N/A	N/A
Affect	0*	0	N/A	N/A	N/A
Commitments	Wanting to reclaim lost funds	85	6.16[1.24]	7[1–7]	6.18[6.14]
Ego	Assertiveness (altruism Δ)	55	4.98[1.42]	5[1–7]	4.83[5.09]

□We have employed grey highlighting for factors that surfaced on more than 10 occasions as a part of the spontaneous qualitative text box questions. The 10-response cut off was employed as a discretionary criterion.

Δ 18 out of the 55 responses were driven by an explicit need to protect others and or a strong sense of right and wrong, which is why it is meaningful to draw out "altruism" as a specific sub-component of Assertiveness. The calculated statistics do not distinguish "altruism" from "Assertiveness", instead they are performed on all 55 responses.

* Since these MINDSPACE factors were not revealed via our research that informed the survey questions a discretionary exclusion criterion was applied to them.

APPENDIX I

Table A. 8
Victims study survey comparison of qualitative vs. percentage survey data on DETERRING FACTORS:

MINDSPACE	FACTORS	(Qual.)	(Quan.)Responses 6 or 7 in %	(Quan.)	(Quan.)
		COUNT		Responses 5, 6 or 7 in %	Responses 1, 2 or 3 in %
Messenger	Lack of faith in police	87	72	89	6
	Limited legal knowledge	5	52	74	14
	Language barrier	2	73	83	6
	Trust towards offender	2	30	51	35
Incentivization	Crime too minor	56	81	90	6
	Matter has been resolved	54	54	74	18
	Police unpreparedness	14	75	91	3
Norms	Degraded workplace culture	1	52	72	19
	Insider threat	0	70	83	7
	Incorrect legal terminology	0	26	52	26
Defaults	Not understanding what to report	25	67	88	6
	Trans-national nature of cybercrime	6	33	51	31
Salience	Dated systems	1	50	74	14
Priming	Fear of sanctions	6	39	58	28
Affect	Embarrassment	41	49	71	22
	Fear of sanctions	6	39	58	28
Commitments	HR failure	0	38	54	28
Ego	Embarrassment	43	49	71	22
	Victim blaming	10	53	75	19
	Police unhelpfulness, insincerity and naivety	6	76	92	4
	Substance abuse	0	35	55	27

□We have employed grey highlighting for factors that surfaced on more than 10 occasions as a part of the spontaneous qualitative text box questions. The 10-response cut off was employed as a discretionary criterion

APPENDIX J

Table A. 9
Victims study survey comparison of qualitative vs. percentage survey data on PROMOTING FACTORS:

MINDSPACE	FACTORS	COUNT	(Quan.)Responses 6 or 7 in %	(Quan.) Responses 5, 6 or 7 in %	(Quan.) Responses 1, 2 or 3 in %
Messenger	Access to specialist police	1	66	85	5
Incentivization	Wanting to reclaim lost funds	85	80	85	5
	Large scale harm	17	77	90	4
Norms	Best practices	5	59	79	8
	Having in-house security	0	70	89	5
	Multi-agency support	0	55	82	5
Defaults	Best practices	5	59	79	8
	Multi-agency support	0	55	82	5
Salience	Post reporting feedback	1	48	71	15
	Access to specialist police	1	66	85	5
Priming*	0	0	N/A	N/A	N/A
Affect*	0	0	N/A	N/A	N/A
Commitments	Wanting to reclaim lost funds	85	80	85	5
Ego	Assertiveness (altruism Δ)	55	40	66	14

□We have employed grey highlighting for factors that surfaced on more than 10 occasions as a part of the spontaneous qualitative text box questions. The 10-response cut off was employed as a discretionary criterion.

Δ 18 out of the 55 responses were driven by an explicit need to protect others and or a strong sense of right and wrong, which is why it is meaningful to draw out "altruism" as a specific sub-component of Assertiveness. The calculated statistics do not distinguish "altruism" from "Assertiveness", instead they are performed on all 55 responses.

