The Dynamics of Business, Cybersecurity and Cyber-victimization: Foregrounding the Internal Guardian in Prevention

DOI:
10.1080/15564886.2020.1814468

Document Version
Accepted author manuscript

The Dynamics of Business, Cybersecurity and Cyber-victimization: Foregrounding the Internal Guardian in Prevention

[This article has been accepted for publication in Victims & Offenders, published by Taylor & Francis.]

Authors
David Buil-Gil. Department of Criminology, University of Manchester
Nicholas Lord. Department of Criminology, University of Manchester
Emma Barrett. Department of Criminology, University of Manchester

Contact details of corresponding author
David Buil-Gil. G18 Humanities Bridgeford Street Building, Cathie Marsh Institute for Social Research, University of Manchester. E-mail address: david.builgil@manchester.ac.uk

Acknowledgements
The authors would like to thank Jose Pina-Sánchez for comments that greatly improved the manuscript.

Abstract
Private organizations suffer great losses due to cybersecurity incidents, and they invest increasing resources to prevent attacks, but little is known about the effectiveness of cybersecurity measures for prevention. Based on the framework of Routine Activity Theory, this paper analyzes the impact of companies' online activities and cybersecurity measures on victimization. Our analysis of the UK Cybersecurity Breaches Survey shows that the most promising ways to minimize cyber-attacks and their impacts is to invest in in-house cybersecurity human resources and enhance the employees' online self-protection by providing cybersecurity training, rather than just basic software protection and guidance about strong passwords.

Keywords: data breaches, cybercrime, victimization survey, self-protection, cyber fraud, cybersecurity.

Full reference
Buil-Gil, D., Lord, N., Barrett, E. (2021). The Dynamics of Business, Cybersecurity and Cyber-victimization: Foregrounding the Internal Guardian in Prevention. *Victims & Offenders*. DOI:10.1080/15564886.2020.1814468

1. Introduction

The digital space and digital systems are core operating contexts for most businesses and their associated activities, whether entering into economic relations with customers purchasing goods and services, storing and sharing data, or undertaking commercially sensitive activities that involve confidential information (Office for National Statistics, 2019). As a result, one eighth of the UK National Gross Domestic Product depends directly on the digital economy (National Audit Office, 2019). The digital space, however, offers many new opportunities for crimes, including frauds, that may be enabled by, or dependent on, Internet-connected systems. In 2017, the UK Annual Fraud Indicator estimated that frauds were responsible for £140 billion losses for the private sector, £40 billion losses for the public sector and £6.8 billion losses for individuals (Crowe, 2017), and a report published by the National Audit Office (2017) identified that more than half of all frauds were committed online. Other cybersecurity risks, such as malware and denial of service attacks targeting businesses, have also increased in recent years (National Cyber Security Centre, 2017). Given that the private sector is a primary target of cybersecurity attacks and suffers from the greatest economic losses, private companies are investing more resources every day to prevent cybersecurity threats (EY, 2019; Levi et al., 2015), but little is known about the effectiveness of these measures to prevent cyber-attacks (e.g., Bilodeau et al., 2019; Rantala, 2008; Richards, 2006; Williams et al., 2019).

Despite the considerable financial losses suffered by businesses as a result of cybersecurity attacks, criminological research has typically focused on studying cyber-victimization among individual citizens (e.g., Holt and Bossler, 2016; Leukfeldt and Yar, 2016; Marcum et al., 2010). This is likely to be due to the lack of available and reliable sources of data to examine cybersecurity attacks on businesses. To fill this gap in literature, this article analyzes the dynamics of online business activities, cybersecurity measures and cyber-victimization. This article aims to illuminate which cybersecurity measures are effective in preventing cybersecurity breaches and attacks, and which measures are inefficient or ineffective. Based on the theoretical framework of Routine Activity Theory (RAT; Cohen and Felson, 1979) and considering the suitability of crime targets by their value, inertia, visibility and accessibility ('VIVA'), this paper analyzes how certain online activities and protective measures implemented by organizations affect their likelihood of falling victims to cyber-attacks. Thus, the original contribution of this paper is to show the utility of RAT for understanding businesses' victimization by cybersecurity attacks and breaches, and more specifically to foreground the internal guardian and personal self-protection as effective ways

to minimize cybersecurity attacks and their impacts. This research is concerned mainly with businesses' victimization by cyber-dependent crimes such as computer viruses, spam, hacking and denial of service attacks (Wall, 2007).

The remainder of this paper is organized as follows. Section 2 examines the role of businesses' online activities and cybersecurity measures for cybercrime prevention. Section 3 applies the notions of guardianship and the VIVA to business victimization by cybersecurity attacks. Section 4 introduces the data and methods used. Section 5 presents the results of our models. Finally, section 6 discusses the results and presents conclusions and implications.

2. Businesses online activities, cybersecurity and cyber-victimization

Few empirical studies have analyzed cybercrimes suffered by organizations. In this section we summarize the results of the main research analyzing the impact of organizations' cybersecurity measures and online activities on cybercrime victimization.

Rantala (2008) analyzed data from the 2005 US National Computer Security Survey and found that 67% of the 7,818 participant companies had suffered at least one cybersecurity incident in the previous year. The most common cybercrimes suffered by organizations were spyware, adware, phishing and spoofing. Richards (2006) conducted a survey of 4,000 businesses in Australia and found that the most common types of cybercrime suffered by organizations were virus and malware infections, and the most prevalent impact of cybercrime on businesses was the corruption of hardware or software. Moreover, Richards (2006) showed that only eight percent of victims reported cybersecurity incidents to the police, which highlights the value of survey data and the limitations of relying on police-recorded incidents for cybercrime research (Kemp et al., 2020). HISCOX (2018) surveyed 4,103 professionals responsible for the cybersecurity of UK small businesses and found that 30% had suffered cybersecurity breaches in the previous year. Incidents had an average direct cost of £25,700 (e.g., ransom paid, hardware replaced). Bilodeau et al. (2019) analyzed a survey of 10,794 businesses in Canada and found that 21% of organizations were impacted by cybersecurity incidents at least once in the last twelve months (mainly scam, online fraud, phishing and computer viruses). Williams et al. (2019) surveyed 751 businesses in the UK in order to analyze insider cybercrime victimization and found that less than 10% of organizations reported experiencing insider cyber-victimization.

The prevalence of cybercrimes, however, varies across business sectors and sizes, and certain cybersecurity measures appear to have better results for cybercrime prevention than

others. For example, Rantala (2008) found that telecommunication businesses, computer system design companies and manufacturers of durable goods have a higher prevalence of cyber-victimization, whereas administrative support, finance and food service businesses suffer from greatest economic losses. Forestry, fishing, hunting and agriculture businesses had the lowest victimization rates. Bilodeau et al. (2019) show that banking institutions, universities and pipeline transportation companies suffer more cyber-attacks than other business sectors. Large companies tend to report the largest expenditures on cybersecurity, but these are also more likely to be targeted by cybercriminals and suffer the greatest financial losses (Bilodeau et al., 2019; Levi et al., 2015; Rantala, 2008; Richards, 2006).

Regarding the use of cybersecurity measures for prevention, Rantala (2008) observed that companies that outsource all or part of their cybersecurity to external providers have, on average, a higher prevalence of cybersecurity incidents, while companies with in-house cybersecurity services suffer fewer attacks. There are, however, different types of outsourced security practices. For instance, companies that outsource their physical security are much more likely to report cybercrimes than companies with in-house physical security, but organizations with outsourced network watch centers have a smaller prevalence of incidents than those with in-house network watch centers (Rantala, 2008). This shows the need to distinguish between outsourced and in-house forms of guardianship when analyzing cybercrime victimization among businesses. Similarly, others argue that the best measures to prevent future cyber-attacks are to encourage employees and managers to become self-protected by increasing cyber threat awareness at all levels of an organization, having a dedicated cybersecurity budget, and instituting ongoing cybersecurity training (HISCOX, 2018; Williams et al., 2019). Williams et al. (2019) also show that companies with a cybersecurity manager appear to suffer more risk of cyber-victimization than companies without cybersecurity managers, but they argue that this may be because previous criminal victimization motivates businesses to adopt new security measures.

Rantala (2008) noted that most companies report that the use of antivirus software, internal controls, e-mail filters and firewalls are all inadequate to prevent cybersecurity incidents, whereas companies tend to report that biometrics, digital certificates, password generators and encryption are more adequate cybersecurity measures. Moreover, organizations where employees are provided with business-owned laptops reduce their risk of cybercrime victimization (Rantala, 2008), and companies that store confidential data are more likely to suffer cyber-attacks than companies that do not store confidential customer information

(Williams et al., 2019). Finally, Williams et al. (2019) did not find statistically significant associations between use of social media, e-commerce systems, WIFI networks and personal devices and insider cybercrime victimization.

Williams et al. (2019) argue that organizations' chances to suffer cyber-attacks may be reduced by applying cybersecurity measures aimed at preventing offenders from getting in contact with suitable targets under the absence of guardians (either by increasing the awareness and self-protection of employees or using measures to hindering the access to targets and making targets less visible online). They suggest applying RAT to understand how companies' characteristics and online protective measures can reduce the risk of online victimization.

3. Routine activities, the VIVA and cyber-attacks

Individual citizens' cyber-victimization has been primarily analyzed through a RAT lens (e.g., Bossler et al., 2012; Buil-Gil et al., 2020; Leukfeldt and Yar, 2016). RAT explains crime opportunities by the convergence in space and time of a potential offender, a suitable target and the absence of a guardian capable of protecting such target (Cohen and Felson, 1979). As Miró Llinares and Johnson (2017: 889) argue, "cybercrime can only happen when, through IT, an offender –or the outcome of his or her actions (e.g., when malware is opened)– converges at a certain place in cyberspace at a given moment with a suitable target in the absence of a guardian capable of preventing the event". In digital contexts, criminals can target many victims simultaneously, thus increasing opportunities for the triple convergence described by RAT (Miró Llinares and Johnson, 2017; Miró-Llinares and Moneva, 2020; Yar, 2005).

Others argue that the elements of VIVA (originally described by Cohen and Felson [1979] to explain the suitability of crime targets under the RAT) are key to assessing the attractiveness of online targets of crime (Yar, 2005). In the context of cybercrimes in e-commerce systems, Newman and Clarke (2003) argued that the Internet allows for an increased 'visibility' and 'accessibility' to crime targets, due to the absence of capable online guardians and the frequency and variety of everyday activities that individual users conduct online. Leukfeldt and Yar (2016) studied the effect of the elements of VIVA on six types of online crimes suffered by individual victims and concluded that the digital 'visibility' of users (i.e., the extent of online routine activities) increases the risk of cybercrime victimization. Leukfeldt and Yar (2016) also showed that the use of antivirus software (a form of technical guardianship) does not prevent most types of cybercrimes, using certain operating systems and browsers ('accessibility' to targets) may increase malware infections, and the users' knowledge and

awareness of online risks (i.e., personal guardianship or self-protection) reduces the risk of victimization by hacking and stalking. Similarly, many have shown that improving users' education about information security and promoting safe online behaviors is key to preventing various cybercrimes (Bossler and Holt, 2009; Bossler et al., 2012). Some argue that actions taken by individual persons to protect themselves should not be studied as forms of guardianship, but as self-protection strategies, since the guardian was originally conceptualized as a third party external to the victim and the offender (Miró Llinares, 2015).

