To report or not to report: exploring the motivations and factors associated with reporting of ransomware victimisation among entrepreneurs

Matthijsse, S.R.; Hoff-de Goede, M.S. van ’t; Leukfeldt, E.R.

Journal of Criminal Justice 97 (2025) 102378

Contents lists available at ScienceDirect

Journal of Criminal Justice

journal homepage: www.elsevier.com/locate/jcrimjus

To report or not to report: Exploring the motivations and factors associated with reporting of ransomware victimisation among entrepreneurs

Sifra R. Matthijsse [a,b,*], M. Susanne van't Hoff-de Goede [a,c], E. Rutger Leukfeldt [a,b,c]

[a] Centre of Expertise Cyber Security, The Hague University of Applied Sciences, Johanna Westerdijkplein 75, 2521 EN, The Hague, The Netherlands
[b] Leiden University, Rapenburg 70, 2311 EZ, Leiden, The Netherlands
[c] Netherlands Institute for the Study of Crime and Law Enforcement, De Boelelaan 1077, 1081 HV, Amsterdam, The Netherlands

ARTICLE INFO

Keywords:
Ransomware
Cybercrime
Victimisation
Reporting

ABSTRACT

Although ransomware attacks are considered to be a prominent cyberthreat for organisations, little is known about reporting by entrepreneurs after ransomware victimisation. The current study uses two surveys to explore reporting behaviour among freelancers and small and medium-sized enterprises in the Netherlands. One survey was conducted among entrepreneurs who were victimised by ransomware (n=189). Another survey was conducted among entrepreneurs who were not victimised by ransomware (n=2,496) and included a vignette experiment. While about 92% of the entrepreneurs in the vignette experiment indicated that they would contact the police, only about 18% of the victims did, citing reasons such as solving it themselves or with the help of another party and the belief that the police will not do anything about it. Reporting to the police and to other organisations was related to the emotional and financial impact, with the exception of reporting to the police by victims. There was no association between a negative affective response and situational factors such as having a back-up and reporting among victims and non-victims.

1. Introduction

Each year, a substantial number of individuals and organisations across the globe are victimised by cybercrime. This can have profound negative consequences for not only the victim, but also for society as a whole, ranging from financial costs to feelings of unsafety (Borwell et al., 2025; Leukfeldt et al., 2018). In the response to cybercrime victims play a crucial role as victim reports are a primary source of information for the police and often trigger the start of a criminal investigation (Gottfredson & Gottfredson, 1988; Goudriaan, 2006; Greenberg & Ruback, 1992). In this regard, the victim is often referred to as a principal "gatekeeper" of the criminal justice system (Gottfredson & Gottfredson, 1988). However, many cybercrimes go unreported. While this is also the case for traditional types of crime, such as theft or assault (e.g. Baumer & Lauritsen, 2010; Goudriaan, 2006), underreporting is even more evident for various types of cybercrime (Graham et al., 2020; Van de Weijer et al., 2019). This lack of reporting is problematic, as reporting is vital to the criminal justice system to adequately prevent and respond to cybercrime, deter (potential) offenders and provide appropriate support to victims (Kemp et al., 2023; Skogan, 1984).

While extensive knowledge is available about the aspects that influence reporting behaviour for traditional crimes (e.g. Goudriaan, 2006; Greenberg & Ruback, 1992; Skogan, 1984), research on the reporting of cybercrime is still in its infancy. Research has been conducted on specific types of cybercrime, including fraud, malware and hacking (e.g. Akkermans et al., 2023; Kemp et al., 2023; Van de Weijer et al., 2019). However, little attention has been paid to the reporting of ransomware victimisation, despite its recognition as being one of the most prominent and damaging cyberthreats (European Union Agency for Cybersecurity, 2023; Europol, 2024). The studies that have been conducted on this topic suggest that reporting rates for ransomware victimisation among individuals and organisations are even lower than for other (cyber)crimes. Research indicates that between 77% and 95% of ransomware incidents are not reported to the police (European Commission, 2022; Simoiu et al., 2019; Statistics Netherlands, 2023; Van de Weijer et al., 2020; Voce & Morgan, 2022). Many victims tend to seek help from alternative sources, such as friends or family, a cybersecurity firm or financial institution (Statistics Netherlands, 2023; Van de Weijer, Leukfeldt, & Van der Zee, 2020; Voce & Morgan, 2022). Furthermore, there is a limited understanding of the motivations and factors that are related to the decision to report ransomware incidents and the extent to which these align with the motivations and factors that

* Corresponding author.
E-mail addresses: S.R.Matthijsse@hhs.nl (S.R. Matthijsse), M.S.vantHoff-deGoede@hhs.nl (M.S. van't Hoff-de Goede), E.R.Leukfeldt@hhs.nl (E.R. Leukfeldt).

https://doi.org/10.1016/j.jcrimjus.2025.102378
Received 20 December 2024; Received in revised form 19 February 2025; Accepted 19 February 2025
Available online 26 February 2025

are related to reporting of other cybercrimes or traditional crimes. In addition, most studies that examine crime reporting focus on individuals. There is a lack of research on cybercrime reporting among entrepreneurs (e.g. Kemp et al., 2023; Van de Weijer et al., 2021), even though they are often victimised and may potentially demonstrate different decision-making compared to individuals. For instance, companies might refrain from reporting to law enforcement due to concerns about how it could affect their reputation or business (Leukfeldt & Holt, 2020, p. 341), or because they prioritize ensuring business continuity over reporting the crime (Cybbar & CSD, 2023).

There is a need for research into the extent to which victims report ransomware victimisation, what formal organisations they report to and what their motivation(s) for doing so are. This could enhance understanding of the needs and decision-making of victims and how reporting of ransomware can be encouraged. To address this gap in the literature, the current study aims to gain insight into the reporting decisions of entrepreneurs in the Netherlands following victimisation of ransomware, and the factors and motivations that are associated with these decisions. This study seeks to answer the following research questions:

Q1. : To what extent are entrepreneurs willing to report ransomware victimisation, and what organisations do they report to?

Q2. : What are the most important motivations for reporting ransomware victimisation to the police among entrepreneurs?

Q3. : What factors are associated with the willingness to report ransomware victimisation to the police and other organisations among entrepreneurs?

2. Literature review

2.1. Reporting of traditional crimes

There are various theoretical perspectives that explain why victims report crime, each focusing on a different level of aggregation (micro, meso and macro). In general, a distinction can be made between an economic, psychological and broader sociological perspective (Goudriaan, 2006; Xie & Baumer, 2019).

The economic perspective views the decision to report a crime as a rational choice resulting from an analysis of the perceived costs and benefits (Skogan, 1984; Tarling & Morris, 2010). In this regard, the characteristics or seriousness of the crime plays an important role. For example, the willingness to report increases if more (financial) loss or injury is involved (Skogan, 1984; Tarling & Morris, 2010). Possible benefits for reporting may include wanting to recover goods, claim financial compensation or insurance payment, or moral considerations, such as feeling like it is an obligation to do so or to prevent victimisation of others (Skogan, 1984; Tarling & Morris, 2010). On the other hand, reporting a crime can also incur costs. A barrier towards reporting can be the belief that the police can't do anything (Kidd & Chayet, 1984; Skogan, 1984). Victims may be afraid to waste the police's time, especially if there is a low chance of successfully solving the crime (Tarling & Morris, 2010). Furthermore, victimisation may lead to feelings of helplessness or incompetence, which the victim may not only apply to themselves, but also to the criminal justice system (Kidd & Chayet, 1984). Moreover, attitudes towards the police can play a role (Xie & Baumer, 2019). Other barriers towards reporting may include feeling that it takes too much effort, time or money (for example because the victim is required to go to the police station or attend a court hearing), not wanting to acknowledge own's own vulnerability, fear of disapproval or further victimisation, or fear of compromising one's privacy (Kidd & Chayet, 1984; Tarling & Morris, 2010). However, the economic perspective has been criticised for oversimplifying decision-making. Victims may not always have the capacity or necessary information to fully evaluate the benefits and costs and make a rational decision (Gottfredson & Gottfredson, 1988; Goudriaan, 2006). Moreover, this perspective has a limited focus on emotions, normative responses and the role of the social environment in decision-making (Goudriaan, 2006; Xie & Baumer, 2019).

The psychological perspective, on the other hand, views decision-making as "semireasoned" because victims will not always carefully weigh the costs and benefits of each decision, or consider *all* the options, given that they are in a stressful situation (Greenberg & Ruback, 1992). As first suggested by Greenberg & Ruback (1992, p. 181), victim reporting decision-making can be captured into a three-step model in which an individual; 1) *labels the event as a crime*, i.e. the situation an individual finds themselves in matches their definition of a crime; 2) *determines the seriousness*, which depends on the extent to which they feel they have been wronged (e.g. physical, material and/or psychological harm) and their perceived vulnerability to being victimised again; 3) *decides how to respond*, which includes seeking a private solution, notifying the police, reevaluating the situation or doing nothing. In each step of the process, emotions such as distress and social influence may affect an individuals' decision-making. Similar to the economic perspective, the psychological perspective posits that serious crimes are more often reported to the police. However, unlike the economic model, this is an indirect influence, as the perceived seriousness of the crime influences the affective reaction (e.g. stress), which in turns influences decision-making (Goudriaan, 2006; Greenberg & Ruback, 1992).

