When do businesses report cybercrime? *Findings from a UK study*

Steven Kemp[1,2], David Buil-Gil[3], Fernando Miró-Llinares[2] and Nicholas Lord[3]

[1]University of Girona, Spain
[2]Miguel Hernández University of Elche, Spain
[3]University of Manchester, UK

Abstract

Although it is known that businesses report cybercrime to public authorities at a low rate, and this hinders prevention strategies, there is a lack of research on companies' decisions to report cyber victimisation. This paper analyses the UK Cyber Security Breaches Survey to explore factors associated with cybercrime reporting by businesses. Results indicate that the type of cybercrime is relevant to the reporting decision, and that the likelihood of reporting increases when cybersecurity incidents generate negative impacts and when the company places high priority on cybersecurity. However, we find no association between having cybersecurity insurance and reporting. Finally, while having outsourced cybersecurity management is associated with reporting to anyone outside the organisation but not to public authorities, in-house cybersecurity teams seem more inclined to report to public authorities. Findings are discussed in relation to the role of the private cybersecurity sector and the criminal justice system in combatting cybercrime.

Full citation

Kemp, S., Buil-Gil, D., Miró-Llinares, F., and Lord, N. (2021). When do businesses report cybercrime? Findings from a UK study. *Criminology and Criminal Justice.*

1. Introduction

Cybercrime poses a growing threat to private organisations in the United Kingdom. The National Crime Agency has stated that cyber criminality is rising and criminals are increasingly targeting businesses (National Crime Agency, n.d.), while Williams et al. (2019) describe cybercrime as one of the main threats to economic security in the UK. Greater levels of homeworking related to COVID-19 may have further exacerbated existing cybercrime threats, and research has shown that reports of certain types of online fraud against organisations rose during the pandemic (Kemp et al., 2021). It should also be noted that the issue does not only affect large businesses. As the National Cyber Security Centre (2020: 3) states, "[i]f you're a small or medium-sized enterprise (SME) then there's around a 1 in 2 chance that you'll experience a cyber security breach".

Yet, despite the widespread recognition that cybercrime is a salient issue for businesses of all sizes, criminological research on the topic is relatively scarce, which has been attributed to a lack of reliable data (Buil-Gil et al., 2021; Williams et al., 2019). In this regard, one particular problem may be that reporting of crime victimisation by businesses is particularly low (Caneppele and Aebi, 2017; Lavorgna, 2020), which means the dark figure hidden from official statistics hinders research on the topic. This is concerning as, in addition to aiding academic research, reporting is key to the design of effective prevention and response strategies to cybercrime and fraud threats (Kemp et al., 2020; Reep-van den Bergh and Junger, 2018; van de Weijer et al., 2019). If data are lacking with respect to cybercrime against businesses, current prevention strategies may be inadequately informed (Levi et al., 2017). Furthermore, reports are a means to start police investigations into crime, and, thus, low levels of reporting may signify that private organisations consider that formally involving the police or other government agencies is not the most suitable response to cybercrime victimisation. This in turn may exemplify the expectations and challenges faced by the criminal justice system with regard to cybercrime, as well as the fact that responses to cybercrime are often based on a private model of justice or public-private partnerships (Dupont, 2017; Wall, 2007/10).

In order to improve crime reporting rates, and therefore shed light on the dark figure of cybercrime against businesses and better inform strategies to combat the issue, it is necessary to first understand which factors are associated with the decision to report cybercrime. This may also improve comprehension of the expected role of the criminal justice system with regard to this type of criminal activity. There is extensive research on crime reporting by individuals, but research on the crime reporting practices of businesses is scarce (Isenring et al., 2016; van de Weijer et al., 2021). In fact, to the authors' knowledge there have been no academic attempts to empirically explore cybercrime reporting by businesses in the United Kingdom and, thus, the present paper aims to begin to fill this salient gap in the literature.

2. Review of the extant literature

2.1 Crime reporting by individuals

Much criminological inquiry has sought to identify the factors associated with crime reporting, with research showing that the decision to report a crime to the police varies according to the victim's characteristics and attitudes, external situational factors, the impact of the criminal event and the perceived costs and benefits of reporting (Xie and Baumer, 2019).

Studies have found that certain demographic characteristics of crime victims, such as gender or age, are associated with reporting (Baumer and Lauritsen, 2010; Goudriaan et al., 2006;

Tarling and Morris, 2010; Schoepfer and Piquero, 2009; Van Wyk and Mason, 2001). Individual attitudes towards the criminal justice system also affect the decision to report a crime to the police (Tolsma et al., 2012; Tyler and Fagan, 2008). With regard to contextual factors, lower reporting has been found in neighbourhoods with economic deprivation along racial lines (Xie and Lauritsen, 2012) and higher crime rates (Bowles et al., 2009).

It has been argued that crime reporting is based on rational choice decision-making processes, with various authors finding that crime victims balance the perceived costs of reporting against the expected benefits (Bowles et al., 2009; Felson et al., 2002; Goudriaan et al., 2006; Tolsma et al., 2012). The costs of reporting can refer to the time and economic resources required to collect evidence, contact the police or participate in the judicial process (Bowles et al., 2009). Victims also consider whether reporting is likely to achieve their objectives (Felson et al., 2002), such as identifying the culprit, retribution, reclaiming stolen property or recovering losses through insurance (Bowles et al., 2009; Tarling and Morris, 2010). Further evidence of a rational element in reporting can be found in studies that correlate more severe financial or physical consequences of crime with increased reporting (Baumer and Lauritsen, 2010).

With regard to cybercrime reporting, it has been stated that reporting rates may be lower than for traditional crime (van de Weijer et al., 2019; Yar and Steinmetz, 2019). This could be due to a number of factors, such as a) lack of awareness of victimisation or that the act constitutes a crime, b) relatively low losses on an individual level may make reporting seem overly costly, c) lack of confidence in the police’s ability to adequately respond to cybercrime, d) concerns about embarrassment or reputational damage (Lagazio et al., 2014; Lavorgna, 2020), or e) a realisation that informal resolutions through extra-legal/informal channels might be more productive (e.g., due to cost, privacy, competition, commercial sensitivities). Nevertheless, academic studies specifically focussed on cybercrime reporting are relatively scarce.