*Since these MINDSPACE factors were not revealed via our research that informed the survey questions a discretionary exclusion criterion was applied to them.

References

Ballreich, F.L., Volkamer, M., Mullman, D., Berens, B.M., Haussler, E.M., Renaud, K.V., 2023. Encouraging Organisational Information Security Incidents Reporting. Eur. Symp. Usable Secur. (Eur. 2023) 224–236. https://doi.org/10.1145/3617072.3617098

Baror, S.O., Ikuesan, R.A., & Venter, H.S. (2020). A defined digital forensic criteria for cybercrime reporting. In: International Conference on Cyber Warfare and Security (617-XVIII). Academic Conferences International Limited.

BBC (2019). Employee who fell for £200k email scam feared she would lose her home. BBC UK. Available at: 〈https://www.bbc.co.uk/news/uk-scotland-glasgow-west-50432294〉 [Accessed 18/04/2023].

Bidgoli, M., Grossklags, J., 2016. End user cybercrime reporting: what we know and what we can do to improve it. IEEE Int. Conf. Cyber Comput. Forensic (ICCCF) 1–6.

Bidgoli, M., Grossklags, J., 2017. Hello. This is the IRS calling".: a case study on scams, extortion, impersonation, and phone spoofing. Presented eCrime Res. Summit, eCrime, 57–69. https://doi.org/10.1109/ECRIME.2017.7945055

Braun, V., Clarke, V., 2021. One size fits all? What counts as quality practice in (reflexive) thematic analysis? Qual. Res. Psychol. *18* (3), 328–352.

Braun, V., Clarke, V., 2021. Conceptual and design thinking for thematic analysis. Qual. Psychol. *9* (1), 3–26. https://doi.org/10.1037/qup0000196

Breen, C., Herley, C., Redmiles, E.M., 2022. A large-scale measurement of cybercrime against individuals. Proc. 2022 CHI Conf. Hum. Factors Comput. Syst. 1–41.

Brooks-Hay, O., 2019. Doing the "Right thing"? Understanding why rape victim-survivors report to the police. Fem. Criminol. *15* (2), 174–195. https://doi.org/10.1177/1557085119859079

Buil-Gil, D., Trajtenberg, N., & Aebi, M.F. (in press, 2023). Measuring Cybercrime and Cyberdeviance in Surveys. In Routledge International Handbook of Online Deviance. Routledge.

Cheng, C., Chau, M.C.L., & Chan, M.L. (2018). A social psychological analysis of the phenomenon of underreporting cybercrimes and the concomitant underlying factors: Three real local case studies. Social Psychological Analysis. Official Guide to ICT Industry in Hong Kong. 〈https://www.cahk.hk/OfficialGuide2019/social-psychological-analysis.pdf〉.

Cobb, Stephen, 2020. Advancing accurate and objective cybercrime metrics. J. Natl. Secur. Law Policy *10* (3), 605–630.

Correia, S.G., 2019. Responding to victimisation in a digital world: a case study of fraud and computer misuse reported in Wales. Crime. Sci. *8* (4), 1–12. https://doi.org/10.1186/s40163-019-0099-7

Cross, C., 2020. Oh we can't actually do anything about that': the problematic nature of jurisdiction for online fraud victims. Criminol. Crim. Justice *20* (3), 358–375. https://doi.org/10.1177/1748895819835910

Cross, C., Grant-Smith, D., 2021. Recruitment fraud: increased opportunities for exploitation in times of uncertainty? Soc. Altern. *40* (4), 9–14.

Curtis, J., Oxburgh, G., 2022. Understanding cybercrime in 'real world' policing and law enforcement. Police J. *96* (4), 573–592. https://doi.org/10.1177/0032258X221107584

Delaney, J. (2023). University working with police and government after cyber attack. STV News. Glasgow & West. Available at: 〈https://news.stv.tv/west-central/university-of-west-of-scotland-working-with-police-and-government-after-cyber-attack〉 [Accessed 07/07/2023].

Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., 2012. Influencing Behaviour: the MINDSPACE way. J. Econ. Psychol. *33*, 264–277.

