

The Role of Responsibilised Non-Policing Agencies (RNPAs) in Facilitating Italian and Scottish Cybercrime Reporting

Juraj Sikra^{1,2}[0000–0003–4557–1256]
Karen V. Renaud^{2,3,4,5}[0000–0002–7187–6531]
Daniel R. Thomas²[0000–0001–8936–0683]

¹ Karlsruhe Institute of Technology (KIT)

² University of Strathclyde

³ Rhodes University (Department of Information Systems)

⁴ University of South Africa (School of Computing)

⁵ Abertay University (Division of Cybersecurity)

{juraj.sikra,karen.renaud,d.thomas}@strath.ac.uk

Abstract. Cybercrime responsabilisation denotes a state’s delegation of responsibility for navigating the aftermath of cybercrimes onto victims and private and third sector organisations: **Responsibilised Non-Policing Agencies (RNPAs)**. We explored the current role of RNPAs to elicit their views on how reporting incidence can be improved. We also compared the experiences of RNPAs in countries with different implementations of responsabilisation: Scotland (state cyber responsabilizes but provides some assistance) and Italy (state cyber responsabilizes and provides no assistance). We augmented the interview findings by surveying cybercrime victims to gain additional insights. The RNPAs in both countries believed that awareness-raising would improve reporting of incidence. This seems naïve, especially when known reporting barriers are not simultaneously addressed and dismantled. We conclude by highlighting the need for a more holistic approach to improve reporting incidence.

Keywords: Cybercrime, Reporting, Responsibilisation, Scotland, Italy

1 Introduction

Cybercrime causes major harm to individuals, businesses and public institutions worldwide. The economic costs of cybercrime can reach up to 10.29 trillion dollars in repair costs [32].

According to the United Kingdom (UK)’s National Crime Agency (NCA), cybercrime is a significant issue. It is estimated that up to 1 million cyber-dependent crimes (e.g., phishing) and cyber-enabled crimes (i.e., fraud) were committed in 2019 in England and Wales [18, p.47]. Cyber-dependent crimes are those that can only be committed using Information and Communication Technology (ICT) [6]. Cyber-enabled crimes are those that: “*do not depend on*

computers or networks but have been transformed in scale or form by the use of the internet and communications technology [6].”

Cybercrimes are often under-reported [28]. This under-reporting could be explained by a lack of faith in police [28]. Moreover, up to 80% of ransomware victims choose to pay the criminals [29,36], thereby removing the need to report to the police. This suggests another possible explanation, relatively unexplored at this time: the possibility that cyber responsabilisation might act as a barrier to crime reporting to authorities in countries with neoliberal governments. *Responsibilisation* is the shifting of responsibility for crime control from the state onto citizens [11]. With responsabilisation, the state mainly provides self-protection advice, but provides little support if citizens fall victim.

A widely-applied cyber responsabilisation strategy might, perhaps unwittingly, dissuade victims from reporting to the crime-fighting arm of the very government who has assigned responsibility to the victim. The victim may feel that they have fallen victim because they have failed to act upon their assigned responsibilities. The logical conclusion would be that reporting would be futile. Even so, some kinds of cybercrime might almost force victims to report, perhaps if the person needs to reclaim lost funds, for example.

If victims do not feel able to report to state authorities, but still want to resolve their victimhood, this creates a new set of unmet needs which will probably be satisfied by other organizations: we refer to these organizations as *Responsibilised Non-Policing Agencies (RNPAs)* [11,25]. RNPAs are unlikely to be in a position to meet cybercrime reporting needs as comprehensively as possible, and the choice of this venue means that the authorities do not gain a comprehensive and accurate view of the extent of online cybercrime victimization. It is clear that this phenomenon, and the nature of the role of RNPAs, and what it should be, ought to be investigated. Figure 1 outlines the structure of this paper.

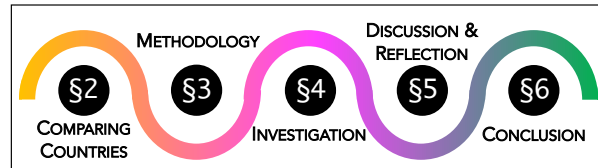


Fig. 1: Paper Structure

We used qualitative and quantitative methodologies to explore the research question: ***What is the nature of RNPAs’ role with respect to cybercrime reporting?***

(1) Interviews with RNPAs to answer the following sub-questions:

RQ1a *What are RNPAs currently doing in terms of cybercrime reporting?*

RQ1b *Is there a difference between the role of RNPAs in cybercrime reporting depending on responsabilisation implementation strategy?*

RQ1c *How do RNPAs think reporting incidence can be improved?*

(2) Survey with actual cybercrime victims to answer the following sub-question:

RQ2 *Who do victims prefer to report cybercrimes when they are victimised?*

2 Comparing Countries

It is helpful to compare two responsibilised countries to examine cybercrime reporting. This is especially useful if the countries being compared have different responsibilisation implementations. This allows us to observe the impact of responsibilisation on cybercrime reporting.

UK citizens are cyber responsibilised [22]. Here, we focus only on Scotland because Scotland has withdrawn from Action Fraud, the UK’s centralized cybercrime reporting mechanism [7,13]⁶. This has left Scottish victims without an obvious place to report cyber crimes. This might make reporting to RNPAs more likely. Scotland was chosen as the first country to support comparison.

For the second country, we needed a country that would be comparable with Scotland in terms of its neo-liberal responsibilisation strategies, but also sufficiently different in other aspects to allow us to study the impact of responsibilisation on cybercrime reporting. We chose Italy because it offers a meaningful point of comparison due to similarities and diplomatic links between the two countries. Most importantly: **(1)** because Scotland and Italy while both responsibilising their citizens, do so in different ways, and **(2)** neither country has a centralised reporting system, which will manifest as people reporting across different reporting gateways.

We now discuss some differences, similarities and links between the two countries.

2.1 Diplomatic links between Scotland and Italy

An agreement was reached in Rome to enhance the bilateral collaboration between the two countries in various areas such as trade and traditional crime control. Hence, this research is of critical importance because it augments the “*the deep friendship between our countries* [30].” Nevertheless, this agreement does not mention cybersecurity and cybercrime, which is why this research is an important extension of the existing relationship between the UK (inc. Scotland) and Italy.