Both the economic and psychological perspective look at the motivations and characteristics of individuals and their direct environment, overlooking the broader social context. On the contrary, the (macro-) sociological perspective posits that law – and by extension reporting behaviour - varies across societies and individuals and is influenced by dimensions of social life such as culture, organisation and social control (Black, 1976). For example, reporting rates will be higher among strangers than intimates, and higher among organisations compared to individuals (Gottfredson & Hindelang, 1979). However, empirical studies on the theory have yielded mixed results, and the theory has been criticised for not taking into account individual decision-making and characteristics (Gottfredson & Hindelang, 1979; Goudriaan, 2006; Xie & Baumer, 2019).

Additionally, personal characteristics can also influence crime reporting rates. For example, women, older victims and victims who are married or have a partner are more likely to report crime (e.g. Baumer & Lauritsen, 2010; Goudriaan, 2006; Skogan, 1984; Tolsma et al., 2012), while results for other socio-demographic characteristics such as education and ethnicity vary (e.g. Baumer & Lauritsen, 2010; Goudriaan, 2006; Skogan, 1984).

The previously described theoretical perspectives are mainly based on reporting by individuals. Less research has been conducted on reporting by organisations after victimisation. However, the limited research available indicates that similar considerations play a role for entrepreneurs as they do for individuals. For example, reporting is related to aspects such as the seriousness of the incident (Dugato et al., 2013; Home Office, 2024; Isenring et al., 2016; Kennedy, 2016; Smith, 2008; Taylor, 2002; Walker, 1994), the time and resources it takes to report (Smith, 2008; Taylor, 2002; Walker, 1994), lack of evidence (Dugato, Favarin, Hideg, & Illyes, 2013; Isenring et al., 2016; Smith, 2008; Taylor, 2002; Walker, 1994), attitudes towards the police or criminal justice system and their ability to provide an effective response (Dugato, Favarin, Hideg, & Illyes, 2013; Home Office, 2024; Kennedy, 2016; Smith, 2008; Taylor, 2002; Walker, 1994) or dealing with the incident internally (Dugato, Favarin, Hideg, & Illyes, 2013; Kennedy, 2016; Smith, 2008). In addition, reporting may be related to size or location of the business (Dugato, Favarin, Hideg, & Illyes, 2013; Isenring et al., 2016).

2.2. Reporting of cybercrimes and ransomware

Previous research shows underreporting of cybercrime to the police among individuals and organisations (Akkermans, Arends, Derksen, &

Reep, 2023; de Kimpe, 2020; Kemp et al., 2023; Van de Weijer et al., 2019), particularly in comparison to traditional crime, although reporting rates vary for different cybercrimes (Graham et al., 2020; Van de Weijer et al., 2019). Underreporting can occur because victims do not perceive the incident as serious, handle the incident internally or with the help of another organisation, or lack trust in the police when it comes to combating cybercrime (Cybbar & CSD, 2023; Graham et al., 2020; Kemp et al., 2023; Van de Weijer, Leukfeldt, & Van der Zee, 2020; Veenstra et al., 2015; Wanamaker, 2019). On the other hand, common reasons for reporting include wanting to prevent it from happening to someone else, creating a safer (online) environment, wanting the perpetrator to get caught or feeling like it is their duty to report (Van de Weijer, Leukfeldt, & Van der Zee, 2020; Veenstra, Zuurveen, & Stol, 2015). Personal or organisational characteristics, such as gender, education, company size and sector may also influence reporting rates, although findings are mixed (de Kimpe, 2020; Graham et al., 2020; Kemp et al., 2023; Van de Weijer et al., 2019, 2021).

When it comes to reporting of ransomware victimisation, results vary, especially when comparing the intention to report among persons who have not (yet) been victimised and actual reporting rates among victims. Although research shows that 69% of SMEs would be willing to report the incident to the police if they were (hypothetically) victimised by ransomware (European Commission, 2022), international self-report studies indicate that the reporting rate of ransomware to the police by citizens and organisations who have been victimised ranges between 9% and 23% (European Commission, 2022; Simoiu et al., 2019; Voce & Morgan, 2022). In the Netherlands, only 5.7% of the citizens victimised by ransomware reported the incident to the police, which is lower than for other cybercrimes such as identity fraud or cyberstalking (47.4%, 30% among citizens, respectively) (Van de Weijer, Leukfeldt, & Van der Zee, 2020). Companies show a slightly higher willingness to report, with between 13% and 16.7% of Dutch companies reporting ransomware victimisation to the police (Statistics Netherlands, 2023; Van de Weijer, Leukfeldt, & Van der Zee, 2020). Contrary to the reporting rates for citizens, ransomware is one of the most commonly reported cybercrimes by organizations, only preceded by marketplace fraud (28.2%) and identity theft (50%) (Van de Weijer, Leukfeldt, & Van der Zee, 2020). Reporting is more common among medium- and large-sized companies compared to freelancers and micro- and small businesses (Statistics Netherlands, 2023). Motivations for reporting ransomware include wanting to prevent it from happening to themselves or another person, to create a safer online environment and to get money back or receive compensation for damages. Motivations for not reporting include resolving the incident themselves, not viewing the incident as a serious crime or not believing the police can do anything about it (Voce & Morgan, 2022).

While the willingness to go to the police after victimisation is low, several studies have shown that victims of ransomware often seek help from other parties, such as from friends or family, external advisers, an internet service provider, a cybersecurity company or a financial institution (European Commission, 2022; Statistics Netherlands, 2023; Voce & Morgan, 2022). For example, an Australian study found that 10% of ransomware victims reported the crime to the police, whereas a higher percentage sought help from other parties, such as from friends or relatives (29%), an internet service provider (14%) or a financial institution (14%) (Voce & Morgan, 2022). Furthermore, some victims don't report the incident to anyone (European Commission, 2022; Voce & Morgan, 2022).

In summary, research on ransomware reporting is limited, especially regarding the factors and motivations related to reporting behaviour. To address this gap in the literature, the current study explores reporting decisions of entrepreneurs in the Netherlands after falling victim to ransomware.

3. Methods

3.1. Sample

This study is part of a larger research project on victimisation of ransomware among consumers and entrepreneurs in the Netherlands (Matthijsse et al., 2025). Data for the current study was collected amongst a sample of entrepreneurs in the Netherlands that were previously victimised by ransomware and who were in a position to answer questions about the incident and their decision-making, as well as a sample of entrepreneurs that were *not* previously victimised by ransomware and who could answer questions about what they would do in a hypothetical ransomware scenario.[1] The focus was on freelancers and small- and medium-sized enterprises (SMEs) in the Netherlands, as freelancers and SMEs make up the vast majority of the business economy in the Netherlands (Statistics Netherlands, 2024). Furthermore, there are some indications that small- and medium sized enterprises are increasingly at risk of victimisation of ransomware (Europol, 2024), while reporting seems to be less common among freelancers and micro- and small businesses compared to medium- and large sized companies (Statistics Netherlands, 2023). In the current study, SMEs were defined as "enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million" (Article 2, Recommendation 2003/361/EC).

We relied on two panels from the research firm I&O Research (now called Ipsos I&O) to administer surveys to a sample of freelancers and SMEs in the Netherlands. I&O Research employs a consumer panel of more than 37,000 Dutch citizens of 16 years and older, including about 2,600 entrepreneurs, who are selected through random sampling (e.g., from residence registers). In addition, I&O Research employs an entrepreneurial panel of about 4,500 Dutch entrepreneurs (Ipsos I&O, n.d).

A total of 6,664 entrepreneurs in the consumer and entrepreneurial panel were invited between September 25 and October 29, 2023, to participate in the study.[2] To ensure that potential respondents belonged to the target group, two filter questions were included at the beginning of the survey. First, respondents were asked to indicate for eight types of cybercrime (including ransomware) if this had ever happened to their company. Ransomware was defined as "your company's files, data or device(s) were locked or encrypted, and a ransom was demanded to regain access to them". Second, the respondents that replied in the affirmative were presented with the same definition of ransomware and asked again if this had ever happened to their company.

The respondents that replied in the affirmative to both filter questions were included in the victim sample and directed to a survey about their experiences with victimisation of ransomware. The respondents that were *not* previously victimised by ransomware were included in the non-victim sample and directed to a survey about decision-making in a hypothetical ransomware scenario. Although we tried to encourage respondents to answer honestly by emphasizing that they would remain anonymous and that their answers could not be traced back to them or their company, the possibility remains that respondents did not feel comfortable in reporting their victim status, thus ending up in the non-victim sample. This should be taken into account with regards to the results.

After filtering out the speeders[3] and incomplete surveys, the total

[1] Ethical advice for the study was received from the Ethics Committee for Legal and Criminological Research of VU Amsterdam.

[2] Originally, 7,072 respondents were invited to participate, but 408 respondents were excluded because information on the size of their company was unavailable. For this group, the only available information was that they owned a company with two or more employees.

[3] Speeders were defined as those respondents with a response time less than 1/3 of the median of the response time in minutes.

sample consisted of 2,685 respondents (response rate: 40.3%), of which 189 respondents were included in the first study and 2,496 respondents were included in the second study. In the total sample, there was an underrepresentation of freelancers (69.2% versus 80.9%), the industry, construction and utilities (9.6% versus 15.5%) and the sector trade, logistics and catering (13% versus 19%) in comparison to the population of Dutch freelancers and SMEs in the Netherlands (Statistics Netherlands, 2024). Therefore, the results of this study might not be representative for all freelancers and SMEs.

3.2. Instruments

In order to collect the data, two online surveys were administered in Dutch. The survey for victims included questions about background characteristics, circumstances of the attack, the ransom note and extortion phase, the impact of the incident, and contact with various organisations following the incident. The questions were based in part on previous research (Akkermans, Arends, Derksen, & Reep, 2023; Johns, 2021; Matthijsse et al., 2024; Simoiu et al., 2019; Van de Weijer, Leukfeldt, & Van der Zee, 2020; Voce & Morgan, 2021, 2022). The survey for entrepreneurs that were not previously victimised by ransomware included questions about background characteristics and a vignette experiment that was used to elicit various responses, including the decision to report the ransomware incident.

