Cybercrime Reporting Behaviors Among Small- and Medium-Sized Enterprises in the Netherlands

Steve van de Weijer[1], Rutger Leukfeldt[12], Sophie van der Zee[3]

[1] Netherlands Institute for the Study of Crime and Law Enforcement (NSCR)

[2] Centre of Expertise Cybersecurity, The Hague University of Applied Sciences

[3] Applied Economics, Erasmus University Rotterdam

Preprint

First Online: 04 May 2021

Final paper: https://link.springer.com/chapter/10.1007/978-3-03

To cite:

Van de Weijer S.G.A., Leukfeldt R., Van der Zee S. (2021). Cybercrime Reporting Behaviors Among Small- and Medium-Sized Enterprises in the Netherlands. In: *Weulen Kranenbarg M., Leukfeldt R. (eds) Cybercrime in Context. Crime and Justice in Digital Society*, vol I. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-60527-8_17.

Corresponding author: Steve van de Weijer, Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), svandeweijer@nscr.nl.

Abstract:

Despite the high prevalence of cybercrime victimization among businesses, only few of these crimes are reported to the police. This study used a sample of 529 Dutch small- and medium enterprise (SME) owners, to examine which characteristics of the offence, the SME, and the SME-owner predict cybercrime reporting behaviors. Moreover, the motives to either report cybercrime victimization to the police or not, were examined. All respondents were shown three vignettes about fictional cybercrime incidents, and were asked how they would react in this situation. Next, they were also asked about their reporting behaviors after actual cybercrime victimization. The large majority of SME-owners said that they would report the incidents from the vignettes to the police, but after actual victimization only 14.1 percent of the cybercrimes was reported to the police. Seriousness and type of offense were the best predictors for cybercrime reporting, with cyber-enabled crimes being more often reported to the police than cyber-dependent crimes. Characteristics of the SME and the SME-owner were often not related to reporting behaviors. Victims report cybercrime to the police because they want the perpetrator to be caught and to prevent him from doing the same to others, and they do not report cybercrimes because they think the police will not do anything and rather solve it themselves. When victims did report their victimization to the police, they were often unsatisfied because the police were indifferent and because the problems were not solved. Implications of these results for practice and future research are discussed.

Keywords: cybercrime, reporting, businesses, police, SME

Introduction

While society is facing an ongoing digitalization, also the risk of cybercrime victimization has increased, for both citizens and businesses. In the Netherlands, the country on which the current study focuses, 13 percent of the citizens reported that they were a victim of cybercrime in 2019. Online consumer fraud and hacking have even become the two most common types of crime in the Netherlands, with victimization rates of 4.6 and 5.5 percent, respectively (Dutch Statistics, 2020a). Victimization rates are even higher among businesses: Veenstra and colleagues (2015) found that about 28 percent of small and medium-sized enterprises (SME) were confronted with cybercrime in a period of twelve months.

Despite this high prevalence of cybercrime victimization, only few of these crimes are reported to the police. Only 13 percent of Dutch citizens who were a cybercrime victim in 2019 reported their victimization to the police (Dutch Statistics, 2020a), while only 7.2 percent was reported to the police by SMEs (Veenstra et al., 2015). Similar low reporting rates were found in other countries. Wanamaker (2019), for example, showed that among Canadian businesses who were victimized by cybercriminals only 8.4 and 12.5 percent of, respectively, small- and medium-sized businesses reported these incidents to the police.

It is, however, important for police and law enforcement that victims report crimes to the police, as it is usually necessary to start a criminal investigation into the offenders. Moreover, knowledge on the trends and prevalence of different types of crime can help to identify the most urgent problems, to more effectively allocate resources, and to form better policies. Therefore, it is also crucial to gain more knowledge about the determinants and motives for cybercrime reporting behaviors in order to be able to increase these reporting behaviors.

The vast majority of empirical studies on crime reporting behaviors of victims have focused solely on traditional types of crime (see e.g., Goudriaan, 2006 for an overview).

Recently, a couple of studies did focus specifically on the determinants and motives for reporting cybercrime victimization to the police (Graham, Kulig & Cullen, 2020; Jong, Leukfeldt & Van de Weijer, 2018; Van de Weijer, Leukfeldt & Bernasco, 2019; Van de Weijer, Leukfeldt & van der Zee, 2020), while other, more qualitative studies, focused on the experiences of cybercrime victims with reporting these crimes to the police (e.g., Cross, Richards & Smith, 2016; Leukfeldt, Notté & Malsch, 2019). However, these studies only examined crime reporting behaviors among citizens and still little is known about the determinants and motives of cybercrime reporting among business-owners. Their reactions after cybercrime victimization might differ from those of citizens, for example because they might have employees responsible for cybersecurity, might be afraid for reputation loss, and are legally obliged to notify the Dutch Data Protection Authority in case of a data breach. Therefore, the current study will focus on reporting behaviors of Dutch SME-owners after cybercrime victimization.

Literature review

Two theoretical perspectives that are often used to explain crime reporting behaviors are the economic and psychological perspective (Goudriaan, 2006). According to the economic perspective, victims will report crime when the costs of crime reporting (e.g., time and effort) are smaller than the benefits of crime reporting (e.g., retrieving stolen goods, compensation by offender or insurance company). Based on this perspective it can be expected that crime reporting is more likely for more serious offenses (e.g., with more financial damage) and when the time and effort to report crime is limited. In addition, also psychological factors, such as feelings of shame or guilt and the relationship between offender and victim, might play a role as well. In case the victim knows the offender personally there could be empathy, and the crime may not be reported to avoid negative consequences for the offender. Moreover, dozens of studies have shown that several demographic variables are associated with crime reporting

behaviors after victimization of traditional types of crime (see e.g., Goudriaan, 2006; Slocum et al., 2010; Torrente, Gallo & Oltra, 2017).

Much less is known, however, about crime reporting behaviors after cybercrime. Recently, Van de Weijer and colleagues (2019) used data on 97.186 Dutch victims to examine whether such characteristics also predicted crime reporting behaviors of cybercrime victims. They found that male victims were more likely to report cybercrimes to the police, while female victims more often reported traditional crimes. Moreover, a higher income was positively related with reporting traditional offenses to the police, but a negative association was found with reporting cybercrime. Neighborhood characteristics, such as social cohesion, nuisance, and safety in neighborhoods, did not predict the reporting of cybercrime to the police, while they were associated with the reporting of traditional crimes. Although victims of cybercrime did not often report their victimization to the police, Van de Weijer and colleagues (2019) showed that they were more likely to report it to other organizations than the police.

Graham et al. (2020) and Jong et al. (2018) both used vignette techniques to study respondents' willingness to report cybercrime. Graham and colleagues analyzed the intentions of 534 American respondents to report five types of traditional crime and five types of cybercrime to the police. Their results showed that respondents were more willing to report traditional crimes to the police than cybercrimes. Among the cybercrimes, reporting intentions were higher in case of identity theft and online death threats than in case of hacking and unwanted sexual comments or contacts. The demographic variables associated with this willingness to report crime, however, were the same for traditional crime and cybercrime. Younger, black, female, and married respondents were more likely to report victimization of both cybercrimes and traditional crimes to the police, compared to older, white, male, and unmarried respondents.

