Computers & Security 127 (2023) 103089

Contents lists available at ScienceDirect

Computers & Security

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

Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach

Steven Kemp

Department of Law, Pompeu Fabra University, Edificio Roger de Llúria (campus de la Ciutadella), Ramon Trias Fargas, 25-27, 08005 Barcelona, Spain

ARTICLE INFO

Article history:
Received 30 August 2022
Revised 3 December 2022
Accepted 30 December 2022
Available online 31 December 2022

Keywords:
Cybersecurity
Organizations
Awareness-raising
Cyber essentials
Model uncertainty

ABSTRACT

Cybercrime is a pressing concern for governments and businesses around the globe, but little is known about what policy interventions work to prevent and mitigate threats to organizations. Thus, empirical studies on cybercrime prevention policies and tools are needed to understand their effectiveness and to improve implementation and evaluation. This article analyzes whether two UK government schemes aimed at encouraging and helping businesses to adopt cybersecurity controls and policies ('Cyber Essentials' and '10 Steps to Cyber Security') are associated with safer organizational behavior and whether adopting the recommended measures is related to lower levels of cybercrime victimization and its impacts. Bayesian model averaging is employed on a representative sample of 5,872 businesses from four rounds (2018–2021) of the UK Government's Cyber Security Breaches Survey. The results show that awareness of the Government schemes is associated with more cyber secure practices, but we do not find evidence of lower likelihood of victimization or negative consequences for companies that implement the recommended measures. Findings are discussed in relation to policy, practice and future research.

1. Introduction

Businesses around the globe are frequently faced with the threat of cybercrime victimization (Buil-Gil et al., 2021; Tam et al., 2021; Williams et al., 2019). For instance, ransomware is now a major professionalized crime (Wall, 2021), and in the United Kingdom, which is the focus of this study, reports of certain cyber-enabled frauds against organizations rose sharply during the COVID-19 pandemic (Kemp et al. 2021b). The UK National Cyber Security center (NCSC) highlights that not only large businesses are at risk but that small and medium enterprises also have a fifty percent chance of suffering a cybersecurity incident (NCSC, 2020). The issue was already considered sufficiently pressing that, in 2015, the UK Government described cyber threats as one of the greatest dangers to national and economic security (UK Government, 2015) and, thus, pledged to invest £1.9 billion in the five years between 2016 and 2021 (UK Government, 2016).

The UK National Cyber Security Strategy 2016–2021 stated that one of its objectives was to "ensure that individuals and organizations, regardless of size or sector, are taking appropriate steps to protect themselves, and their customers, from the harm caused by cyber attacks" (UK Government, 2016:42); hence, part of the aforementioned investment was on programs designed to protect private enterprises by raising awareness, advising, and providing support. For instance, the NCSC oversees the Cyber Essentials scheme that set outs five types of technical controls that can be implemented to protect organizations against cyberattacks. Specifically, these controls are firewalls, secure configuration, user access control, malware protection, and security update management (NCSC, n.d.b). The scheme provides businesses with access to a 'Cyber Essentials readiness toolkit' and offers the opportunity for certification of compliance with the guidelines. Similarly, the 10 Steps to Cyber Security guidance, which is also run by the NCSC, breaks down cybersecurity into ten areas to help organizations manage cyber risks (NCSC, n.d.a). These ten areas are risk management, engagement and training, asset management, architecture and configuration, vulnerability management, identity and access management, data security, logging and monitoring, incident management, and supply chain management. The guidance is aimed at medium and large organizations and affirms that "[*a*]dopting security measures covered by the 10 Steps reduces the likelihood of cyber attacks occurring, and minimises the impact to your organization when incidents do occur". However, although these cybersecurity public policies have been widely promoted, there is still only limited evidence that they result in businesses strengthening their cy-

E-mail address: steven.kemp@upf.edu

https://doi.org/10.1016/j.cose.2022.103089

ber defenses and in lower levels of victimization and impact. A review commissioned by the NCSC noted a lack of awareness of the Cyber Essentials scheme and concerns from non-participants about the value of certifying compliance (Britain Thinks, 2021).