This paper uses the theoretical framework of RAT and the VIVA to analyze the impact of organizations' online activities and cybersecurity measures on victimization by cybersecurity attacks. More specifically, we analyze which forms of online personal, social and technical guardianship are effective in preventing cybercrime victimization, and which elements of VIVA can be used to explain cybercrime suffered by organizations.

Capable guardianship and self-protection

Capable guardians serve to protect the targets and potential victims from crime victimization. Some cybercrime researchers argue that, in cyberspace, the guardian can take the form of personal and technical self-protection as well as formal and informal forms of social control (e.g., Holt and Bossler, 2008, 2016; Marcum et al., 2010); while others argue that the concept of 'capable guardian' only refers external parties (e.g., parents, neighbors, friends, line managers, colleagues, police), who reduce the likelihood of cybercrime victimization (Miró Llinares, 2015; Miró Llinares and Johnson, 2017). We distinguish among the following forms of guardianship and self-protection in our analyses:

(a) Technical self-protection. This mainly refers to the use of software security applications to protect digital systems from malicious content. Technical self-protection may refer to the use of access control software, anti-malware, anti-spyware, firewalls, antivirus software and other software aimed at defending computer systems against intrusions and unauthorized use of resources. Research has shown that software protection is usually not enough to prevent cybercrime victimization (e.g., Leukfeldt and Yar, 2016; Rantala, 2008).

(b) Personal self-protection. This describes those behaviors and actions taken by employees to protect themselves and the company from internal and external cybersecurity attacks (Miró Llinares, 2015). Thus, it refers to behavioral changes that those working in an organization can take to become better informed about digital risks

and mitigate potential cybersecurity threats (Bossler et al., 2012). Personal self-protection can involve, for example, the use of strong passwords, general awareness about digital risks, avoiding doing business with suppliers that fail to adhere to cybersecurity standards, or attending cybersecurity seminars and training (Klein, 1990; Williams et al., 2019).

(c) In-house guardianship. In the context of individual cybercrime prevention, the concept of 'social guardianship' is used to refer to family or peers who protect the victim from an attack (Holt and Bossler, 2016). 'Social guardianship' measures actions taken by someone other than the potential victim to protect the latter from becoming a victim of crime. Here we distinguish between in-house and outsourced forms of social guardianship, given that previous research has found that these have different effects on businesses' cybercrime victimization (Rantala, 2008). 'In-house guardianship' refers to whether companies implement internal cybersecurity controls and have members of the staff dedicated to cybersecurity (e.g., employees whose role includes information security, board members with responsibility for cybersecurity). In other words, by 'in-house guardianship' we refer to actions taken by personnel with cybersecurity responsibility within the company to protect the organizations' systems.

(d) Outsourced guardianship. Many businesses outsource their cybersecurity to third-party expert companies. Outsourced cybersecurity services appear to have different effects on cybercrime victimization than in-house cybersecurity teams. For instance, Rantala (2008) observed that those organizations who outsource their physical security, equipment decommissioning, periodic audits, risk assessments, disaster recovery plans, or the regular review of systems are more likely to report cyber-attacks than those businesses that have in-house teams to conduct these activities. Thus, by 'outsourced guardianship' we measure actions taken by third-party companies to protect the cybersecurity of the organization.

Value

Those individuals and objects which cybercriminals perceive to be more valuable are those that are more frequently targeted (Holt et al, 2020). While offline 'value' is frequently associated with monetary worth, in cyberspace it tends to be an expression of information (as a route to financial gain): "the focus of cybercrime, therefore, is to acquire information in order to extract its value" (Wall, 2007: 36). This is why Yar (2005) argues that most cybercrime targets are 'informational' in nature. Information held by businesses can be exploited for financial gain,

including by holding data to ransom, using confidential information to facilitate fraud, or selling customer details to other criminals to be used in identity fraud. Those businesses with confidential customer information, for instance, may be perceived as more valuable by cybercriminals (Williams et al., 2019).

Inertia

Cohen and Felson's (1979) original concept of 'inertia' refers to an object's physical properties (size, weight, shape) that define the ease with which it can be removed. Since objects in cyberspace are not defined by physical properties, the notion of 'inertia' takes on a different meaning in cybercrime. Some argue that the volume of data of electronic files and their technological specifications retain inertia properties, since these offer resistance for the target to be taken or copied (Yar, 2005). Other cybersecurity measures, such as the use of encryption, may also be seen as forms of inertia, since they impede or make it difficult for offenders to remove valuable information from compromised files and infected systems (Rantala, 2008).

Visibility

Objects and individuals that are more visible to offenders are more likely to become crime targets. Online, targets become visible to cybercriminals through users' communication and interaction with others: "when goods are introduced, voluntarily or not, and if they are not protected, they are exposed to risk, but they will only be suitable targets when they become visible to the offender" (Miró Llinares, 2015: 51). The more interaction an object or user has with others online, the higher its visibility and the more likely it is of becoming a target of a cybercrime. Newman and Clarke (2003) argued that the variety of activities that Internet users conduct increase their online visibility, and Leukfeldt and Yar (2016) showed that users' online visibility is one of the main predictors of most forms of cyber-victimization (see also Marcum et al., 2010).

Accessibility

The concept of 'accessibility' refers to the ease with which offenders can come into direct contact with a target. As argued by Leukfeldt and Yar (2016), while in the physical world 'accessibility' refers to the characteristics of micro places that allow offenders to approach targets, in cyberspace the accessibility is party determined by the operating systems and web browsers used by users, since offenders *access* the target by abusing the holes in such systems. Restricting the access to confidential files or information to certified users also reduces the accessibility to data (Miró Llinares and Johnson, 2017). For instance, Rantala (2008) probed

businesses' perceptions of adequacy of cybersecurity measures and found that the use of biometrics and digital certificates were considered adequate cybersecurity measures.

4. Data and methods

This section introduces the data and modeling approaches used to analyze cybersecurity attacks to UK businesses and charities. After describing the UK Cybersecurity Breaches Survey (CSBS) and its sampling strategy, we present our dependent variables, predictors and control variables. Finally, we introduce the modeling approaches used in this paper.

4.1 Cybersecurity Breaches Survey

The CSBS is a survey of UK businesses and charities that records information about digital threats faced by organizations and preventive measures to deter cybersecurity attacks and breaches. It has been conducted annually since 2016, and this paper examines data recorded in its 2018 edition. The survey included a quantitative random probability sample of 1,519 businesses and 569 charities, and qualitative interviews with 50 organizations. We have been granted access to the quantitative dataset, but not the interviews, to conduct this research.

The CSBS sample is designed to be representative of all UK businesses across different sizes and sectors and all charities across all income bands (Department for Digital, Culture, Media & Sport, 2018). The sampling frame is all private companies and non-profit organizations (whole organizations, not local establishments) with more than one employee, including universities, schools and colleges. Public sector organizations are not included in the sample, since these are typically subject to high cybersecurity standards. Businesses in the agriculture, forestry and fishing sectors are also excluded from the sample given their relative lack of e-commerce. Organizations without computers, websites or online presence and sole traders are also excluded.

The sample of businesses is proportionately stratified by UK regions and disproportionately stratified by the organizations' size and sector. This is done to effectively include medium and large businesses in the sample, which represent only a small proportion of all UK companies. Post-survey weighting is then used to correct for disproportionate stratification. Similarly, the sample of charities is proportionately stratified by country and disproportionately stratified by income bands to allow for a sample of high-income charities (Department for Digital, Culture, Media & Sport, 2018). Interviews were conducted using Computer-Assisted Telephone Interviewing (CATI) between October and December 2017.

Non-interlocking Random Iterative Method (RIM) was used by the original survey administrators to compute survey weights that allow adjusting for non-response bias and disproportionate sampling. Thus, the weighted sample is representative of the UK population of businesses and charities. RIM weighting by size and sector is used for businesses and RIM by income band and county for charities (Department for Digital, Culture, Media & Sport, 2018). Table 1 summarizes the characteristics of the sampled businesses and charities before and after applying the survey weights.

Table 1. Characteristics of businesses and charities sampled (frequency and percentage).

	Unweighted	Weighted
Business or charity (n = 2088)		
Business (including social enterprise)	1502 (71.9%)	1509 (72.3%)
Charity or voluntary sector organization	569 (27.3%)	569 (27.2%)
Don't know	17 (0.8%)	10 (0.5%)
Sector of business (n = 1519)		
Retail and wholesale	217 (14.3%)	280 (18.4%)
Administration or real estate	150 (9.9%)	190 (12.5%)
Construction	145 (9.5%)	189 (12.4%)
Food or hospitality	119 (7.8%)	151 (9.9%)
Finance or insurance	105 (6.9%)	25 (1.6%)
Health, care or social work	101 (6.6%)	73 (4.8%)
Information or communication	99 (6.5%)	93 (6.1%)
Other	583 (38.4%)	517 (34.0%)
Income, turnover or sales (n = 2088)		
Less than £100,000	344 (16.5%)	636 (30.4%)
£100,000 to less than £500,000	455 (21.8%)	524 (25.1%)
£500,000 to less than £5 million	488 (23.4%)	449 (21.5%)
£5 million or more	418 (20.0%)	127 (6.1%)
Don't know	383 (18.3%)	352 (16.8%)
Companies' size (employees, volunteers or trustees) (n = 2088)		
1 to 9	789 (37.8%)	1203 (57.6%)
10 to 49	600 (28.7%)	750 (35.9%)
50 to 249	384 (18.4%)	110 (5.3%)
More than 250	315 (15.1%)	25 (1.2%)
Digital characteristics (n = 2088; categories are not exclusive)		
Email addresses for your organization	1945 (93.2%)	1881 (90.1%)
A website or blog	1808 (86.6%)	1663 (79.7%)
Accounts on social media sites	1396 (66.9%)	1205 (57.2%)
The ability for users to make transactions online	727 (34.8%)	544 (26.1%)
Personal information about customers, users or donors held electronically	1347 (64.5%)	1102 (52.8%)

Source: Cybersecurity Breaches Survey 2018

4.2 Dependent variables

We apply various regression modeling approaches to explain three dependent variables: (a) the likelihood of suffering at least one cybersecurity breach or attack in the last 12 months, (b) the likelihood of suffering at least one negative impact or outcome due to cyber-attacks in the last 12 months, and (c) the number of cybersecurity attacks in the last 12 months. The first measure distinguishes organizations that have suffered at least one form of cyber-victimization from those that have not suffered any cyber-attack, which is the most common measure of cyber-victimization used in previous research (e.g., Bossler et al., 2012; Leukfeldt and Yar, 2016;

Williams et al., 2019). The second measure discriminates those UK businesses and charities that have suffered negative outcomes or impacts due to cybersecurity attacks from those that have not, in order to analyze the overall harm of cyber-victimization (see Paoli et al., 2018). And the third measures the number of attacks reported by each organization, which allows us to analyze whether variables that explain the binary outcome of cyber-victimization also explain the number of crimes (Hope, 2015).