Italy is one of the UK’s (inc. Scotland’s) closest research allies [10]. Italian staff make up one of the largest UK research communities, which supports collaboration with the Italian research sector [10].

⁶ Action Fraud was deemed too expensive, i.e., £459 324 per annum [16] and did not facilitate a tailored assessment of victims’ vulnerability. A vulnerability assessment is possible if victims report via the non-emergency 101 number [16].

2.2 Similarities

No Centralised Reporting System. Both countries lack a centralised reporting mechanism such as Action Fraud. Therefore, Italians have to report cybercrime directly to the police or to RNPAs.

Outsourcing Cybercrime Responsibilities. Scotland outsources some of its crime-control responsibilities [37]. This is typical of a responsabilisation strategy preferred by these governments. Michel Foucault links this to the notion of governmentality, which denotes the process by which the state extends its influence by connecting itself: *“to a diversity of forces and groups that in different ways had long tried to shape and administer the lives of individuals in pursuit of various goals [25, p.87].”*

2.3 Differences

Trust. A recent survey found that, in Scotland, less than a half of respondents had a lot of confidence in the police [33]. Italians, on the other hand, have higher levels of confidence in the police [31].

Cybercrime Recording. In Italy, various cybercriminal offences are captured in written and nuanced ways in the Italian court systems [17]⁷, which can support victims to feel visible. To the contrary, in Scotland, the search function on the written judgements of Scots courts connects “cybercrime” with crimes of sexual abuse. Consequently, victims of non-sexual cybercrimes are less visible to the court system, which can increase their sense of isolation and responsibility for their ordeal [28].

Cybercrime Responsibilisation Implementation in Scotland and Italy. We conceptualise a responsabilised society as one that is defined by four factors (see: Figure 2). These factors interact and demonstrate co-dependence. For example, high levels of citizen responsibility will produce high levels of trust in business, as both have learned to rely on themselves, as opposed to relying on the state’s apparatus.

In our research, we were keen to identify the relationship between the responsabilisation strategy applied in Italy vs. that chosen by Scotland, given that we did not find any studies which had already delineated the differences.

These are not exhaustive themes by which responsabilisation can be illustrated. Instead, they serve an explanatory purpose. We used the themes as keywords to conduct research online for information that would support an effective

⁷ A bilingual (It + En) summary of average judgements, which encompasses both convictions (i.e., *sentenze/decreti di condanna*) and plea bargains (i.e., *patteggiamenti*) per year in Italy from 2017-2021 for various non-sexual cybercrimes is available upon request. This is a useful resource for cybercrime research as it showcases the granulated approach of the Italian legal system towards cybercrime.

comparison of responsabilisation strategy implementation in Italy and Scotland.

Factor 1. is closely connected to the subject of this research and examines the use of RNPAs in the two countries. **Factors 2. & 3.** pertain to trust in government and the police respectively. These factors were purposively selected as both are useful for illustrating the effects of responsabilisation on public trust. Lastly, **Factor 4.** which is about trust in business, was selected because responsabilisation predicts a prominent role for the private sector. Taken together, these factors are useful for purposively describing responsabilisation in Italy and Scotland.

1. High Responsibility for Responsibilised Non-Policing Agencies (RNPAs). In *Italy*, according to an Italian cyber-expert from Sant’Anna School of Advanced Studies (Pisa), Dr. G. Fiorinelli⁸:

“there is no general state-funded legal aid system that provides basic legal advice universally. Subject to income-based eligibility, the State can cover legal fees (“patrocinio a spese dello Stato”), but only when a client formally engages a lawyer. Free legal advice can otherwise be provided by local, voluntary, or pro bono initiatives, or through some non-profit organizations or university legal clinics, which usually specialize on specific areas (such as immigration law, labor law).”

In *Scotland*, the Scottish state responsabilizes the non-state multi-agency approach to support victims of cybercrime. For example, the state does this by funding RNPAs to impart legal advice. These agencies consist of charities, which are partially state-funded, and companies that substitute the police [26].

2. Low Trust in Government. In *Italy*, 40% Italians trust their government, which is a 2% decrease from 2024⁹. This qualifies as distrust in the government [9]. In *Scotland*, 37% of UK citizens (inc. Scotland) trust their government, which is a 7% increase from 2024. This still qualifies as distrust in the government [9].

3. Varied Trust in Police. In *Italy*, citizens have elevated levels of trust in the police [15] potentially prioritizing it over the judiciary, which could reflect right-wing policies [1]. In fact, in 2024, 63.5% Italians declared that they have trust in the State Police [31]. This is not characteristic of neo-liberal societies, where a *“lack of faith in police”* is expected. In *Scotland*, it was found that Scots *“lack faith”*[28] in police, which is likely to increase reporting to RNPAs. In fact, during 2017/2018, only 45% of respondents said that they *“have a lot of confidence in the police”* [33]. Moreover, the trust of Scottish citizens in the judiciary has steadily declined from 2019-2025 [40]. This is characteristic of neo-liberal

⁸ Received by the article’s authors in writing on 24 June 2025.

⁹ According to the 2025 Edelman Trust Barometer, if between 1-49% respondents trust the government, then this is rated as distrust, when 50-59% respondents trust the government, then this is rated as neutral and when 60-100% respondents trust the government, then this is rated as trust [9]. This metric extends to all trust measures in the ETB, including business (p. 41).

societies, where the public feels responsible for their own safety and mistrusts the state.

4. High Trust in Business. In *Italy*, 56% of Italians trust business, which is a 1% decrease from 2024. This qualifies as neutral. This is characteristic of neo-liberal responsibilised societies, where citizens associate the private sector with high credibility vs. the public sector [9]. In *Scotland*, 51% of UK (inc. Scotland) citizens trust business, which is a 3% increase from 2024. This is characteristic of neo-liberal responsibilised societies, where citizens associate the private sector with high credibility vs. the public sector. Nevertheless, this still qualifies as a neutral level of trust.