In the vignette study of Jong and colleagues (2018), 175 students of a Dutch University were asked about their willingness to report victimization of hacking, online consumer fraud, and malware to the police. They found that respondents were most willing to report victimization of consumer fraud to the police, while they were least willing to report malware infections. Also more serious offenses were found to be more likely to be reported to the police. The different ways in which the respondents could report their victimization to the police (police station, phone, internet, smartphone app) as well as the respondents' age, gender, and attitudes towards the police were not related to their willingness to report cybercrime victimization.

Van de Weijer, Leukfeldt and Van der Zee (2020) measured both intentions to report cybercrime victimization and actual reporting behavior by asking Dutch respondents both how they would act in fictional situations and about their previous reactions after victimization. They found a large discrepancy between intended and actual reporting behaviors: most respondents indicated that they would report the situations in the vignettes to the police, while they almost never went to the police when they actually became the victim of cybercrime. Moreover, their results showed that type of crime and the seriousness of the offenses were the best predictors of crime reporting, while almost all relationships with demographic characteristics of respondents were not significant.

The abovementioned studies, however, all focused solely on citizens. Less is known about the reporting behaviors of businesses that were the victim of cybercrime. Veenstra and colleagues (2015) showed that the large majority of Dutch businesses do not report cybercrime victimization to the police. Only 7.2 percent of the SMEs and 13.0 percent of the individual entrepreneurs in their sample contacted the police, and in most cases this did not result into an official complaint. However, more than 60 percent of these business-owners expressed the intentions to report future cybercrime victimization to the police.

Wanamaker (2019) found that less than ten percent of Canadian businesses that became a victim of cybercrime, reported an incident to the police. These reporting rates were positively related to business size: small businesses reported cybercrime victimization (8.4%) less often than medium (12.5%) and large (15.0%) businesses. Moreover, businesses that put in place risk management protocols and that offered formal training to employees were more likely to report cybercrime victimization to the police, while businesses that share best practices with their employees were less likely to report their cybercrime victimization.

These Canadian businesses most often did not report to the police because the incidents were already resolved internally or through an IT consultant and because it was too minor of an incident (Wanamaker, 2019). Veenstra and colleagues (2015) also found that most Dutch businesses solved the problems themselves and that they did not report to the police because there was no damage, it was not that important, or because they did not expect the police to act upon the report. Most mentioned reasons to report cybercrime victimization to the police, on the other hand, were because Dutch business-owners want the perpetrator to get caught and because they consider it their duty to report it to the police (Veenstra et al., 2015).

The current study

Despite these previous studies on cybercrime reporting, still little is known about the characteristics of cybercrimes, businesses, and their owners that are associated with reporting cybercrime victimization to the police. Therefore, the current study focuses on this topic by asking owners of Dutch SMEs about their intended reporting behaviors, using a vignette design, and, if applicable, about their actual reporting behaviors after victimization of their company or personal victimization. Moreover, these SME-owners will be asked about their reasons to either report or not and, if applicable, about their past experiences when reporting cybercrime to the police. The research question is threefold. First, to what extent do owners of SMEs report cybercrime victimization to the police or to other organizations? Second, which characteristics

of the offense, the SME, and the SME-owner predict cybercrime reporting behaviors? And third, what are the most important motives to either report cybercrime victimization to the police or not?

Methods

Sample

In order to examine the factors that play a role in reporting cybercrime victimization, a sample of 529 owners of SMEs from a research panel was used (response rate 40.1%). The sectors in which the SMEs were active were divided in six categories: Business and financial services (38.6% of the respondents), Government and healthcare (21.2%), Trade, transport and hospitality (9.6%), Construction, industry and energy (8.3%), Agriculture and fisheries (2.6%), and Culture recreation and other services (19.7%). Most SME-owners in the sample had a sole proprietorship (72.8%), while about one in five (20.8%) had a company with 2 to 9 working places, and the remaining 6.4 percent had ten or more working places, which is comparable to the distribution of business sizes among all Dutch businesses (Dutch Statistics, 2020b). Moreover, the SME-owners in our sample were, on average, older (57 years) and more often women (41%) than the total population of SME-owners in the Netherlands (46 years and 36% women; KVK, 2020)

Vignettes

In the first part of the questionnaire, all respondents were shown three vignettes about hypothetical cybercrime victimization and were asked to imagine that this situation happened to them and what they would do in such a situation. Figure 1 shows an example of such a vignette. Four crime and reporting characteristics were manipulated across the vignettes. First, the types of cybercrime varied between credit card fraud, online consumer fraud, malware, hacking, and DDoS-attacks. The second manipulation concerned the seriousness of the offense (more vs. less serious). For example, 100 euro or 1000 euro damage after credit card fraud. The

third manipulation concerned the relationship between victim and offender, varying between three categories: “you do not know who the perpetrator is”, “you know the perpetrator personally”, and “you do not know the perpetrator personally” (i.e., the identity of the perpetrator is known, but it is not an acquaintance of the victim). The fourth and final manipulation concerned the possibilities of reporting cybercrime to the police, as these likely influence the time and effort it takes to report the crime: “on the police station”, “over the phone or on the police station”, and “on the internet, over the phone or on the police station”. In sum, respondents answered question about 3 out of a possible 90 vignettes (5 types of cybercrime x 2 seriousness of crime x 3 victim-offender relationship x 3 reporting possibilities). Figures A1-A5 in the appendix summarize all possible vignettes.

****FIGURE 1 ABOUT HERE ***

Dependent variables

After reading each vignette respondents were asked whether or not they would report this cybercrime to the police. They could answer on a five-point scale ranging from 1 ‘Certainly not’ to 5 ‘Certainly’. Respondents who scored 4 or 5 on this scale where asked what their most important motive to report the crime to the police would be, while respondents who scored 1 or 2 where asked about the most important motive to not report the crime. Tables 2 and 3 show the list of motives respondents could choose from. Next, respondents were also asked on a five-point scale whether they would report this crime to another organization than the police. The respondents’ intentions to report the cybercrime to the police and to other organizations were used as the dependent variables in ordered logistic regression analyses, as these variables were measured on an ordinal scale.

Independent variables

The independent variables in this study include the four random factors from the vignettes, based on the economic (type of crime, seriousness of crime, and reporting modality) and

psychological perspective (victim-perpetrator relationship), as well as several demographic characteristics that previously have been found to be related to reporting behaviors of victims of traditional crime (see e.g., Goudriaan, 2006; Slocum et al., 2010; Torrente, Gallo & Oltra, 2017) and/or cybercrime (Van de Weijer et al., 2019). Since each respondent answered questions on three different vignettes, observations were clustered within respondents. Robust standard errors that take into account this clustering were therefore calculated in order to control for this violation of the assumption of independent observations.