Table 2 shows the frequency and percentage of organizations reporting various types of cybersecurity incidents. The most prevalent type of victimization is the receipt of fraudulent emails by members of the staff (reported by 27.5% of the weighted sample), followed by the impersonation of the organization by third parties (10.3% of weighted organizations) and the infection of computers by viruses (8.9%). The least common forms of cyber-victimization were hacking of bank accounts (2.7%), unauthorized use of hardware or software by staff members (2.4%) and other cybersecurity attacks (1.8%). In total, 36.6% of companies were victims of at least one form of cybersecurity attack in the last year.

Table 2. Proportion of businesses and charities that reported being victims of different forms of cybersecurity breaches or attacks during the last 12 months (weighted).

	Frequency and percentage
Staff receiving fraudulent emails or being directed to fraudulent websites	575 (27.5%)
People impersonating your organization in emails or online	215 (10.3%)
Computers infected with other viruses, spyware or malware	186 (8.9%)
Unauthorized use or hacking of PCs or networks by people outside your company	108 (5.2%)
Computers infected with ransomware	106 (5.1%)
Attacks that try to take down your website or online services	92 (4.4%)
Hacking or attempted hacking of online bank account	56 (2.7%)
Unauthorized use of computers, networks or servers by staff (even if accidental)	50 (2.4%)
Any other type of cybersecurity breaches or attacks	38 (1.8%)
Victims of at least one cybersecurity breach	764 (36.6%)

Source: Cybersecurity Breaches Survey 2018

With regards to the effect of cybersecurity attacks on organizations, 21.2% of companies reported suffering at least one negative impact or outcome due to cyber-attacks in the last year. As shown in Table 3, the most common impacts were the implementation of new measures to prevent future attacks (reported by 13.4% of the weighted sample), the use of additional staff time to deal with a breach (11.8%) and staff being stopped from carrying their daily work due to an attack (9.6%). Only 0.6% of organizations lost assets, trade secrets or intellectual property, 0.5% had to offer compensations or discounts to customers, and the 0.4% were fined by regulators or authorities or had to cover other legal costs.

Table 3. Proportion of companies that have experienced negative impacts or outcomes due to cybersecurity breaches or attacks during the last 12 months (weighted).

	Frequency and percentage
New measures needed to prevent future breaches	280 (13.4%)
Additional staff time to deal with the breach or attack	246 (11.8%)
Stopped staff from carrying out day-to-day work	201 (9.6%)
Temporary loss of access to files or networks	170 (8.1%)
Any other repair or recovery costs	145 (6.9%)
Software or systems corrupted or damaged	112 (5.4%)
Website or online services taken down or made slower	80 (3.8%)
Lost access to third-party services you rely on	55 (2.6%)
Prevented provision of goods or services to customers	45 (2.2%)
Money was stolen	41 (2.0%)
Complaints from customers	38 (1.8%)
Permanent loss of files (other than personal data)	38 (1.8%)
Loss of revenue or share value	30 (1.4%)
Reputational damage	27 (1.3%)
Discouraged from carrying out a future business activity	24 (1.1%)
Personal data altered, destroyed or taken	15 (0.7%)
Lost or stolen assets, trade secrets or intellectual property	13 (0.6%)
Goodwill compensation or discounts given to customers	10 (0.5%)
Fines from regulators or authorities, or associated legal costs	9 (0.4%)
Victims of at least one cybersecurity breach with at least one negative impact	442 (21.2%)

Source: Cybersecurity Breaches Survey 2018

More specifically, concerning the economic impact of cyber-victimization, 84.3% of the weighted sample of organizations reported no economic impact and 6.3% reported an economic impact of less than £500 (see Table 4). Only 1.4% of companies report financial losses greater than £10,000.

Table 4. Economic impact of cybersecurity attacks on businesses and charities (weighted).

Economic impact	Frequency and percentage
None	1347 (84.3%)
Less than £500	100 (6.3%)
£500 to less than £1,000	33 (2.1%)
£1,000 to less than £5,000	71 (4.4%)
£5,000 to less than £10,000	24 (1.5%)
£10,000 to less than £20,000	12 (0.8%)
£20,000 to less than £50,000	8 (0.5%)
£50,000 to less than £100,000	0 (0.0%)
£100,000 to less than £500,000	1 (0.1%)
£500,000 or more	0 (0.0%)
NAs	491

Source: Cybersecurity Breaches Survey 2018

Table 5 shows the summary statistics of our dependent variables. The binary measures of suffering at least one cybersecurity attack (including and excluding fraudulent emails) and suffering at least one negative impact or outcome do not show extreme distributions and can be analyzed by using logistic regressions for binary outcomes. However, the number of cybersecurity breaches is affected by a zero-inflated distribution and extreme values, which have a large impact on the sample's average and variance. A few organizations reporting a

large number of cyber-attacks affect the assumptions underlying statistical modeling and the robustness of our analyses. We apply a simple, but efficient, double square root transformation (or fourth root transformation) to stabilize the effect of large values and allow analyzing the number of cybersecurity attacks. The double square root transformation is applied because the single square root transformation did not effectively reduce the influence of extreme values. The double square root transformation is a well-known solution for skewed positive count variables used to diminish the impact of large numbers of crime victimization on the sample (see Xie et al., 2000, 2002). This data-transformation approach is preferred over other approaches since it can be easily performed also in the presence of zeros. Moreover, this transformation allows analyzing the full sample without the need to delete outliers.

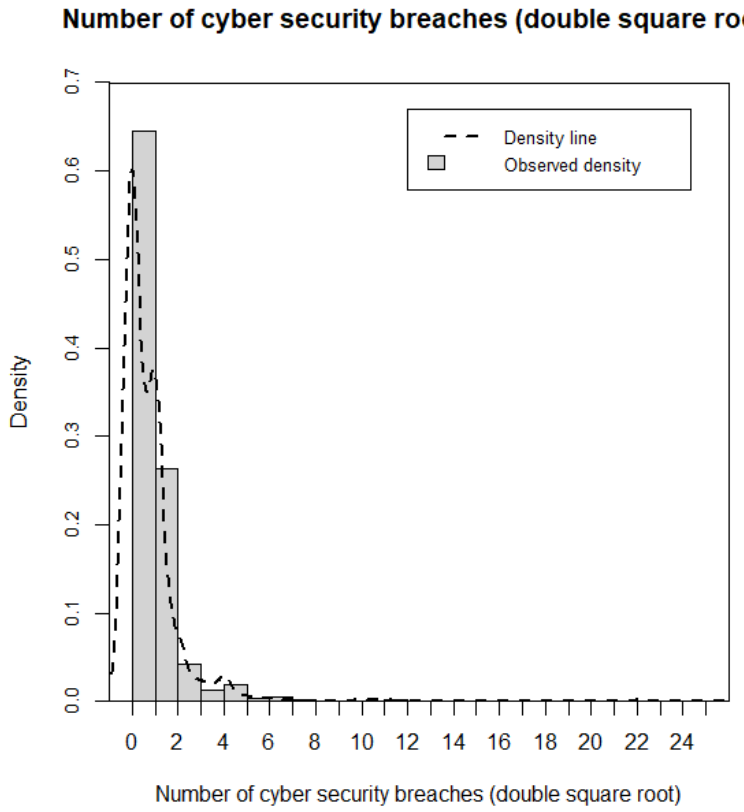
Table 5. Summary statistics about cybersecurity attacks on businesses and charities (weighted).

	Min.	1st q.	Mean	Median	3rd q.	Max.
At least one cybersecurity attack (0/1)	0	0	0.37	0	1	1
At least one cybersecurity attack – excluding fraudulent emails (0/1)	0	0	0.23	0	0	1
At least one negative impact due to cybersecurity attack (0/1)	0	0	0.21	0	0	1
Number of cybersecurity attacks – original	0	0	283.30	0	1	397795
Number of cybersecurity attacks – transformed by single square root	0	0	2.56	0	1	630
Number of cybersecurity attacks – transformed by double square root	0	0	0.59	0	1	25

Source: Cybersecurity Breaches Survey 2018

After transforming the dependent variable of number of cyber-attacks, the transformed average number of cybersecurity incidents faced by businesses is 0.59 and the maximum is 25. Nevertheless, the distribution of the number of cybersecurity attacks faced by companies still shows a zero-inflated distribution (see Figure 1), given that 64.5% of companies did not report any cybersecurity attacks in the previous year. In other words, most businesses and charities suffered zero breaches and attacks. Thus, the assumption of normal distribution is not met, and traditional linear models cannot be used. Instead, we use a Hurdle Negative Binomial model for zero-inflated data to analyze the number of cybersecurity breaches faced by organizations (see Section 4.5).

Figure 1. Distribution of number of cybersecurity breaches and attacks reported by businesses and charities (transformed by double square root).



4.3 Predictors

We will examine which cybersecurity measures effectively reduce the likelihood of falling victim to cybersecurity attacks, and which measures are inefficient or counter effective. Aside from the income and the digital characteristics of each company (e.g., use of social media, website or blog, personal information held electronically), which are summarized above in Table 1, we will also analyze those cybersecurity measures and online activities that may have an effect on the businesses' victimization by cybersecurity attacks. We use the companies' income and the measure of storing personal data electronically as proxy measures of 'value' (see Leukfeldt and Yar, 2016; Wall, 2007; Williams et al., 2019). Various measures of online presence (use of social media, websites, and institutional email addresses, amongst others) are used as indicators of the companies' 'visibility' to the general public (Miró Llinares, 2015; Newman and Clarke, 2003).

Amongst all cybersecurity measures reported by UK businesses and charities, the most commonly used are the application of software updates (applied by 87.1% of the weighted sample), updated malware protection (85.2%) and use of firewalls with appropriate

configuration (83.4%). These three represent forms of technical self-protection (Holt and Bossler, 2016; Leukfeldt and Yar, 2016). Restricting IT access rights to specific users, which is a measure of 'access', was also used by a large proportion of organizations (74.6%). Table 6 presents the frequency and percentage of companies that use each cybersecurity measure.

Table 6. Cybersecurity measures to prevent or manage breaches or attacks (weighted).