Figure 3 summarises this section. We now report on an empirical study on RNPAs in Italy and Scotland.

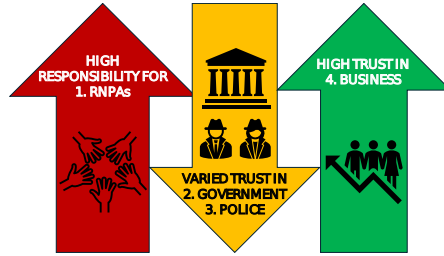


Fig. 2: 4-Factor Model of responsibilisation referencing the four factors

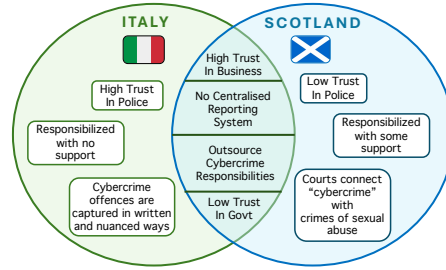


Fig. 3: Summary

3 Methodology

This section outlines the research methodology commencing with the research paradigm followed by the research framework. Subsequently, the empirical and qualitative methods used in this study are presented, supplying information on the design, recruiting of participants, and data analysis¹⁰.

Research Paradigm. The current study addresses a complex problem from multiple angles and engages various quantitative and qualitative approaches in a flexible way. Consequently, this approach corresponds tightly to the pragmatic paradigm [20]. The pragmatic paradigm postulates that reality is fluid and impacted by experiences (i.e., ontology). This presupposition is evident from the research because it is the participants' own words that assume the dominant role in answering the research question. Furthermore, the pragmatic paradigm

¹⁰ The full list of interview questions for the Scottish and Italian RNPAs is available in the Appendix

instructs that knowledge is evaluated based on its utility and the results it brings forward (i.e., epistemology). Lastly, the pragmatic paradigm is a value-based construct because it aspires to solve real-world problems (i.e., axiology). Take, for instance, responsabilisation, which is a value-based socialist concept that underlines much of the reasoning within.

Research Framework. As already noted, the research framework within is that of “responsibilisation,” which denotes the retraction of the state from the area of crime control in favour of solutions produced by the citizens themselves alongside private and charity sector organizations [11]. In fact, the purpose of this work is to investigate these private and charity sector organizations as stand-alone entities involved in cybercrime reporting. This work refers to these organizations as Responsibilised Non-Policing Agencies (RNPAs).

Interviews. were carried out in two locations: Scotland (11 Scottish RNPAs) and Italy (4 RNPAs - Italian lawyers)¹¹. There were more interviewees than there were RNPAs as some RNPAs (i.e, RNPA- University and RNPA- Regulators of commerce) supplied multiple interviewees.

Scottish RNPAs The interviewing process was based on person-centred values and approaches from the field of mental health. The interviews lasted around 20-45 minutes. They have taken place via the Zoom or Microsoft Teams online communication tools and participants could have their cameras turned off if they so wished. The transcription was done manually by the first author.

Italian RNPAs - lawyers Participants answered the questions in writing as they were not comfortable with live interviews. The questions were distributed as Microsoft word documents by an Italian collaborator with a doctorate in a relevant field. Our collaborator also translated these into English, which enabled further analysis.

Survey. When constructing the simple survey, we ensured face validity by formulating the questions in a way that was easily relatable, content validity was ensured by sampling representative information of the underlying research questions and reliability was ensured by articulating questions that resulted in people’s consistent responses (i.e., all respondents answered in the same way) [35].

Scottish Survey. We surveyed 407 Scottish participants¹² via Prolific closely following the methodology of previous research [28] which included an attention test as a part of the survey to ensure valid participant responses. Moreover, in correspondence to the approach, we have reimbursed participants £10.42 per hour, which would have amounted to £2.00 per survey. Of these participants, 27 were excluded for failing the attention test. Our final sample contained 203 females, 177 males, 6 non-binary/ third gender and 1 that preferred not to say.

¹¹ The Scottish and Italian interviews were approved by the authors’ primary university’s departmental ethics committee and granted the ID 2090.

¹² The Scottish victims’ study was approved by the authors’ primary university’s departmental ethics committee and granted the ID 2570.

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.

This study is concerned with analysing the data of 151 participants that filed a report and detailed the reporting gateway. We organized participants' responses to the question: "*Who did you report cybercrime to?*" into Table 1. We organized participants' responses to the question: "*Why did you report the cybercrime?*" in Section §4.4.

Italian Survey. We surveyed 425 Italian participants via Prolific¹³. Of these participants, 25 were excluded for failing the attention test. Our final sample contained 157 females, 234 males, 8 non-binary/ third gender and 1 that preferred not to say. These participants were surveyed across age ranges. Subsequently, in the range 18-30 (106 males, 103 females, 8 non-binary/ third gender, prefer not to say 1), 31-40 (72 males, 25 females, 0 non-binary/ third gender), 41-50 (40 males, 17 females, 0 non-binary/ third gender), 51-60 (14 males, 8 females, 0 non-binary/ third gender), Over 60 (2 males, 4 females). Of these participants, 264 did not report cybercrime and 136 participants did. We did not test for gender effects as this was not included in our research questions or ethics approval application in the interests of data minimisation.

This study is concerned with analysing the data of 136 participants that filed a report and detailed the reporting gateway. We organized participants' responses to the question: "*Who did you report cybercrime to?*" into Table 1. We organized participants' responses to the question: "*Why did you report the cybercrime?*" in Section §4.4.

3.1 Participant Recruitment

Interviews. In the terminology of previous research [3], the principles underlying our participant selection align with both "convenience" and "purposive" sampling approaches (p.14). The former involves recruiting easily recruitable participants and the latter involves recruiting participants with a specific profile. We purposively recruited organizations whose representatives accept reports of cybercrime, which they use to build up an informational and statistical picture of the effects of cybercrime upon citizens. Nevertheless, they do not investigate crimes.