The independent variables include, first of all, the *age* (*M*: 56.75; *SD*: 9.68) and *gender* (58.8% male) of the SME-owners, and the *sector* and *size* of the SMEs. Next, *marital status* was included with four different answer categories: single (15.7%), living together with a (marital) partner (71.3%), not living together with a (marital) partner (10.2%), and widowed (2.8%). The independent variable *parenthood* was measured using three categories: no children (25.9%), children not-living at home (41.4%), and children living at home (32.7%). *Educational level* was measured on an ordinal scale from 1 'primary school' to 7 'Master's degree or higher', with an average of 5.80 (*SD*: 1.28). The independent variable *income* was measured as the personal monthly income before taxes, divided in 12 categories ranging from 1 'no income' to 12 'More than 10.000 euro', with a mean of 5.88 (i.e., an income between 2000 and 4000 euro). Multiple imputation was used to estimate the income of 103 respondents (19.5%) who did not report their income, as this method leads to less-biased estimates with even high proportions of missing data (Lee & Huber, 2011). Moreover, respondents were also asked about *previous cybercrime victimization* (see also the next section). Based on the information from these questions a variable was computed with three categories: never a victim of cybercrime (42.2%), a victim of cybercrime but never reported it to the police (46.1%), and a victim of cybercrime and reported it to the police at least once (11.7%). *Satisfaction with the police* was measured using nine different items on police functioning in general (Dutch

Statistics, 2020a; see Table A1 in the Appendix). Respondents could answer on a five-point scale ranging from 1 ‘very unsatisfied’ to 5 ‘very satisfied’. These items had an excellent internal consistency as shown by the Cronbach’s alpha of 0.91. An independent variable indicating *fear for cybercrime victimization* was constructed based on eight items (Van ’t Hoff-de Goede et al., 2019) on which the respondents could answer with a five-point scale ranging from 1 ‘Totally disagree’ to 5 ‘Totally agree’ (see Table A2 in the Appendix). The internal consistency of these items was also good, as indicated by the Cronbach’s alpha of 0.87. Factor analyses were used to compute factor scores for all respondents on these two variables. Finally, IT-knowledge was measured by asking respondents which of the following statements applied most to them (Holt & Bossler, 2008): 1) ’I can use the Internet and commonly used software like Word and Excel, but I cannot solve computer problems myself’ (37.2%), 2) ‘I can use several software programs and solve some computer problems myself’ (52.9%), and 3) ‘I can use Linux and most other software programs and I can solve most computer problems myself’ (9.8%).

Self-reported victimization

In addition to the experimental vignette-study, respondents were also asked to self-report their victimization of ten types of cybercrimes (see Figure 2 for offense types). It is important to mention that, in contrast to the vignettes, this question does not specifically refer to victimization of the businesses of SME-owners but instead to victimization in general. It is therefore possible that the SME-owners also report cybercrimes that they experienced as a private person. In total, 306 respondents (57.8%) reported to have ever been a victim of 595 cybercrimes. The most prevalent types of cybercrimes were phishing (23.0%), malware (22.2%), and online consumer fraud (14.3%). For each type of cybercrime that victims had experienced, they were asked whether they reported the last incident to the police and/or to other organizations. In case the victim had never reported cybercrime victimization to the

police, they were asked what the most important motive was for not reporting their most recent incident to the police. If the victim had reported a cybercrime to the police at least once, they were asked for the most important motive to report the cybercrime.

Logistic regression analyses were used to examine the associations between reporting behavior and victim characteristics, since reporting to the police and to other organizations were operationalized as binary variables. As a respondent could have been a victim of multiple types of cybercrime, robust standard errors were again calculated to control for this clustering.

Results

Vignette study

In the first part of the analyses, the SME-owners intentions to report cybercrime victimization to the police and other organizations were analyzed using the data from the vignette study. The results from the vignette study show that more than two thirds of the respondents indicated that they were likely (18.7%) or very likely (50.9%) to report victimization to the police, while only few indicated that it was unlikely (10.1%) or very unlikely (7.1%) that they would report it to the police. The majority of the respondents also indicated that they were likely (21.6%) or very likely (38.1%) to report the cybercrime victimization to other organizations than the police, while only 11.1 and 7.8 percent, respectively, indicated that they were unlikely or very unlikely to do this.

In Table 1 the results of the ordered logistic regression analyses are displayed in which the intentions of the SME-owners to report cybercrime victimization to the police (Model 1) and other organizations (Model 2) were predicted. First of all, the results in Model 1 show that the intention to report cybercrime victimization to the police was the highest in the case of credit card fraud. The intentions to report the other types of cybercrime to the police were all significantly lower, with the respondents being the least likely to report online consumer fraud to the police. A significant effect was also found for the seriousness of the offense, showing

that the SME-owners had significantly higher intentions to report more serious cases of cybercrime to the police (B=1.12, p<.001). Moreover, the results show that respondents indicated that it would be significantly less likely that they reported the cybercrime to the police when the offender was someone they personally know (B=-0.45, p<.01), compared to when the offender was unknown. The number of possibilities to report victimization to the police, however, did not influence respondent's intentions of crime reporting.

The results in Model 1 further shows that the characteristics of the SME were unrelated to the cybercrime reporting intentions of the owner: for neither the sector nor the size of the SME significant results were found. Moreover, none of the demographic variables except age were significantly related to an increased likelihood of reporting cybercrime victimization. The association with age showed that older respondents more often indicated that they would report the cybercrime to the police. Moreover, previous cybercrime victimization was significantly related to the SME-owners' intentions to report cybercrime to the police. Those who had been a victim before but did never report this to the police had significantly less intentions to report their cybercrime victimization to the police than non-victims (B=-0.29, p<.05), while those who had been victimized before and had reported this to the police had significantly higher intentions to report cybercrimes to the police (B=0.70, p<.01). Satisfaction with the police, fear for cybercrime, and IT-knowledge were all unrelated to the reporting intentions of SME-owners.

Model 2 of Table 1 shows the results of the ordered logistic regression analyses in which reporting to other organizations than the police was predicted. The respondents were significantly more likely to report victimization of credit card fraud to other organizations than victimization of malware (B=-0.28, p<.05), but no significant differences were found in the comparisons with other types of crime. Similar to the results in Model 1, the seriousness of the offense and the relation with the offender did influence the intentions to report cybercrime

victimization to the police. These intentions were significantly higher in cases of more serious cybercrimes (B=0.34, p<.001) and when the offender was a stranger (B=0.20, p<.05), but significantly lower when the offender was someone they personally know (B=-0.56, p<.001). The possibilities to report cybercrime victimization to the police did not have an impact on how likely respondents said they were to report to other organizations.