Four factors with two variations each were included in the vignette experiment, thus employing a 2 x 2 x 2 x 2 design resulting in 16 different vignettes. The included factors were the ransom demand, having a back-up, being advised to pay and double extortion (explained in more detail in 3.3.2). The factors were based on previously described theories and research stating that the willingness to report is related to the seriousness of the incident (e.g. Cybbar & CSD, 2023; Skogan, 1984; Veenstra, Zuurveen, & Stol, 2015; Voce & Morgan, 2022; Wanamaker, 2019). We hypothesized that, in the case of ransomware, this could be related to the previously mentioned factors. It was therefore expected that respondents that were shown a higher ransom demand, were threatened with data leakage (double extortion), had no back-up and were advised to pay were more inclined to report the ransomware incident. Following a between-subjects design to allow for comparisons between respondents, participants were randomly assigned to one of sixteen groups of roughly the same size. Each group was presented with one vignette scenario with a different combination of factor variations. The distribution of vignettes across respondents is included in the appendix (Table A.1).

In the vignette, all respondents were asked to imagine the hypothetical situation that their organisation was victimised by ransomware, and that they were given the responsibility to decide whether or not to report the incident. All respondents were shown a ransom note (figure 1), after which they were told that they were sent to a personalised ransom website (figure 2). The virtual image of this website included a running timer and the vignette factors. To increase the realism of the vignette, both the ransom note and the website were based on real life examples (among others from Cl0p, Lockbit, BlackCat and Royal).

After being presented with the vignette, respondents were asked to indicate the likelihood that they would report the crime, the organisations to which they would report and motivations for (not) reporting to the police. In addition, they were asked questions about other decision-making (e.g. negotiating, paying) and the expected impact of the incident.

3.3. Measures

3.3.1. Dependent variables

3.3.1.1. Reporting (0-1). For the purpose of this study, reporting is defined as any contact with an organisation after ransomware victimisation, including asking for advice as this also signifies help-seeking behaviour. In both surveys, respondents were asked whether they had contacted (victims) or would contact (non-victims) a list of eight organisations, including the police, a financial institution, an insurance company, a cybersecurity company or IT-provider, No More Ransom, victim support, the Fraud Help Desk[4], or another organisation (open ended). Respondents were able to indicate multiple responses. *Reporting to the police* is a binary variable where 0 is "no" and 1 is "yes". In order to measure *reporting to other organisations*, all organisations other than the police were taken together into a binary variable, where respondents contacted (victims) or would contact (non-victims) any of the above-mentioned organisations were scored 1 "yes". Respondents that had contacted or would contact none of the organisations were scored with 0 "no".

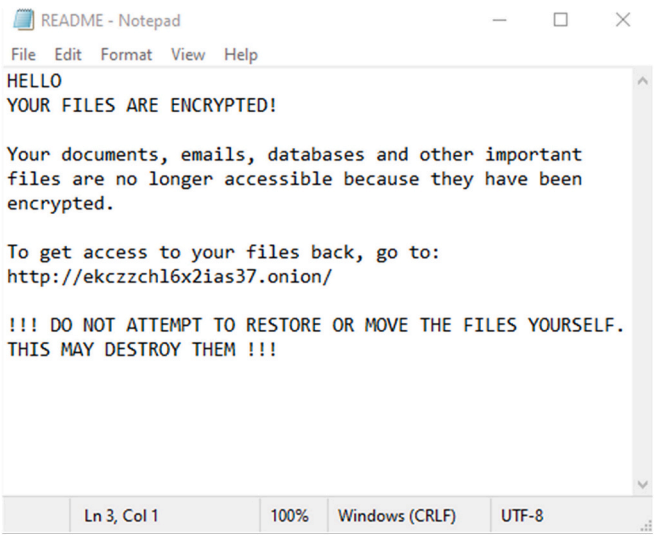

Fig. 1. Ransom note included in vignette

3.3.2. Independent variables

3.3.2.1. Ransom demand (0-1). The ransom demand was the first factor that was included in the vignette experiment for non-victims, where 0 is "1% of the annual turnover of their organisation in Bitcoin" and 1 is "25% of the annual turnover of their organisation in Bitcoin". Victims were asked about the ransom demand with an open question, where they were able to indicate the amount and the currency (Euro, USD, Bitcoin, other) of the demand. However, this factor was excluded from the regression models, as only about one-third of the victims indicated the ransom demand.

3.3.2.2. Advised to pay (0-1). The second factor included in the vignette experiment for non-victims was being advised to pay, where it was described that the people around the respondent and a hired cybersecurity company advised them on whether or not to pay. Here, 0 is "no" and 1 is "yes". In the victim survey, the respondents that had paid the ransom were able to indicate that being advised to pay was a possible motivation for paying the ransom. However, this factor was excluded from the regression models based on the victim sample due to the small number of respondents.

3.3.2.3. Back-up (0-1). The third factor that was included in the vignette experiment for non-victims was having a back-up of the encrypted data, where 0 is "no" and 1 is "yes". In the survey for victims,

[4] A Dutch anti-fraud hotline.

Fig. 2. Example of ransom website included in vignette.

respondents were asked if they had a series of cybersecurity measures in place prior to victimisation, of which one was having a back-up of their data. Here 0 is "no" and 1 is "yes".

3.3.2.4. Double extortion (0-1). The fourth factor that was included in the vignette experiment for non-victims was whether the offenders threatened to leak previously stolen data (i.e. double extortion). In one version of the ransom website, no mention was made of data leakage, whereas in another version the following text was included: "To decrypt your files and prevent data leakage you need to buy our special software", in combination with "If you do not pay, data will be published on our portal. Anyone will be able to see your confidential information, including your financial reports, intellectual property, employee and client data". Here, value 0 is "no" and 1 is "yes". In the survey for victims, respondents were asked if the offenders made any additional threats, of which threatening to leak stolen data was one option. Here, value 0 is "no" and 1 is "yes".

3.3.2.5. Payment. In the survey for non-victims, the *likelihood of a ransom being paid (0-10)* after the vignette experiment was measured on an 11-point Likert-scale from 0% to a 100%, (0 = 0%, 1 = 10%, 2 = 20%, etc). In the survey for victims, respondents were asked if they had *paid the ransom demand (0-1)*, where 1 was "Yes, I paid part of the ransom demand", 2 was "Yes, I paid the full ransom demand" and 3 was "No, I did not pay the ransom demand". For the analysis, values 1 and 2 were combined. As a result, ransom paid is a binary variable where 0 is "No" and 1 is "Yes".

3.3.2.6. Negative affective response (0-1). In both surveys respondents were asked about their emotion(s) or affective response after first being confronted with the ransom note. They were provided with different emotions such as feeling angry, anxious or relaxed and were able to select multiple responses. In addition, respondents could indicate other emotions in an open-ended answer-category. For the analysis, all the respondents that mentioned a negative emotion were scored as having a negative affective response. Therefore, negative affective response is a binary variable where 0 means that respondents did not have a negative affective response, and 1 means that they did.

3.3.2.7. Emotional impact (0-1). Respondents in both surveys were asked whether the ransomware incident had any (temporary) emotional or psychological consequences, or if it would have in the hypothetical ransomware scenario. They were provided with 8 categories, including feeling less safe and having trouble sleeping. Respondents could indicate multiple responses. This variable was recoded into a binary variable, where 0 means that respondents did not experience an emotional impact, and 1 means that they did.

3.3.2.8. Financial impact (1-5) (excluding the ransom amount paid). Respondents in both surveys were asked to indicate the costs of the ransomware incident (victims) or expected costs in a hypothetical ransomware scenario (non-victims) excluding a ransom payment. This can include, for example, repair or recovery costs. In both questionnaires, 1 was "None", 2 was "Less than €1,000", 3 was "€1,000 - "€5,000", 4 was "€5,000 - €10,000", 5 was "€10,000 - €50,000", 6 was "€50,000 to €100,000", 7 was "€100,000 to €250,000", 8 was "€250,000 to €500,000", 9 was "more than €500,000", and 10 was "I don't know". For the analysis, categories 2 and 3 were combined, categories 5 up to 9 were combined, and value 7 was indicated as missing value. In the regression models, the category "none" serves as reference category.

3.3.3. Control variables

The size, sector and annual turnover of the organisation, and being insured for cyber incidents were included in the analysis as control variables, since these factors may be related to the reporting decisions.

3.3.3.1. Size (1-4). The size of the organisation is a categorical variable where 1 is "freelancer", 2 is "micro (2-9 employees)", 3 is "small (10-49 employees)" and 4 is "medium (50-250 employees)". In the regression models, the category "freelancer" serves as reference category.

3.3.3.2. Sector (1-5). The sector of the organisation is a categorical variable where 1 is "Agriculture/fishing", 2 is "Industry, construction and utilities", 3 is "Trade and logistics, catering", 4 is "Financial and business services" and 5 is "Government, education, healthcare and other". In the regression models, the category "financial and business services" serves as reference category.

3.3.3.3. Annual turnover (1-3). The annual turnover of the organisation is a categorical variable, where 1 is "less than €500,000", 2 is "€500,000 - €1,000,000" and 3 is more than "€1,000,000". In the regression models, the category "less than €500,000" serves as reference category.