In terms of demographics, we only collected gender and not other information to ensure GDPR data minimization. 9 males and 6 females representing different RNPAs were involved, of which 3 females and 1 male were Italian (all

¹³ This study was approved by the authors' primary university's departmental ethics committee and granted the ID 2700.

private lawyers). The interviewed participants varied in terms of educational attainment, social class, and nationality. Selected quotes that follow are supplied to provide insight into the participants’ connection to cybercrime reporting. Due to the small number of interviewees, it would be inappropriate to report age ranges.

Survey. Participants were recruited via the Prolific crowd working platform and paid £2.00 for their time during the survey, which lasted around 10 minutes. This payment exceeded the UK’s living wage of £10.42 per hour at the time. The participants read a brief advert on the Prolific platform, which informed them about the study’s aims. The advert merely stated that: *“In this study we are exploring the factors that are influential in decisions to report cybercrimes. We are looking for people who have been a victim of cybercrime in the past to complete this survey.”* As per Section §3, we recruited 407 Scottish and 425 Italian cybercrime victims.

3.2 Analysis

Interviews. We analysed the data with NVivo 1.3 using the rationale for small sample sizes [23] and methodology that fits closely with: *coding reliability thematic analysis (TA)*, which is an approach where themes are: *“often deductive in orientation, in the sense that themes are developed early on in, or even prior to, analysis.”* [3, p. 333].

In line with qualitative theorizing, our themes are best understood as summaries of topics, in connection with what improves and/or impedes reporting [3]. Firstly, the 15 interview files were classified according to the nationality of the RNPA. Thus, two file classifications were created: 01. Scottish RNPAs, 02. Italian RNPAs. Secondly, the file classifications were each coded to extract themes for what improves cybercrime reporting whilst responsabilisation was not separately coded but extracted from the data by way of immersive qualitative analysis [24].

Survey. We analysed the data from the surveys by extracting it from the Excel spreadsheets via the filter function, which supplied us with information about “Reporting Gateway” of Italian and Scottish cybercrime victims as depicted in Table . Our data suggest that both Italy and Scotland outsource its cybercrime responsibilities from organisations such as banks, which is a similarity (see: Section §2.2). However, as can be seen from Table 1, the Scots are nearly 6 times more likely to report cybercrime to their bank than their Italian counterparts.

4 Investigation

4.1 RQ1a: What are RNPAs doing in terms of cybercrime reporting?

In both Italy and Scotland, RNPAs are collecting information about cybercrime on behalf of the state and contributing to the mitigation of cybercrime harm. In

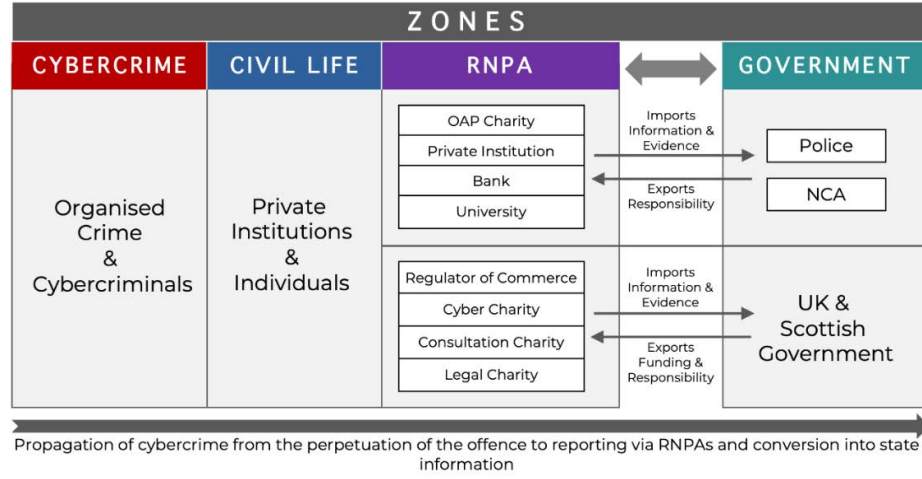


Fig. 4: Propagation of cybercrime via RNPAs

particular, RNPAs - Banks reimburse lost funds in both countries, which is why victims approach them. An important finding from this research is the following: the difference between the two countries is that in Scotland, RNPAs are far more embedded in the cybercrime reporting arena which is why they are able to provide a lot more support. RNPAs - Charities give support to victims by signposting them to the police, imparting education and a degree of aftercare. These charities also pass cybercrime information to the state, which in return awards them with funding. Italy does not have the equivalent of RNPAs - Charities in the cybercrime reporting domain. This is why the following passage will visually answer the research question by using Scotland as an example.

Figure 4 visualises what RNPAs are doing when cybercrime is propagated via the responsibilised environment in Scotland. Figure 4 was derived from the qualitative interviews that were analysed in Section §4.3.

The figure is not exhaustive, as any number of agencies can be RNPAs (including places of worship, for example). Nevertheless, it does offer an effective illustration of how selected RNPAs operate. Moving from left to right, cybercrime originates in the cybercrime zone, where organized crime and cybercriminals reside. Using frameworks from past research, we consider attacked victims as being either private institutions or individuals [27]. Naturally, cybercriminals also attack public institutions, but these do not form a part of the argument concerning RNPAs because these are, by definition, a part of government and hence receive automatic multi-agency support post-attack [27].

After cybercrime is perpetuated in the cybercrime zone, it propagates into the civil life zone, where it impacts private institutions and individuals, who may or may not report the incident to other organizations, including the police. In line with the prediction of Garland (2002), some victims will report to private

institutions and community organizations, which are referred to as RNPAs and depicted in Figure 4.

Hence, victims will submit their reports via the RNPAs zone, which houses various RNPAs. RNPAs respond to the victims by offering advice on how to resolve their situation and encouraging them to report cybercrime to the police. Under certain circumstances, RNPAs, which are banks, will reimburse victims for money lost. As a rule of thumb, RNPAs will impart some form of post-victimization education and care whilst compiling the details of cybercrime as a part of their own information picture. The imparting of education is a fixture of neoliberal policies [21] and this principle extends to the activities of the RNPAs.

As shown in Figure 4, a dividing line splits the RNPA and government zones. After the RNPAs have compiled the victims' data into an information picture, they then pass this to the authorities, which is where the dividing line becomes significant.