	Frequency and percentage
Applying software updates	1818 (87.1%)
Update malware protection	1779 (85.2%)
Firewalls with appropriate configuration	1741 (83.4%)
Restricting IT admin and access rights to specific users	1558 (74.6%)
Backing up data securely via means other than a cloud service	1367 (65.5%)
Guidance on acceptably strong passwords	1277 (61.2%)
Security controls on company-owned devices (e.g. laptops)	1225 (58.7%)
Externally-hosted web services	1211 (58.0%)
Only allowing access via company-owned devices	1182 (56.6%)
Backing up data securely via a cloud service	1105 (52.9%)
Outsourced provider that manages cybersecurity	866 (41.5%)
Monitoring of user activity	751 (36.0%)
Staff members whose role include information security	745 (35.7%)
Encrypting personal data	738 (35.4%)
Business-as-usual health checks to identify cybersecurity risks (last 12 months)	683 (32.7%)
A segregated guest wireless network	620 (29.7%)
Company directors are given updates around cybersecurity at least monthly	596 (28.6%)
Board members with responsibility for cybersecurity	592 (28.4%)
Formal policy covering cybersecurity risks	533 (25.5%)
A risk assessment covering cybersecurity risks (last 12 months)	469 (22.4%)
Someone has attended seminars or training on cybersecurity (last 12 months)	439 (21.0%)
Health checks beyond regular to identify cybersecurity risks (last 12 months)	423 (20.3%)
Internal audit to identify cybersecurity risks (last 12 months)	405 (19.4%)
Cyber risks documented in the Business Continuity Plan	365 (17.5%)
Require suppliers to adhere to cybersecurity standards or good practices	242 (11.6%)
Formal cybersecurity incident management processes	235 (11.3%)
Cyber risks documented in Company-level risk register	219 (10.5%)
Cyber risks documented in an Internal Audit Plan	200 (9.6%)
Cyber risks documented in Departmental risk registers	167 (8.0%)
Specific cybersecurity insurance policy	162 (7.8%)
Invested in threat intelligence (last 12 months)	150 (7.2%)

Source: Cybersecurity Breaches Survey 2018

In our regression models, we will only analyze as independent variables those cybersecurity measures that are related to at least one form of guardianship (or self-protection) or at least one of the elements of VIVA (Cohen and Felson, 1979; Yar, 2005). We will also analyze those measures implemented to facilitate the detection of digital vulnerabilities associated with one or multiple elements of VIVA (e.g., extraordinary checks to identify and document risks) and organizations' perceived preparedness for cybersecurity (i.e., agree that the company has enough people with the right skills and knowledge to effectively manage cybersecurity). Most predictors have been recoded as binary variables to distinguish between companies that apply and do not apply each measure. The companies' income was recoded as five dummy variables.

Moreover, we note that some explanatory variables have been aggregated to reduce the number of predictors in our models, in order to keep the models parsimonious and avoid multicollinearity. In this case, variables were aggregated directly by recoding various categorical questions asked within the surveys to binary measures of software protection, preparedness for cybersecurity, extraordinary cybersecurity checks, online platforms, and cybersecurity training. However, future research may explore the use of Latent Class Analysis to construct data-driven multidimensional constructs. For example, a new variable of 'basic software protection' has been constructed from the variables 'applying software updates', 'update malware protection' and 'firewalls with appropriate configuration', giving a score of 1 to those businesses that implement the three of them (74.6% of the weighted sample) and a score of 0 to the others. Similarly, a measure of perceived preparedness for cybersecurity is recoded from the questions "people dealing with cybersecurity in our organization have the right cybersecurity skills and knowledge to do this job effectively" and "we have enough people dealing with cybersecurity in our organization to effectively manage the risks". We assign a score 1 when the organization agrees with both statements (59.9%) and 0 otherwise. Having enough staff dedicated to cybersecurity may not be enough to prevent incidents if such group of people do not have adequate cybersecurity expertise, and having staff with cybersecurity skills may not be enough to reduce attacks if they are very few.

A variable of 'extraordinary cybersecurity checks' has been recoded from those measures identifying activities other than business-as-usual to identify digital risks (i.e., internal audit, ad-hoc check beyond regular processes, risk assessment, threat intelligence, external audit), with a score of 1 given to companies that undertook at least one of them in the last year (44.6% of the sample). We have also merged the measures of having a website and social media accounts, since these were highly correlated, to create a new variable that distinguishes those organizations that have both website and social media (54.0%) from the others. And the variable 'cybersecurity training' measures those companies in which someone has attended at least one cybersecurity seminar or conference or attended internal or external training on cybersecurity in the last year (21.0% of weighted sample).

4.4 Control variables

To minimize the risk of confounding bias, we include two groups of control variables in our models. First, we incorporate nine dummy variables to distinguish between companies' sectors (see Table 1), given that certain sectors are known to be more frequently victimized than others

(Bilodeau et al., 2019; Rantala, 2008; Richards, 2006). Second, the models also control for five dummy variables of total economic investment in cybersecurity, which allow examining whether cybersecurity breaches are affected by the cybersecurity measures included in the models or other investments in cybersecurity ignored by our models.

With regards to the organizations' overall economic investment in cybersecurity, most companies do not directly invest financial resources on this. As shown in Table 7, the proportion of businesses that do not invest in cybersecurity is large even among companies with large turnovers.

Table 7. Economic investment in cybersecurity by companies' turnover (weighted).

		Companies' turnover			
		Less than £100,000	£100,000 to £500,000	£500,000 to £5M	£5M or more
Investment in cybersecurity	Don't invest	357 (66.0%)	145 (21.3%)	110 (28.3%)	16 (16.7%)
	Less than £1,000	151 (28.0%)	206 (44.3%)	120 (30.9%)	19 (19.4%)
	£1,000 to less than £10,000	31 (5.8%)	98 (21.1%)	121 (31.1%)	33 (33.9%)
	£10,000 to less than £50,000	1 (0.2%)	15 (3.2%)	27 (6.9%)	21 (20.9%)
	£50,000 or more	0 (0.0%)	1 (0.1%)	10 (2.7%)	9 (9.2%)
	n	540	465	388	98
	%	100	100	100	100

Source: Cybersecurity Breaches Survey 2018
Note: n=1491 (NAs excluded)

4.5 Methods: Modeling strategy

We will make use of logistic regressions for binary outcomes to analyze the companies' likelihood of suffering at least one cybersecurity breach or attack in the last year (including and excluding fraudulent emails) and the companies' likelihood of suffering at least one negative outcome or impact due to cybersecurity attacks in the last year. We will use a Hurdle negative binomial regression for zero-inflated data to analyze the number of breaches suffered by UK businesses and charities.

Binary logistic regression is used to analyze the association between the likelihood of suffering at least one cybersecurity attack or at least one negative outcome and all independent and control variables (see Bonney, 1987). We will examine the Odds Ratio (OR) of each predictor and control variable, which is an indicator of the likelihood that the outcome under study (i.e., cybercrime victimization or negative outcome) occurs in one group (e.g., organizations that use basic software protection) relative to the odds of the reference group (e.g., no basic software protection). The R package 'stats' is used to fit the logistic regression models (R Core Team, 2020).

Hurdle negative binomial regression for zero-inflated data is used to model the organizations' number of cybersecurity breaches or attacks in last 12 months. Hurdle regression models are used to analyze discrete dependent variables with an excess of zeros, as is our case (see Fig. 1). It is a two-part modeling approach: the first part, the zero Hurdle model, estimates the binary outcome of having suffered zero or non-zero breaches or attacks in the last 12 months, whereas the second part, the so-called truncated Negative Binomial model, estimates the number of crimes suffered by companies with at least one reported victimization (see Cameron and Trivedi, 2005; Zeileis et al., 2008). As with binary logistic regression models, we will examine the predictors' OR relative to the reference group. We use the 'pscl' R package to fit the Hurdle negative binomial models (Jackman, 2020). We also considered the use of zero-inflated negative binomial regression models to analyze the number of cyber-attacks reported by organizations, but the Hurdle model showed better indices of goodness-of-fit (see subsection 5.4) and adjusted better to our data. In short, Hurdle models assume that there is one process to explain whether organizations are victimized or not and a second process that determines the number of crimes suffered by organizations with non-zero crime counts, while zero-inflated models assume that the process that explains the number of crimes may also explain suffering zero cyber-attacks. Arguably, the Hurdle model allows for more direct interpretations in a field where regression models for zero-inflated data have rarely been applied before, although future research may also apply zero-inflated models to examine if results are consistent across modeling approaches.

5. Predicting cybersecurity breaches

This section is divided as follows: subsection 5.1 presents the results of the models estimated to explain the likelihood of falling victim to at least one cybersecurity attack, subsection 5.2 shows the results of the model estimated to explain the likelihood of suffering at least one negative impact due to cybersecurity attacks, subsection 5.3 presents the results of the Hurdle models of number of attacks reported by organizations, and subsection 5.4 presents model diagnostics.

5.1 Predicting odds of falling victim to cybersecurity attacks

Table 8 shows the binary logistic regression models used to predict the likelihood that organizations report at least one form of cybersecurity attack and at least one form of negative impact or outcome due to cybersecurity attacks. Model 1 shows the results of the model predicting the odds of falling victim to least one cybersecurity attack, Model 2 presents the

results of the model predicting cybersecurity attacks (excluding fraudulent emails), and Model 3 shows the results of the model predicting negative impacts or outcomes due to cyber-attacks.

First, in Model 1, Table 8, we can see that all business sectors are more likely to suffer cybersecurity attacks than charities or voluntary sector organizations, except for businesses dedicated to food and hospitality, which show an OR smaller than 1 but not significant. For instance, companies in the construction sector are almost three times more likely to report cyber-attacks than charities, and businesses dedicated to the information or communication sector are 2.5 times more likely to be targeted by cybercriminals than charities. Second, organizations that invest more financial resources in cybersecurity are also those with higher odds of suffering at least one attack. As an example, organizations that invest £10,000 or more in cybersecurity are 2.5 times more likely to report at least one cyber-attack than companies that do not invest financial resources in cybersecurity.

The organization's income is significantly associated with the likelihood of suffering at least one cyber-victimization: companies that earn $5 million or more every year are more than 3 times more likely to suffer at least one cyber-attack than companies with incomes smaller than £100,000. Organizations that are visible online via their website and social media, externally-hosted website, guest wireless network or institutional email addresses are all statistically more likely to report suffering cybersecurity breaches or attacks than organizations without such visibility. For example, companies with externally-hosted websites are 80% more likely to suffer cyber-attacks than companies without websites or with internally-hosted websites, and organizations with institutional email addresses are 88% more likely to report at least one attack than businesses and charities without organizational email addresses.

The encryption of personal data shows a statistically significant positive association with victimization by cybersecurity attacks: organizations that encrypt personal data are 49% more likely to report suffering attacks than organizations that do not encrypt information or do not deal with personal data. Organizations that use basic software protection are 42% more likely to report at least one cyber-attack compared to companies that do not use software protection programs; whereas the monitoring of users' activity seems to reduce the likelihood of cyber-victimization by 20%. Organizations that have one board member with responsibility for cybersecurity and update their directors about cybersecurity monthly are around 30% more likely to report at least one cyber-attack than companies without these measures. And finally, businesses and charities that perceive themselves to have enough staff with cybersecurity skills and knowledge to prevent cyber-attacks are 28% less likely to reporting falling victims to at

least one cybercrime than companies that do not agree with this statement. All the other independent variables show non-significant associations with our dependent variable.