FBI (no date). Business E-mail Compromise. How can we help you. Scams and Safety. Available at: 〈https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise#Overview〉 [Accessed 28/06/2023].

Friend, C., Grieve, L.B., Kavanagh, J., Palace, M., 2020. Fighting cybercrime: a review of the irish experience. Int. J. Cyber Criminol. *14* (2), 383–399. https://doi.org/10.5281/zenodo.4766528

Garland, D., 2002. 103 Policy predicament: adaptation, denial, and acting out. In: Garland, D. (Ed.), The Culture of Control: Crime and Social Order in Contemporary Society. Oxford University Press, pp. 103–138. https://doi.org/10.1093/acprof:oso/9780199258024.003.0005

GOV (2023). 5. A safe and secure cyberspace – making the UK the safest place in the world to live and work online. UK Digital Strategy (2017). Available at: 〈https://www.gov.uk/government/publications/uk-digital-strategy/5-a-safe-and-secure-cyberspace-making-the-uk-the-safest-place-in-the-world-to-live-and-work-online〉 [Accessed 18/01/2024].

Graham, A., Kulig, T.C., Cullen, F.T., 2020. Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice. Polic. Int. J. *43* (1), 1–16. https://doi.org/10.1108/PIJPSM-07-2019-0115

Greenberg, A. (2023). The Mirai confessions: Three young hackers who built a web killing monster finally tell their story. WIRED. Available at: 〈https://www.wired.com/story/mirai-untold-story-three-young-hackers-web-killing-monster/〉 [Accessed 17/12/2023].

Horgan, S., Collier, B., 2016. Barriers to a Cyberaware Scotland. Scott. Justice Matters *4* (3), 19–20.

Hudson, M., Weinglass, S., Turner, M., & Gunter, J. (2023). On the hunt for the businessmen behind a billion-dollar scam. BBC Eye Investigations. Available at: 〈https://www.bbc.co.uk/news/world-65038949〉 [Accessed 12/04/2023].

Hunter, P., 2008. UK shadow home secretary victim of online card fraud. Comput. Fraud Secur. (*6*), 4. https://doi.org/10.1016/S1361-3723(08)70094-0

Hymas, C., & Butcher, B. (2023). Half of police forces not investigating crime properly. The Telegraph. Available at: 〈https://www.msn.com/en-gb/news/uknews/half-of-police-forces-not-investigating-crime-properly/ar-AA1marX3〉 [Accessed 01/01/2024].

Jayanetti, C. & Townsend, M. (2022). Revealed: half of English police forces fail to meet standards in crime investigations. The Guardian. Retrieved from: 〈https://www.theguardian.com/uk-news/2022/nov/26/revealed-half-of-english-police-forces-fail-to-meet-standards-in-investigations〉 [Accessed 19/01/2024].

Lord Justice Clerk, Lady Paton, & Lord Menzies (2015a). Malik Iqbal Against Her Majesty's Advocate. Scot Courts. Available at: 〈https://www.scotcourts.gov.uk/search-judgments/judgment?id=1c68e6a6-8980-69d2-b500-ff0000d74aa7〉 [Accessed 12/03/2023].

Kemp, S., Buil-Gil, D., Miró-Llinares, F., Lord, N., 2023. When do businesses report cybercrime? Findings from a UK study. Criminol. Crim. Justice 23 (3), 468–489. https://doi.org/10.1177/17488958211062359

Lawson, A., & Isaac, A. (2023). UK nuclear revelations: how bad could they get and could they affect the US and Europe? The Guardian. Nuclear Leaks. The Energy Industry. Available at: 〈https://www.theguardian.com/business/2023/dec/06/nuclear-leaks-uk-nuclear-site-sellafield-hacking〉 [Accessed: 07/12/2023].