RNPAs that sit above the black dividing line (private institutions, bank, and universities, but not OAP charity) report to the police and the NCA. Specifically, the private institution, which is a first responder post-attack, reports to the police via informal channels in a way that passes on information about cybercrime trends but does not identify the clients - victims. The banks pass on reports of cybercrime to the police so that cybercriminals do not put them into a position where they run the risk of fund reimbursement towards harmed clients. However, the police often do not have the resources to pursue investigations based on the evidence supplied. The university reports to the NCA in cases where it suspects that money laundering is occurring. The OAP charity, which supports the elderly, does not report to anybody but instead advises its clients to report to the police. This is a missed opportunity, because said RNPA could help to deliver insights into the cyber-victimization of a vulnerable population [19].

RNPAs that sit below the dividing line (regulators of commerce, cyber charity, consultation charity, and legal charity) report to the Scottish government directly although some also cooperate with the police to a lesser degree. Specifically, the regulator of commerce reports to the UK government because that is where it receives its funding from. The remaining RNPAs report to the Scottish government for the same reason. All these charities, apart from the cyber charity, have taken up cybercrime reporting over and above their mission, which is cyber unrelated, usually via a combination of pressing societal need and available government tenders. The cyber charity is the only organization founded by the government to help people and SMEs attacked by cybercrime by imparting education and accepting reports of cybercrime.

As we have demonstrated, by the time cybercrime moves from the RNPA zone into the government zone, it has been repackaged as information about current trends. The state, along with its subsidiaries, the police and NCA, imports this information and exports funding to all RNPAs apart from RNPAs that are banks and private institutions.

4.2 RQ1b: Impact of responsabilisation implementation strategy

RNPAs in both Italy and Scotland serve the same role, but they differ in terms of their level of involvement with the victims. The role of RNPAs in both countries is to substitute the state in cybercrime reporting. In this domain, RNPAs - Banks play a leading role in both countries. Italians and Scots report to RNPAs - Banks to get fund reimbursement.

However, as already mentioned in Section §3.2, Scots are 6 times more likely to report to RNPAs - Banks. In fact, in total Scots prefer to report to the RNPAs before the police because of the high level of involvement RNPAs have in this arena.

On the contrary, Italians are much more active in reporting to the police (see: Table 1). Therefore, the key difference between the countries is not in the role of the RNPAs, but in the role of the police. In Scotland, victims approach the police mainly to get a crime incident number, which the RNPA - Bank requires for fund reimbursement [28]. In Italy victims report the cybercrime across multiple forces out of principle and because there is a lack of RNPAs with a victim support role.

4.3 RQ1c: How do RNPAs think reporting can be improved?

A selection of quotes from the interviews with RNPAs' answers this question.

Scottish RNPA Quotes This section reports the findings from the analysis of the qualitative interviews ¹⁴. Overall, the quotes lend further credibility for using RNPAs to improve cybercrime reporting. The interviewees were asked: “What else is required to improve reporting?”

“I think it’s about making sure the public are aware of what scams look like and aware of what not to do and what to do when they notice something that’s not as it should be, or you know it seems suspicious. So, I think it’s more about education. Education of what scams are, what they look like and especially current trends.” – RNPA OAP Charity, P6 (male)

“The ability to provide the information straight to somebody I knew was actually going to use it. So, the [cybercrime] example I gave earlier, I typed that out and send that as an e-mail, I don’t know whether that went into the Scottish intelligence database or anything like that.” – RNPA Private institution, P5 (male)

¹⁴ The responses that corresponded most to what is required to improve cybercrime reporting were chosen. In cases, where there were multiple interviewees in a single RNPA (e.g., RNPA Regulators of commerce contained responses from 2 males and 1 female), only a single most relevant quotation from one of the participants was included.

“I think it would be great if it was automated, so I think the difficulty is the sheer volume of information that’s being passed on to criminal investigations and the Police just means that the Police are swamped, they have way too much to do and they can’t easily match cases together because they don’t have the capability to do so.” – RNPA Bank, P7 (male)

“I think perhaps better knowledge sharing across organisations. There’s quite a good knowledge sharing across universities but actually as I said in the beginning we are almost as I said in certain aspects the activities, we do are like quite a large company.” – RNPA University, P1 (female)

“(...) it’s common for us to receive reports of cybercrime on behalf of victims and that typically relates to the elderly or people with specific vulnerabilities (...). And there are certain sections of society that are reluctant to report probably because they’re feeling embarrassed for falling victim and I think we need to work to remove that stigma so that people feel more comfortable coming forward and don’t feel that because they’ve fallen victim of a scam, they’re somehow not representative of their cross-section of society.” – RNPA Regulators of commerce, P4 (female)

“I think there should be some easy way of reporting it even if it’s just a simple form on a website that allows you to just fill it in and if you’re aware that it’s not going to be dealt with quickly, it’s not going to be an immediate call, if I want to report something that happened a couple of days ago, then why not just fill a form and then that’s it? Or why not get a Police Scotland App?” – RNPA Cyber charity, P2 (male)

“I think greater consumer awareness of what constitutes cybercrime and that comes with educating people about what cybercrime is and what signs to look out for. (...) I think one of the most interesting things I’ve noticed in the last couple of years is scams and cybercrimes constantly mutate in order to avoid detection and in order to target people.” – RNPA Consulting charity, P3 (male)

“(...) we lost Action Fraud, which can only now be contacted if you’re in England and they now don’t take any reporting from Scotland. It’s only Police Scotland that take that. I think the reinstalment of that organization because there isn’t a single organization that does just fraud.” – RNPA Legal charity, P8 (male)

Italian RNPA Quotes This section displays the evidence from the qualitative interviews with Italian private lawyers. This outcome can be used as advice for government, but also the private and non-governmental sectors to formulate policy and technical solutions to address cybercrime under-reporting. The responses that corresponded most to what is required to improve cybercrime reporting were chosen over others. The interviewees were asked: “What else is required to improve reporting?”