It is important to bear in mind, nevertheless, that the measure of falling victim to cyber-attacks at least once is partly affected by organizations reporting that staff receive fraudulent emails or are being directed to fraudulent websites, which was reported by 27.5% of the sample. In order to check whether our results are disproportionately affected by this type of cyber-victimization, we have fitted the same model after recoding the dependent variable to include only those companies that reported at least one cyber-attack other than receiving fraudulent emails. This reduces the proportion of organizations suffering cyber-attacks from 37% to 23% of our sample. The results of the model fitted after recoding the dependent variable are presented in Model 2, Table 8.

We highlight five important differences observed in the new model, which has a more restrictive measure of suffering at least one cyber-attack: (a) The variables 'restricting access rights' and 'require that suppliers adhere to cybersecurity standards' become positive and significant, showing that organizations that fall victims to cybercrimes more severe than receiving fraudulent emails may take more drastic measures to protect themselves. (b) Those organizations in which employees do not use personally-owned devices to carry out business activities are statistically less likely to report falling victims to cybercrimes (other than receiving fraudulent emails), showing that not allowing employees to use personally-owned devices for work may reduce the likelihood of suffering attacks. (c) Whereas the measures of 'basic software protection' and 'institutional email addresses' were positive and significant in Model 1, these become negative but not significant after excluding receiving fraudulent emails from the list of crimes. (d) The variable 'outsourced cybersecurity provider' becomes significant in the model excluding fraudulent email, showing that organizations with outsourced cybersecurity are more likely to suffer cyber-attacks (other than receiving spam) than companies with in-house cybersecurity (or without cybersecurity staff). (e) The association between having enough staff with skills and knowledge to deal with cybersecurity and falling victim to cyber-attacks becomes even stronger: those companies that agree that they have enough staff with the right cybersecurity skills are 41% less likely to report suffering cyber-attacks than organizations that do not have enough staff with cybersecurity skills or knowledge.

Table 8. Binary logistic regression models to predict odds of suffering at least one cybersecurity attack in last year (1 = experienced victimization) and at least one negative impact or outcome due to cybersecurity breaches (1 = experienced negative outcome).

	Model 1 (at least one cybersecurity attack)			**Model 2** (at least one cybersecurity attack, excluding fraudulent emails)			**Model 3** (at least one negative impact/outcome due to cyber-attacks)		
	OR	95% CI		OR	95% CI		OR	95% CI	
(Intercept)	0.03***	0.02	0.06	0.03***	0.01	0.05	0.02***	0.01	0.04
Control variables									
Company sector (ref: charity or voluntary sector organization)									
Administration or real estate	2.04**	1.30	3.21	1.54	0.92	2.58	1.05	0.61	1.78
Construction	2.96***	1.87	4.70	2.34**	1.39	3.95	1.87*	1.09	3.19
Finance or insurance	2.23^{+}	0.91	5.64	1.87	0.70	4.79	1.08	0.38	2.85
Information or communication	2.46**	1.44	4.24	3.02***	1.70	5.37	1.77^{+}	0.97	3.20
Health, care or social work	1.26	0.67	2.34	1.24	0.60	2.49	1.00	0.47	2.04
Food or hospitality	0.86	0.51	1.44	1.04	0.57	1.88	0.64	0.33	1.20
Retail and wholesale	1.64*	1.07	2.50	0.99	0.60	1.63	0.94	0.57	1.58
Others	1.70**	1.18	2.46	1.66*	1.09	2.55	1.29	0.83	1.99
Economic investment in cybersecurity (ref: no investment)									
Less than £1,000	1.77***	1.33	2.35	1.49*	1.06	2.11	2.27***	1.58	3.29
£1,000 to £10,000	1.92***	1.35	2.73	1.95**	1.31	2.91	2.25***	1.47	3.46
£10,000 or more	2.52**	1.45	4.45	2.39**	1.36	4.21	2.49**	1.38	4.48
Don't know	1.21	0.84	1.73	1.32	0.87	1.99	1.61*	1.03	2.52
Independent variables									
Technical self-protection (ref: no)									
Basic software protection	1.42*	1.06	1.90	0.87	1.14	1.94	1.09	0.76	1.57
Personal self-protection (ref: no)									
Training on cybersecurity	0.80	0.61	1.05	0.80	0.74	1.31	0.75^{+}	0.55	1.01
Guidance strong passwords	1.08	0.84	1.39	0.98	0.96	1.88	0.95	0.71	1.29
Require that suppliers adhere to CS standards	1.13	0.82	1.55	1.35^{+}	0.62	1.22	1.40^{+}	1.00	1.97
In-house guardianship (ref: no)									
Monitoring of user activity	0.80^{+}	0.63	1.02	0.71*	0.80	1.41	0.76^{+}	0.58	1.00
Control company devices	0.92	0.72	1.18	1.06	0.97	1.64	0.84	0.63	1.13
Extraordinary CS checks	1.15	0.91	1.46	1.20	0.59	1.07	1.67***	1.26	2.21
Board member on CS	1.30*	1.03	1.65	1.26^{+}	1.04	1.77	1.18	0.90	1.55
CS updates to director at least monthly	1.32*	1.04	1.68	1.36*	1.15	2.33	1.12	0.85	1.49
Enough people with skills/ knowledge dealing with CS	0.72*	0.56	0.92	0.59***	0.44	0.78	0.61**	0.45	0.82
Outsourced guardianship (ref: no)									
Outsourced provider CS	1.18	0.93	1.49	1.48**	0.54	0.92	1.50**	1.14	1.98
Value (ref: Less than £100,000)									
£100,000 to £500,000	1.38^{+}	0.99	1.92	1.50*	1.01	2.25	1.72*	1.13	2.63
£500,000 to £5 million	1.93***	1.35	2.76	2.35***	1.55	3.58	2.16***	1.40	3.39
£5 million or more	3.11***	1.84	5.29	4.89***	2.82	8.56	4.47***	2.53	7.96
Don't know	1.43^{+}	0.97	2.14	1.78*	1.12	2.86	1.84*	1.12	3.04
Personal data electronically (ref: no)	0.98	0.79	1.23	0.88	0.83	1.45	1.08	0.83	1.41
Inertia (ref: no)									
Encrypting personal data	1.49***	1.17	1.88	1.37*	0.92	1.57	1.57**	1.20	2.05
Visibility (ref: no)									
Transactions online	0.96	0.74	1.23	1.09	0.78	2.45	0.90	0.67	1.20
Institution email addresses	1.88*	1.17	3.13	1.35	1.18	2.02	1.73	0.92	3.56
Website and social media	1.57***	1.24	1.99	1.54**	1.16	1.99	1.59**	1.20	2.11
Externally-hosted web	1.80***	1.43	2.27	1.52**	1.03	1.75	1.67***	1.26	2.23
Guest wireless network	1.38**	1.09	1.76	1.34*	0.64	1.03	1.49**	1.13	1.95
Accessibility (ref: no)									
Employees don't use personal devices to work	0.86	0.70	1.07	0.81^{+}	1.15	2.33	0.82	0.64	1.05
Restricting access rights	0.95	0.72	1.27	1.63**	0.79	1.30	1.21	0.85	1.74
Backing up data securely	1.03	0.83	1.29	1.01	1.05	1.78	0.96	0.74	1.24
$PseudoR^2$	0.20			0.19			0.19		
Log-likelihood	-1116.23			-1036.49			-1022.74		

Note: n=2088; $^{+}$significant at 10% level, *sig. 5%, **sig. 1%, ***sig. 0.1%

5.2 Modeling the odds of suffering negative impacts due to cybersecurity attacks

Given that not all cybercrimes produce the same effects on organizations (see Paoli et al., 2018; Rantala, 2008), and some cyber-attacks do not produce direct negative impacts, we replicate the regression models presented above to analyze the likelihood of suffering at least one of the negative impacts or outcomes described in Table 3. The model results are shown in Model 3, Table 8.

In this case, the effect of the organizations' sector is not as significant as it appeared to be in our Models 1 and 2 (used to predict the likelihood of falling victim to a cybersecurity attack). Only two control variables related to the organizations' sector remain statistically significant in our new model: construction companies are 87% more likely than charities, and information and communication businesses are 77% more likely than charities, to report suffering at least one negative impact due to cyber-attacks. Those businesses and charities that invest more financial resources on cybersecurity are also those that are more likely to report suffering the negative impacts of cybersecurity incidents; and the companies' income is a very good indicator of their likelihood of reporting negative cybersecurity impacts (e.g., organizations that earn £5 million or more are 4.5 times more likely to suffer negative impacts than companies whose income is smaller than £100,000).

Online visibility, and more specifically the use of website and social media, externally-hosted websites and guest wireless networks, is associated with an increased likelihood of suffering negative impacts due to cyber-attacks. In this case, the use of institutional email addresses is not a statistically significant predictor. In terms of access to the targets, those organizations in which employees do not use their personal devices to access business information and work are around 20% less likely to suffer negative impacts of cyber-attacks, but this association is not significant. Encrypting personal data is associated with a larger likelihood of reporting negative impacts from cybersecurity attacks, as shown in the previous models. In this case, however, using extraordinary cybersecurity checks becomes significant and positive: those companies that invest in extraordinary checks are 67% more likely to have suffered negative impacts due to cyber-attacks than companies that do not apply these measures.

Organizations in which employees take cybersecurity training or attend cybersecurity seminars are 25% less likely to suffer negative impacts because of cyber-attacks, and UK businesses and charities that monitor the users' activity are 24% less likely to report negative cybersecurity impacts or outcomes. Similarly, companies that perceive that they have enough

staff with cybersecurity skills are 39% less likely to suffer negative cybersecurity impacts than organizations that perceive otherwise. On the contrary, organizations that outsource their cybersecurity are 50% more likely to report negative impacts than companies that do not. Having a board member with responsibility for cybersecurity and giving monthly cybersecurity updates to the director do not have statistically significant associations with the negative impacts of cyber-attacks. The rest of the independent variables do not show statistically significant coefficients.

5.3 Predicting the number of cybersecurity attacks faced by organizations

In order to analyze the number of victimizations by cybersecurity attacks faced by UK businesses and charities, we make use of a two-part Hurdle negative binomial regression. The first part of the model explains organizations' likelihood of reporting at least one attack (i.e., binary outcome of zero or non-zero cybersecurity incidents), whereas the second part estimates the count of cybercrimes suffered by organizations with at least one reported victimization. Model results are presented in Table 9: Model 1 is estimated from control variables only, Model 2 from independent variables of theoretical interest only, and Model 3 includes all variables.

With regards to the companies' sector, which is used here as a control variable, we can highlight several statistically significant associations. Construction companies are 99% more likely than charities and voluntary sector organizations to report falling victim to cyber-attacks at least once, but the number of attacks faced by those organizations is not significantly larger than the count of attacks reported by charities. Organizations in the administration or real estate sectors are 61% more likely than charities to fall victims to cyber-attacks at least once, and the number of cyber-security attacks faced by administration or real estate companies increases by 89% in contrast to charities. Similarly, retail and wholesale organizations are 41% more likely than charities to fall victim to at least one cyber-attack and the number of attacks increases by 85% when compared to charities. Finally, businesses in the information and communication fields are 61% more likely than charities to suffer cybersecurity attacks at least once, and the number of attacks increases by 2.3 times in comparison to charities.