3.3.3.4. Cyber insurance (0-1). Respondents were asked which of the following best described their situation when it comes to insurance policy. Initially, the variable included 4 values, where 1 was "my company had a specific cybersecurity insurance policy", 2 was "the cybersecurity insurance of my company was part of a wider insurance policy", 3 was "my company was not insured against cyber incidents" and 4 was "I don't know". For the analysis, values 1 and 2 were combined and value 4 was indicated as missing value. As a result, cyber insurance is a binary variable where 0 is "no" and 1 is "yes".

Table 1 shows the descriptive statistics of all the variables that were used in the analyses.

Table 1
Descriptive statistics of the variables included in the regression models.

	Victims (n=189)		Non-victims (n=2,496)	
	n	%/M	n	%/M
Reporting to police (0-1)	189		2,496	
No	156	82.5%	194	7.8%
Yes	33	17.5%	2,302	92.2%
Reporting to other organisations (0-1)	189		2,496	
No	58	30.7%	382	15.3%
Yes	131	69.3%	2,114	84.7%
Ransom demand (0-1)	-	-	2,496	
1% of turnover in Bitcoin			1,260	50.5%
25% of turnover in Bitcoin			1,236	49.5%
Advised to pay (0-1)	-	-	2,496	
No			1,256	50.3%
Yes			1,240	49.7%
Back-up (0-1)	189		2,496	
No	19	10.1%	1,252	50.2%
Yes	170	89.9%	1,244	49.8%
Double extortion (0-1)	189		2,496	
No	161	85.2%	1,240	49.7%
Yes	28	14.8%	1,256	50.3%
Ransom paid (0-1)	189		-	-
No	176	93.1%		
Yes	13	6.9%		
Likelihood of ransom being paid (0-10)	-	-	2,496	1.20
Negative affective response (0-1)	189		2,496	
No	37	19.6%	186	7.5%
Yes	152	80.4%	2,310	92.5%
Emotional impact (0-1)	189		2,496	
No	119	63%	662	26.5%
Yes	70	37%	1,834	73.5%
Financial impact (1-4)	171		1,894	
None	44	25.7%	144	7.6%
Less than €5.000	105	61.4%	1,079	57%
€5.000 - €10.000	12	7%	298	15.7%
€10.000 - €50.000	10	5.8%	373	19.7%
Size (1-4)	189		2,496	
Freelancer (1 employee)	88	46.6%	1,769	70.9%
SME (2-9 employees)	59	31.2%	480	19.2%
Small (10-49 employees)	39	20.6%	214	8.6%
Medium (50-250 employees)	3	1.6%	33	1.3%
Sector (1-5)	188		2,488	
Agriculture/fishing	9	4.8%	74	3%
Industry, construction and utilities	24	12.8%	233	9.4%
Trade and logistics, catering	37	19.7%	310	12.5%
Financial and business services	76	40.4%	1,049	42.2%
Government, education, healthcare and other	42	22.3%	822	33%
Annual turnover (1-3)	175		2,295	
Less than €500.000	106	60.6%	1,802	78.5%
€500.000 - €1.000.000	16	9.1%	152	6.6%
More than €1.000.000	53	30.3%	341	14.9%
Cyber insurance (0-1)	180		2,184	
No	167	92.8%	1,851	84.8%
Yes	13	7.2%	333	15.2%

3.4. Analytic strategy

Analyses were conducted in IBM SPSS Statistics 28.0. To answer the first and second research question regarding willingness to report and motivations for reporting, descriptive statistics were used. To answer the third research question about the factors associated with the willingness to report, logistic regression models were used since the dependent variables are binary. Two models were used to assess the relationship between situational factors, experienced impact, negative affective response and reporting decisions among victims. The first model included the dependent variable 'reporting to the police' and the independent variables 'ransom paid', 'back-up', 'double extortion', 'negative affective response', 'emotional impact', and 'financial impact'. Furthermore, the 'size', 'sector' and 'annual turnover' of the organisation, and 'cyber insurance' were included in the model as control variables. The second model included the dependent variable 'reporting to other organisations' and the same independent and control variables as in the first model. In addition, two models were used to assess the relationship between situational factors, experienced impact, negative affective response and reporting decisions among non-victims. These models used similar factors as in the regression models for the victims, with the addition of the independent variables 'ransom demand' and 'advised to pay'. We used the area under the ROC Curve (AUC) to determine the models' ability to discriminate between groups based on the sensitivity and specificity, where 0.5 indicates no discrimination, between 0.7 and 0.8 indicates acceptable discrimination, between 0.8 and 0.9 indicates excellent discrimination and $>$ 0.9 is considered outstanding discrimination (Hosmer & Lemeshow, 2000, p. 160).

4. Results

4.1. Reporting to various organisations

All respondents that were previously victimised by ransomware were

asked what organisations they contacted after they were victimised, whereas respondents that were not previously victimised were asked what organisations they would contact after being presented with the hypothetical ransomware scenario. Respondents were able to select multiple responses. The majority of the victims (72.5%) contacted at least one organisation (including the police and other organisations), while 27.5% did not contact any organisation. Table 2 shows that victims reported to one organisation on average ($M = 1.20$, $SD = 1.150$). The vast majority of the non-victims also indicated that they would contact at least one organisation (98.9%), with only 1.1% of the respondents indicating that they would not contact any organisation. As shown in table 2, the non-victims would contact three different organisations on average ($M = 2.96$, $SD = 1.515$).

Figure 3 shows that most entrepreneurs that were victimised contacted a cybersecurity company or IT provider (60.8%), followed by the police (17.5%) and the Fraud Help Desk (13.2%). Of the victimised entrepreneurs that contacted the police, 25.8% (n=8) made an official report, which comes down to 4.2% of the total victim sample. Most entrepreneurs that were not previously victimised indicated that they would contact the police (92.2%), followed by a financial institution (47%) and the Fraud Help Desk (42.4%).

4.2. Motivations for (not) reporting to the police

Respondents in both studies were also asked about their reasoning behind reporting or not reporting to the police. As shown in figure 4, for victims the most common reason for reporting to the police was that they wanted the culprit to be caught (22.6%) and to create a safer (online) environment (22.6%), followed by wanting to prevent this from happening to someone else (19.4%). Among the non-victims, the most common reason was that they wanted the culprit to be caught (80.6%), followed by wanting to prevent this from happening to someone else (69.3%) and believing reporting is their duty (65.7%).

Fig. 5 shows that the most common reasons for victims to *not* report to the police was that they solved it themselves or with the help of another party (49.4%), followed by the belief that there is no point because the police will not do anything about it (18.4%) and other reasons (7.6%), including that they experienced little to no impact or because they had not thought of contacting the police. For the non-victims, the most common reason for not reporting to the police in case of ransomware victimisation was the belief that there is no point because the police will not do anything about it (46.2%), followed by the belief that it is a matter for an agency other than the police (24.1%) and because respondents would solve it themselves or with the help of another party (22.6%).

4.3. Determinants for reporting to the police and other organisations

Next, logistic regression models were used to determine whether situational factors, a negative affect response and experienced impact were related to reporting to the police (model 1) and other organisations (model 2) among victims of ransomware.

As shown in table 3, the first model correctly predicted 88.7% of cases and showed acceptable discrimination between classes (AUC = .761, p. = .000). However, the model was not statistically significant when compared to the null model ($\chi 2(18) = 27.627$, $p = .068$, *Nagelkerke* $R^2 = .283$), which means that the data did not provide statistically significant evidence that the factors are related to reporting to the police among victims.

The second model was statistically significant when compared to the null model ($\chi 2(18) = 46.696$, $p = < .001$, *Nagelkerke* $R^2 = .370$), correctly predicted 72.7% of cases and showed excellent discrimination between classes (AUC = .820, p. = .000). There was a statistically significant relationship between reporting to other organisations and emotional impact ($B = .984$, $p = .038$). Respondents that experienced an emotional impact had 2.676 higher odds of reporting to other organisations compared to respondents that did not experience an emotional impact. There was also a statistically significant relationship between a financial impact of between €5,000 and €10,000 and reporting to other organisations ($B = 2.676$, $p = .043$). Respondents that experienced this amount of financial impact had 14.533 higher odds of reporting to other organisations compared to respondents that experienced no financial impact. In addition, company size micro ($B = 1.296$, $p = .019$) and company size small ($B = 2.325$, $p = .015$) were statistically significant. Micro and small companies had respectively 3.654 and 10.229 higher odds of reporting to other organisations compared to freelancers. The sector government, education, healthcare and other was also statistically significant ($B = 1.378$, $p = .018$), which means that companies in this sector had 3.965 higher odds of reporting to other organisations compared to companies in the sector financial and business services. There was no significant relationship between reporting to other organisations and ransom paid ($B = -1.444$, $p = .118$), back-up ($B = .264$, $p = .705$), double extortion ($B = -.068$, $p = .913$) and negative affective response ($B = -.055$, $p = .918$).

To summarize, for victims the decision to report to the police is not related to situational factors, a negative affect response or experienced impact. The intention to report to other organisations among victims is related to experienced emotional and financial impact, as well as the size and sector of the company.

Logistic regression was also conducted to determine whether situational factors, experienced impact and a negative affect response were related to the intention to report a ransomware attack to the police (model 1) and other organisations (model 2) among respondents that were not previously victimised by ransomware (Table 4).