In addition to these examples of investment in awareness-raising and support programs by public institutions, companies themselves also spend considerable amounts on preventing and mitigating cybercrime (Anderson et al., 2019; Button, 2020; Khando et al., 2021). Industry sources indicate that companies now dedicate more than 20% of their IT budgets to cybersecurity (Hiscox, 2021), and the UK Government estimates that the UK cybersecurity sector generated revenue of £8.9 billion in 2020 (Department of Digital, Culture, Media and Sport, 2021b). Yet, despite the extensive economic cybercrime threats faced by businesses, as well as the high public and private expenditure on prevention and mitigation, research is notably exiguous with regard to the victimization of companies and the effectiveness of public policies and prevention strategies to reduce this victimization (Brewer et al., 2019; Dupont, 2019; Maimon and Louderback, 2019). As Maimon (2020) notes, without empirical scientific studies on cybercrime prevention policies and tools, we cannot begin to understand their effectiveness. Existing empirical research on cybercrime victimization has mainly studied individuals rather than organizations (Ho and Luong, 2022), which has been attributed to a lack of reliable and accessible data (Buil-Gil et al., 2021). The present article aims to help fill this gap in the literature on cybercrime and organizations by implementing Bayesian model averaging on a representative sample of UK businesses to examine: firstly, whether businesses that are aware of the NCSC cybersecurity schemes (Cyber Essentials and 10 Steps to Cyber Security) are more likely to have implemented the recommended measures; secondly, whether those businesses that have adopted the controls are less likely to have experienced cybercrime victimization; and, thirdly, whether the consequences of victimization are lower for those businesses. The analyses for the second and third aims are conducted with regard to phishing, malware, identity theft and hacking.

2. Extant literature on cybercrime awareness raising for organizations and cybercrime against businesses

2.1. Cybercrime awareness-raising for businesses and the implementation of prevention measures

Public institutions worldwide conduct cybercrime awareness-raising and support programs directed at businesses. For instance, in addition to the previously mentioned campaigns conducted by NCSC in the UK, one can find examples of guidance and support provided by The National Institute of Standards and Technology at the U.S. Department of Commerce (NIST, n.d.) or various tools offered by the European Union Agency for Cybersecurity (ENISA, n.d.). Nevertheless, communicating cybersecurity advice or standards to businesses can be particularly complicated and often does not lead to greater awareness or, more importantly, behavior change (Bada and Nurse, 2019; Niemimaa and Niemimaa, 2017; Renaud and Ophoff, 2021). In this regard, the UK Cyber Security Strategy 2016–2021 emphasized the complexities of behavior change and aimed "to move beyond raising awareness to persuade companies to take action" (UK Government, 2016:42). The recently published Cyber Security Strategy 2022 also underscores the objective of supporting and guiding businesses to change behavior (UK Government, 2021).

There are scant quantitative studies that have examined whether government cybercrime awareness programs directed at businesses are associated with organizational behavior, i.e., businesses implementing cybercrime prevention and reaction measures. However, several studies can be found in the cybersecurity or information security literature regarding the factors associated with organizational investment and strategies in these areas, especially for small and medium-sized companies (SMEs). In this sense, management priorities, organizational capabilities and external pressures can shape SME information security practices (Herath et al., 2020; Hsu et al., 2012). Heidt et al. (2019) found that limited resources and low implementation of formal processes may explain lower expenditure on information security in comparison to large firms, while Tam et al. (2021) identified that a lack of technical knowledge is a challenge that small businesses need to overcome to effectively use cybersecurity information. In particular, technical expertise can be necessary to follow industry standards, potentially limiting compliance by smaller companies. Renaud and Ophoff (2021) note that the low uptake of the Cyber Essentials program underscores that it cannot automatically be assumed that SMEs will take advantage of freely available guidance and adopt recommended cybersecurity measures. They highlight that SMEs can be unaware that the threats they are being warned about are relevant to them, while lack of resources is also an issue. These authors conducted a survey on a non-representative sample of security industry professionals and found that SMEs often feel overwhelmed by cybersecurity advice, but that cyber situational awareness is correlated with the implementation of security measures. Finally, Osborn and Simpson (2017) highlight how costs can impede smaller companies following standards designed to foster good cybersecurity practices. They specifically highlight how business processes in smaller organizations and the complexity of the Cyber Essentials program can limit its uptake.