Economic investment in cybersecurity is a good predictor of both reporting falling victim to at least one cyber-attack and of the number of attacks faced by organizations, but the latter becomes insignificant when incorporating all control and independent variables into the model. In other words, the specific cybersecurity actions included as independent variables in Model 3 explain most of the variation of victimization counts derived from the companies'

direct cybersecurity measures, and the overall economic investment in cybersecurity becomes insignificant when the model accounts for those specific measures and actions.

An organization's income/sales is a significant predictor of the binary outcome of non-zero victimization, and companies with incomes/turnover larger than £5 million are 2.2 times more likely to suffer at least one attack than organizations with incomes smaller than £100,000. However, in the count part of the model, this variable is only significant when predicting the number of cyber-attacks faced by businesses with incomes smaller than £5 million. The number of cyber-attacks faced by organizations that hold personal data electronically increases by 65% in comparison to those companies that do not hold personal data electronically.

Organizations with more online visibility (having institutional email addresses, website and social media, externally-hosted website, and guest wireless network), are all more likely to suffer at least one attack than organizations without these characteristics, but only the measures of institutional email addresses and website/social media remain significant in the count part of the model. For instance, organizations with institutional email addresses increase the number of attacks they face by almost four times in comparison to companies without organizational email accounts, and companies with website and social media accounts increase their number of cybersecurity incidents by 67%.

Those organizations whose employees do not use their personal devices to conduct business activity show that the number of cyber-attacks they face increase by 65%, whereas the binary part of the model is not significant. On the contrary, while backing up data securely and conducting extraordinary cybersecurity checks had OR larger than one, but not significant, in the binary part of the model, the OR become smaller than one and significant in the count part: those organizations that back up data securely reduce the number of breaches and attacks by 20%, and those that conduct some form of extraordinary cybersecurity check reduce the number of attacks by 17%. Encrypting personal data is associated with higher odds of suffering at least one cyber-attack and an increased number of cybersecurity incidents. The count part of the model also shows that those organizations that provide guidance on strong passwords and require that suppliers adhere to cybersecurity standards tend to suffer a larger number of cyber-attacks. Businesses and charities with outsourced cybersecurity tend be more likely to suffer at least one cyber-attack, but they also reduce the overall number of incidents they face by 48% in comparison to other organizations.

Three variables are associated with reduced odds of suffering at least one attack and also a decreased number of cyber-victimizations. Organizations that train their staff on cybersecurity have 16% lower odds of suffering at least one attack and reduce the number of cybersecurity incidents by 41%. Companies that monitor users' activity are 15% less likely to suffer at least one cyber-attack and they reduce the number of incidents by 29%. Finally, those companies that perceive they have enough staff with cybersecurity skills and knowledge are 34% less likely to suffer at least one attack and the number of cybersecurity attacks they face is reduced by 13%. However, having basic software protection is associated with 36% increased likelihood of falling victim to at least one cyber-attack, having a board member on cybersecurity is associated with 19% higher odds of suffering at least one cybersecurity incident, and giving monthly cybersecurity updates to the organization's director is associated with 23% higher odds of suffering non-zero attacks and a 43% increased number of cybersecurity incidents.

Table 9. Hurdle negative binomial regression to predict number cybersecurity breaches in last 12 months (transformed by double square root).

	Model 1		Model 2		Model 3	
	Binary OR	Count OR	Binary OR	Count OR	Binary OR (95% CI)	Count OR (95% CI)
(Intercept)	0.15***	1.11	0.05***	0.10***	0.05 (0.03-0.08)***	0.10 (0.03-0.31)***
Control variables						
Company sector (ref: charity or voluntary sector organization)						
Administration or real estate	2.40***	1.80***			1.61 (1.14-2.28)**	1.89 (1.29-2.72)***
Construction	2.29***	0.76			1.99 (1.40-2.82)***	1.19 (0.75-1.89)
Finance or insurance	2.24**	1.17			1.63 (0.87-3.04)	1.75 (0.82-3.63)
Information or communication	2.55***	2.12***			1.61 (1.09-2.38)*	2.27 (1.55-3.33)***
Health, care or social work	1.28	0.76			1.06 (0.64-1.73)	0.76 (0.36-1.60)
Food or hospitality	1.04	0.66			0.88 (0.57-1.35)	0.64 (0.33-1.26)
Retail and wholesale	1.85***	1.49*			1.41 (1.01-1.97)*	1.85 (1.30-2.70)***
Others	1.85***	1.05			1.53 (1.14-2.05)**	1.13 (0.80-1.60)
Economic investment in cybersecurity (ref: no investment)						
Less than £1,000	2.03***	0.98			1.57 (1.25-1.98)***	0.83 (0.66-1.05)
£1,000 to £10,000	2.84***	0.77*			1.70 (1.29-2.22)***	0.81 (0.60-1.08)
£10,000 or more	3.87***	0.66*			2.06 (1.43-2.97)***	0.75 (0.50-1.13)
Don't know	1.70***	0.47***			1.19 (0.89-1.59)	0.45 (0.31-0.66)***
Independent variables						
Technical self-protection (ref: no)						
Basic software protection			1.57***	1.24	1.36 (1.06-1.74)*	1.23 (0.93-1.66)
Personal self-protection (ref: no)						
Training on cybersecurity			0.87	0.63***	0.84 (0.69-1.02)$^{+}$	0.59 (0.46-0.76)***
Guidance strong passwords			1.07	1.64***	1.03 (0.85-1.25)	1.59 (1.26-2.03)***
Require that suppliers adhere to CS standards			1.10	1.18	1.08 (0.87-1.36)	1.29 (1.02-1.62)*
In-house guardianship (ref: no)						
Monitoring of user activity			0.83*	0.73**	0.85 (0.71-1.01)$^{+}$	0.71 (0.59-0.89)**
Control company devices			0.96	1.02	0.92 (0.76-1.11)	1.03 (0.82-1.26)
Extraordinary CS checks			1.18^{+}	0.79*	1.15 (0.96-1.38)	0.83 (0.67-1.01)$^{+}$
Board member on CS			1.17^{+}	1.19^{+}	1.19 (1.00-1.41)$^{+}$	1.17 (0.96-1.42)
CS updates to director at least monthly			1.30**	1.37***	1.23 (1.03-1.47)*	1.43 (1.17-1.73)***
Enough people with skills/ knowledge dealing with CS			0.78*	1.04	0.76 (0.63-0.93)**	0.87 (0.74-1.02)$^{+}$
Outsourced guardianship (ref: no)						
Outsourced provider CS			1.18^{+}	0.45**	1.11 (0.93-1.33)	0.52 (0.43-0.65)***
Value (ref: Less than £100,000)						
£100,000 to £500,000			1.53***	1.49**	1.14 (0.87-1.51)	1.38 (1.01-1.86)*
£500,000 to £5 million			2.15***	1.57**	1.55 (1.17-2.06)**	1.35 (0.98-1.87)$^{+}$
£5 million or more			3.21***	0.98	2.18 (1.52-3.13)***	0.79 (0.50-1.23)
Don't know			1.64***	1.11	1.33 (0.97-1.83)$^{+}$	0.97 (0.66-1.42)
Personal data electronically (ref: no)			1.01	1.69***	0.97 (0.82-1.14)	1.65 (1.34-2.05)***
Inertia (ref: no)						
Encrypting personal data			1.31**	1.29**	1.35 (1.14-1.61)***	1.33 (1.09-1.59)**
Visibility (ref: no)						
Transactions online			0.94	1.08	0.98 (0.81-1.17)	1.09 (0.88-1.34)
Institution email addresses			1.92**	3.89*	1.71 (1.11-2.65)*	3.81 (1.34-10.88)*
Website and social media			1.24*	1.56***	1.35 (1.13-1.61)**	1.67 (1.34-2.10)***
Externally-hosted web			1.79***	0.91	1.70 (1.42-2.04)***	0.81 (0.66-1.01)*
Guest wireless network			1.23*	0.99	1.26 (1.06-1.50)**	1.13 (0.92-1.38)
Accessibility (ref: no)						
Employees don't use personal devices to work			0.94	1.37***	0.95 (0.81-1.11)	1.48 (1.24-1.78)***
Restricting access rights			1.00	0.82	1.02 (0.82-1.28)	0.86 (0.68-1.09)
Backing up data securely			1.12	0.83*	1.10 (0.92-1.29)	0.80 (0.66-0.98)*
$PseudoR^2$	0.16		0.27		0.32	
Log-likelihood	-2196.20		-1977.57		-1913.18	

Note: n=2088; $^{+}$significant at 10% level, *sig. 5%, **sig. 1%, ***sig. 0.1%

5.4 Model diagnostics

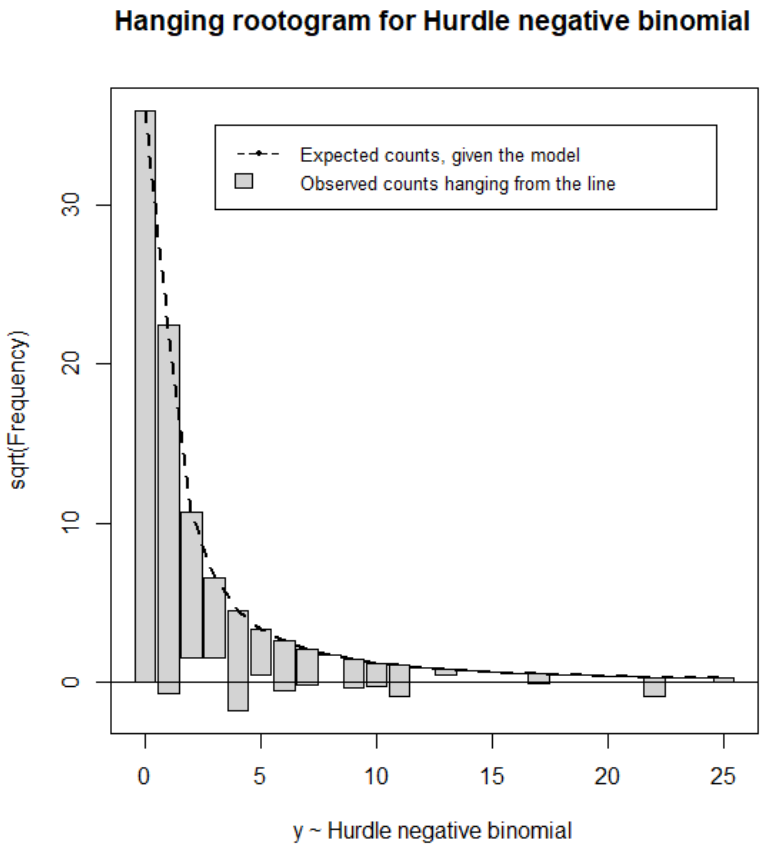
In order to investigate whether the regression models presented above meet the model assumptions and assess whether our results are affected or biased by a small proportion of observations with a large, undue influence, we present some model diagnostics.