Van de Weijer et al. (2019) conducted one of the most extensive studies to date, analysing the extent to which victims' demographic characteristics affect cybercrime and traditional crime reporting in the Netherlands. They analysed reporting behaviour for three types of cybercrime: identity theft, consumer fraud and hacking. They found that cybercrime reporting rates to the police were 26.3%, 24% and 7.1%, respectively, which were lower than for all other offline crime types except vandalism (20.5%). Reporting to other organisations (e.g., banks, financial organisations, consumer associations) differed, with 82.3% of identity theft victims reporting to non-police organisations, 22.4% of consumer fraud victims, and 16.6% for victims of hacking. This underscores the need to analyse cybercrime reporting to both the police and other organisations.

Kemp (2020) examined online fraud reporting in Catalonia. The findings showed that the most important factors associated with reporting online fraud victimisation to the police were whether the victim considered it a crime and whether it had a negative impact. The most selected reason for not reporting a fraud was that the process was too complex, followed by the insignificance of the losses and, thirdly, the belief that there was little the police could do.

Two recent studies have employed vignettes to examine cybercrime reporting. Graham et al. (2020) found that being black, female, married or young were associated with cybercrime reporting. Their model estimated higher perceptions of procedural justice to be the strongest predictor of reporting cyber-victimisation. The findings of van de Weijer et al. (2020) suggest cybercrime is often not reported to the police because individuals believe they can solve it themselves or they think the police will not do anything about it.

2.2 Crime reporting by businesses

Research on the decision by private organisations to report crime victimisation is scant in comparison to analysis on individuals. Nevertheless, some shared conclusions have been drawn from research analysing traditional crime types. Two of the most common findings are that, similarly to crime reporting by individuals, reporting rates differ between crime types (Dugato et al., 2013; Home Office, 2019; Isenring et al., 2016; Taylor, 2002) and the impact of victimisation predicts the decision to report (Home Office, 2019; Isenring et al. 2016; Kennedy, 2016; Taylor, 2002). Some factors such as the size of the business (Isenring et al. 2016) or the country where it is located (Dugato et al. 2013) can also predict reporting. Finally, a common reason given by companies for not reporting is that the criminal justice system may not provide an effective response (Kennedy, 2016; Taylor, 2002).

To the authors' knowledge, no academic studies have examined the reporting practices of businesses with regard to cybercrime in the UK. That said, there are some reports published by government agencies and academic research that provide preliminary insight into the factors that may be associated with cybercrime reporting by enterprises. Surveys conducted at different times in the United States (Rantala, 2008), Australia (Richards, 2009), Canada (Statistics Canada, 2020; Wanamaker, 2019), Netherlands (van de Weijer et al., 2021) and the United Kingdom (Home Office, 2019) all find low levels of cybercrime victimisation reporting to the police (between 8-15%). However, there is higher reporting to non-police organisations or individuals outside the organisation as well as disparities between cybercrime types (Rantala, 2008; van de Weijer et al., 2021). The decision to report to the police may depend on the ability of the organisation to resolve the issue internally or through an information technology consultant (Statistics Canada, 2020; Wanamaker, 2019). The size of the enterprise and the sector where it operates may also correlate with reporting cybercrime incidents (Home Office, 2019; Rantala, 2008; Richards, 2009). Businesses that conduct cybersecurity risk management and cybersecurity training report cybercrime victimisation more often (Wanamaker, 2019). In accordance with the literature on crime reporting in general, the impact of the criminal event (Richards, 2009; Statistics Canada, 2020) and whether the organisation has insurance covering cybersecurity losses (Statistics Canada, 2020) appear relevant. Finally, Lagazio et al. (2014) argue that one of the main reasons for financial businesses not to report cybercrime is to prevent reputational damages associated with customers losing trust in the company and its products.

3. The present study

Given the research gap identified with regard to cybercrime reporting by businesses, the main objective of the present study is to explore which factors are associated with businesses' decisions to report cybercrime. To this end, and based on the factors associated with the reporting of traditional crime and cybercrime against individuals and organisations, the following research questions have been formulated:

RQ1 Are the characteristics of businesses (size, sector, digital activity) associated with cybercrime reporting?

RQ2 Are the attitudes of businesses towards cybersecurity and the cybersecurity practices instituted by businesses associated with cybercrime reporting?

RQ3 Are the characteristics of the cybercrime event associated with reporting?

It has been noted that to understand reactions to crime, it is necessary to look beyond reporting to the police and consider other ways victims seek help following a criminal event (Xie and Baumer, 2019; van de Weijer et al., 2021). As such, the aforementioned research questions refer not only to cybercrime reporting to the police, but also to other relevant public authorities (e.g., Her Majesty's Revenue and Customs, Financial Conduct Authority) and external private organisations (e.g., outsourced cybersecurity provider, bank, credit card company, internet service provider).

3.2 Data

In order to answer the three questions detailed above, data were obtained from the 2018, 2019 and 2020 rounds of the UK Cybersecurity Breaches Survey (CSBS). The CSBS is a survey of UK private organisations that records information about digital threats, cybersecurity strategies and digital characteristics of organisations (Department of Digital, Culture, Media and Sport, 2020).

Sampling and weighting

The CSBS is designed to record data from a random sample of UK businesses and charities across regions, sizes and sectors every year. We have effectively removed charities from this study because previous research has shown that digital threats affecting charities vary substantially from those affecting businesses (Buil-Gil et al., 2021). The sampling frame is all businesses with at least one employee. The sample includes universities and education institutions but excludes public sector organisations (subject to high cybersecurity standards), agriculture, forestry, and fishing businesses (relative lack of online commerce), and organisations without computers or online presence. All interviews were conducted using Computer-Assisted Telephone Interviewing.

The sample of businesses recorded was 1,519 in 2018, 1,566 in 2019 and 1,348 in 2020. In order to effectively include medium and large businesses in the sample, which represent a small percentage of UK companies, the sample was proportionally stratified by regions and disproportionately stratified by businesses' size and sector. For instance, businesses larger than 50 employees only make up 4 percent of all businesses (Department for Business, Energy and Industrial Strategy, 2019), and simple random sampling would likely exclude medium and large companies from the sample. In order to adjust for the disproportionate sampling and the combination of the three rounds, we calculated new weights using rim weighting according to the size and sector of businesses, as suggested by survey administrators (Department for Business, Energy and Industrial Strategy, 2019). This strategy allowed the weight of businesses in our sample to be adjusted to the population of UK businesses (see Appendix). All analyses presented in this paper are based on the weighted sample of businesses recorded by the 2018, 2019 and 2020 rounds of the CSBS. The three editions were combined to increase the effective sample of businesses suffering incidents in our analysis.