“(. . .) greater visibility of risks related to the use of technologies and an increase in educational activities with respect to these risks would be necessary. In terms of reporting cybercrimes, it would be useful to link the previous educational intervention with more extensive information on the ways/times and tools for reporting. Possibly set up a hybrid reporting tool such as to allow, if required, the possibility of an in-person contact with the operators to clarify the consequences and procedures of reporting.” – P1 (female)

“(. . .) the online platform for reporting cybercrimes is temporarily suspended as the infrastructure is being re-engineered. The hope is that the online reporting system will be improved to achieve a simpler submission of relevant information and a faster response capacity of the postal police.” – P2 (female)

“Firstly, more information should be provided to people, especially those who are less familiar with computer systems, so that they are also more familiar with the Internet and the traps associated with it (e.g., phishing and the possibility of recognizing fake e-mails at first sight). On the other hand, greater availability of the police would also be desirable. In the city where I live, the Postal Police, the office responsible for receiving such complaints, is only open two mornings a week.” – P3 (female)

4.4 RQ2: Who do victims prefer to report cybercrimes?

We provide a selection of quoted evidence from the victims who were also asked *why they reported cybercrime*¹⁵ There were 151 Scottish and 136 Italian victims of cybercrime included in the surveys.

Scottish Victims’ Quotes

“Because it was necessary to report it to my bank in order to retrieve the money that was taken from my account through a fraudulent payment link for a false online shopping URL. I would’ve liked to have reported it to the police but would’ve found the process stressful and this would have been for statistical purposes only, since the bank was able to resolve the situation.” – Victim that reported to RNPA– Bank

“To hopefully catch the hacker and to avoid anyone else connected to myself falling victim.” – Victim that reported to RNPA– Commercial website and social media

“I didn’t want anyone else to suffer. We need to support each other against cybercrime. It could happen to anyone.” – Victim that reported to the Police

¹⁵ We have chosen quotations to effectively illustrate the attitudes and motivations that underlay the quantitative data from Table 1.

These quotes confirm that Scots prefer to report cybercrime to RNPAs [26] rather than to the Police [33].

Italian Victims’ Quotes These quotes show that Italians prefer to report cybercrime to the Police [15,31].

“To not lose money and to not have any other problems that could come with such attack.” – Victim that reported to RNPA– Bank

“Because hacking my Meta Facebook profile included sensitive data like my E-Mail, phone number, personal information and pictures.” – Victim that reported to RNPA– Commercial website and social media

“I reported everything because I wanted to be helped, I wanted to be compensated for the theft of money. I wanted to be protected, so that other crimes no longer happen to me or other people.” – Victim that reported to the Police

5 Discussion & Reflection: What is the nature of RNPAs’ role with respect to cybercrime reporting?

RQ1a: It is clear that Scottish RNPA’s are indeed accepting cybercrime reports and dealing with the victims as best they can. It is not clear that these reports are always relayed to the police forces, which impairs their ability to assess the cybercrime footprint across Scotland. Italian victims usually reported to police, so that their police forces are likely to be much more well informed.

RQ1b: Our empirical results support the literature review from Section §2, which identified that there is a high level of responsabilisation towards victims and RNPAs, a low level of trust in police in Scotland (but not Italy), a low level of trust in government and a high level of trust in business. This means that RNPAs and businesses are enablers for improving cybercrime reporting whilst the governments of both countries create barriers for reporting. Police in Italy are an enabler for reporting whilst in Scotland the police is a source of barriers. Despite the identification of police as a barrier, we caution against the use of Artificial Intelligence (AI) to substitute the police in cybercrime reporting. Research on a UK population has found that participants preferred to report crime to live police officers as opposed to AI solution [2]. This could be an asset, especially in Scotland, where in-person community policing has a strong tradition [38,39]. We argue that Scottish community policing can improve cybercrime reporting if it happens in tandem with RNPAs in a way that helps people spot the signs of cyber-victimisation.

RQ1c: Scottish RNPAs related that increased awareness-raising, effective information sharing, automation, stigma reduction [4,41], the use of online contact forms as well as centralization [5] would improve cybercrime reporting in Scotland. This aligns with what Italian counterparts identified as being required

for improving cybercrime reporting in Italy. The Italian RNPAs stated that increased educational activities [34], information provision and the reparation of an online platform will support improved reporting to the police in Italy.

Yet, research on fraud prevention and controls cautions that data sharing between public and private collaborations is not sufficient for tackling this problem because much of it is caused by manipulating individual victims [14]. Therefore, awareness raising interventions must be able to describe the symptoms of cyber-victimisation to their audience, so that people are given more specific tools to recognize that they and their loved ones have fallen victim to a crime.

Moreover, previous research found that there are other barriers to improving cybercrime reporting such as “*lack of faith*” in police and victim blaming whilst factors such as “*fund reimbursement*” improve reporting [28]. When the results from the current study are contrasted with victims’ data, some new and interesting nuances emerge.

RQ2: Scottish victims tend to report to their bank (N=76) for the purposes of “*fund reimbursement*” [28]. However, when the victims were asked *why* they reported, they also said that they did so to protect others from going through the same ordeal. This is useful information that could influence policing practices. For example, Police Scotland has experiences with nudging behaviour by running nationwide campaigns to reduce sexual harassment [12]. Similar campaigns could be rolled out to raise awareness of cybercrime victimisation. Such campaigns could frame the police as a supportive power that functions alongside RNPAs.

On the contrary, Italian victims reported directly to the police (N=104) or multiple police forces simultaneously, which could be explained by a lack of access to RNPAs that could mitigate the impact of their cybercrime victimization [31]. Italians may prefer to report to the police because it substantially invests in the protection of networks that are critical for companies by working with multinational private sector corporations [8]. According to our understanding of RNPAs, multinational private sector corporations qualify as RNPAs because they abet the state in cybercrime control. This directly supports the points that were raised in Section §2.2 where we identified that neoliberal societies outsource cybercrime responsibilities [37,25].

Limitations This study provides a snapshot of an under-investigated problem (i.e., the role of RNPAs in improving cybercrime reporting incidence). It is not intended to be conclusive, but rather a first step towards understanding the issue, and exploring how RNPAs could be supported more effectively in this essential role.