Similar to the results in Model 1, the most characteristics of the SMEs and their owners were not significantly related to their intentions to report cybercrime victimization to other organizations. SME-owners in the sector 'Business and financial services' were only significantly more likely to report victimization to other organizations than those in the sector 'Trade, transport and hospitality' (B=-0.51, p<.05). Moreover, older and female SME-owners were found to be significantly more likely to indicate that they would report victimization to other organizations than younger (B=0.02, p<.05) and male SME-owners (B=0.32, p<.05). Model 2 further shows that those who previously reported cybercrime victimization to the police (B=0.57, p<.05), who had more fear for cybercrime victimization (B=0.21, p<.01), and had more IT-knowledge (B=0.34, p<.01) had significantly more intentions to report cybercrime victimization to other organizations.

****TABLE 1 ABOUT HERE****

Next, the respondents who indicated that they were (very) likely to report cybercrime victimization to the police were asked what the most important motive was to report to the police. Table 2 shows that, among all types of cybercrime, 'I want the perpetrator to be caught' and 'To prevent the perpetrator from doing this again to someone else' were the two most often reported motives. The motive 'To prevent this from happening to me again' was mentioned relatively often in cases of credit card fraud and hacking. Moreover, 'To create a safer online environment' was relatively often reported for the more technical types of cybercrime (i.e., malware, hacking, DDoS-attack), while 'To get the damage compensated' was relatively often the most important motive in cases of credit card fraud and online consumer fraud.

TABLE 2 ABOUT HERE

The SME-owners who indicated that they were not (very) likely to report the cybercrimes from the vignettes to the police were asked for their most important motive to not report the cybercrime to the police. Table 3 shows that the motives 'I will solve it myself' and 'There is no point, the police will not do anything about it' were most often reported. The motive 'It takes too much effort' was relatively often reported in the case of online consumer fraud and DDoS-attacks, while also the motives 'It is not that important' and 'The police does not have the knowledge to tackle this type of crime' were relatively often chosen in the case of DDoS-attacks. Moreover, after vignettes about credit card fraud and malware, respondents relatively often chose the motive 'The police is not responsible for solving this type of crime', while 'I think it is actually my own fault' was relatively often mentioned as a motive after the hacking vignette.

TABLE 3 ABOUT HERE

Self-reported victimization

Next, the SME-owners' actual reporting behavior after cybercrime victimization was analyzed using the self-reported data. In total, 306 SME-owners indicated that they had ever been the victim of a cybercrime. As it was possible to report the victimization of multiple types of cybercrime, a total of 595 cybercrimes were examined. Figure 2 shows how many of the respondents reported each type of cybercrime to the police, or another organization. In total, 14.1 percent of the cybercrimes was reported to the police and 32.3 percent (also) to other organizations, such as banks, credit card companies, online marketplaces and helpdesks. Among the specific types of cybercrime, identity fraud (50%), online consumer fraud (28.2%), and cyberstalking (18.8%), were most often reported to the police. Malware infections (5.3%) and DDoS-attacks (7.1%), on the other hand, were the offenses that were the least likely to be reported to the police. Moreover, victims of identity fraud (55.0%), phishing (49.6%), and online consumer fraud (37.6%) most often reported their victimization to other organizations than the police, while this was the least often done by victims of cyberstalking (12.5%) and online threats (13.7%). It is, however, important to note that some of these percentages are based on a small number of victims, and should be interpreted with some caution.

FIGURE 2 ABOUT HERE*

In Table 4 the results are shown of the logistic regression analyses in which actual cybercrime reporting behaviors were predicted. Model 1 shows the results for reporting cybercrime victimization to the police. In line with Figure 2, the results in Model 1 show that victims of malware infection were the least likely to report victimization to the police, although the differences were only significant with victims of ransomware (OR=3.82, p<.01), phishing (OR=2.75, p<.05), cyberstalking (OR=4.85, p<.05), identity fraud (OR=21.33, p<.001), and online consumer fraud (OR=8.00, p<.001). Moreover, respondents with a business in the sector of 'Trade, transport and hospitality' were significantly less likely to report cybercrimes to the

police compared to those within the 'Business and financial services' sector (OR=0.18, p<.05). Model 1 further shows that respondents who have children who were not living at home were more likely to report cybercrime victimization to the police than those who did not have children (OR=2.80, p<.05). None of the other business or personal characteristics were significantly related to reporting cybercrime to the police.

In Model 2, the results for reporting cybercrime victimization to other organizations are shown. Only three types of cybercrime were significantly more often reported to other organizations than malware infections: phishing (OR=4.10, p<.001), identity fraud (OR=4.71, p<.01), and online consumer fraud (OR=2.44, p<.01). Both characteristics of the SME (i.e., sector and business size) were not related to reporting to other organizations, but male and older SME-owners were found to be significantly more likely to report to other organizations than female (OR=0.40, p<.01) and younger (OR=1.04, p<.05) SME-owners. Moreover, also those respondents with more fear for cybercrime victimization more often reported their victimization to other organizations (OR=1.38, p<.05).

*** TABLE 4 ABOUT HERE***

The SME-owners who indicated that they had become a victim of cybercrime were also asked why they reported the cybercrime to the police, or not. Table 5 shows that, in line with the results from the vignette study in Table 2, the motives 'I want the perpetrator to be caught' (25.8%) and 'to prevent the perpetrator from doing this again to someone else' (25.8%) were most often chosen. The most often mentioned motives to not report cybercrime to the police were also similar as those from the vignette study in Table 3: 'There is no point, the police will not do anything about it' (22.0%) and 'I will solve it myself' (27.1%). The numbers of victims per type of cybercrime were too small to show these percentages separately for all types of crime.

TABLE 5 ABOUT HERE

Finally, the 62 SME-owners in the sample who indicated that they had ever reported cybercrime to the police were also asked about their experiences. Only 15 of them (27.5%) were (very) satisfied with how the police handled their report. Almost half of them (41.9%), on the other hand, were (very) unsatisfied with the way the police handled their reports. The most mentioned reasons for their dissatisfaction were that the police were indifferent (50.0%) and that the problems were not solved (46.2%).

Discussion

In this study, we examined cybercrime reporting behaviors among a sample of 529 SME-owners in the Netherlands. A distinction was made between intended reporting behaviors, using a vignette study, and actual reporting behaviors after self-reported victimization of cybercrimes. Moreover, respondents were asked about their motives to either report a cybercrime or not, and about their past experiences with reporting cybercrime victimization to the police.