Since this research is particularly concerned with businesses that were victims of at least one cybersecurity incident in the last year, to study factors associated with crime reporting, we only analyse those companies that reported suffering at least one incident in the last 12 months. Our sample of businesses victimised by cybersecurity incidents is 708 in 2018, 584 in 2019 and 673 in 2020. This represents 43%, 32% and 46% of the weighted sample, respectively.

After merging the three rounds of the survey, the most common cybersecurity incidents reported are "staff receiving fraudulent emails or being directed to fraudulent websites" (reported by 32.3% of the weighted sample), “people impersonating your organisation in emails or online” (11.0%) and “computers becoming infected with other viruses, spyware or malware” (8.2%). Other cybercrimes reported were “computers becoming infected with ransomware” (4.6%), “unauthorised use or hacking of computers, networks or servers by people outside your organisation” (4.2%), “hacking or attempted hacking of online bank accounts” (3.4%), “attacks that try to take down your website or online services” (2.7%), “other types of cyber security breaches or attacks” (2.0%) and “unauthorised use of computers, networks or servers by staff” (2.0%). For the purpose of this study, in order to reduce the number of variables, we combined viruses, spyware and ransomware under the category of “malware”, and hacking of computers and hacking of bank accounts under “hacking”. Overall, 39.6% of the weighted sample reported suffering at least one cybercrime in the last 12 months.

Dependent variables

When organisations report more than one cybersecurity incident, the CSBS asks which incident, or related series of attacks, caused the most disruption in the last 12 months, and asks businesses whether they informed someone outside the organisation about this incident. Thus, there is a cap of one incident per organisation, which refers to the attack that generated the greatest disruption. In our sample, 56.9% of incidents that caused the most disruption refer to fraudulent emails, 15.0% malware, 12.5% people impersonating the organisation, 6.9% hacking, 4.7% attacks to take down online services, 0.9% internal threats and 2.9% other incidents. We discuss the limitations associated with imposing a cap of one crime per organisation in the Discussion and Conclusions section.

Overall, 39.5% of organisations who suffered at least one cybersecurity attack reported the most disruptive incident to someone outside the organisation. However, only 8.0% reported the incident to a UK public authority.[1] Table 1 summarises organisations to whom cybersecurity incidents were reported. We will estimate separate regression models to explain two dependent variables: (a) cybercrime reporting to anyone outside the organisation and (b) cybercrime reporting to public authorities.

Table 1. Organisation to whom the incident was reported (weighted sample, multiple responses allowed).

Organisation	%	Organisation	%
Outsourced cybersecurity provider	36.11	Professional/industry association	1.47
Bank, credit card company	15.32	Accountant	1.10
Internet service provider	11.03	Antivirus company	0.87
Police	10.50	Information Commissioner’s Office	0.63
Clients/customers	8.42	Cyber Security Information Sharing Partnership	0.45
Website administrator	3.93	Cifas (not-for-profit fraud prevention service)	0.43
Action Fraud	3.93	National Cyber Security Centre	0.23
The company in question (source of attack)	3.77	Auditor	0.19
Supplier	3.71	Was publicly declared	0.07
Her Majesty's Revenue and Customs	2.96	Parent company	0.06
Other government agency	2.95	Centre for the Protection of National Infrastructure	0.01
Head office, board of directors	2.00	UK Computer Emergency Response Team	0.00
Service provider (e.g., Amazon, Vodafone, Ebay)	1.85	Other	3.56
Financial Conduct Authority or other regulator	1.50	Don’t know or no answer	30.83

[1] The list of UK public authorities to whom businesses may report cyber-attacks is: Action Fraud, Centre for the Protection of National Infrastructure, UK Computer Emergency Response Team, Cyber Security Information Sharing Partnership, Information Commissioner's Office, police forces, Financial Conduct Authority or other regulators, National Cyber Security Centre, Her Majesty's Revenue and Customs, or other government agencies.

Independent variables

Based on the literature review presented above, and in order to analyse the effect of businesses' size and sector on crime reporting, we analyse three dummy business size variables (i.e., 1-49, 50-249, and 249+ employees) and four dummy business sector variables: a) manufacturing, transportation and construction, b) retail, accommodation and entertainment services, c) information, administrative and financial services, and d) tech, knowledge and health.[2]

We also analyse the crime type in question: a) malware, b) attacks to take down website or online services, c) receiving fraudulent emails, d) hacking of bank accounts or computers, e) impersonating the organisation in emails or online and f) unauthorised use of computers by staff; and the impact of the crime (i.e., whether there was some form of negative impact or outcome). Moreover, we analyse whether having outsourced or in-house cybersecurity resources is associated with cybercrime reporting, and also consider the level of priority given to cybersecurity (i.e., whether cybersecurity is high or very high priority). We also examine if the digital characteristics of businesses (i.e., whether they hold personal data electronically, have systems to pay or order online, or have an online bank account), employees using personally-owned devices for work, having cybersecurity insurance, conducting activities to

[2] The "manufacturing, transportation and construction" group refers to businesses in the manufacturing (SIC code C), transportation and storage (H), and construction (F) sectors. The "retail, accommodation and entertainment services" group describes companies in the wholesale and retail trade (G), arts, entertainment and recreation (R), and accommodation and food service (I) sectors. The "information, administrative and financial services" group defines those businesses that fall within one of the following sectors: information and communication (J), administrative and support service (N), real estate (L), and financial and insurance activities (K). Finally, the "tech, knowledge and health" group refers to businesses dedicated to professional, scientific and technical activities (M), education (P), and human health and social work activities (Q). These groups have been designed on the basis of previous research on cybersecurity threats faced by organisations (Buil-Gil et al., 2021; Rantala, 2008; Richards, 2009; van de Weijer et al., 2021), but also according to the type of data or digital characteristics that typically define these companies.

identify cybersecurity risks, or seeking cybersecurity information from government sources have significant effects on cybercrime reporting.

Finally, we also consider two further measures that were included in the 2018 and 2019 editions of the survey, but not in 2020, related to the perceived cybersecurity preparedness of the company (i.e., whether the company has enough people with the right skills to manage cybersecurity risks) and cybersecurity training (i.e., whether someone attended cybersecurity conferences or training in the last 12 months).