There has been extensive survey-based research on cybercrime awareness and protection strategies adopted by individual users. Some of these findings may help guide the study of businesses. For example, with the aim of providing evidence for police-led cyberfraud prevention program, Drew and Farrell (2018) found that in their Australian sample, awareness of cyber risks did not have statistically significant relationship with cyberfraud prevention knowledge and use of prevention strategies.

Several studies have applied Protection Motivation Theory to analyze whether an individual's perceptions of threats and the responses to threats are associated with their willingness to implement cybercrime prevention measures (for example, Dang-Pham and Pittayachawan, 2015; Hanus and Wu, 2016; Martens et al., 2019; van Bavel et al., 2019). Protection Motivation Theory (PMT) originates from psychology research on healthcare behavior and describes the cognitive processes that influence protective behavior when faced with potential harm (Maddux and Rogers, 1983; Rogers, 1975). While its application in criminological studies has been limited, it has been found to be a useful framework to understand the adoption of protective measures against criminal victimization (Clubb and Hinkle, 2015). In accordance with the framework, an individual's motivation to protect themselves depends on their assessment of the threat – "threat appraisal" – and their evaluation of strategies to deal with the threat – "coping appraisal". The threat appraisal is comprised of the perceived seriousness of the threat and its potential consequences (perceived severity) as well as the perceived probability it will happen to them (perceived vulnerability). The coping appraisal involves three factors. Firstly, the individual's belief in their ability to respond to the threat (self-efficacy). Secondly, the anticipated benefits of this response with regard to the threat (response efficacy). Finally, the individual will consider the costs of responding to the threat in terms of money, time or effort (response costs).

In general, studies in this area consistently find that mere awareness of threats or possible responses are insufficient to prompt behavior change, but rather, the perceived severity of the threat as well as having a positive perception of one's ability to

respond to threats and the effectiveness of these responses are associated with greater likelihood of adopting cybercrime protection methods (van Bavel et al., 2019; Workman et al., 2008). This is a relevant finding for the design of awareness-raising campaigns and guidance and support programs. Studies using surveys of individuals in organizational contexts support the conclusion that providing information on the efficacy of measures and increasing workers' perceived ability to implement these measures is related to greater likelihood of them doing so (Blythe and Coventry, 2018; Safa et al., 2015; Vrhovec and Mihelič, 2021).

2.2. Cybercrime victimization of businesses

Businesses can suffer many forms of cyber victimization, such as data breaches, DDoS attacks, phishing, and ransomware. An incipient body of literature has begun to detail the harms caused by these attacks (Agrafiotis et al., 2018; Furnell et al., 2020) and to identify some factors that may correlate with suffering ransomware (Connolly et al., 2020), data breaches (Sarabi et al., 2016), or malware and phishing attacks (Okutan et al., 2018). In this regard, it has been found that some organizational characteristics, activities and cybersecurity practices can be related to risk of victimization and its impact.

Firstly, several studies have identified that large companies are more likely to suffer cyberattacks than small and medium-sized enterprises (Bilodeau et al., 2019; Rantala, 2008; Richards, 2009; Williams et al., 2019), which may be due to them being perceived as more valuable targets by offenders. Certain sectors have also been found to concentrate a higher prevalence of cybercrime incidents. For example, Buil-Gil et al. (2021) and Rantala (2008) found Communication and IT businesses to be at greater risk, while Bilodeau et al. (2019) found greater levels of cybersecurity incidents in banking institutions. Other studies, however, have not found a significant relationship between sector and suffering cybercrime (Richards, 2009; Williams et al., 2019). The routine activities approach (Cohen and Felson, 1979) has provided the theoretical lens for the handful of criminological studies that have examined how organizations' activities may impact their risk of cybercrime. Maimon et al. (2013) analyzed computer-focused crimes against a large university, finding an association between the number of foreign network users and the rate of these crimes. They posit that this could be related to an increase in the visibility of computer networks to potential attackers. Buil-Gil et al. (2021) used data from the 2018 wave of the UK Cyber Security Breaches Survey to examine the applicability of the VIVA elements of the routine activity approach to cybercrime against organizations. Their results found that the Value of the organization in terms of its turnover and storing personal data may increase susceptibility to cyberattacks. The Visibility of the organization was also correlated with cybersecurity incidents via having a company email address, website and social media, or a guest wireless network. Furthermore, limiting Access to organizational targets by restricting IT admin and access rights was found to correlate with higher levels of cybercrime. On the other hand, there is less evidence of a relationship between organization routine activities and insider business cybercrime. The only activity correlated with victimization in a UK study conducted by Williams et al. (2019) was organizations storing confidential data.