In line with previous studies (Veenstra et al., 2015; Wanamaker, 2019), our results show that the majority of SME-owners do not report cybercrime victimization to the police. After actual cybercrime victimization, only 14.1 percent of the offenses were reported to the police while only 32.3 percent was (also) reported to another organization. It is, however, remarkable that when the same respondents were asked about the cybercrime incidents as described in the vignettes, a large majority indicated that they would report these offenses to the police, as well as to other organizations. This discrepancy between intended and actual reporting behaviors after cybercrime victimization could be the consequence of our research design in which the vignettes were specifically about victimization of the businesses while the self-reported victimization could also be personal. However, it is unlikely that this offers a full explanation since this discrepancy was also found in previous studies that only examined victimization among businesses (Veenstra et al., 2015) or only personal victimization (Van de Weijer et al.,

2020). Another possible explanation for this finding is that our vignettes describe more serious cases of cybercrimes, than the respondents' actual experiences. In line with this explanation, our results also show that people are more willing to report more serious offenses to the police. It is also a possibility that reporting intentions of respondents as expressed in vignette studies might not result in this behavior in real world situations. This phenomenon, also referred to as the intention-behavior gap (Sheeran & Webb, 2016), is also known from research into other types of behavior, such as quit smoking (Kovač & Rise, 2007), exercising (De Bruin et al, 2012), and safe online behavior (Van 't Hoff-de Goede et al., 2019). It would be interesting for future studies to examine possible obstacles that victims experience when they want to report cybercrime victimization and how the intention-behavior gap can be decreased.

In line with the economic perspective, our results further showed that the best, and most consistent, predictors for reporting cybercrime victimization were the seriousness of the offense and the type of cybercrime. In the vignette study, credit card fraud was reported to the police most often, while identity fraud, online consumer fraud, and cyberstalking were the most reported offenses after actual victimization. Victimization of malware, hacking, and DDoS-attacks, on the other hand, were seldom reported after actual victimization. These results indicate that cyber-enabled crimes (i.e., traditional types of crime committed through the use of IT but not aimed at IT) are more often reported to the police than cyber-dependent crimes (i.e., novel types of crime committed through the use of IT and aimed at IT), which is in line with previous studies among citizens (Van de Weijer et al., 2019; 2020; Dutch Statistics, 2020a). This might suggest that victims think that the police is not responsible or does not have the knowledge to tackle cyber-dependent crimes. However, these were not often mentioned as the most important reasons to not report victimization to the police.

The results from the vignette study further showed that the number of possibilities to report victimization to the police did not influence the SME-owners' reporting intentions. This

result is in contrast with what could be expected based on the economic perspective, and suggests that increasing the number of ways to report crimes to the police will not be an effective way to increase the reporting rates. However, given the large discrepancy between intended reporting behaviors and actual reporting behaviors in this study, this result should be interpreted with some caution as victims might respond differently to actual reporting possibilities.

In contrast to previous studies (Veenstra et al., 2015; Wanamaker, 2019), no relationship was found between business size and cybercrime reporting intentions and behaviour. Also most other characteristics of SMEs and their owners were not related to crime reporting behaviors. This is in line with previous results from Van de Weijer and colleagues (2020), who found that most demographic characteristics of Dutch citizens were not related to crime reporting either. As there is no clear profile of victims that do not report cybercrime to the police, it seems more effective to make use of general interventions or campaigns to increase cybercrime reporting, rather than targeting a specific group. Moreover, the similarities in results between citizens and SME-owners suggest that no specific interventions or campaigns are necessary for businesses.

The motives of respondents to report cybercrime to the police were very similar in the vignette study and the self-reported study. Victims report crimes because they want the perpetrator to be caught and to prevent him from doing the same to someone else, and they do not report cybercrimes because they think the police will not do anything about it and rather solve it themselves. Similar reasons were previously mentioned in studies among businesses (Veenstra et al., 2015; Wandamaker, 2019) and among citizens (Van de Weijer et al., 2020). Reporting to the police in order to get the damage compensated was seldom mentioned as the most important reason. Possibly this is the consequence of many citizens and businesses not being insured for the damage that cybercrime can cause. For several types of traditional crimes, such as burglary and car or bicycle theft, many people in the Netherlands are insured. In those

cases, a police report is needed in order to get the stolen goods reimbursed. Moreover, cybercrime victims do not often state that they do no report to the police because they think the police do not have the responsibility or the knowledge to tackle cybercrime. Low reporting rates, thus, seem to be the consequence of a more general lack in confidence that the police will act upon their report rather than of a specific lack in confidence regarding the way the police handle cybercrime.

Our results further show that many victims who did previously report cybercrime victimization to the police were (very) unsatisfied with the way the police handled their reports, as the police were indifferent and their problems were not solved. Previous studies also reported much dissatisfaction about the way the police deal with victims of cybercrime, as they often feel like they are not taken seriously or even send away from the police station (Cross et al., 2016; Leukfeldt et al., 2019). It is therefore important that the police will take victims of cybercrimes more seriously in the future, and that they will try to help to solve the problems.

Finally, in line with previous studies (e.g., Van de Weijer et al., 2019; 2020) it was found that cybercrime victims more often report their victimization to other organizations than the police. In order to gain insights in the prevalence and trends of different types of cybercrime, it might therefore be effective if the police actively collaborates with other organizations, such as banks, credit card companies, and online help desks. Moreover, the effectiveness of such partnerships that already exist should be examined in future research.

Limitations

Although the current study offers more insights in the factors and motives that play a role in the cybercrime reporting behaviors of businesses, it is also limited in several ways. First of all, we found a large discrepancy between the results from our vignette study and the self-reported study. It is therefore questionable whether intentions to report cybercrime to the police also lead

to actual reporting behavior. The results from the vignette study should therefore be interpreted as intended behavior only.

Second, when asking the SME-owners about previous victimization, no distinction was made between victimization as a private person and victimization of their businesses. We made this methodological choice because previous research by Veenstra and colleagues (2016) showed that private and business internet use is strongly intertwined and the majority of SME-owners use their computer for both private and business purposes. As a result, it may be difficult for SME-owners to make a distinction between private and work related victimization and we allowed participants to report incidents from both categories. This could explain why very similar results were found as compared to previous studies among citizens (e.g., Van de Weijer et al., 2020).

Third, although the distribution of business sizes in our sample was representative of the entire population of Dutch businesses, the large majority of the SME-owners in our sample had a sole proprietorship (72.8%) or a company with 2 to 9 working places (20.8%). Consequently, the results may not be generalizable to larger companies. Possibly their reporting behaviors are different as larger companies might be more likely to have employees who are responsible for cybersecurity and might be more afraid for reputation loss. However,. Moreover, due to the focus on relatively small businesses in the current study, only business size and sector were included as characteristics of the SMEs. Future studies that examine cybercrime reporting among larger businesses should also examine other characteristics such as the company culture, IT training for employees, and cyber security measures (see also Wanamaker, 2019).

Fourth, the memory of respondents is a potential source of bias when studying self-reported victimization and reporting behaviors. Respondents were asked whether they were ever victimized, and particularly when offenses took place a longer time ago, victims might

forget about the offense or might not remember whether they reported it to the police or other organizations. Moreover, in the case of cybercrime, people might not even know that they became a victim and consequently are not able to report it to the police. Victimization of malware infections, for example, will not be noticed by respondents with limited IT-knowledge, until it is reported by their cyber security software.

In conclusion, our study shows that Dutch SME-owners seldom report cybercrime victimization to the police. Types of cyber-enabled crimes and more serious offences were most often reported to the police, while reporting possibilities and most characteristics of the SMEs or its owners did not explain reporting behaviors. The few respondents that did report cybercrime victimization to the police were often unsatisfied with how the police handled their report. The police should therefore take cybercrime victims more seriously in the future, in order to increase reporting rates. Moreover, active collaborations between the police and other organizations, such as banks, credit card companies, and online help desks, could be useful for the police, as victims were more likely to report to such organizations.