3.3 Methods

We follow a two-fold strategy to analyse the effect of all independent variables on our two outcome measures (i.e., likelihood of reporting to anyone outside the organisation, and likelihood of reporting to public authorities). First, we use binary logistic regression models to estimate the effect of all independent variables (except measures of cybersecurity preparedness and training, which were excluded from the 2020 CSBS) on cybercrime reporting among all businesses in our sample. Second, in order to also estimate the effect of cybersecurity preparedness and training on reporting, and given that these measures were only included in the 2018 and 2019 rounds, we select the sample from these two years and estimate the full models with all variables. This is done to analyse both cybercrime reporting to anyone and to public authorities specifically. More specifically, we examine the Odds Ratio (OR) of all independent variables, which is an indicator of the likelihood that the outcome under study (i.e., cybercrime reporting) occurs in one group (e.g., companies with cybersecurity insurance) relative to the odds of the reference group (e.g., no insurance). All analyses were conducted in R software (R Core Team, 2021).

4. Results

In this section, the results of our study are presented according to whether businesses reported cybercrime victimisation to anyone outside the organisation, including external private organisations and public authorities (Models 1 and 2, Table 2), or UK public authorities in particular (Models 3 and 4, Table 3).

4.1 Reporting to anyone outside the organisation

Table 2 displays the results of the binary logistic regression models used to estimate the likelihood that businesses report cybercrime victimisation to anyone outside the organisation. With regard to the sample made up of the three editions (Model 1), it can be observed that the effect of the businesses' size and sector is not statistically significant, but the type of cybercrime victimisation is associated with reporting to someone outside the company. Firstly, businesses are more likely to report receiving fraudulent emails or being directed to fraudulent websites, hacking of their bank account or computer systems, and someone impersonating the organisation online than they are to report the reference category of computers becoming infected with malware. The OR show that businesses are three times more likely to report hacking and impersonating the business, and almost two times more likely to report fraudulent emails than to report being victimised by malware. Similar results are found in Model 2, which uses the sample with only the 2018 and 2019 rounds and includes the measures for cybersecurity preparedness and training. In this model, receiving fraudulent emails and being directed to fraudulent websites, hacking, and impersonation of the business show a statistically significant positive association with reporting in comparison to malware victimisation. In both models, suffering attacks to the website and online services also shows a relatively weaker statistical association with cybercrime reporting (p<0.1). Regarding the influence of the severity of the offence, both models find that experiencing a negative impact/outcome from cybercrime victimisation is associated with greater likelihood of reporting: cybercrimes that cause negative impacts/outcomes are 77% (Model 1) and 89% (Model 2) more likely to be reported to someone outside the organisation than those that do not have negative effects.

Having arrangements for cybersecurity risk management is also associated with reporting cyber incidents to someone outside the organisation. In Model 1, businesses with external cybersecurity risk management are twice as likely to report cybercrime incidents to someone external than those without cybersecurity risk management. In contrast, organisations with internal cybersecurity risk management are 37% less likely to report cyber victimisation to someone outside the organisation in comparison to those with no cybersecurity arrangements. The results of Model 2 are similar with regard to the positive association between having external cybersecurity risk management and reporting cybercrime victimisation. However, in this model no association is found in relation to internal risk management arrangements and reporting cybercrime. With regard to the priority given to cybersecurity, in Model 2, organisations that consider cybersecurity a high priority are 69% more likely to report to anyone outside the organisation than enterprises that do not place high priority on cybersecurity. The OR is also greater than 1 in Model 1, but the statistical association is weak (p<0.1).

Table 2. Logistic regression models of business cybercrime reporting (overall reporting to someone outside the organisation)

	Model 1 (2018, 2019 and 2020 rounds)			Model 2 (2018 and 2019 rounds)		
Predictor	*OR*	*95% CI*	*p-value*	*OR*	*95% CI*	*p-value*
(Intercept)	0.11	0.06-0.20	<0.001	0.09	0.05-0.19	<0.001
Business size (ref: small)						
Medium	0.79	0.45-1.39	0.423	0.83	0.42-1.63	0.597
Large	0.62	0.15-2.19	0.475	0.68	0.13-2.96	0.615
Business sector (ref: Manufacturing, transportation and construction)						
Retail, accommodation and entertainment services	0.78	0.56-1.09	0.144	0.81	0.54-1.22	0.315
Information, administrative and financial services	0.85	0.61-1.19	0.357	0.75	0.49-1.17	0.208
Tech, knowledge and health	0.94	0.71-1.26	0.693	1.05	0.72-1.51	0.808
Crime type (ref: Malware)						
Attack to website/online service	1.63	0.91-2.88	0.096	1.70	0.92-3.13	0.087
Fraudulent email	1.85	1.31-2.62	<0.001	1.98	1.31-3.01	0.001
Hacking bank accounts or computers	3.42	2.03-5.83	<0.001	4.07	2.18-7.75	<0.001
Impersonating business	3.09	2.03-4.73	<0.001	2.85	1.73-4.74	<0.001
Unauthorised use of computer by staff	1.41	0.37-5.02	0.599	2.24	0.44-13.07	0.331
Other	1.29	0.62-2.65	0.490	2.30	0.84-6.30	0.101
Management of cybersecurity (ref: no management)						
External	2.12	1.43-3.16	<0.001	2.07	1.24-3.49	0.006
Internal	0.63	0.41-0.97	0.034	0.63	0.36-1.11	0.109
High priority *(ref: no)*	1.40	0.96-2.04	0.079	1.69	1.08-2.69	0.024
Received Government information *(ref: no)*	1.23	0.94-1.62	0.135	1.16	0.82-1.65	0.403
Negative outcome or impact *(ref: no)*	1.77	1.37-2.28	<0.001	1.89	1.37-2.61	<0.001
Insurance *(ref: no)*	1.16	0.90-1.51	0.255	1.19	0.79-1.79	0.417
Personal data held electronically *(ref: no)*	1.00	0.77-1.28	0.971	0.68	0.50-0.94	0.020
System to pay or order online *(ref: no)*	0.88	0.67-1.15	0.347	0.89	0.64-1.25	0.505
Online banking *(ref: no)*	1.27	0.92-1.74	0.145	1.04	0.71-1.52	0.854
Personally-owned devices *(ref: no)*	0.94	0.75-1.18	0.596	1.01	0.76-1.35	0.947
Activities to identify risks *(ref: no)*	1.20	0.88-1.63	0.244	1.49	1.01-2.21	0.045
Preparedness *(ref: no)*				1.17	0.83-1.65	0.367
Training *(ref: no)*				1.12	0.81-1.55	0.490
Sample		1,621			1,089	
McFadden’s Pseudo R^2		0.10			0.12	
Nagelkerke’s Pseudo R^2		0.17			0.19	
Veall-Zimmermann 's Pseudo R^2		0.21			0.23	

Finally, in Model 2 some cybersecurity-related activities show a statistical association with reporting cybercrime to someone outside the organisation. On the one hand, businesses that electronically hold data about their customers are 32% less likely to report cybercrime victimisation to external organisations than businesses that do not hold customer data. On the other hand, companies that carry out activities to identify cybersecurity risks are 49% more likely to report the incident they suffered than companies that do not try to identify cyber risks. We do not find statistically significant associations between cybercrime reporting and having cybersecurity insurance, seeking cybersecurity information from government sources, having systems to pay or order online, using online banking, and employees using personally-owned devices. Perceived cybersecurity preparedness and training to employees are not associated with cybercrime reporting either.