In addition to the prevalence of cybercrime against businesses, understanding the consequences of incidents is also of academic and government interest. In surveys conducted on US (Rantala, 2008) and Australian (Richards, 2009) businesses, most companies suffered losses and some form of harm, such as downtime or corruption of hardware or software. Businesses that participated in a Belgian study reported that harms to their internal operational activities were greater than losses of revenue (Paoli et al., 2018). Research in Canada identified several frequent negative impacts, such as preventing employees from carrying out daily tasks, the company experiencing downtime, or costs of recovery and repair (Bilodeau et al., 2019). The Canada study also linked harm to routine activities, as businesses that stored data on externally-hosted web services or allowed employees to use personally-owned devices were more likely to have suffered impactful incidents. Taking the analytic strategy a step further, Buil-Gil et al. (2021) modelled the relationship between routine activities and the negative impacts of cyber-attacks in the UK. They found that using websites and social media, and providing guest wireless networks were correlated with greater likelihood of suffering negative consequences. On the other hand, employees using personal devices was associated with reduced likelihood of harm.

Regarding prevention and limiting the impact of cybercrime in organizations, the cybersecurity management regime may play a relevant role. Outsourcing cybersecurity has been associated with greater prevalence of reported incidents (Buil-Gil et al., 2021; Rantala, 2008), as has employing a dedicated cybersecurity manager (Williams et al., 2019), or having a stronger organizational security posture (Connolly et al., 2020). In the Australian study, higher levels of cybersecurity knowledge and ability was related to suffering a greater number of incidents (Richards, 2009). However, this may be due to greater capacity to detect incidents. Conflicting results have been found for technical cybercrime controls. For instance, Buil-Gil et al. (2021) concluded that basic software protection may not be effective at preventing cybersecurity incidents, while backing up data and carrying out cybersecurity checks were associated with fewer cybercrime incidents but not with lower likelihood of negative impacts. In a study on a large American university, Maimon et al. (2014) found that the presence of a warning banner in a target computer may not limit the number of incidents but it can significantly shorten the duration of attacks. Finally, research on hospitals has linked IT security management with the effectiveness of IT security. Angst et al. (2017) conclude that more IT security is insufficient for preventing cyber victimization and that institutional factors such as the integration of security into IT processes and practices are central to the effectiveness of prevention measures.

In short, it appears that certain organization characteristics, digital activities, and cybersecurity processes and controls may influence the likelihood of suffering cybercrime and its negative impacts.

3. Materials and methods

The introduction to this paper identified that cybercrime can have notable economic consequences for businesses of all sizes and that public and private expenditure on cybersecurity is high. Public institutions around the globe have developed awareness-raising campaigns and support programs to encourage and help companies protect themselves against cybercrime and limit the possible impact. However, as noted, research is scarce regarding the effectiveness of these policies to encourage businesses to implement cybersecurity measures, and on whether the interventions are associated with reduced cyber victimization of businesses and its consequences. Given these salient gaps in the literature, the present paper seeks to respond to three research questions:

Research Question 1: Are businesses that are aware of UK Government cybersecurity campaigns more likely to implement the recommended cybersecurity measures?

Research Question 2: Are businesses that have implemented the UK Government-recommended cybersecurity measures less likely to suffer cybercrime victimization?