References

Bruin, de M., Sheeran, P., Kok, G., Hiemstra, A., Prins, J. M., Hospers, H. J., & van Breukelen, G. J. (2012). Self-regulatory processes mediate the intention–behavior relation for adherence and exercise behaviors. *Health Psychology, 31*(6), 695–703.

Cross C.A., Richards K.M., Smith R., (2016). The reporting experiences and support needs of victims of online fraud, *Trends and Issues in Crime and Criminal Justice, 518,* 1-14.

Dutch Statistics (2020a). *Veiligheidsmonitor 2019*. Den Haag: Centraal Bureau voor de Statistiek.

Dutch Statistics (2020b). *CBS Statline*. Retrieved from: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/81588NED/table?ts=1581922608045.

Goudriaan, H. (2006). *Reporting crime: Effects of social context on the decision of victims to notify the police*. Veenendaal: Universal Press.

Graham, A., Kulig, T. C., & Cullen, F. T. (2019). Willingness to report crime to the police. *Policing: An International Journal.*

Hoff-de Goede, S. van 't, van der Kleij, R., van de Weijer, S.G.A., & Leukfeldt, E.R. (2019). *Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie, en online gedrag van Nederlanders.* Den Haag: WODC.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1-25.

Jong, L., E.R. Leukfeldt & S. van de Weijer (2018) Aangiftebereidheid na slachtofferschap van cybercrime. *Tijdschrift voor Veiligheid. 17*(1-2) 66-78.

Kovač, V. B., & Rise, J. (2007). The relation between past behavior, intention, planning, and quitting smoking: The moderating effect of future orientation. *Journal of Applied Biobehavioral Research, 12*(2), 82–100.

KVK (2020). *KVK Data over de Bedrijvendynamiek.* Utrecht: Kamer van Koophandel.

Lee, J.H., & Huber J. J. (2011)Multiple imputation with large proportions of missing data: How much is too much? In: *United Kingdom Stata Users' Group Meetings 2011.*

Leukfeldt, E.R., R.J. Notté & M. Malsch (2019) Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. *Victims and Offenders*. DOI:10.1080/15564886.2019.1672229.

Sheeran, P., & Webb, T. L. (2016). The intention-behavior gap. *Social and Personality Psychology Compass, 10*(9), 503-518.

Slocum, L.E.E., Taylor, T.J., Brick, B.T., & Esbensen, F.A.. (2010). Neighborhood structural characteristics, individual-level attitudes, and youths' crime reporting intentions. *Criminology*, *48*(4), 1063-1100.

Torrente, D., Gallo, P., & Oltra, C. (2017). Comparing crime reporting factors in EU countries. *European journal on criminal policy and research*, *23*(2), 153-174.

Veenstra, S., Zuurveen, R., & Stol, W.Ph. (2015). *Cybercrime onder bedrijven. Een onderzoek naar slachtofferschap van cybercrime onder het Midden- en Kleinbedrijf en Zelfstandigen zonder Personeel in Nederland*. Leeuwarden: Lectoraat Cybersafety.

Wanamaker, K. A. (2019). *Profile of Canadian Businesses who Report Cybercrime to Police.* Ottowa: Public Safety Canada.

Weijer, van de, S.G.A., E.R. Leukfeldt, & W. Bernasco (2019) Reporting crime to the police: a comparison between traditional crime and cybercrime. *European Journal of Criminology, 16*(4), 486-508.

Weijer, van de, S.G.A., E.R. Leukfeldt, & S. van der Zee (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal.*

Figure 1: Example of a vignette on credit card fraud

Someone has retrieved the details of the credit card of your business via the internet and has charged 1000 euros. You do not know who the perpetrator is. If you want to report the crime to the police, this is po*ssible on the internet, over the phone or on the police station.*

Figure 2. Cybercrime reporting to the police and other organizations.

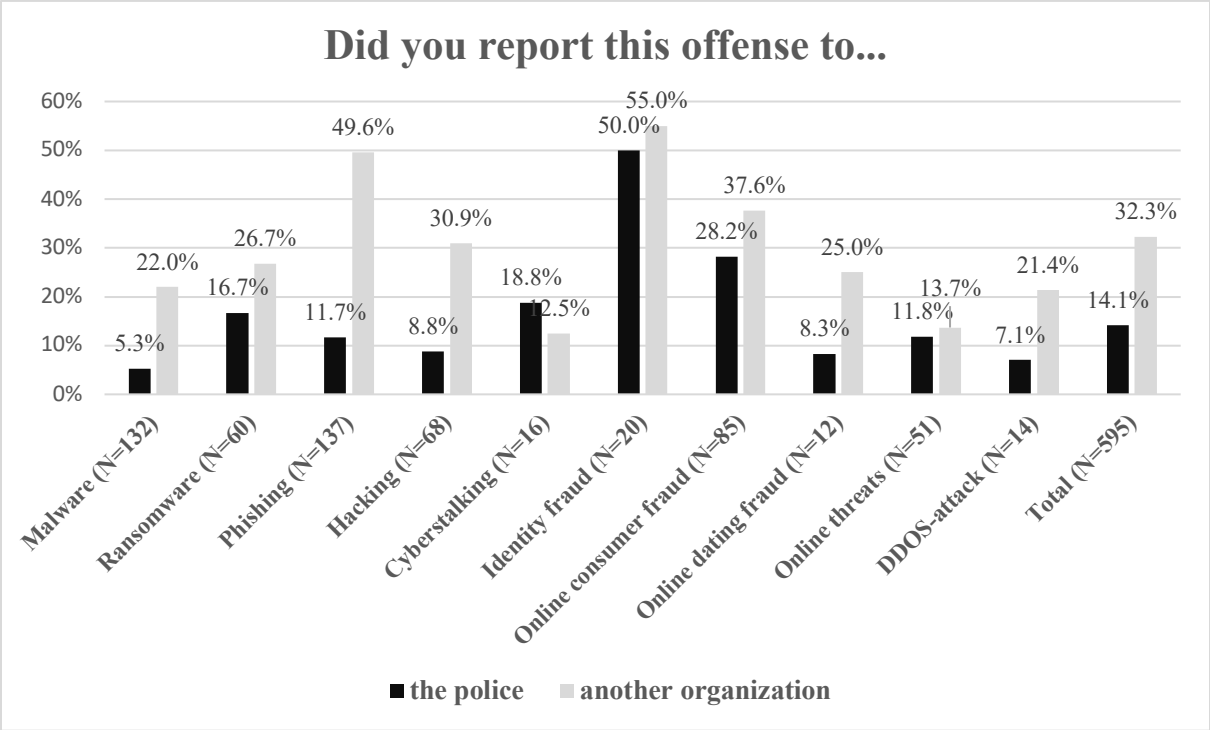

Table 1. Ordinal logistic regression analyses on intentions to report cybercrime victimization