Leukfeldt, E., Notte, R., Malsch, M., 2020. Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. Vict. Offenders *15* (1), 60–77. https://doi.org/10.1080/15564886.2019.1672229

Levi, M., Burrows, J., 2008. Measuring the impact of fraud in the UK: a conceptual and empirical journey. Br. J. Criminol. *48* (3), 293–318. https://doi.org/10.1093/bjc/azn001

Lingard, L., 2019. Beyond the default colon: Effective use of quotes in qualitative research. Perspect. Med. Educ. *8*, 360–364. https://doi.org/10.1007/s40037-019-00550-7

Loggen, J., Leukfeldt, E.R., 2022. Unravelling the crime scripts of phishing networks: an analysis of 45 court cases in the Netherlands. Trends Organ. Crime. *25* (6), 205–225. https://doi.org/10.1007/s12117-022-09448-z

Lord Summers (2019). OPINION OF LORD SUMMERS In the cause PEEBLES MEDIA GROUP LTD against PATRICIA REILLY. Scot Courts. Available at: ⟨https://www.scotcourts.gov.uk/docs/default-source/cos-general-docs/pdf-docs-for-opinions/2019csoh89.pdf?sfvrsn = 0⟩ [Accessed 18/04/2023].

Lord Justice Clerk, Lord Brodie, & Lord Drummond Young (2015b). Appeal Against Conviction By Ian Geddes Against Her Majesty's Advocate. Scot Courts. Available at: ⟨https://www.scotcourts.gov.uk/search-judgments/judgment?id = 5db2c7a6-8980-69d2-b500-ff0000d74aa7⟩ [Accessed 12/03/2023].

Lord Justice General, Lord Menzies, & Lord Turnbull (2020). Opinion of the Court delivered by Lord Turnbull in a Scottish Criminal Case Review Referral in Appeal Against Sentence by Mark Conway Against Her Majesty's Advocate. Scot Courts. Available at: ⟨https://www.scotcourts.gov.uk/docs/default-source/cos-general-docs/pdf-docs-for-opinions/2020hcjac48.pdf?sfvrsn = 0⟩ [Accessed 12/03/2023].

Lord Menzies and Lord Turnbull (2018). Opinion of the Court delivered by Lord Menzies in Appeal Against Sentence by Rameez Hamid Against Her Majesty's Advocate. Scot Courts. Available at: ⟨https://www.scotcourts.gov.uk/docs/default-source/default-document-library/2019hcjac16.pdf?sfvrsn = 0⟩ [Accessed 12/03/2023].

Lyon, A. (2023). Police issue warning over new mobile phone provider scam. Clydebank post. News. Crime. Available at: ⟨https://www.clydebankpost.co.uk/news/23622148.police-issue-warning-new-mobile-phone-provider-scam/⟩ [Accessed 30/06/2023].

MacDonald, K. (2019). Action Fraud (No. V3-A0718). SPC, Tulliallan.

Maltz, M.D., 1977. Crime statistics: a historical perspective. Crime. Delinquency *23* (1), 32–40. https://doi.org/10.1177/001112877702300103

Martin, P. (2024). Insider risk and personnel security: An introduction. Routledge. 4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN.

McMurdie, C., 2016. The cybercrime landscape and our policing response. J. Cyber Policy *1*, 85–93. https://doi.org/10.1080/23738871.2016.1168607

NCSC (2020). Whaling: How it works, and what your organisation can do about it. Guidance. Available at: ⟨https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it⟩ [Accessed 28/06/2023].

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]. Mail on Sunday 1. Available at: ⟨https://www.pressreader.com/uk/the-scottish-mail-on-sunday/20230122/281496460407154⟩ [Accessed 05/04/2023].

Lady Paton, Lady Clark of Calton, & Lord Clarke (2014). Petr Kupka + Michal Rondos v. Her Majesty's Advocate. Scot Courts. Available at: ⟨https://www.scotcourts.gov.uk/search-judgments/judgment?id = a2af8aa6-8980-69d2-b500-ff0000d74aa7⟩.

Pfeffer, J. (1998). The Human Equation: Building Profits By Putting People First. Boston, MA: Harvard Business School Press.

Popham, J., McCluskey, M., Ouellet, M., Gallupe, O., 2020. Exploring police-reported cybercrime in Canada: Variation and correlates. Polic. Int. J. *43* (1), 35–48.