Therefore, it is evident that a more comprehensive and detailed study must be conducted to clarify the issues surrounding cybercrime under-reporting. Consequently, we recommend the implementation of a statistical methodology in future research. Employing a statistical approach would enable researchers to model the phenomenon of cybercrime under-reporting more accurately and to formulate practice-based recommendations grounded in significance levels. Additionally, a more representative sample of interviewed RNPAs should be recruited,

and the potential risks and benefits of utilising the Prolific platform must also be carefully considered.

6 Conclusions

We explored the role RNPAs play in accepting cybercrime reports. The RNPAs did indeed play a vital role and made some valuable recommendations to improve cybercrime reporting. The implications are that improving cybercrime reporting will require a multi-disciplinary conjoint effort of a team of technical (e.g., IT, programming, etc.) and non-technical (e.g., psychologists, sociologists, etc.) staff.

Future comparative studies between different countries would be instructive. They should seek to explore a range of responsabilisation implementation strategies and consider how these impact reporting. Moreover, it would be good to study a country where cybercrime reporting incidence is higher than both Scotland and Italy to see how they have encouraged this. Another promising research avenue might be exploring how RNPAs could receive additional support with cybercrime reporting. This could result in the creation of an online reporting channels that would pass on information to the police.

ACKNOWLEDGEMENTS

The authors acknowledge and thank the Scottish Institute for Policing Research (SIPR) (Grant no.: SIPR21MFS_003), the University of Strathclyde and the Scottish Information and Computer Alliance (SICSA) for their financial support.

Moreover, the authors are grateful to Prof. Stefano Chessa, Dr. Federica Casarosa and Dr. Gaia Fiorinelli for facilitating the bilateral exchange of knowledge as well as their help with data collection, translation and legal texts interpretation. We greatly valued the learning we were able to take away from our Italian collaborators and hope that we can continue to learn from them in the future.

References

1. Batasin, C.: Georgia Meloni should rethink her European Strategy: An assessment of Italy’s government two years after its inauguration (2024), LUISS – Institute for European Analysis and Policy <https://leap.luiss.it/wp-content/uploads/2024/>
2. Bradford, B., Kyprianides, A., Andrews, W., Aston, E., Clayton, E., O’Neill, M., Wells, H.: ‘To whom am I speaking?’; Public responses to crime reporting via live chat with human versus AI police operators. *Policing and Society: An International Journal of Research and Policy* pp. 1036–1052 (2025)
3. Braun, V., Clarke, V.: One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative Research in Psychology* **18**, 328–352 (2021)
4. Brooks-Hay, O., Burman, M., Glinski, J.: Victim-survivor views and experiences of sentencing for rape and other offences (2024), <https://www.scottishsentencingcouncil.org.uk/>,

5. Burman, M., Brooks-Hay, O., Friskney, R.: Operationalizing coercive control In: The criminalization of violence against women. In: Douglas, H., Fitz-Gibbon, K., Goodmark, L., Walklate, S. (eds.) *Comparative Perspectives*, chap. 10. Oxford University Press (2024)
6. CPS: Cybercrime- prosecution guidance (2024), <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>
7. Dyson, I.: FOI Scotland Act (2002) Our Ref: IM-FOI-2021-0347 (2019), Chief Constables/ PCCs City of London Police HQ
8. Engineering Group: The Italian State Police and Engineering Group sign an agreement to prevent and combat cybercrime (2025), <https://www.eng.it/en/news/press-releases/2024/>
9. ETB: 2025 Edelman Trust Barometer: Trust and the crisis of grievance (2025), <https://www.edelman.com/trust/2025/trust-barometer>
10. FCDO, DSIT: Research and analysis: UK Science and Innovation Network Summary: Italy (2024), <https://www.gov.uk/government/publications/>
11. Garland, D.: 103 policy predicament: Adaptation, denial, and acting out. In: *The Culture of Control: Crime and Social Order in Contemporary Society*, pp. 103–138. Oxford University Press (2002)
12. Horgan, S., Collier, B., Stewart, J., Thomas, D.: Influence policing: Domestic digital influence campaigns and algorithmic strategic communications in UK law enforcement and homeland security. *The British Journal of Criminology* **65**(3), 480–503 (2025)
13. Hunter, P.: UK shadow home secretary victim of online card fraud. *Computer Fraud & Security* p. 4 (2008)
14. Levi, M.: Frauds and their controls: Some scholarly reflections. *Crime and Justice* pp. Pre-print (2025)
15. Loner, E., Giorgi, I., Berti, C.: Cross-platform political communication: A comparative analysis of social media campaigning by Italian populist radical right leaders. *Mediascapes Journal* **23**(1), 84–108 (2024)
16. MacDonald, K.: Action fraud- VR-a0718. SPC, Tuliallan (2019)
17. Mura, A.: Camera dei deputati – analisi tecnico normativa XIX legislatura n. 1717 (2024), <https://www.camera.it/leg19/995>
18. NCA: National strategic assessment of serious and organized crime (2020), <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/>, NCA
19. Nicholson, J., Morrison, B., Dixon, M., Holt, J., Coventry, L., McGlasson, J.: Training and embedding cybersecurity guardians in older communities. In: *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. vol. 86, pp. 1–15 (2021)
20. Pretorius, L.: Demystifying research paradigms: navigating ontology, epistemology, and axiology in research. *The Qualitative Report* **29**(10), 2698–2715 (2024)
21. Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., Oregon, C.: Is the responsabilization of the cyber security risk reasonable and judicious? *Computers & Security* **78**, 198–211 (2018)
22. Renaud, K., Orgeron, C., Warkentin, M., French, E.: Cyber security responsabilization: an evaluation of the intervention approaches adopted by the Five Eyes countries and China. *Public Administration Review* **80**(4), 577–589 (2020)
23. Ritchie, J., Lewis, J.: *Qualitative research practice: A guide for social science students and researchers*. SAGE Publications Ltd. London (2003)
24. Robinson, O.: Conducting thematic analysis on brief texts: The structured tabular approach. *Qualitative Psychology* **9**(2), 194–208 (2021)