	Model 1: Reporting to the police			Model 2: Reporting to other organizations		
	B	Robust S.E.	OR	B	Robust S.E.	OR
Type of crime:						
Credit card fraud	(ref.)			(ref.)		
Online consumer fraud	-1.40***	0.15	0.25	0.01	0.14	1.01
Malware	-0.78***	0.15	0.46	-0.28*	0.13	0.76
Hacking	-0.33*	0.15	0.72	-0.26	0.14	0.77
DDoS-attack	-0.87***	0.16	0.42	-0.13	0.15	0.88
Seriousness	1.12***	0.10	3.06	0.34***	0.10	1.40
Relation with offender:						
Identity offender is unknown	(ref.)			(ref.)		
Offender is an acquaintance	-0.45**	0.12	0.64	-0.56***	0.12	0.57
Offender is a stranger	0.18	0.12	1.20	0.20*	0.12	1.22
Reporting possibilities:						
Police office	(ref.)			(ref.)		
Police office and telephone	0.14	0.13	1.15	-0.12	0.12	0.89
Police office, telephone and online	-0.00	0.12	1.00	-0.15	0.12	0.86
Sector:						
Business and financial services	(ref.)			(ref.)		
Government and healthcare	0.26	0.18	1.30	-0.06	0.17	0.94
Trade, transport and hospitality	-0.07	0.28	0.93	-0.51*	0.25	0.60
Construction, industry and energy	-0.03	0.26	0.97	0.20	0.27	1.22
Agriculture and fisheries	-0.00	0.41	1.00	-0.50	0.46	0.61
Culture, recreation and other services	0.25	0.18	1.28	-0.32	0.18	0.73
Business size:						
One person	(ref.)			(ref.)		
Two-nine persons	0.06	0.18	1.06	-0.02	0.19	0.98
Ten or more persons	-0.17	0.31	0.84	-0.30	0.28	0.74
Gender (male=ref.)	0.04	0.15	1.04	0.32*	0.14	1.38
Age	0.02*	0.01	1.02	0.02*	0.01	1.02
Marital status:						
Single	(ref.)			(ref.)		
Relationship, living together	-0.01	0.18	0.99	0.29	0.19	1.34
Relationship, not living together	-0.04	0.26	0.96	0.02	0.27	1.02
Widow	0.57	0.43	1.77	-0.34	0.46	0.71
Children:						
No	(ref.)			(ref.)		
Yes, not living at home	0.01	0.19	1.01	0.02	0.19	1.02
Yes, living at home	-0.15	0.19	0.86	-0.12	0.18	0.89
Education	0.04	0.06	1.04	0.03	0.05	1.03
Income	0.02	0.03	1.02	-0.02	0.03	0.98
Previous cybercrime victimization:						
No	(ref.)			(ref.)		
Yes, never reported to police	-0.29*	0.14	0.75	0.12	0.14	1.13
Yes, ever reported to police	0.70**	0.23	2.01	0.57*	0.22	1.77
Satisfaction with police	0.08	0.08	1.08	0.11	0.07	1.12
Fear for cybercrime victimization	0.09	0.07	1.09	0.21**	0.07	1.23
IT-knowledge	0.18	0.12	1.20	0.34**	0.12	1.40
N vignettes	1497			1497		
N respondents	529			529		

*Note: * p<.05; **p<.01; ***p<.001 (two-sided).*

Table 2. Motives to report to the police

	Credit card fraud	Online consumer fraud	Malware	Hacking	DDoS attack	Total
I want the perpetrator to be caught	100 (36.9%)	54 (31.8%)	86 (40.2%)	95 (38.8%)	43 (30.3%)	378 (36.3%)
To prevent the perpetrator from doing this again to someone else	64 (23.6%)	75 (44.1%)	56 (26.2%)	59 (24.1%)	44 (31.0%)	298 (28.6%)
To prevent this from happening to me again	38 (14.0%)	6 (3.5%)	23 (10.8%)	44 (18.0%)	16 (11.3%)	127 (12.2%)
To create a safer online environment	21 (7.8%)	10 (5.9%)	29 (13.6%)	32 (13.1%)	24 (16.9%)	116 (11.3%)
To get the damage compensated	27 (10.0%)	13 (7.7%)	6 (2.8%)	3 (1.2%)	6 (4.2%)	55 (5.3%)
It is my duty to report crime	19 (7.0%)	10 (5.9%)	10 (4.7%)	7 (2.9%)	5 (3.5%)	51 (4.9%)
Other	2 (0.7%)	2 (1.2%)	4 (1.9%)	5 (2.0%)	4 (2.8%)	17 (1.6%)
Total	271(100%)	170(100%)	214 (100%)	245 (100%)	142 (100%)	1.042(100%)

Table 3. Motives to not report to the police

	Credit card fraud	Online consumer fraud	Malware	Hacking	DDoS attack	Total
There is no point, the police will not do anything about it	5 (22.7%)	36 (39.6%)	25 (38.5%)	14 (31.8%)	15 (42.9%)	95 (37.0%)
I will solve it myself	13 (59.1%)	23 (25.3%)	15 (23.1%)	16 (36.4%)	4 (11.4%)	71 (27.6%)
It takes too much effort	0 (0.0%)	16 (17.6%)	4 (6.2%)	1 (2.3%)	6 (17.1%)	27 (10.5%)
I think it is actually my own fault	1 (4.6%)	5 (5.5%)	4 (6.2%)	4 (9.1%)	0 (0.0%)	14 (5.5%)
It is not that important	0 (0.0%)	5 (5.5%)	1 (1.5%)	2 (4.6%)	5 (14.3%)	13 (5.1%)
The police is not responsible for solving this type of crime	2 (9.1%)	1 (1.1%)	5 (7.7%)	3 (6.8%)	0 (0.0%)	11 (4.3%)
The police does not have the knowledge to tackle this type of crime	1 (4.6%)	1 (1.1%)	2 (3.1%)	2 (4.6%)	4 (11.4%)	10 (3.9%)
I have little confidence in the police	0 (0.0%)	2 (2.2%)	3 (4.6%)	2 (4.6%)	0 (0.0%)	7 (2.7%)
I am afraid the perpetrator will take revenge	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
I am ashamed that I fell victim to the crime	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
Other	0 (0.0%)	2 (2.2%)	6 (9.2%)	0 (0.0%)	1 (2.9%)	9 (3.5%)
Total	33(100%)	85 (100%)	65 (100%)	44 (100%)	35 (100%)	257 (100%)