4.2 Reporting to public authorities

Table 3 presents the results of the binary logistic regression models used to estimate the likelihood of businesses reporting cybercrime to public authorities. Firstly, we see in Model 3 (rounds 2018 to 2020) that information, administrative and financial service businesses are less likely to report cybercrime to public authorities than manufacturing, transportation and construction businesses, but the statistical association is relatively weak ($p<0.1$). We also observe that four cybercrime types are associated with increased odds of reporting victimisation to public authorities in comparison to the reference category of malware infections: Suffering attacks to the website or online services, receiving fraudulent emails or being directed to fraudulent websites, hacking of the company bank account or computer system, and impersonation of the organisation in emails or online. This is the case for both Model 3 and Model 4. Experiencing a negative impact also shows a positive statistical association with reporting cyber-victimisation to public entities. In both models, the likelihood of reporting to public authorities is almost three times greater when the cybercrime incident produces a negative outcome or impact.

With regard to the priority given to cybersecurity, the results of Model 4 show that businesses that state cybersecurity is a high priority are almost four times more likely to report cyber victimisation to public authorities than organisations that consider it is not a high priority. In contrast to the results of the models for reporting cybercrime to anyone outside the organisation (Models 1 and 2), having external cybersecurity risk management arrangements is not associated with reporting to public authorities. Having internal cyber risk management may be associated with greater odds of cybercrime reporting to public organisations (OR=2.13, Model 3), but the p-value indicates a very weak statistical association (p=0.085).

The cybersecurity activities conducted by businesses do not appear to be associated with reporting cybercrime to public authorities. The only variable that shows a weak association is whether the members of the organisation use personal devices for work-related activities. In Model 3 the OR is 0.69 (p=0.07) and in Model 4 the OR is 0.66 (p=0.096), thereby suggesting that organisations that use personal devices for work may be less likely to report cybercrime incidents to public authorities in comparison to organisations that do not use personal devices. As seen above, we do not find statistically significant associations between reporting to public authorities and receiving government information on cybersecurity, having insurance, enabling systems to pay/order online, using online banking, perceived cybersecurity preparedness and providing cybersecurity training. Moreover, in this case, conducting specific activities to identify cybersecurity risks does not show a significant association with cybercrime reporting.

Table 3. Logistic regression models of businesses' cybercrime reporting to public authorities

	Model 3 (2018, 2019 and 2020 rounds)			Model 4 (2018 and 2019 rounds)		
Predictor	*OR*	*95% CI*	*p-value*	*OR*	*95% CI*	*p-value*
(Intercept)	0.00	0.00-0.01	<0.001	0.00	0.00-0.02	<0.001
Business size (ref: small)						
Medium	0.85	0.29-2.05	0.742	0.71	0.19-2.04	0.558
Large	1.15	0.11-5.72	0.884	1.13	0.07-7.29	0.909
Business sector (ref: Manufacturing, transportation and construction)						
Retail, accommodation and entertainment services	1.01	0.57-1.78	0.973	0.83	0.39-1.72	0.611
Information, administrative and financial services	0.52	0.26-0.99	0.053	0.73	0.32-1.59	0.438
Tech, knowledge and health	1.05	0.63-1.74	0.858	1.29	0.69-2.44	0.434
Crime type (ref: Malware)						
Attack to website/online service	4.69	1.27-18.03	0.019	4.46	1.12-19.80	0.036
Fraudulent email	5.24	2.16-16.14	0.001	5.35	1.93-19.71	0.004
Hacking bank accounts or computers	18.14	6.83-58.90	<0.001	19.91	6.46-78.03	<0.001
Impersonating business	13.88	5.55-43.44	<0.001	17.40	6.14-65.04	<0.001
Unauthorised use of computer by staff	0.30		0.734	0.55		0.867
Other	1.65	0.13-9.91	0.623	1.51	0.01-15.96	0.783
Management of cybersecurity (ref: no management)						
External	1.62	0.73-3.90	0.255	1.30	0.48-3.89	0.622
Internal	2.13	0.93-5.27	0.085	1.93	0.69-5.95	0.227
High priority *(ref: no)*	1.88	0.88-4.56	0.129	3.76	1.33-14.31	0.025
Received Government information *(ref: no)*	1.16	0.71-1.93	0.559	1.14	0.62-2.17	0.687
Negative outcome or impact *(ref: no)*	2.80	1.76-4.53	<0.001	2.71	1.53-4.93	0.001
Insurance *(ref: no)*	0.91	0.58-1.43	0.700	1.64	0.87-3.03	0.120
Personal data held electronically *(ref: no)*	1.15	0.73-1.83	0.550	0.89	0.52-1.56	0.681
System to pay or order online *(ref: no)*	0.77	0.46-1.24	0.298	0.77	0.41-1.36	0.376
Online banking *(ref: no)*	0.84	0.50-1.48	0.530	0.67	0.36-1.31	0.225
Personally-owned devices *(ref: no)*	0.69	0.46-1.03	0.070	0.66	0.40-1.07	0.096
Activities to identify risks *(ref: no)*	0.86	0.49-1.58	0.627	0.92	0.45-1.93	0.817
Preparedness *(ref: no)*				0.81	0.46-1.49	0.492
Training *(ref: no)*				0.85	0.48-1.49	0.579
Sample		1,621			1,089	
McFadden's Pseudo R^2		0.14			0.18	
Nagelkerke's Pseudo R^2		0.18			0.22	
Veall-Zimmermann 's Pseudo R^2		0.20			0.25	

5. Discussion and conclusions

Despite the growing threat cybercrime poses to private enterprises in the United Kingdom, there is scant research on cybercrime reporting by businesses. This notable gap in the literature is made even more salient given the extensive literature on traditional crime reporting by individuals, the emerging research on cybercrime reporting by individuals, and the importance of crime reporting for the design, implementation and evaluation of crime prevention and reaction strategies. In fact, incident reporting is a recurring theme in the UK Government Cyber Security Strategy 2016-2021 and is mentioned on several occasions as a key element in the sections entitled "Managing incidents and understanding the threat", in which the need for clear, centralised incident reporting processes is highlighted, and "Reducing cyber crime", which emphasises the importance of promoting timely reporting to aid prevention and reaction strategies (UK Government, 2016). To begin to fill this research gap, the present study analysed data from the CSBS to answer three research questions regarding whether the characteristics of businesses, the cybersecurity strategies used by businesses, and the characteristics of the cybercrime event are associated with cybercrime reporting to anyone outside the organisation or to public authorities.