Protrka, N., 2021. Cybercrime. Roycroft, Mark, Brine, Lindsey (Eds.), Mod. Police Leadersh.: Oper. Eff. Every Lev. 143–155. https://doi.org/10.1007/978-3-030-63930-3_13

Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., Orgeron, C., 2018. Is the responsibilization of the cyber security risk reasonable and judicious? Comput. Secur. *78*, 198–211. https://doi.org/10.1016/j.cose.2018.06.006

Renaud, K., Musarurwa, A., & and Zimmermann, V. (2021b) Contemplating blame in cyber security. 16th International Conference on Cyber Warfare and Security. 23rd-24th November 2021. Islamabad, Pakistan.

Renaud, K., Searle, R., Dupuis, M., 2021a. Shame in cyber security: effective behavior modification tool or counterproductive foil? (New Hampshire). N. Secur. Paradig. Workshop 70–87. https://doi.org/10.1145/3498891.3498896

Ritchie, J., & Lewis, J. (2003). Qualitative research practice: A guide for social science students and researchers. SAGE Publications Ltd. London.

Scottish Government (2022a). Recorded Crime in Scotland, 2021-2022. Publication-Statistics. Available at: ⟨https://www.gov.scot/publications/recorded-crime-scotland-2021-2022/pages/15/⟩ [Accessed 28/06/2023].

Scottish Government (2022b). Scottish Crime and Justice Survey 2021/22: Main findings. Publication- Law and Order. Available at: ⟨https://www.gov.scot/publications/scottish-crime-justice-survey-2021-22-main-findings/pages/12/⟩ [Accessed 30/11/2023].

Scully, M. (2022). EXCLUSIVE: Brothers make millions using webcam girls to sell "sob" stories to desperate men. Mirror. Available at: ⟨https://www.mirror.co.uk/news/uk-news/brothers-make-millions-using-webcam-26508739⟩ [Accessed 17/04/2023].

Sikra, J., Renaud, K.V., Thomas, D.R., 2023. UK cybercrime, victims and reporting: a systematic review. Commonw. Cyber J. *1* (1), 28–59.

Stewart, S. (2022). Experts fear Kremlin cyber attacks: Security analysts warn of imminent assaults by Russian hacker gangs. Sunday Post 17. Available at: ⟨https://www.sundaypost.com/fp/experts-fear-kremlin-cyber-attacks/⟩ [Accessed 17/04/2023].

Sweeney, M. (2023). Royal Mail resumes overseas deliveries via post offices after cyber-attack. The Guardian. Available at: ⟨https://www.theguardian.com/business/2023/feb/21/royal-mail-international-deliveries-cyber-attack-ransom-strikes⟩. [Accessed 16/04/2023].

Tims, A. (2022). Online fraud: victim blaming and the emotional price of falling for a scam. The Guardian. Retrieved from: ⟨https://www.theguardian.com/money/2022/feb/20/online-victim-blaming-and-the-emotional-price-of-falling-for-a-scam⟩.

Travis, A. (2017). Simple numbers tell story of police cuts under Theresa May. The Guardian. Retrieved from: ⟨https://www.theguardian.com/uk-news/2017/jun/05/theresa-may-police-cuts-margaret-thatcher-budgets⟩.

Van der Bruggen, & Grubb, A, 2014. A review of the literature relating to rape victim blaming: An analysis of the impact of observer and victim characteristics on attribution of blame in rape cases. Aggress. Violent Behav. *19* (5), 523–531. https://doi.org/10.1016/j.avb.2014.07.008

Wanamaker, K.A. (2019). Profile of Canadian businesses who report cybercrime to police. The 2017 Canadian Survey of Cyber Security and Cybercrime. ⟨https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2019-r006/index-en.aspx⟩.

Whitty, M.T., Buchanan, T., 2012. The online romance scam: a serious cybercrime. Cyber Psychol. Behav. Soc. Netw. *15*, 181–183. https://doi.org/10.1089/cyber.2011.0352