As shown in table 4, the first model was statistically significant when compared to the null model ($\chi 2(20) = 45.084$, $p = 0.001$, *Nagelkerke* $R^2 = .063$), correctly predicted 91.7% of cases and showed acceptable discrimination between classes (AUC = .661, p. = .000). There was a significant relationship between the intention to report to the police and emotional impact ($B = .421$, $p = .041$). Respondents that expected to experience an emotional impact had 1.524 higher odds of reporting to the police than respondents that expected to experience no emotional impact. Financial impact was also statistically significant. Respondents that expected to experience less than €5,000 ($B = .645$, $p = .023$), between €5,000 and €10,000 ($B = .725$, $p = .042$), and more than €10,000 ($B = 1.255$, $p = .002$) in costs had respectively 1.906, 2.065 and 3.507 higher odds of reporting to the police compared to respondents that expected to experience no financial impact. The variables ransom demand ($B = .351$, $p = .064$), likelihood of ransom being paid ($B = .095$, $p = .097$), back-up ($B = -.091$, $p = .623$), double extortion ($B = -.323$, $p = .083$), advised to pay ($B = -.185$, $p = .319$) and negative affective response ($B = .475$, $p = .120$) were not statistically significant.

As shown in table 4, the second model was statistically significant when compared to the null model ($\chi 2(20) = 116.435$, $p = < .001$, Nagelkerke $R^2 = .118$), correctly predicted 83.9% of cases and showed acceptable discrimination between classes (AUC = .701, p. = .000).

Table 2
Descriptives of number of different organisations contacted after ransomware victimisation

	Victims (n=189)				**Non-victims** (n=2,496)			
	Min	Max	*M*	*SD*	Min	Max	*M*	*SD*
Number of different organisations contacted	0	6	1.20	1.150	0	8	2.96	1.515

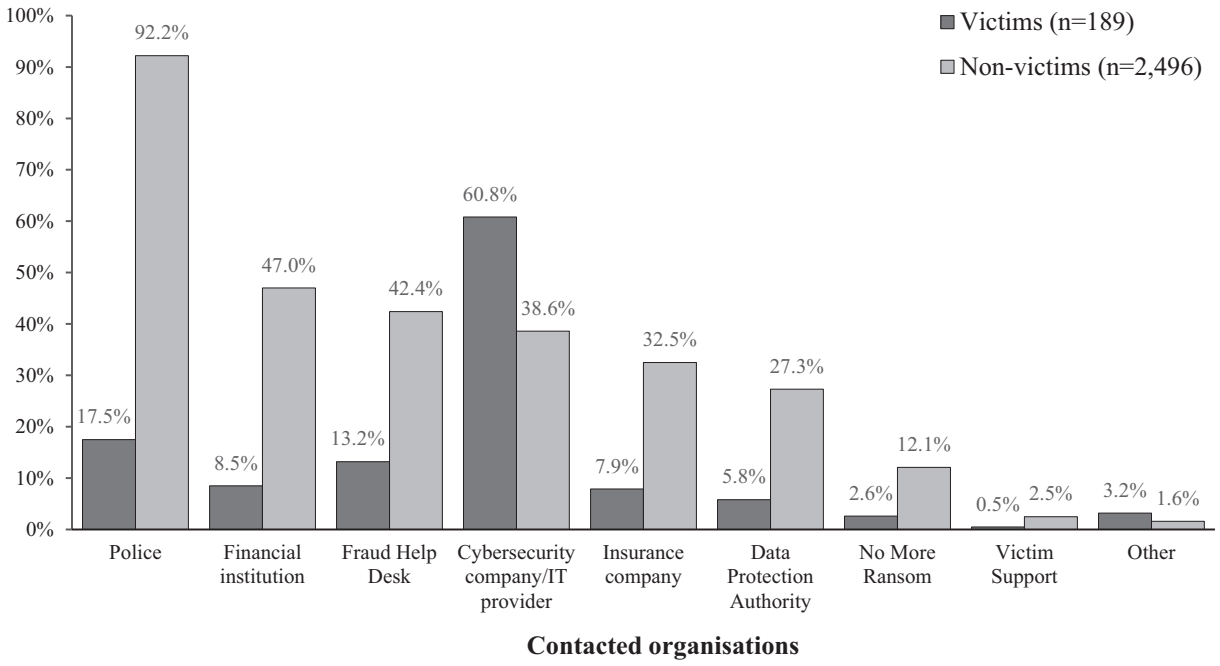

Fig. 3. Percentages of reporting ransomware victimisation to various organisations (*multiple responses)*

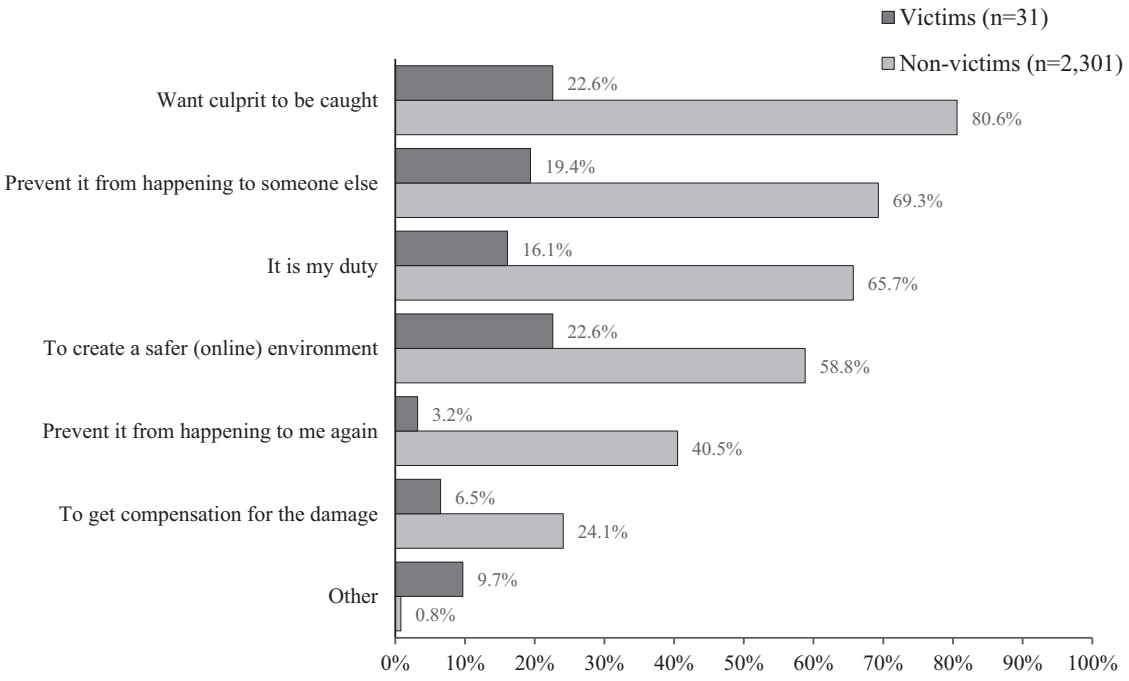

Fig. 4. Motivations for reporting ransomware victimisation to the police.
Respondents that were previously victimised were asked to select the most important reason and could only select one option, whereas respondents that were not previously victimised could give multiple responses.

There was a significant relationship between emotional impact and the intention to report to other organisations ($B = .385$, $p = .019$). Respondents that expected to experience an emotional impact had 1.469 higher odds of reporting to the other organisations than respondents that expected to experience no emotional impact. In addition, there was a significant relationship between reporting to other organisations and financial impact. Respondents that expected to experience less than €5,000 ($B = .858$, $p = < .001$), between €5,000 and €10,000 ($B = 1.333$, $p = < .001$), and more than €10,000 ($B = 1.581$, $p = < .001$) in costs had respectively 2.359, 3.792 and 4.862 higher odds of reporting to other organisations compared to respondents that expected to experience no financial impact. In addition, an annual turnover of more than €1,000,000 was statistically significant ($B = .853$, $p = .029$), which means that companies with this turnover had 2.347 higher odds compared to companies with an annual turnover of less than €500,000. Lastly, there was a statistically significant relationship between cyber insurance and reporting to other organisations ($B = 1.513$, $p = < .001$). Respondents with a cyber insurance had 4.539 higher odds of reporting