Previous research has found a statistical association between the characteristics of individuals and businesses and the decision to report to the police or other authorities (Baumer and Lauritsen, 2010; Goudriaan et al., 2006; Isenring et al., 2016; Taylor, 2002; van de Weijer et al., 2019). The present study finds limited evidence of this, as the size and sector of the businesses show, in most cases, no association with reporting cybercrime to someone outside the organisation. We found, however, preliminary indicators that administrative and financial service companies may be less likely to report cybercrime victimisation to public authorities than other business sectors. Although further evidence is needed, one may expect administrative and financial sector businesses to be particularly concerned about the potential reputational damage that cyber-attacks may have for the company, since customers losing trust in financial products and services may have severe financial implications (Lagazio et al., 2014). This could explain why specific, distinct organisational reporting structures (i.e., hierarchical structures within an organisation through which cybersecurity information is communicated and that define how decisions are made) have been identified in these sectors (Karanja, 2017).

Inconsistent results are found for certain activities carried out by businesses, such as holding personal data electronically, conducting cybersecurity risk identification activities, and employees using personal devices for work-related tasks. The findings indicate that businesses in which staff use personal devices for work are less likely to report cybercrime victimisation to public authorities, while this association was not significant in the models of reporting to anyone outside the organisation. On the one hand, this could be related to the greater difficulty to gather evidence of attacks when the security perimeter is so wide. Collecting evidence to demonstrate to public authorities that a cybercrime has been committed may involve company access to personal devices, which could generate complications with regard to privacy legislation. It has been noted that rapid regulatory changes with regard to data protection can lead enterprises to feel like they are "operating in a constant fog" (Caldwell, 2012: 5). Alternatively, it could be that this is related to a shift in who is considered the "guardian" of companies' information systems. Secure teleworking is especially relevant in the post-COVID world, and businesses that allow staff to perform work-related tasks on personal devices may also consider that employees are therefore responsible for cybersecurity and reacting to cyber-attacks. This has been suggested as a potential motive for the lack of discernible rises in cybercrime reported by organisations during the early stages of the pandemic (Kemp et al.,

2021) and points to an important line of future research: how does homeworking affect perceptions of capable guardianship in relation to cybercrime?

The relationship between attitudes towards the criminal justice system and crime reporting has been subject to much criminological inquiry, with somewhat inconclusive results (Xie and Baumer, 2019). While the survey employed in this study did not probe opinions on the criminal justice system, the present article inquires about the relationship between businesses' attitudes towards cybersecurity and cybercrime reporting. In this sense, three of the models used herein find that organisations that consider cybersecurity a high priority are more likely to report cyber-victimisation. The rational-choice model of crime reporting suggests that the possible benefits of reporting crime are not only related to recovering direct losses from victimisation but may also include helping to create a safer environment for all (Bowles et al., 2009). Victimisation reporting can be perceived to help achieve these benefits by raising awareness of the problem and encouraging greater investment in prevention (Laube and Böhme, 2016). The association between the priority given to cybersecurity by businesses and cybercrime reporting may be related to the perceived benefit of helping create a safer cyber environment.

Rational choice decision-making in relation to cybercrime reporting by businesses is also evidenced in our study by the fact that there is a positive association between suffering a negative impact/outcome from victimisation and the likelihood of reporting. Previous research found the severity of the crime to be a strong predictor of reporting traditional crime (Goudriaan et al., 2006) and, in this sense, the benefits of reporting may appear greater and the related costs of reporting may appear smaller when the severity of the crime is higher. However, having cybersecurity insurance, which can help to reduce the negative consequences of victimisation, is not associated with reporting cyber victimisation in our study. This is somewhat surprising given prior research has found having insurance to positively influence crime reporting (Statistics Canada, 2020; Tarling and Morris, 2010). This may be because insurance is only relevant for cybercrimes that produce notable negative impacts that can be quantified economically, for instance, CEO frauds involving considerable amounts, or DDoS attacks that generate large economic losses as a result of the collapse of the main online purchasing system. Future research could examine the severity of crime in terms of economic losses and how this is associated with reporting. Similarly, certain types of negative impacts may activate mandatory reporting requirements (e.g., GDPR) that are likely to shape reporting, and this may account for some of the decision-making (Laube and Böhme, 2016). However, it is important for policy-makers to consider reporting incentives and to not generate an "underreporting loop" when mandating reporting (Basuchoudhary and Searle, 2019: 3).

The present study has found that the type of cybercrime suffered is a strong predictor of the likelihood of reporting. The results have shown that in comparison to malware infections, there is greater likelihood of reporting cybercrimes such as attacks that try to take down websites or online services, receiving fraudulent emails or being directed to fraudulent websites, hacking of bank accounts or computer systems, and impersonation of the organisation in emails or online. Nevertheless, due to the small sample size and the nature of the secondary data employed herein, our study does not allow analysis of very specific crime types, such as CEO fraud or DDoS attacks, or specific negative impacts, such as financial losses. Future research should delve deeper into how the different outcomes from various crime types affect the response from businesses, and how having insurance or the legal obligations to report interact with this process.

Finally, the findings of the present study generate notable discussion regarding the role of private cybersecurity companies and the criminal justice system in the prevention of cybercrime. The descriptive results show that only 8% of the most disruptive incidents suffered by businesses were reported to public authorities, while 39.5% were reported to someone outside the organisation (including private and public agencies). This figure is similar to those found in previous research (Rantala, 2008; Wanamaker, 2019) and could be indicative of private entities preferring a private model of crime control regarding cybercrime. In this sense, low levels of business reporting to public authorities may be the result of a lack of confidence in the capacity of public authorities to provide a suitable response, perceptions that attacks can straightforwardly be dealt with 'internally', concerns about potential reputational damage by 'going public', or not wishing to share internet or business activity history with public authorities (Caneppele and Aebi, 2017; Lavorgna, 2020). Indeed, the disparity between reporting to public authorities and reporting to anyone outside the organisation exemplifies the rise of private policing that has been documented with regard to cybercrime (Button, 2020). Some argue that police forces appear underprepared to deal with this type of crime (Bossler et al., 2020; Hadlington et al., 2018) and, thus, the criminal justice system focuses its scarce resources on more 'manageable' local crime. Cybercrime, which is characterised by its transnationality, becomes the domain of the private security sector and the police take a more minor role (Button, 2020).