Research Question 3: Are businesses that have implemented the UK Government-recommended cybersecurity measures less likely to suffer negative outcomes and impacts from cybercrime victimization?

3.1. Data and weighting

To answer these questions, data from the 2018, 2019, 2020 and 2021 rounds of the cross-sectional UK Cyber Security Breaches Survey (CSBS) were obtained from the UK Data Service website. The CSBS is an annual survey of businesses, charities and education institutions in the UK conducted by the Government Department for Digital, Culture, Media and Sport (DCMS) since 2016 to provide information on the cybersecurity threats faced by organizations and the strategies implemented to prevent and mitigate them. One of its stated aims is to support policymaking in accordance with the National Cyber Security Strategy 2016–2021 that was mentioned in the Introduction to this paper (DCMS 2021a). The administrators conduct a random probability telephone survey using a sample frame from the UK Government's Inter-Departmental Business Register.

Once the data from the four rounds were obtained, charities and education institutions were removed and then the four samples were subsequently merged into a single sample consisting of all business respondents for the four rounds ($n = 5872$). Four rounds were combined so as to increase the sample size and ensure it included a suitable number of businesses that had suffered cybersecurity incidents. Charities and education institutions were excluded because the CSBS consistently finds they suffer a particularly low rate of incidents and, moreover, to allow the business sample to be weighted to make it representative of the universe of UK businesses with at least one employee. Weighting was necessary because the survey employs disproportionate stratified sampling to account for the relatively low proportion of medium and large businesses in the UK and also to allow sector analysis. If the survey used proportional stratification for size, there would be very few medium and large businesses in the sample as approximately ninety-six percent of businesses in the UK are small enterprises (Department for Business, Energy and Industrial Strategy, 2020). Thus, the sample of medium and large enterprises is boosted, as are certain sectors to allow analysis of sector subgroups.

To correct for the disproportionate sampling, the survey administrators use rim weighting to weight the survey respondents to the universe of UK businesses. The present study applied this same method of weighting to correct the sample created from the four rounds of the survey. Using the iterake package in R (Rodriguez and Witherell, 2021), the sample was weighted to ensure it is representative of UK businesses with regard to size, sector and region. The estimates for the actual proportions of businesses in the UK were obtained from UK Government Statistics (Department for Business, Energy and Industrial Strategy, 2020) The sample was already proportionally stratified by region by the survey administrators. All analyses conducted in this paper are performed on the weighted sample.

3.2. Variables

With respect to Research Question 1 (relationship between awareness of Government campaigns and implementation of security measures), there are two outcome variables of interest derived from the fact the Cyber Security Breaches Survey enquires about a range of technical rules, controls and management regimes that form the requirements for the Cyber Essentials and 10 Steps programs. Firstly, we analyze a binary variable that measures the implementation of all the measures recommended by the NCSC Cyber Essentials scheme. The Cyber Essentials scheme is made up of five areas of technical controls (firewalls, secure settings, access controls, malware protection, and updates) and the survey maps these areas to individual questions. The binary Cyber Essentials variable corresponds to whether participants in the survey report having controls in all these five areas or not. The survey administrators calculate and provide the Cyber Essentials variable in the open dataset.

Secondly, we analyze a binary variable that measures how many of the government's 10 Steps to Cyber Security guidance have been met (less than seven steps or seven and above). The CSBS maps the 10 Steps to Cyber Security to specific questions regarding the company's information risk management regime, secure configurations, network security, management of user privileges, user education and awareness, incident management, malware protection, monitoring, removable media controls, and home and mobile working. The survey administrators calculate an ordinal 10 Steps variable that captures how many of the 10 Steps the respondent reports (0–10). To facilitate the exploratory analysis herein, we divided the ordinal variable into the binary categories of less than seven steps and seven and above. This division was chosen because the mean of the ordinal 10 Steps variable is 6.2 and, therefore, we are approximately comparing those above the mean and those at the mean or below. In the weighted sample, 49.2% of businesses report controls in all areas of Cyber Essentials and 31.5% report seven or more of the 10 Steps to Cyber Security. Table 1

Table 1
Companies that are aware of and have implemented government schemes.