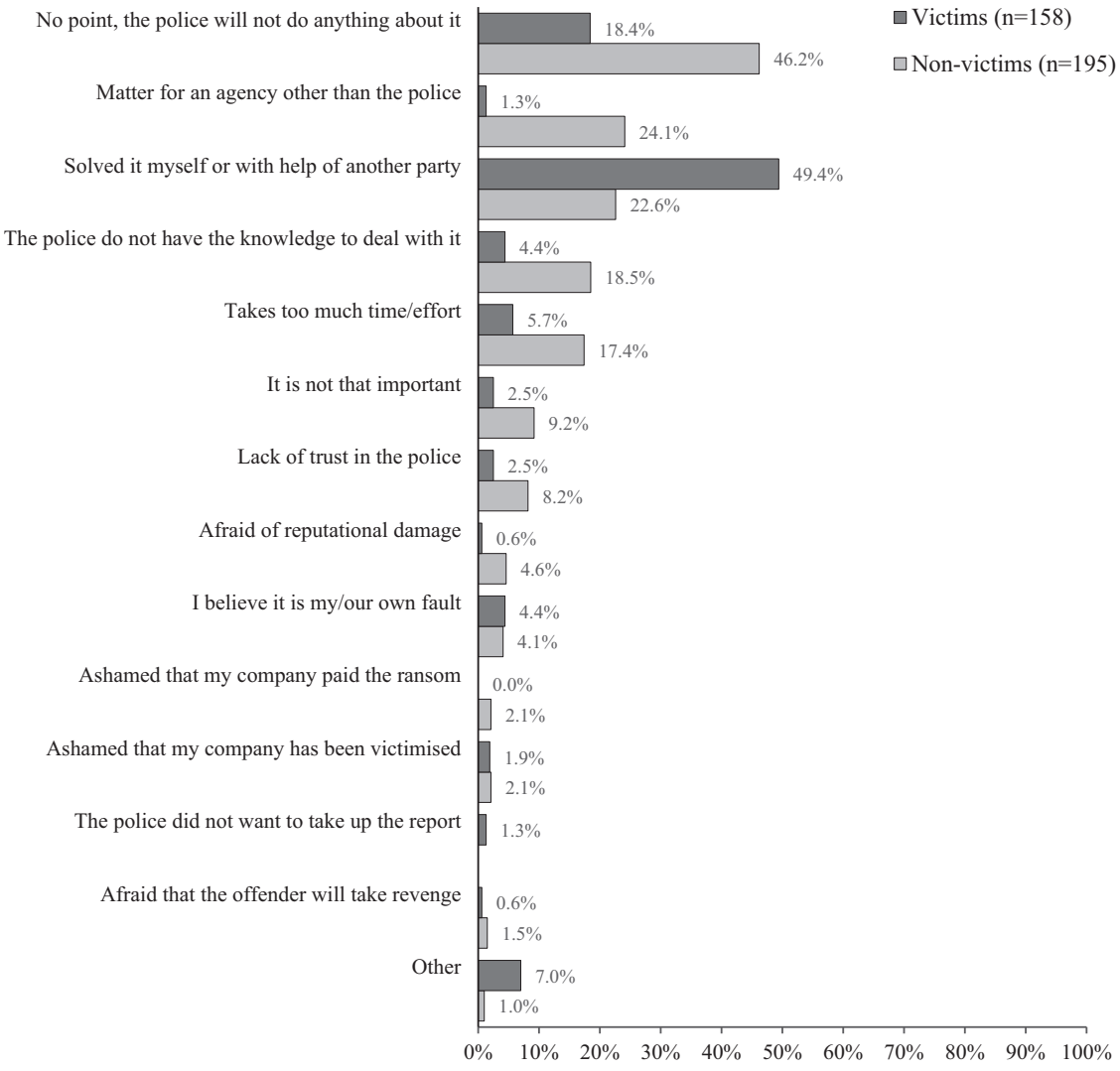

Fig. 5. Motivations for not reporting ransomware victimisation to the police.
Respondents that were previously victimised were asked to select the most important reason and could only select one option, whereas respondents that were not previously victimised could give multiple responses.
The option "The police did not want to take up the report" was solely given to victims.

to other organisations compared to respondents that were not insured against cyber incidents. The variables ransom demand (B = -.108, p = .447), likelihood of ransom being paid (B = .010, p = .804), back-up (B = -.237, p = .094), double extortion (B = -.051, p = .721), advised to pay (B = .094, p = .508) and negative affective response (B = .396, p = .128) were not statistically significant.

In summary, for non-victims the intention to report to the police and other organisations is related to the emotional and financial impact. In addition, the intention to report to other organisations is also related to annual turnover and having cyber insurance.

5. Discussion

Despite extensive research on reporting of traditional crime, research on cybercrime reporting, particularly ransomware, is still in its infancy. The current study examined the reporting behaviour of freelancers and SMEs in the Netherlands following victimisation of ransomware, and the factors and motivations associated with this decision. In order to do so, a survey was conducted among 189 entrepreneurs who were previously victimised by ransomware, to measure actual reporting behaviour, and a survey with a vignette experiment was conducted among 2,496 entrepreneurs who were not previously victimised by ransomware, to measure their intention to report. The results indicate underreporting of ransomware, particularly to the police, and discrepancies between the reporting behaviour of victims and intention to report among non-victims that were presented with a hypothetical scenario.

Most victims contacted at least one organisation, in most cases a cybersecurity company, followed by the police and Fraud Help Desk. Less than one out of five the victims contacted the police, and of those, just one in four filed an official report. These results are in line with previous research that stipulates that few entrepreneur contact the police after ransomware victimisation (European Commission, 2022;Statistics Netherlands, 2023; Van de Weijer, Leukfeldt, & Van der Zee, 2020; Voce & Morgan, 2022) and that many victims (also) seek help or advice from parties other than the police (Statistics Netherlands, 2023; Van de Weijer, Leukfeldt, & Van der Zee, 2020; Voce & Morgan, 2022). In contrast, almost all of the non-victims that were presented with a vignette expressed a high intention to report to the police, followed by financial institutions and the Fraud Help Desk. This divergence between actual reporting behaviour and intended reporting behaviour in a hypothetical scenario is in line with previous studies (European Commission, 2022; Van de Weijer, Leukfeldt, & Van der Zee, 2020). While this

Table 3
Logistic regression on reporting ransomware victimisation among victims (n=150)

	Model 1: Report to police			Model 2: Report to other organisations		
Variable	**B**	**S.E.**	**Exp (B)**	**B**	**S.E.**	**Exp (B)**
(Constant)	-2.132	1.174	.119	-1.379	.887	.252
Ransom paid (0-1)	-.909	1.362	.403	-1.444	.925	.236
Back-up (0-1)	-1.248	.904	.287	.264	.699	1.303
Double extortion (0-1)	1.068	.676	2.910	-.068	.620	.934
Negative affective response (0-1)	-.586	.642	.557	-.055	.532	.946
Emotional impact (0-1)	.015	.599	1.015	.984*	.474	2.676
Financial impact						
None (0-1)	REF			REF		
Less than €5,000 (0-1)	.952	.746	2.592	.528	.460	1.695
€5,000 - €10,000 (0-1)	1.047	1.170	2.849	2.676*	1.324	14.533
More than €10,000 (0-1)	2.760*	1.129	15.807	21.222	13,374.097	1,646,618,569.1
Company size						
Freelancer (0-1)	REF			REF		
Micro (0-1)	1.000	.674	2.717	1.296*	.554	3.654
Small (0-1)	-.146	.989	.864	2.325*	.958	10.229
Medium (0-1)	-18.472	28,335.500	.000	.126	1.756	1.134
Sector						
Agriculture/fishing (0-1)	.254	1.376	.1290	.145	1.050	1.156
Industry, construction and utilities (0-1)	-.170	1.066	.844	.709	.761	2.032
Trade and logistics, catering (0-1)	.548	.684	.1730	-.226	.598	.798
Government, education, healthcare, other (0-1)	1.014	.734	2.756	1.378*	.581	3.965
Financial and business services (0-1)	REF			REF		
Annual turnover						
Less than €500,000 (0-1)	REF			REF		
€500,000 - €1,000,000 (0-1)	1.044	.817	2.840	-.275	.808	.759
More than €1,000,000 (0-1)	.179	.889	1.196	-.119	.811	.888
Cyber insurance (0-1)	.976	.868	2.630	.999	1.180	2.716
χ^2 (18)	27.627			46.696***		
Cox & Snell R^2	.168			.268		
Nagelkerke R^2	.283			.370		
ROC-AUC	.761***			.820***		

*p< .05, **p< .01, ***<.001

difference could be the result of the way the vignette experiment was designed, it also possible that the findings demonstrate the existence of an intention-behaviour gap for reporting, i.e. the discrepancy between the intention to do something and actual behaviour (Sheeran & Webb, 2016). It is conceivable that entrepreneurs believe that the police is the right organisation to contact, but that there are barriers towards reporting in the event of victimisation.

Both victims and non-victims cited similar reasons for reporting to the police, primarily wanting the culprit to be caught, wanting to prevent it from happening to someone else, creating a safer (online) environment and believing it is their duty. These motivations largely correspond with the literature on reporting of traditional crime (Skogan, 1984; Tarling & Morris, 2010), as well as cybercrime (Van de Weijer, Leukfeldt, & Van der Zee, 2020; Veenstra, Zuurveen, & Stol, 2015; Voce & Morgan, 2022). Common reasons for both groups not to report included handling the problem themselves or with the help of another party, and the belief that there is no point because the police will not do anything about it, echoing previous findings in research on traditional reporting (Kidd & Chayet, 1984; Skogan, 1984) and cybercrime reporting (Cybbar & CSD, 2023; Graham et al., 2020; Kemp et al., 2023; Van de Weijer, Leukfeldt, & Van der Zee, 2020; Veenstra, Zuurveen, & Stol, 2015; Voce & Morgan, 2022; Wanamaker, 2019).

The study also examined the association between situational factors, a negative affective response and perceived impact and the likelihood of reporting ransomware victimisation to the police and other organisations. The findings showed that the emotional and financial impact is related to reporting to other organisations for victims, and related to both reporting to the police and other organisations for non-victims. This is in accordance with the economic and psychological perspectives on crime reporting, which state that serious crimes, often determined by the extent of physical, financial or psychological harm, are more likely to be reported (Gottfredson & Hindelang, 1979; Goudriaan, 2006; Greenberg & Ruback, 1992; Skogan, 1984; Tarling & Morris, 2010). At the same time, we did not find evidence that the affective reaction is related to this decision-making process, as stated in the psychological perspective (Goudriaan, 2006; Greenberg & Ruback, 1992). Furthermore, while we hypothesized that the seriousness of the crime may also be related to situational factors such as the ransom demand or threat of data being leaked, this was not the case. Combined with the fact that the victim model related to reporting to the police was not statistically significant and that the ability of the regression models for non-victims to discriminate between classes was only acceptable according to the ROC-curve, this may imply that factors beyond those included in this study could affect reporting behaviour. As we could only include a limited number of factors in the current study, other aspects were not taken into account. For example, the influence of the social environment as described in the psychological perspective (Greenberg & Ruback, 1992) or broader societal context as described in the sociological perspective (Black, 1976) were not included in this study. In addition, other costs and benefits related to the economic perspective were not included, such as attitudes towards the police or criminal justice system, fear of disapproval or further victimisation, or moral considerations (Kidd & Chayet, 1984; Tarling & Morris, 2010; Xie & Baumer, 2019). Future research could look into other factors that are associated with the decision to report ransomware victimisation.