The results show that businesses with outsourced cybersecurity management report more to other organisations but not to public authorities. Could this indicate that cybersecurity companies, either directly or indirectly, discourage reporting to public authorities due to a lack of confidence in their ability to deal with the issue? Is there potentially an economic interest in reducing the involvement of public authorities? Like all private enterprises, the main objective of cybersecurity companies is to generate profits, and in a highly competitive sector, minimising the role of the public sector could help achieve this goal. On the other hand, our findings reveal that while businesses with internal cybersecurity teams show a negative association with reporting to someone else, this association becomes positive (although weak) when analysing reporting to public authorities. Do in-house cybersecurity teams trust public authorities more? Are they less driven by a direct profit motive and thus more inclined to seek external public help? These questions advocate for further qualitative research on the decision-making process with regard to reporting cybercrime and how this relates to organisations' "security regimes" (Dupont, 2014). Qualitative research along these lines would provide further insight into the reasons that motivate reporting by businesses, and to whom incidents are reported, thereby generating knowledge on the dynamics that shape policing in the digital era. The CSBS also records in-depth qualitative data from interviewing a smaller sample of organisations, which may bring valuable information to enhance our analysis. While interview transcripts are not available for download, future research could request access to these to obtain further insights into the reporting of cybersecurity incidents.

While the results presented in this paper are first-of-its-kind and have important implications for research and practice, they are not free from limitations. There are some considerations that may affect the secondary data being used, and which further research should consider when developing *ad hoc* questionnaires or recording qualitative information. First, it is likely that the cap of one crime recorded by businesses may increase crime reporting rates artificially, since the survey only probes reporting practices for the most disruptive attack suffered by each organisation, and thus the one that is most likely to be reported. It is therefore expected that cybercrime reporting rates may be even lower than those observed here. Second, in order to study cybercrime reporting to public authorities, we relied on businesses informing about the organisation to whom they reported crime, but the proportion of victimised businesses who answered “don’t know” or “no answer” is large (30.8%), and thus in our sample few businesses reported to public authorities. Future survey research should consider including a more direct question on reporting to public authorities (e.g., “Was this breach or attack reported to a UK public/Government authority?”). Thirdly, it is important to bear in mind that there may be a degree of overlap with the cybercrime categories. For instance, a malware infection could be the result of receiving fraudulent emails and could lead to hacking of online bank accounts. Distinguishing cybercrimes can be complex, and it is therefore essential that survey administrators ensure respondents can identify how the incident occurred. Relatedly, it may also be pertinent for future rounds of the survey to probe organisations about the types of incidents included in the Home Office Counting Rules for Recorded Crime (Home Office, 2013), thereby helping to promote homogeneity in terminology. Finally, previous research has indicated that one of the main reasons for businesses not to report a cyber-attack to authorities is the fear of reputational damage, and it is yet unknown whether some companies may also not disclose cybercrimes to the survey for the same reasons. Future qualitative research may provide further insights about the link between fear of reputational damage and reporting practices.

Appendix

Table A1. Characteristics of businesses in the Cyber Security Breaches Survey and the UK population of businesses

	Cyber Security Breaches Survey (unweighted)	Cyber Security Breaches Survey (weighted)	UK businesses
Size			
Small (1-49 staff)	3,001 (67.7%)	4,282 (96.6%)	1,223,545 (96.6%)
Medium (50-249 staff)	760 (17.1%)	124 (2.8%)	35,585 (2.8%)
Large (more than 250 staff)	672 (15.2%)	26.6 (0.6%)	7,685 (0.6%)
Sector			
Administration or real estate	321 (7.2%)	520 (11.7%)	625,365 (11.7%)
Construction	419 (9.5%)	862 (19.5%)	1,037,280 (19.5%)
Education	599 (13.5%)	255 (5.8%)	306,915 (5.8%)
Arts and entertainment	431 (9.7%)	241 (5.4%)	289,885 (5.4%)
Finance or insurance	297 (6.7%)	75.8 (1.7%)	90,730 (1.7%)
Food and hospitality	343 (7.7%)	168 (3.8%)	201,745 (3.8%)
Health, social care and social work	257 (5.8%)	300 (6.8%)	360,670 (6.8%)
Information and communications	347 (7.8%)	307 (6.9%)	369,545 (6.9%)
Professional, scientific or technical	456 (10.3%)	721 (16.3%)	867,880 (16.3%)
Retail or wholesale	214 (4.8%)	455 (10.3%)	547,380 (10.3%)
Transport or storage	259 (5.8%)	300 (6.8%)	360,485 (6.8%)
Utilities or production	490 (11.1%)	230 (5.2%)	276,190 (5.2%)

References

Basuchoudhary A and Searle N (2019) Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets. *Computers & Security* 87: 101591.

Baumer EP and Lauritsen JL (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.

Bossler AM, Holt TJ, Cross C and Burruss GW (2020) Policing fraud in England and Wales: Examining constables' and sergeants' online fraud preparedness. *Security Journal* 33(2): 311–328.

Bowles R, Garcia Reyes M and Garoupa N (2009) Crime Reporting Decisions and the Costs of Crime. *European Journal on Criminal Policy and Research* 15(4): 365-377.

Buil-Gil D, Lord N and Barrett E (2021) The Dynamics of Business, Cybersecurity and Cyber-victimization: Foregrounding the Internal Guardian in Prevention. *Victims and Offenders* 16(3): 286-315.

Button M (2020) The "New" Private Security Industry, the Private Policing of Cyberspace and the Regulatory Questions. *Journal of Contemporary Criminal Justice* 36(1): 39–55.

Caldwell T (2012) Reporting data breaches. *Computer Fraud & Security* 7: 5–10.

Caneppele S and Aebi MF (2017) Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. *Policing: A Journal of Policy and Practice* 13(1): 66–79.

Department for Business, Energy and Industrial Strategy (2019) Business population estimates 2019. Available at: https://www.gov.uk/government/statistics/business-population-estimates-2019 (accessed 13 March 2021).

Department of Digital, Culture, Media and Sport (2020) *Cyber Security Breaches Survey 2020. Technical annex.* Department of Digital, Culture, Media and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/874693/Technical_annex_-_Cyber_Security_Breaches_Survey_2020.pdf (accessed 15 March 2021).