25. Rose, N., O'Malley, A., Valverde, M.: Governmentality. *Annu. Rev. Law. Soc. Sci* **2**, 83–104 (2006)
26. Sikra, J.: The role of responsibilised non-policing agencies (RNPAs) in improving cybercrime reporting in Scotland. In: *Cybercrime Centre: Sixth Annual Cybercrime Conference*. pp. 1–12. Cambridge - UK (2023)
27. Sikra, J., Renaud, K., Thomas, D.: UK cybercrime, victims and reporting: a systematic review. *Commonwealth Cybercrime Journal* **1**(1), 28–59 (2023)
28. Sikra, J., Renaud, K., Thomas, D.: Investigating what promotes and deters scottish cybercrime reporting. *Journal of Economic Criminology* **6**, 100103 (2024)
29. Sillars, J.: Cyber attacks: '80%' of ransomware victims pay up, insurer says (2025), <https://news.sky.com/story/cyber-attacks-80-of-ransomware-victims-pay-up-insurer-says-13441131>
30. Starmer, K., Meloni, G.: PRESS RELEASE joint statement between UK and Italy: 16 september 2024 (2024), UK Government, <https://www.gov.uk/government/news/>
31. Statista: Level of public trust in the State Police in Italy from 2013-2024 (2024), <https://www.statista.com/statistics/579685/public-trust-in-state-police-italy/>
32. Statista: Cybercrime worldwide (2025), <https://www.statista.com/study/203640/cybercrime-worldwide/>
33. Statista: Share of respondents who agreed with the following statements about the police in Scotland in 2017/18 (2025), <https://www.statista.com/statistics/329096/public-attitudes-police-scotland-social-deprivation/>
34. Taccini, F., Rossi, A., Mannarini, S.: Women's EmotionS, trauma and EmpowErMent (w-ES.t.EEM) study protocol: a psychoeducational support intervention for victims of domestic violence – a randomised controlled trial. *BMJ-Open* **12**, e060672 (2022)
35. Taherdoost, H.: Validity and reliability of the research instrument; how to test the validation of a questionnaire/ survey in research. *International Journal of Academic Research in Management (IJARM)* **5**, hal-02546799 (2016)
36. Temara, S.: The ransomware epidemic: Recent cybersecurity incidents demystified. *Asian Journal of Advanced Research and Reports* **18**(3), 1–16 (2024)
37. Venugopal, R.: Neoliberalism as concept. *Economy and Society* **44**(2), 165–187 (2015)
38. Wooff, A.: Relationships and responses: Policing anti-social behaviour in rural scotland. *Journal of Rural Studies* **39**, 287–295 (2015)
39. Wooff, A.: 'Soft' policing in rural Scotland. *Policing* **11**(2), 123–131 (2016)
40. YouGov: Confidence in the British judicial system (2025), <https://yougov.co.uk/topics/society/trackers/confidence-in-the-british-judicial-system>
41. Zauner, J.: The continuum of symbolic violence: how sexting education neglects image-based sexual abuse, dismisses perpetrators' responsibility, and violates rights to sexual autonomy. *Journal of Gender-Based Violence* **5**(3), 483–498 (2021)

A Appendix

Table 1: A comparison of the number of Italian ($N=136$) vs. Scottish victims ($N=151$) that report cybercrime via Reporting Gateways. Some respondents reported via multiple gateways, which is why the summary of responses in columns “Italy” and “Scotland” exceeds the total number of responding participants in each category.

Reporting Gateway	Italy	Scotland
RNPAs – Banks	13	76
RNPAs – Commercial website and social media	13	20
RNPAs – Private institution	0	6
RNPAs – Cyber charity	0	1
RNPAs – University	0	1
Police	104	70
Error responses	8	0

RNPAs’ Interview Questions

Demographics: (i) Gender? (ii) Age range: 18-24; 25-34; 35-44; 45-54; 55-64; 64+

Scottish Questions

- (1) What was your understanding of scams and cybercrime before you started this job?
- (2) How did reporting cybercrime become a part of your agenda? Did you notice any trends in cybercrime in Scotland whilst you’ve been addressing it?
- (3) What kind of IT technology do you use in your everyday life? How comfortable are with using this technology?
- (4) Please walk me through how you receive reports of cybercrime. Please include as much factual detail as possible about what is reportable including, for example, date and time, but also your surroundings and anything else that comes to mind.
- (5) Who do you report your findings to? Why did you go to them? Can you please provide an example of something they said or did that was helpful? Can you please provide an example of something they said or did that was unhelpful?
- (6) 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?
- (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 reporting victimisation?
- (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) Please describe whether you encountered any obstacles in terms of your ability or accessibility to technology when reporting the cybercrime?

- (10) What would an ideal reporting system look like?
- (11) What else is needed to improve cybercrime reporting in Scotland?

Italian Questions - English Version

- (1) If an Italian citizen falls victim to an online scam, phishing, or malware attack, who do they usually report this too? Please elaborate on the benefits and disadvantages of the usual reporting pathway in Italy.
- (2) There are different obstacles because people are reluctant to report being victimised by cybercrime. An internal obstacle might be shame and an external obstacle might not know who to report the crime to. Please elaborate on what you see as the common obstacles to cybercrime reporting in Italy considering both the internal motivations of victims as well as structural challenges.
- (3) Vulnerability to cybercrime does not have a universal definition, however it is commonly viewed in connection to living with a disability (both physical and mental) as well as being an elderly person or a child. Does the usual cybercrime reporting pathway in Italy take vulnerability into consideration when working with victims of cybercrime? Please elaborate on the benefits and disadvantages that may arise for a vulnerable Italian cybercrime victim during the reporting process.
- (4) Responsibilisation in cybercrime is when the criminal justice system educates citizens about the risks of cybercrime but does not designate resources for effective reporting and response. This is due to the assumption that if the citizen was educated about internet safety and still became victimised, then it is their fault. How would you describe the Italian criminal justice system in connection to responsibilisation? Please elaborate on the benefits and disadvantages of the Italian criminal justice system with respect to responsibilisation in cybercrime.
- (5) What kind of changes should take place in Italy to improve the reporting of cybercrime to the police? Please elaborate on a realistic as well as an ideal scenario.