In the case of the three binary logistic regression models used to analyze the odds of reporting at least one cybersecurity attack and reporting at least one negative impact due to attacks, and given that we use several predictors and control variables, we assessed the multicollinearity of all variables for each model using variance inflation factors (VIF), as suggested by Midi et al. (2010). Multicollinearity is found when a model is estimated with two or more predictors which are highly linearly related, thus affecting the reliability of the coefficients of individual predictors. As a rule of thumb, a VIF larger than 5 may indicate problematic multicollinearity in our data. In our case we detect no multicollinearity: the largest VIF is 2.62 in the model estimated to predict at least one attack (referred to the predictor 'other company sector'), and 2.82 in the model estimated to predict at least one negative impact (referred to the predictor '£500,000 to £5 million invested in cybersecurity'). Moreover, in the three models, the log likelihood values (LLV) are higher (closer to zero) in the model fitted from all control and independent variables, which indicates a better goodness of fit of the full model.

In the case of the Hurdle negative binomial models used to analyze the number of cybersecurity attacks faced by organization, we assess whether the regression fits the data by using a hanging rootogram and the LLV. Figure 2 shows the hanging rootogram of the Hurdle model predicting the number of attacks, which represents the difference between observed and predicted values hanging from the curve. The Hurdle model fits perfectly the number of zeros in the distribution as well as most positive values, but we also observe a slight under-fitting at the counts 3 and 4. In other words, while the model appears to fit the data very well, it may underestimate the number of businesses reporting 3 and 4 cyber-victimizations in the last year. The LLV are also higher in the model fitted from all control and independent variables in comparison to models with fewer variables, which is a good indicator of goodness-of-fit of the full model. Moreover, we compared the goodness-of-it of our Hurdle model with a zero-inflated negative binomial model estimated from the same data, and the Hurdle model shows better results in all indices examined. The Akaike Information Criterion (AIC) and the Bayesian Information Criterion (BIC) are smaller in the Hurdle model (AIC=3980.2, BIC=

4405.6) than the zero-inflated model (AIC= 4051.6, BIC= 4476.9), and the LLV is higher in the Hurdle model (LLV= -1914.1) than the zero-inflated model (LLV= -1949.7).

Figure 2. Hanging rootogram of Hurdle negative binomial regression predicting number of cybersecurity attacks (transformed by double square root).



6. Discussion and conclusions

The study of cybercrime victimization suffered by private organizations has been mostly neglected in criminological research due to the lack of available sources of data. Addressing this gap in research is important, given the growing financial impact of cyber-attacks on the private sector (Crowe, 2017; Paoli et al., 2018) and the fact that organizations are investing more resources every year to prevent cybersecurity breaches and attacks (EY, 2019). In this article we have analyzed data recorded by the CSBS 2018 to identify cybersecurity measures which appear more effective at preventing cybersecurity breaches and attacks and which ones do not show significant effects for crime prevention.

We have applied the theoretical framework of RAT and the elements of VIVA to analyze the impact of businesses' online activities and cybersecurity measures, as indicators of various forms of capable guardianship and suitability of crime targets, on cybercrime

victimization, as suggested in previous research (e.g., Miró Llinares and Johnson, 2017; Newman and Clarke, 2003; Williams et al., 2019; Yar, 2005). We have combined the use of modeling approaches traditionally used to study cybercrime victimization (i.e., logistic regression models for binary victimization outcomes, see Bossler et al., 2012; Leukfeldt and Yar, 2016; Williams et al., 2019) with novel approaches to analyze the negative impact and harms of cybercrime victimization on organizations (e.g., Paoli et al., 2018) and the number of crimes suffered by businesses and charities. This gives us information not only about the likelihood of organizations reporting falling victim to at least one cybersecurity breach, but also the likelihood of suffering the negative consequences of such criminal activities, and the number of crimes they may face. For instance, the use of Hurdle models for zero-inflated data is an understudied method in criminological research even though it adjusts very well to zero-inflated distributions observed in victimization research (e.g., Hope, 2015; Hope and Trickett, 2008). The use of this triple methodological approach allows us to identify several important findings that advance understanding of the dynamics of business, cybersecurity and cyber-victimization.

Firstly, before applying RAT to interpret the impact of organizations' online activities and cybersecurity measures on cybercrime victimization, we briefly examine the key differences across business sectors. Rantala (2008) had already observed that communication and IT businesses have a higher prevalence of cyber-victimization than other sectors (i.e., a larger proportion of these companies are victimized at least once), but our Hurdle count models show that these companies also suffer from a greater incidence of attacks: the number of cybersecurity incidents faced by communication and IT businesses increases by more than two times compared to charities. This is probably due to the perceived 'value' of these companies, since they manage large volumes of personal data (Wall, 2007; Yar, 2005), but also because their online 'visibility' and exposure to the general public tends to be large. Surprisingly, finance and insurance companies did not show significant associations with cybercrime victimization in most models. One may argue that even though these organizations plausibly manage highly 'valuable' information, they are typically not characterized by a large frequency and variety of visible online activities (in terms of exposure to the general public), which may reduce their 'visibility' and overall attractiveness following Cohen and Felson's (1979) conceptualization of VIVA. For instance, whereas 54.0% of organizations in our sample have a website and social media, this value is only 37.0% in the case of businesses in the financial and insurance sectors; and while 26.1% of all companies have some sort of functionality to

enable online transactions, only 15.0% of financial and insurance businesses have online platforms that allow transactions.

We observe in our models that those organizations that invest more financial resources in cybersecurity are generally more likely to report suffering cyber-attacks and their negative effects. This result appears to be counter-intuitive, as one would expect that allocating more financial resources to cybersecurity would help prevent attacks (Srinidhi et al., 2015), but there are two potential explanations that could account for this. First, we can speculate that decision-making processes in those organizations that, in the first instance, are more likely to suffer attacks will favor major investments in cybersecurity to mitigate risks (Fielder et al., 2016). Thus, results observed in our models may show that organizations that anticipate major cybersecurity threats invest more resources in cybersecurity. There is, however, a second potential interpretation: investing more resources in cybersecurity may enable detecting more crimes, thus enlarging the prevalence of 'detected' cybercrime victimization. These interpretations, however, cannot be checked on the basis of cross-sectional methods, and future research should use longitudinal and quasi-experimental methods to illuminate the underlaying causal associations between cybersecurity investment and cyber-attacks victimization.

Our analyses show that organizations' turnover/income is a good predictor of the prevalence and incidence of cyber-attacks reported by companies and the harm these crimes cause. When considering cyber-victimization of individuals, Leukfeldt and Yar (2016) argued that a person's financial characteristics are likely to affect how cyber-attackers view their value. In the case of private organizations this is even more likely to be the case, given that details of organizations' revenues are often publicly available. Others argue, however, that in cyberspace the 'value' is frequently an expression of information as a route to financial gain (Wall, 2007; Yar, 2005), and Williams et al. (2019) found that organizations with confidential customer information were more likely to suffer insider business cybercrime victimization. Our model results show that those organizations that store personal information suffer more cyber-attacks, although this variable does not predict the negative impacts of cybercrime (e.g., loss of access to files, systems corrupted, stopped staff from carrying out their daily work).

Our results also show that those organizations that encrypt personal data as a cybersecurity control are more likely to report suffering cybersecurity incidents and their negative consequences. Although this cybersecurity measure may be interpreted as an indicator of the target's 'inertia', since it is intended to create difficulties for criminals to extract meaningful information from compromised files, it may also be an indicator of the target's

perceived ‘value’, given that valuable business information will most probably be encrypted when stored digitally (Rantala, 2008). In-depth qualitative studies with cybercriminals are needed to further understand how they assess the ‘value’ of targets online. As well as signaling that the data being protected by encryption is of value, encrypted systems could be attractive to those criminals who are motivated by the challenge of overcoming digital system defenses rather than simply by the desire to obtain valuable data (Campbell and Kennedy, 2009; Holt et al., 2017). Future research should also analyze whether the use of encryption techniques applied to obstruct illegitimate access to digital systems helps prevent cybersecurity incidents (Noore, 2003).

In terms of visibility, research has shown that those individuals who become visible to offenders by increasing the frequency and variety of activities they conduct online are those who are more frequently targeted (Leukfeldt and Yar, 2016; Marcum et al., 2010; Newman and Clarke, 2003). In the case of businesses’ digital victimization, we find evidence that four specific forms of online interaction increase an organization’s online visibility and are associated with an increased risk of cyber-attacks: having a website and social media, a externally-hosted website, a guest wireless network, and institutional email addresses. We note, however, that amongst the previous variables, the only ones that are significant to predict the number of cybersecurity incidents are having institutional email addresses and having a website and social media accounts. Those organizations that provide employees with institutional email addresses are particularly affected by receiving fraudulent emails, which generally produce less damaging effects than other forms of cybercrime.

Restricting IT administration and access rights to specific users, which may be analyzed as a measure of ‘access’ to targets under the VIVA acronym (Miró Llinares and Johnson, 2017), is associated with a higher likelihood of reporting having suffered at least one cybersecurity attack (excluding fraudulent emails). It is, nevertheless, negative but not significant in the models predicting harms of cyber-attacks and the number of cyber-victimizations suffered by organizations. Our interpretation of this finding is that organizations may apply these restrictions to IT administration and access rights after detecting a first attack, and this prevention strategy may help them prevent future attacks and mitigate the negative effects of cybersecurity incidents. As Williams et al. (2019: 1127) suggest, “criminal incidents often motivate the adoption of avoidance or security behaviors”.

Those organizations that prevent their employees from using their personal devices to conduct business activity tend to report a larger number of cyber-attacks, as shown in the

Hurdle count model. This is explained by the frequency of fraudulent emails reported by organizations, which would be otherwise received by personal devices instead of company-owned machines. When we exclude receiving fraudulent emails from the list of cybercrimes and estimate logistic regressions of cyber-victimization (other than receiving spam), we observe that this measure may prevent other forms cybercrime but does not prevent receiving fraudulent emails.

With regard to the various forms of organizational self-protection analyzed in this paper, we find that when employees are encouraged to become better-informed about cybersecurity (through training and attending seminars) the number of cyber-attacks and their negative impact are reduced (HISCOX, 2018). As argued by Jahankhani (2013: 260), perhaps one of the most effective strategies to prevent cybercrimes is "to improve on cognitive development and behavioral skills by developing a set of education, training, and awareness programs specific to Internet exposure risks and cyber behaviors". Moreover, backing up data securely and conducting extraordinary cybersecurity checks also reduce the number of cybercrimes suffered by organizations, but these do not appear to prevent the negative impacts of cybercrime.