Table 4. Logistic regression analyses on cybercrime reporting behaviors

	Model 1: Reporting to the police			Model 2: Reporting to other organizations		
	B	Robust S.E.	OR	B	Robust S.E.	OR
Type of crime:						
Malware	(ref.)			(ref.)		
Ransomware	1.34**	0.47	3.82	0.19	0.29	1.21
Phishing	1.01*	0.47	2.75	1.41***	0.26	4.10
Hacking	0.57	0.51	1.77	0.62	0.33	1.86
Cyberstalking	1.58*	0.72	4.85	-0.62	0.72	0.54
Identity fraud	3.06***	0.62	21.33	1.55**	0.54	4.71
Online consumer fraud	2.08***	0.46	8.00	0.89**	0.31	2.44
Online dating fraud	0.53	0.73	1.70	-0.20	0.64	0.82
Online threats	0.76	0.55	2.14	-0.62	0.44	0.54
DDoS-attack	0.13	0.65	1.14	-0.06	0.55	0.94
Sector:						
Business and financial services	(ref.)			(ref.)		
Government and healthcare	-0.19	0.46	0.83	0.25	0.36	1.28
Trade, transport and hospitality	-1.70*	0.76	0.18	0.37	0.46	1.45
Construction, industry and energy	-0.30	0.61	0.74	-0.51	0.50	0.60
Agriculture and fisheries	-0.46	0.95	0.63	-0.47	0.60	0.63
Culture, recreation and other services	0.22	0.49	1.25	0.33	0.39	1.39
Business size:						
One person	(ref.)			(ref.)		
Two-nine persons	0.77*	0.39	2.16	-0.05	0.32	0.95
Ten or more persons	0.65	0.83	1.92	-0.71	0.60	0.49
Gender (male=ref.)	-0.52	0.37	0.59	-0.91**	0.29	0.40
Age	-0.03	0.02	0.97	0.04*	0.02	1.04
Marital status:						
Single/widow[1]	(ref.)			(ref.)		
Relationship, living together	0.04	0.44	1.04	-0.21	0.35	0.81
Relationship, not living together	-0.48	0.67	0.62	-0.41	0.49	0.66
Children:						
No	(ref.)			(ref.)		
Yes, not living at home	1.03*	0.48	2.80	0.22	0.35	1.25
Yes, living at home	0.72	0.43	2.05	0.33	0.32	1.39
Education	0.18	0.13	1.20	-0.01	0.10	0.99
Income	-0.14	0.10	0.87	-0.00	0.06	1.00
Satisfaction with police	-0.36	0.22	0.70	-0.02	0.16	0.98
Fear for cybercrime victimization	-0.04	0.6	0.96	0.32*	0.16	1.38
IT-knowledge	-0.40	0.26	0.67	0.19	0.21	1.21
N cybercrimes	595				595	
N respondents	306				306	
Pseudo R2	0.16				0.13	

*Note: * p<.05; **p<.01; ***p<.001 (two-sided). [1] In none of the 21 cases in which a widow was the victim of cybercrime, the cybercrime was reported to the police. In order to prevent these 21 cases to be excluded from the analyses, the categories 'single' and 'widow' have been combined to one category.*

Table 5: Motives to (not) report cybercrime

Motives to report cybercrime		**Motives to not report cybercrime**	
To prevent the perpetrator from doing this again to someone else	16 (25.8%)	I will solve it myself	74 (27.1%)
I want the perpetrator to be caught	16 (25.8%)	There is no point, the police will not do anything about it	60 (22.0%)
To create a safer online environment	11 (17.7%)	It is not that important	33 (12.1%)
To prevent this from happening to me again	7 (11.3%)	The police is not responsible for solving this type of crime	25 (9.2%)
To get the damage compensated	7 (11.3%)	It takes too much effort	11 (4.0%)
It is my duty to report crime	3 (3.2%)	The police does not have the knowledge to tackle this type of crime	6 (2.2%)
Other	3 (4.8%)	I think it is actually my own fault	6 (2.2%)
		I have little confidence in the police	4 (1.5%)
		I am ashamed that I fell victim to the crime	5 (1.8%)
		I am afraid the perpetrator will take revenge	0 (0.0%)
		Other	49 (17.9%)
Total	62 (100%)	Total	273 (100%)

Appendix

Figure A1: Vignette credit card fraud

Someone has retrieved the details of the credit card of your business via the internet and has charged *100 / 1000 euros.* *You do not know who the perpetrator is / You know the perpetrator personally / You do not know the perpetrator personally.* If you want to report the crime to the police, this is possible *on the police station / over the phone or on the police station / on the internet, over the phone or on the police station.*

Note: Words in *italic* differed randomly between respondents.

Figure A2: Vignette online consumer fraud

You have purchased a *USB stick / laptop* on Marktplaats[1] for your business and paid in advance. However, you have never received the item and the seller is no longer responding to your contact attempts. You suspect that you have been scammed. *You do not know who the perpetrator is / You know the perpetrator personally / You do not know the perpetrator personally.* If you want to report the crime to the police, this is possible *on the police station / over the phone or on the police station / on the internet, over the phone or on the police station.*

Note: Words in *italic* differed randomly between respondents. [1]*Marktplaats* is a popular Dutch advertising site which was acquired by eBay in 2004.

Figure A3: Vignette malware

You have a virus on your business computer. As a result of this virus, *files have become inaccessible / files have become inaccessible and ransom has been requested.* *You do not know who the perpetrator is / You know the perpetrator personally / You do not know the perpetrator personally.* If you want to report the crime to the police, this is possible *on the police station / over the phone or on the police station / on the internet, over the phone or on the police station.*

Note: Words in *italic* differed randomly between respondents.

Figure A4: Vignette hacking

Someone gained access to your business email account and used this access to *view / publicly distribute* your emails with sensitive business information *You do not know who the perpetrator is / You know the perpetrator personally / You do not know the perpetrator personally.* If you want to report the crime to the police, this is possible *on the police station / over the phone or on the police station / on the internet, over the phone or on the police station.*

Note: Words in *italic* differed randomly between respondents.

Figure A5: Vignette online threat

The website of your business was targeted in a DDoS-attack, causing your website to be unavailable to potential costumers for *1 day / 1 week.* *You do not know who the perpetrator is / You know the perpetrator personally / You do not know the perpetrator personally.* If you want to report the crime to the police, this is possible *on the police station / over the phone or on the police station / on the internet, over the phone or on the police station.*

Note: Words in *italic* differed randomly between respondents.

Table A1: Items used to measure satisfaction with the police

The police know how to catch criminals.
The police want to be in contact with citizens.
The police take into account the wishes of society.
The police work well with the residents.
If it really matters, then the police are there for you.
The police are easy to approach.
The police inform the citizens.
The police are successfully fighting crime.
If it really matters, the police will do their utmost to help you.

Table A2: Items used to measure fear for cybercrime victimization

I am scared of becoming a victim of cybercrime in the near future.
The idea that someone can log into my online bank account without permission scares me.
I am concerned that I can become a victim of phishing.
I am concerned about the possibility that my computer can be hacked.
I think it can easily happen that I get scammed online.
The fact that I can get ransomeware on my computer, worries me.
It is quite possible that I will become a victim of cybercrime in the coming year.
If I became a victim of cybercrime, it could have serious consequences.