Variable	%
Companies aware of Cyber Essentials	13.1
Companies with controls in all areas of Cyber Essentials	49.2
Companies aware of 10 Steps	18.1
Companies with seven or more of 10 Steps	31.5

Research Question 2 (relationship between implementing Government-recommended cybersecurity measures and cyber victimization) involves four binary outcome variables that correspond to having experienced or not one of the following four types of cybersecurity incident in the previous twelve months: malware, hacking, identity theft, and phishing. In accordance with the survey questions, malware refers to businesses that stated that in the previous twelve months their computers had become infected with ransomware or with other malware (e.g., viruses or spyware). Businesses that suffered hacking stated they had experienced hacking or attempted hacking of online bank accounts or unauthorised accessing of files or networks by internal or external actors. Identity theft refers to companies that affirmed that people had impersonated their organization in emails or online. Phishing corresponds to staff receiving fraudulent emails or visiting fraudulent websites. Table 2 details the percentages of businesses who reported having suffered these incidents in the previous 12 months.

Finally, to respond to Research Question 3 (relationship between implementing Government-recommended cybersecurity measures and the impact or outcome of cyber victimization) we analyze two binary variables related to the consequences for those businesses that stated they had suffered at least one cybersecu-

Table 2
Businesses that reported having suffered a cybersecurity incident.

Incident	%
Phishing	33.3
Identity theft	11.5
Malware	9.5
Hacking	6.0
Any of the above incidents	40.9

Table 3
Outcomes and impacts from cybersecurity incidents.

Outcomes	% (n = 2804)
Any negative outcome	26.7
Temporary loss of access to files or networks	15.0
Software or systems corrupted or damaged	8.8
Website, applications, or online services taken down or made slower	6.4
Money was stolen	5.1
Lost access to third-party services you rely on	5.1
Permanent loss of files	3.1
Personal data altered, destroyed, or taken	2.0
Lost or stolen assets, trade secrets or intellectual property	1.3
Impacts	% (n = 2804)
Any impact	43.9
New measures needed to prevent or protect against future breaches or attacks	29.8
Additional staff time to deal with the breach or attack, or to inform customers or stakeholders	25.2
Stopped staff from carrying out their day-to-day work	18.4
Any other repair or recovery costs	12.6
Prevented provision of goods or services	4.4
Loss of revenue or share value	4.1
Complaints	3.4
Reputational damage	2.5
Discouraged you from a planned future business activity	2.5
Goodwill compensation or discounts given to customers	1.2
Fines from regulators or authorities, or associated legal costs	0.7

rity incident. In accordance with the categorization used by the survey administrators, the variable titled "outcome" refers to having suffered any of the following negative outcomes from an incident: software or systems were corrupted or damaged; personal data was altered, destroyed or taken; permanent loss of files (other than personal data); temporary loss of access to files or networks; lost or stolen assets, trade secrets or intellectual property; money was stolen; money was paid as a ransom; website, applications or online services were taken down or made slower; lost access to any third-party services you rely on; physical devices or equipment were damaged or corrupted; or compromised accounts or systems used for illicit purposes (e.g. launching attacks).

The variable called "impact" examines whether the companies stated they had experienced at least one of the following impacts as a result of an incident: staff stopped from carrying out their day-to-day work; loss of revenue or share value; additional staff time to deal with the breach or attack, or to inform customers or stakeholders; any other repair or recovery costs; new measures needed to prevent or protect against future breaches or attacks; fines from regulators or authorities, or associated legal costs; reputational damage; prevented provision of goods or services; discouraged from carrying out a future business activity you were intending to do; complaints; or goodwill compensation or discounts given to customers. Table 3 details the frequency of the different outcomes and impacts for companies that reported having suffered a cybersecurity incident (n = 2804).