Several limitations should be taken into account while interpreting the results. For one, differences in reporting between victims and non-victims may be the result of the way the vignette experiment was designed. In order for a vignette experiment to be effective, vignettes need to be as realistic as possible (Aguinis & Bradley, 2014; Baguley et al., 2022). Although realistic elements were included in the vignette design, such as a ransom message and a ransom website mimicked after real life examples, the vignette may not have fully immersed respondents. Moreover, victimisation of ransomware is a high-stake

Table 4
Logistic regression on intention to report ransomware victimisation among non-victims (n=1,635).

	Model 1: Report to police			Model 2: Report to other organisations		
Variable	**B**	**S.E.**	**Exp (B)**	**B**	**S.E.**	**Exp (B)**
(Constant)	1.017*	.412	2.765	-.033	.338	.968
Ransom demand (0-1)	.351	.189	1.420	-.108	.143	.897
Likelihood of ransom being paid (0-10)	.095	.058	1.100	.010	.041	1.010
Back-up (0-1)	-.091	.185	.913	-.237	.141	.789
Double extortion (0-1)	-.323	.186	.724	-.051	.141	.951
Advised to pay (0-1)	-.185	.186	.831	.094	.143	1.099
Negative affective response (0-1)	.475	.306	1.608	.396	.260	1.485
Emotional impact (0-1)	.421*	.206	1.524	.385*	.164	1.469
Financial impact						
None (0-1)	REF			REF		
Less than €5,000 (0-1)	.645*	.284	1.906	.858***	.223	2.359
€5,000 - €10,000 (0-1)	.725*	.356	2.065	1.333***	.295	3.792
More than €10,000 (0-1)	1.255**	.403	3.507	1.581***	.322	4.862
Company size						
Freelancer (0-1)	REF			REF		
Micro (0-1)	-.030	.261	.970	.161	.214	1.175
Small (0-1)	-.113	.461	.893	-.335	.438	.715
Medium (0-1)	-.048	1.107	.953	.261	1.104	1.298
Sector						
Agriculture/fishing (0-1)	-.217	.471	.805	-.350	.392	.705
Industry, construction and utilities (0-1)	.492	.379	1.636	.201	.280	1.223
Trade and logistics, catering (0-1)	.533	.339	1.704	.091	.247	1.095
Government, education, healthcare, other (0-1)	.135	.215	1.144	.070	.163	1.072
Financial and business services (0-1)	REF			REF		
Annual turnover						
Less than €500,000 (0-1)	REF			REF		
€500,000 - €1,000,000 (0-1)	-.239	.394	.787	.035	.337	1.035
More than €1,000,000 (0-1)	.010	.387	1.010	.853*	.390	2.347
Cyber insurance (0-1)	-.398	.257	.672	1.513***	.356	4.539
χ^2 (20)	45.084**			116.435***		
Cox & Snell R^2	.027			.069		
Nagelkerke R^2	.063			.118		
ROC-AUC	.661***			.701***		

*p< .05, **p< .01, ***<.001

scenario, which can only be mimicked to a certain extent in a vignette experiment (Aguinis & Bradley, 2014). Although respondents were given an impression of the stakes (such as the cost of the ransom or the imminent loss of data) and the sense of urgency due to a running timer, it was clear to respondents at all times that this was a hypothetical scenario. As a result, it is conceivable that the vignette did not create the same context as in 'real life', potentially generating a different response (Aguinis & Bradley, 2014) and raising questions about the suitability of using a vignette experiment in the context of ransomware victimisation. At the same time, these differences could also signify an intention-behaviour gap for reporting, as previously discussed. In this respect, future research could look into explanations for the difference between the intention to report crime and actual reporting behaviour.

In addition to possible limitations in the design of the vignette, another limitation of this study is that fact that the majority of the entrepreneurs were victimised more than 12 months ago. As a result, there could be a recall bias due to not fully or correctly recalling characteristics of the incident. In addition, changes in both the modus operandi of ransomware and the law enforcement response over the years may also mean that past experiences and behaviour of victims don't fully represent current experiences. In future research, it would be beneficial to measure victimisation shortly after the incident for more valid responses.

Furthermore, underrepresentation of freelancers and the sectors industry, construction and utilities, and trade, logistics and catering in the sample, means that the results may not be generalisable to the general population of freelancers and SMEs in the Netherlands. Similarly, although the reporting rates in the current study are similar to findings in international studies, caution should be exercised in generalizing results to other countries. While some of the motivations and factors included the current study are most likely not country-specific, such as having a back-up, double extortion, or the experienced impact, other aspects such as general attitudes towards paying the ransom or attitudes towards the police (as included in the motivations) might be. For example, confidence in the police differs across countries. While the level of confidence in the police is relatively high in The Netherlands and seems comparable to countries such as Germany, Austria or the United States, other countries exhibit lower (e.g. Bulgaria, Croatia) or higher (e.g. Finland, Denmark, Australia, New Zealand) levels of confidence in the police (Choi & Kruis, 2021), which may affect reporting decisions. Furthermore, while reporting processes were beyond the scope of the current study, it must be noted that the way ransomware can be reported may vary across countries. For instance, in The Netherlands it is currently not possible for entrepreneurs to report ransomware victimisation online, which could be a barrier towards reporting, while this might be the case in other countries.

Lastly, it should be noted that some of the coefficients and odds ratios in the logistic regression models for victims were extremely high, indicating separation. In particular, this was the case for a financial impact of more than €10.000 and medium company size, likely due to a small number of observations for these categories. We decided not to omit or collapse categories as to not lose information or introduce bias. However, this should be taken into account while viewing the results of the victim sample.

Despite its limitations, this study has given additional insights into reporting behaviour after ransomware victimisation. It highlights, for instance, that victims often look beyond the police for assistance, possibly due to a lack of confidence in law enforcement's ability to deal with ransomware. This underscores that the willingness to report should be improved. Enhancing public awareness on the value of reporting for

victims and society (e.g. by providing information on the website of the police, sharing "success stories" of police actions or through campaigns) and providing a unified message across all relevant organisations may encourage reporting. At the same time, it is important for the police to manage expectations about their capabilities. For instance, the results show that some victims reported to the police because they wanted the perpetrator to be caught, while for ransomware this need cannot always be met. A mandatory reporting requirement, as explored in Germany and the UK (Martin, 2024) could also be explored, although this requires careful consideration of the legal possibilities, and potential impact on victims and law enforcement capacity.

Funding

This work was supported by the research programma Police & Science of the Netherlands Police Academy.

CRediT authorship contribution statement

Sifra R. Matthijsse: Writing – review & editing, Writing – original draft, Project administration, Methodology, Funding acquisition, Formal analysis, Data curation, Conceptualization. **M. Susanne van't Hoff-de Goede:** Writing – review & editing, Writing – original draft, Supervision, Project administration, Methodology, Funding acquisition, Data curation, Conceptualization. **E. Rutger Leukfeldt:** Writing – review & editing, Writing – original draft, Supervision, Project administration, Methodology, Funding acquisition, Data curation, Conceptualization.

Declaration of competing interest

The authors have no conflicts of interest to declare.

Appendix

Table A.1
Distribution of vignettes across respondents (n=2,496).

Group	Vignette				Distribution	
	Ransom demand	Advised to pay	Back-up	Double extortion	N	%
1	1% of annual turnover	No	No	Yes	162	6.5%
2	1% of annual turnover	No	Yes	Yes	164	6.6%
3	1% of annual turnover	Yes	No	Yes	156	6.3%
4	1% of annual turnover	Yes	Yes	Yes	160	6.4%
5	25% of annual turnover	No	No	Yes	150	6%
6	25% of annual turnover	No	Yes	Yes	157	6.3%
7	25% of annual turnover	Yes	No	Yes	161	6.5%
8	25% of annual turnover	Yes	Yes	Yes	146	5.8%
9	1% of annual turnover	No	No	No	156	6.3%
10	1% of annual turnover	No	Yes	No	157	6.3%
11	1% of annual turnover	Yes	No	No	150	6%
12	1% of annual turnover	Yes	Yes	No	155	6.2%
13	25% of annual turnover	No	No	No	156	6.3%
14	25% of annual turnover	No	Yes	No	154	6.2%
15	25% of annual turnover	Yes	No	No	161	6.5%
16	25% of annual turnover	Yes	Yes	No	151	6%

References

Aguinis, H., & Bradley, K. J. (2014). Best Practice Recommendations for Designing and Implementing Experimental Vignette Methodology Studies. *Organizational Research Methods, 17*(4), 351–371. https://doi.org/10.1177/1094428114547952

Akkermans, M., Arends, J., Derksen, E., & Reep, C. (2023). Online veiligheid en criminaliteit 2022 (pp. 1–71). Statistics Netherlands. https://www.cbs.nl/-/media/_pdf/2023/19/online-veiligheid-en-criminaliteit-2022.pdf.

Baguley, T., Dunham, G., & Steer, O. (2022). Statistical modelling of vignette data in psychology. *British Journal of Psychology, 113*, 1143–1163. https://doi.org/10.1111/bjop.12577

Baumer, E. P., & Lauritsen, J. L. (2010). Reporting crime to the police, 1973-2005: A multivariate analysis of long-term trends in the National Crime Survey (NCS) and National Crime Victimization Survey (NCVS). *Criminology, 48*(1), 131–185.

Black, D. (1976). *The Behavior of Law*. Academic Press.