Contrary to expectations, providing guidance about strong passwords to employees is associated with a larger number of cybersecurity incidents reported by organizations. This measure does not appear to reduce the number of cybersecurity incidents when applied alone, and it may have a counterproductive effect by allowing organizations to believe they are taking sufficient steps to prevent crime, and that other measures are unnecessary. Previous research had already suggested that guidance on passwords may "lull" organizations into a false sense of security and indirectly lead to increased attacks (e.g., Klein, 1990; Stone and Madigan, 2006). In our sample, 73% of organizations that provide guidance on strong passwords do not encourage employees to take any cybersecurity training, and more than half of those organizations do not monitor users' activity. Thus, encouraging one good cybersecurity practice (in this case, strong passwords) may be dysfunctional more broadly if it deters organizations from instituting other important cybersecurity measures. Moreover, as suggested by the National Cyber Security Centre (2018), those organizations that place unrealistic demands on users in their 'strong passwords guidance' (e.g., asking employees to change the password frequently or using long passwords with special characters) may actually lead to a 'password overload' which causes that users re-use the same passwords across systems, use predictable passwords or write passwords down in places where they can be easily found.

Requiring suppliers to adhere to cybersecurity standards shows a positive association with the negative harms of cybersecurity attacks, which may indicate that organizations take this decision after suffering the negative impact of a cyber-attack, but this measure does not significantly prevent future cybercrimes. Another explanation may be that organizations that have complex supply chains are more likely to require suppliers to adhere to cybersecurity measures, but they are also more likely to suffer attacks.

The use of basic software protection, as a measure of technical self-protection, does not seem to be an effective measure to prevent cyber-attacks either (Leukfeldt and Yar, 2016; Rantala, 2008). This finding, however, may be explained by the inclusion of fraudulent emails as a form of cybercrime in our analyses, since software protection programs do not successfully prevent receiving spam emails. After excluding this type of crime from our analyses this variable becomes negative but not significant.

The use of outsourced forms of guardianship, which refers to the hiring of external cybersecurity providers, is associated with a higher likelihood of having suffered at least one cybersecurity attack (Rantala, 2008), but it also reduces the number of cybersecurity incidents suffered by companies. It is plausible that hiring external cybersecurity helps organizations prevent future attacks, but longitudinal studies are needed to further examine the causal associations between hiring outsourced cybersecurity and preventing attacks. (This shows the need for using Hurdle count models in cybercrime research, since this would have remained hidden if we had only used traditional logistic regression models.) Nevertheless, outsourcing cybersecurity does not appear to reduce the likelihood of suffering the negative impacts of cyber-attacks.

On the contrary, enhancing the in-house guardian by developing cybersecurity teams within the organization seems to generate the best results for preventing cyber-attacks and their negative impacts. The monitoring of users' activity is associated with a reduced number of cyber-attacks and it lowers the likelihood to suffer the negative impact of cybercrime. Those organizations that control company devices are less likely to suffer negative impacts or outcomes due to cyber-attacks, although this association is not significant. And finally, while establishing high-level cybersecurity controls (i.e., board members on cybersecurity, monthly cybersecurity updates to the director) is not associated with reduced cyber-attacks (Williams et al., 2019), foregrounding the internal guardian by having enough members of staff with skills and knowledge to manage cybersecurity seems to be the most promising cybersecurity measure to prevent future cyber-attacks and their negative impacts.

In summary, this article shows that the framework established by RAT can be used to further understand cyber-victimization in private organizations. More specifically, our results show that investing in in-house cybersecurity human resources and enhancing employees' online self-protection by providing cybersecurity training, rather than just basic software protection and guidance about strong passwords, are the most promising ways to minimize cyber-attacks and their impacts. These results can be used by researchers to further understand the effect of organizational cybersecurity measures on cybercrime prevention, but our analyses may also serve to guide organizational practices for cybercrime prevention. For instance, these results point towards the need to invest in in-house cybersecurity teams and internal cybersecurity training programs to mitigate cybersecurity risks and prevent future victimization (Jahankhani, 2013; Levi et al., 2015; Williams et al., 2019).

There is, however, a need for new research analyzing cybercrime victimization suffered by businesses and charities in other geographic contexts and using alternative sources of data. National governments from various countries are developing new surveys to record data on cybercrime victimization, which may become key sources of information to further investigate corporate cyber-victimization and to guide businesses' evidence-based cybersecurity practices.

References

Bilodeau, H., Lari, M., & Uhrbach, M. (2019). *Cyber security and cybercrime challenges of Canadian businesses, 2017* (Report No. 85-002-X). The Canadian Centre for Justice Statistics, Statistics Canada.

Bonney, G. E. (1987). Logistic regression for dependent binary observations. *Biometrics, 43*, 951-973.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400-420.

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among a juvenile population. *Youth & Society, 44*(4), 500-523. https://doi.org/10.1177/0044118X11407525

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies*. https://doi.org/10.1080/14616696.2020.1804973

Cameron, A. C., & Trivedi, P. K. (2005). *Microeconomics. Methods and applications*. Cambridge: Cambridge University Press.

Campbell, Q., & Kennedy, D. M. (2009). The psychology of computer criminals. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook, 5th edition*. New Jersey: Wiley.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608. https://doi.org/10.2307/2094589

Crowe. (2017). *Annual Frau Indicator 2017. Identifying the cost of fraud to the UK economy*. UK: Crowe.

Department for Digital, Culture, Media & Sport. (2018). *Cyber Security Breaches* Survey (Technical annex). UK: Department for Digital, Culture, Media & Sport.

EY. (2019). *Is cybersecurity about more than protection? EY Global Information Security Survey 2018-19.* EY's Advisory Services. Global: EY.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems, 86*, 13-23. https://doi.org/10.1016/j.dss.2016.02.012

HISCOX. (2018, October 18). *UK small businesses targeted with 65,000 attempted cyber attacks per day*. HISCOX. https://www.hiscoxgroup.com/news/press-releases/2018/18-10-18

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1-25. https://doi.org/10.1080/01639620701876577

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress. Theory and prevention of technology-enabled offenses*. New York: Routledge.

Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Exploring the subculture of ideologically motivated cyber-attackers. *Journal of Contemporary Criminal Justice, 33*(3), 213-233. https://doi.org/10.1177/1043986217699100

Holt, T. J., Leukfeldt, R., & van de Weijer, S. (2020). An examination of motivation and routine activity theory to account for cyberattacks against Dutch web sites. *Criminal Justice and Behavior*. https://doi.org/10.1177/0093854819900322

Hope, T. (2015). Understanding the distribution of crime victimization using "British Crime Survey" data: An exercise in statistical reasoning. In *Oxford Handbooks Online*. Oxford: Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199935383.013.41

Hope, T., & Trickett, A. (2008). The distribution of crime victimisation in the population. *International Review of Victimology, 15*(1), 37-58. https://doi.org/10.1177/026975800801500103

Jackman, S. (2020). *pscl: Classes and methods for R developed in the political science computational laboratory* (R package version 1.5.5) [Computer software]. United States Studies Centre, University of Sydney, Sydney, Australia.

Jahankhani, H. (2013). Developing a model to reduce and/or prevent cybercrime victimization among the user individuals. In B. Akhgar, & S. Yates (Eds.), *Strategic Intelligence Management: National Security Imperatives and Information and Communications Technologies* (pp. 258-268). Waltham: Butterworth-Heinemann.

Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The dark figure and the cyber fraud rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*. https://doi.org/10.1007/s10610-020-09439-2

Klein, D. V. (1990). "Foiling the cracker": A survey of, and improvements to, password security. *Proceedings of the 2nd USENIX Security Workshop*, 5-14.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2015). *The implications of economic cybercrime for policing* (Research report). City of London Corporation.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, 31(5), 381-410. https://doi.org/10.1080/01639620903004903

Miri, H., Sarkar, S. K., & Rana, S. (2010). Collinearity diagnostics of binary logistic regression model. *Journal of Interdisciplinary Mathematics*, 13(3), 253-267. https://doi.org/10.1080/09720502.2010.10700699

Miró Llinares F. (2015). That cyber routine, that cyber victimization: Profiling victims of cybercrime. In R. G. Smith, R. C. C. Cheung, & L. Y. C. Lau (Eds.), *Cybercrime risks and responses* (pp. 47-63). London: Palgrave Macmillan.

Miró Llinares, F., & Johnson, S. D. (2017). Cybercrime and place: Applying environmental criminology to crimes in cyberspace. In G. J. N. Bruinsma, & S. D. Johnson (Eds.), *The Oxford Handbook of Environmental Criminology* (pp. 883-906). New York: Oxford University Press.

Miró-Llinares F., & Moneva A. (2020). Environmental criminology and cybercrime: Shifting focus from the wine to the bottles. In T. Holt, & A. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 491-511). Cham: Palgrave Macmillan.

National Audit Office. (2017). *Online fraud* (Report by the Comptroller and Auditor General). UK: National Audit Office.

National Audit Office. (2019). *Progress of the 2016-2021 National Cyber Security Programme* (Report by the Comptroller and Auditor General). UK: National Audit Office.

National Cyber Security Centre. (2017). *The cyber threat to UK businesses* (2016/2017 Report). UK: National Audit Office.

National Cyber Security Centre. (2018, November 19). *Password policy: updating your approach.* National Cyber Security Centre. https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

Newman, G. R., & Clarke, R. V. (2003). *Superhighway robbery: Preventing e-commerce crime*. Portland: Willan Publishing.

Noore, A. (2003). A secure conditional access system using digital signature and encryption. *2003 IEEE International Conference on Consumer Electronics*, 220-221. IEEE. https://doi.org/10.1109/ICCE.2003.1218894

Office for National Statistics. (2019). *E-commerce and ICT activity, UK: 2018* (Statistical bulletin). UK: Office for National Statistics.

Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium. *Crime, Law and Social Change, 70*, 397-420. https://doi.org/10.1007/s10611-018-9774-y

R Core Team. (2020). *R: A language and environment for statistical computing* [Computer software]. R Foundation for Statistical Computing, Vienna, Austria.

Rantala, R. R. (2008). *Cybercrime against businesses, 2005* (Special report). United States: Bureau of Justice Statistics.

Richards, K. (2009). *The Australian Business Assessment of Computer User Security (ABACUS): A national survey* (Research and Public Policy Series). Australia: Australian Institute of Criminology.

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems, 75,* 49-62. https://doi.org/10.1016/j.dss.2015.04.011

Stone, J., & Madigan, E. (2006). A managerial framework for network security. *Proceedings of the 2006 International Conference on Telecommunication Systems - Modeling and Analysis*. Reading: Peen State Berks.

Wall, D. S. (2007). *Cybercrime. The transformation of crime in the information age*. Cambridge: Policy Press.

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior, 40*(9), 1119-1131. https://doi.org/10.1080/01639625.2018.1461786

Xie, M., Goh, T. N., & Kuralmani, V. (2002). *Statistical models and control charts for high-quality processes*. Boston: Springer.

Xie, M., Goh, T. N., & Tang, X. Y. (2000). Data transformation for geometrically distributed quality characteristics. *Quality and Reliability Engineering International, 16*, 9-15. https://doi.org/10.1002/(SICI)1099-1638(200001/02)16:1<9::AID-QRE278>3.0.CO;2-8

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/10.1177/147737080556056

Zeileis, A., Kleiber, C., & Jackman, S. (2008). Regression models for count data in R. *Journal of Statistical Software, 27*(8). https://doi.org/10.18637/jss.v027.i08