Dugato M, Favarin S, Hideg G and Illyes A (2013) *Final Report of the Project: EU Survey to assess the level and impact of crimes against business*. European Commission.

Dupont B (2017) Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change* 67(1): 97–116.

Felson RB, Messner SF, Hoskin AW and Deane G (2002) Reasons for Reporting and Not Reporting Domestic Violence to the Police. *Criminology* 40(3): 617–648.

Goudriaan H, Wittebrood K and Nieuwbeerta P (2006) Neighbourhood Characteristics and Reporting Crime: Effects of Social Cohesion, Confidence in Police Effectiveness and Socio-Economic Disadvantage. *The British Journal of Criminology* 46(4): 719–742.

Graham A, Kulig TC and Cullen FT (2019) Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice. *Policing: An International Journal of Police Strategies and Management* 43(1): 1–16.

Hadlington L, Lumsden K, Black,A and Ferra F (2018) A Qualitative Exploration of Police Officers’ Experiences, Challenges, and Perceptions of Cybercrime. *Policing: A Journal of Policy and Practice* 090.

Home Office (2013) *Home Office Counting Rules for Recorded Crime*. Available at: https://www.gov.uk/government/publications/counting-rules-for-recorded-crime (accessed 21 July 2021).

Home Office (2019) *Crime against businesses: Findings from the 2018 Commercial Victimisation Survey* (Statistical Bulletin 17/19). Home Office. https://www.gov.uk/government/statistics/crime-against-businesses-findings-from-the-2018-commercial-victimisation-survey (accessed 15 March 2021).

Isenring GL, Mugellini G and Killias M (2016) The willingness to report employee offences to the police in the business sector: *European Journal of Criminology* 13(3): 372-392.

Karanja E. (2017) The role of the chief information security officer in the management of IT security. *Information & Computer Security* 25(3): 300–329.

Kemp S (2020) Fraud reporting in Catalonia in the Internet era: Determinants and motives. *European Journal of Criminology* 1477370820941405.

Kemp S, Buil-Gil D, Moneva A, Miró-Llinares F and Díaz-Castaño N (2021) Empty Streets, Busy Internet. A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. *Journal of Contemporary Criminal Justice*. Online First

Kemp S, Miró-Llinares F and Moneva A (2020) The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research* 26: 293-312.

Kennedy JP (2016) Shedding Light on Employee Theft's Dark Figure: A Typology of Employee Theft Nonreporting Rationalizations. *Organization Management Journal* 13(1): 49–60.

Lagazio M, Sherif N and Cushman M (2014) A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers and Security* 45: 58-74.

Lavorgna A (2020) *Cybercrimes: Critical Issues in a Global Context*. London: Red Globe Press.

Laube S and Böhme R (2016) The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* 2(1): 29–41.

Levi M, Doig A, Gundur R, Wall D and Williams M (2017) Cyberfraud and the implications for effective risk-based responses: Themes from UK research. *Crime, Law and Social Change* 67(1): 77–96.

National Crime Agency (n.d.) *Cyber crime*. Available at: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime (accessed 1 March 2021).

National Cyber Security Centre (2020) *Cyber Security Small Business Guide*. National Cyber Security Centre. Available at: https://www.ncsc.gov.uk/files/NCSC_A5_Small_Business_Guide_v4_OCT20.pdf (accessed 15 March 2021).

R Core Team (2021) *R: A language and environment for statistical computing*. R Foundation for Statistical Computing, Vienna, Austria.

Richards K (2009) *The Australian Business Assessment of Computer User Security: A national survey*. Australian Institute of Criminology.

Rantala RR (2008) *Cybercrime against Businesses, 2005*. Bureau of Justice Statistics. https://www.bjs.gov/index.cfm?ty=pbdetailandiid=769 (accessed 21 March 2021).

Reep-van den Bergh CMM and Junger M (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science* 7(1): 5.

Schoepfer A and Piquero NL (2009) Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice* 37(2): 209–215.

Statistics Canada (2020) *About one-fifth of Canadian businesses were impacted by cyber security incidents in 2019*. Statistics Canada. Available at: https://www150.statcan.gc.ca/n1/en/daily-quotidien/201020/dq201020a-eng.pdf?st=S7vCLC81 (accessed 22 March 2021).

Tarling R and Morris K (2010) Reporting Crime to the Police. *The British Journal of Criminology* 50(3): 474–490.

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

Tolsma J, Blaauw J and 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.

Tyler TR and Fagan J (2008) Legitimacy and Cooperation: Why Do People Help the Police Fight Crime in Their Communities. *Ohio State Journal of Criminal Law* 6: 231–275.

UK Government. (2016). *National Cyber Security Strategy 2016-2021*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (accessed 21 July 2021).

van de Weijer SGA, Leukfeldt R and Bernasco W (2019) Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology* 16(4): 486-508.

van de Weijer SGA, Leukfeldt R and van der Zee S (2020) Reporting cybercrime victimization: Determinants, motives, and previous experiences. *Policing: An International Journal* 43(1): 17–34.

van de Weijer SGA, Leukfeldt R and van der Zee S (2021) Cybercrime reporting behaviors among small- and medium-sized enterprises in the Netherlands. In: Weulen Kranenbarg M and Leukfeldt R (eds) *Cybercrime in context, crime and justice in digital society*. Switzerland: Springer, pp.303-325.

Van Wyk J and Mason KA (2001) Investigating Vulnerability and Reporting Behavior for Consumer Fraud Victimization: Opportunity as a Social Aspect of Age. *Journal of Contemporary Criminal Justice* 17(4): 328–345.

Wall DS (2007/10) Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace (Revised May 2010). *Police Practice and Research* 8(2): 183-205.

Wanamaker KA (2019) *Profile of Canadian Businesses who Report Cybercrime to Police. The 2017 Canadian Survey of Cyber Security and Cybercrime.* Research Report 2019–R006. Ottawa: Public Safety Canada.

Williams ML, Levi M, Burnap P and Gundur RV (2019) Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory. *Deviant Behavior* 40(9): 1119–1131.

Xie M and Baumer EP (2019) Crime Victims’ Decisions to Call the Police: Past Research and New Directions. *Annual Review of Criminology* 2(1): 217–240.

Xie M and Lauritsen JL (2012) Racial Context and Crime Reporting: A Test of Black’s Stratification Hypothesis. *Journal of Quantitative Criminology* 28(2): 265–293.

Yar M and Steinmetz KF (2019) *Cybercrime and society*. Third edition. London: SAGE.