Borwell, J., Jansen, J., & Stol, W. (2025). Exploring the impact of cyber and traditional crime victimization: Impact comparisons and explanatory factors. *International Review of Victimology, 31*(1), 156–181. https://doi.org/10.1177/02697580241282782

Choi, J., & Kruis, N. E. (2021). Social integration and confidence in the police: A cross-national multi-level analysis. *Policing and Society, 31*(6), 751–766. https://doi.org/10.1080/10439463.2020.1751160

Cybbar & CSD. (2023). *Cybercrime against businesses in the EU: Challenges to Reporting [Policy Brief] (pp. 1–4)*. https://cybbar.eu/wp-content/uploads/2023/01/CYBBAR-Policy-Brief_EN.pdf.

Dugato, M., Favarin, S., Hideg, G., & Illyes, A. (2013). *The crime against businesses in Europe: A pilot survey (pp. 1-131). The Gallup Organisation/Transcrime*. https://www.transcrime.it/wp-content/uploads/2013/11/1EU-BCS-final-report_galluptranscrime-executive_summary-1.pdf.

European Commission. (2022). *Flash Eurobarometer 496—SMEs and cybercrime*. https://doi.org/10.2837/89101

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023: July 2022 to June 2023*. Publications Office. https://data.europa.eu/doi/10.2824/782573.

Europol (2024). Internet Organised Crime Threat Assessment (IOCTA). (pp. 1–37). https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf.

Gottfredson, M. R., & Gottfredson, D. M. (1988). The Victim's Decision to Report a Crime. In M. R. Gottfredson, & D. M. Gottfredson (Eds.), *Decision Making in Criminal Justice (pp. 15–46)*. Springer US. https://doi.org/10.1007/978-1-4757-9954-5_2.

Gottfredson, M. R., & Hindelang, M. J. (1979). A Study of the Behavior of Law. *American Sociological Review, 44*(1), 3–18. https://doi.org/10.2307/2094813

Goudriaan, H. (2006). *Reporting crime: Effects of social context on the decision of victims to notify the police* [Doctoral dissertation]. Leiden University

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

Greenberg, M. S., & Ruback, R. B. (1992). *After the Crime*. Springer US. https://doi.org/10.1007/978-1-4615-3334-4

Home Office. (2024). *Crime against businesses: Findings from the 2023 Commercial Victimisation Survey*. Home Office. https://www.gov.uk/government/statistics/crime-against-businesses-findings-from-the-2023-commercial-victimisation-survey/crime-against-businesses-findings-from-the-2023-commercial-victimisation-survey#:~:text=2.-,Prevalence%20of%20crime,compared%20with%20last%20year's%20survey.&text=The%20CVS%20measures%20a%20specific%20set%20of%20crimes%20against%20businesses.

Hosmer, D. W., & Lemeshow, S. (2000). *Applied logistic regression* ((2nd ed.). John Wiley & Sons.

Ipsos I&O. (n.d.). Onderzoeksmethoden. Retrieved 10 October 2024, from https://www.ipsos-publiek.nl/onderzoeksmethodes/.

Isenring, G. L., Mugellini, G., & Killias, M. (2016). The willingness to report employee offences to the police in the business sector. *European Journal of Criminology, 13*(3), 372–392. https://doi.org/10.1177/1477370815623569

Johns, E. (2021). *Cyber Security Breaches Survey 2021 (pp. 1-63)*. Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021.

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

Kennedy, J. P. (2016). Shedding Light on Employee Theft's Dark Figure: A Typology of Employee Theft Nonreporting Rationalizations. *Organization Management Journal, 13*(1), 49–60. https://doi.org/10.1080/15416518.2015.1110513

Kidd, R. F., & Chayet, E. F. (1984). Why Do Victims Fail to Report? The Psychology of Criminal Victimization. *Journal of Social Issues, 40*(1), 39–50. https://doi.org/10.1111/j.1540-4560.1984.tb01081.x

de Kimpe, L. (2020). *The Human Face of Cybercrime: Identifying targets, victims, and their coping mechanisms* [Doctoral dissertation]. Universiteit van Antwerpen/Ghent University

Leukfeldt, R., & Holt, T. J. (Eds.). (2020). *The human factor of cybercrime*. Routledge.

Leukfeldt, R., Notté, R., & Malsch, M. (2018). *Slachtofferschap van online criminaliteit: Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit (pp. 1-186). Netherlands Institute for the Study of Crime and Law Enforcement.* https://repository.wodc.nl/bitstream/handle/20.500.12832/2355/2839_Volledige_Tekst_tcm28-368216.pdf?sequence=1&isAllowed=y.

Martin, A. (2024, May 21). Exclusive: UK to propose mandatory reporting for ransomware attacks and licensing regime for all payments. In *The Record*. https://therecord.media/uk-proposal-mandatory-reporting-ransomware-attacks.

Matthijsse, S. R., Moneva, A., Van't Hoff-de Goede, M. S., & Leukfeldt, E. R. (2024). Examining ransomware payment decision-making among small and medium-sized enterprises. *European Journal of Criminology, 0*(0), 1–21. https://doi.org/10.1177/14773708241285671

Matthijsse, S. R., Van 't Hoff-de Goede, M. S., & Leukfeldt, E. R. (2025). *[Forthcoming]. Onderhandelen, betalen en melden na slachtofferschap van ransomware: Een mixed methods onderzoek naar de factoren die bijdragen aan beslissingsgedrag van burgers en ondernemers*. The Hague University of Applied Sciences.

Sheeran, P., & Webb, T. L. (2016). The Intention–Behavior Gap. *Social and Personality Psychology Compass, 10*(9), 503–518. https://doi.org/10.1111/spc3.12265

Simoiu, C., Gates, C., Bonneau, J., & Goel, S. (2019). 'I was told to buy a software or lose my computer. I ignored it': A study of ransomware. In *USENIX Symposium on Usable Privacy and Security (SOUPS)* (pp. 155–174).

Skogan, W. G. (1984). Reporting Crimes to the Police: The Status of World Research. *Journal of Research in Crime and Delinquency, 21*(2), 113–137.

Smith, R. G. (2008). Coordinating individual and organisational responses to fraud. *Crime, Law and Social Change, 49*(5), 379–396. https://doi.org/10.1007/s10611-008-9112-x

Statistics Netherlands. (2023). *Cybersecuritymonitor 2022 (pp. 1-65). Statistics Netherlands*. https://www.cbs.nl/-/media/_pdf/2023/31/cybersecuritymonitor_2022.pdf.

Statistics Netherlands. (2024). *Bedrijven; bedrijfsgrootte en rechtsvorm* [Dataset]. *StatLine*. https://opendata.cbs.nl/#/CBS/nl/dataset/81588NED/table?dl=AEB16.

Tarling, R., & Morris, K. (2010). Reporting Crime to the Police. *British Journal of Criminology, 50*(3), 474–490. https://doi.org/10.1093/bjc/azq011

Taylor, N. (2002). Under-Reporting Of Crime Against Small Businesses: Attitudes Toward Police And Reporting Practices. *Policing and Society, 13*(1), 79–89. https://doi.org/10.1080/1043946032000050562

Tolsma, J., Blaauw, J., & te Grotenhuis, M. (2012). When do people report crime to the police? Results from a factorial survey design in the Netherlands, 2010. *Journal of Experimental Criminology, 8*(2), 117–134. https://doi.org/10.1007/s11292-011-9138-4

Van de Weijer, S. G. A., Leukfeldt, E. R., & Van der Zee, S. (2020). *Slachtoffer van online criminaliteit, wat nu? Een onderzoek naar de aangiftebereidheid onder burgers en ondernemers* (pp. 1–102). SDU Uitgevers. https://www.politieenwetenschap.nl/publicatie/politiewetenschap/2020/slachtoffer-van-onlinecriminaliteit-wat-nu-356/.

Van de Weijer, S. G. A., Leukfeldt, E. R., & van der Zee, S. (2021). Cybercrime Reporting Behaviors Among Small- and Medium-Sized Enterprises in the Netherlands. In M. Weulen Kranenbarg, & R. Leukfeldt (Eds.), *Cybercrime in Context. Crime and Justice in Digital Society* (1st ed., pp. 303–325). Springer. https://doi.org/10.1007/978-3-030-60527-8_17.

Van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology, 16*(4), 486–508. https://doi.org/10.1177/1477370818773610

Veenstra, S., Zuurveen, R., & Stol, W. (2015). *Cybercrime onder bedrijven Een onderzoek naar slachtofferschap van cybercrime onder het Midden-en Kleinbedrijf en Zelfstandigen Zonder Personeel in Nederland* (pp. 1–242). NHL Hogeschool/Politieacademie/Open Universiteit. https://cybersciencecenter.nl/media/1054/2015-05-13-cybercrime-onder-bedrijven-def.pdf.

Voce, I., & Morgan, A. (2021). Ransomware victimisation among Australian computer users. *Statistical Bulletin, 35*, 1–17. https://doi.org/10.52922/sb78382

Voce, I., & Morgan, A. (2022). Help-seeking among Australian ransomware victims. *Statistical Bulletin, 38*, 1–13. https://doi.org/10.52922/sb78504

Walker, J.R. (1994). *The first Australian national survey of crimes against businesses* (1. publ) (pp. 1-134). Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2020-05/first-australian-national-survey-crimes-against-businesses.pdf.

Wanamaker, K. A. (2019). *Profile of Canadian businesses who report cybercrime to police: The 2017 Canadian Survey of Cyber Security and Cybercrime* (pp. 1–15). Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2019-r006/2019-r006-en.pdf.

Xie, M., & Baumer, E. P. (2019). Crime Victims' Decisions to Call the Police: Past Research and New Directions. *Annual Review of Criminology, 2*(1), 217–240. https://doi.org/10.1146/annurev-criminol-011518-024748