The review of the literature in Section 2 commands the inclusion of several covariates, some of which are present in all analyses herein and some of which are only relevant to a specific research question. The first control variables present in all analyses are the size of the businesses (1–49, 50–249, and 249+ employees) and their sector of activity: a) manufacturing, transportation and construction, b) retail, accommodation and entertainment services, c) information, administrative and financial services, and d) tech, knowledge, and health.[1] Secondly, we examine certain digital characteristics of businesses that could be associated with the decision to adopt cybersecurity measures or with the risk of victimization and its impact. Specifically, whether they: have social media accounts; offer customers an online payment, ordering or booking system; use online banking; have an industrial control system; hold customer information electronically; and whether employees use personally owned devices for work, which we label 'mobile working'. Finally, we analyze several variables related to cybersecurity that are not captured by the Cyber Essentials or 10 Steps variables described above but may be relevant based on prior research. In the analysis for each research question, we examine the effect of whether cybersecurity is a high or low priority, of holding cybersecurity insurance, having outsourced cybersecurity management, and if there is a board member with responsibility for cybersecurity.

We also examine variables that are available in the CSBS and could be of interest for only one particular question. In this sense, to respond to Research Question 1, the relationship between implementing prevention measures and awareness of Government cybersecurity programs is central, thus we include variables on whether the respondent has heard of the Cyber Aware program, the Cyber Essentials scheme, or the 10 Steps Guidance. We also examine the relevance of whether the company has specifically sought information from a Government source and if there is a board member with responsibility for cybersecurity. Furthermore, when modeling the implementation of Cyber Essentials, a variable is included for whether the organization has a formal policy covering cybersecurity risks and if the board is updated on cybersecurity at least quarterly. These are not included in any other models because the associated questions in the survey are mapped to the 10 Steps variable by the survey administrators. In response to Research Question 2, we include the All Cyber Essentials and 10 Steps variables as predictors to analyze whether following the recommendations is associated with lower cyber victimization and we also incorporate a variable that captures if the company has a separate guest Wi-Fi network. Finally, for Research Question 3, as well as the All Cyber Essentials, 10 Steps, and separate guest Wi-Fi variables, we also examine the relevance of having suffered more than one incident.

3.3. Analytic strategy: Bayesian model averaging

To answer the three research questions, Bayesian model averaging (BMA) was used. BMA has been widely employed in economics (for a review see Steel, 2020), machine learning (e.g. Dash and Cooper, 2004), weather forecasting (e.g. Sloughter et al., 2013), and many other areas (for a review see Fragoso et al., 2018). Its implementation in social sciences has been considerably less frequent and the technique has been described as "severely underutilized" (Hinne et al., 2020:201), with researchers advocating for its inclusion in social scientists' "standard toolbox for analysis" (Vakhitova and Alston-Knox, 2018:1).

One of the main aims of BMA is to better account for model uncertainty (Ando, 2010; Fragoso et al., 2018; Hinne et al., 2020;

[1] The "Manufacturing, transportation and construction" group is formed by companies in the manufacturing (SIC code C), transportation and storage (H), and construction (F) sectors. The "retail, accommodation and entertainment services" group refers to enterprises in the wholesale and retail trade (G), arts, entertainment, and recreation (R), and accommodation and food service (I) sectors. The "information, administrative and financial services" group refers to businesses from the following sectors: information and communication (J), administrative and support service (N), real estate (L), and financial and insurance activities (K). Finally, the "tech, knowledge and health" group describes companies involved in professional, scientific, and technical activities (M), education (P), and human health and social work activities (Q). These groups have been classified based on previous research on cybersecurity threats faced by organizations (Buil-Gil et al., 2020; Kemp et al., 2021a; Rantala, 2008; Richards, 2009; van de Weijer et al., 2021), but also according to the type of data or digital characteristics that typically define these companies.

Hoeting et al., 1999; Raftery, 1995). In social sciences, it is not uncommon to have many possible predictors and, therefore, a very large model space (Raftery et al., 2005), meaning manual selection by researchers is not plausible. Rather than examining a very small set of candidate models chosen by the researcher, all possible models are considered in BMA and the posterior distribution of coefficients are calculated by averaging the coefficients in the competing models and weighting them based on each individual model's posterior probability (of being the correct model). In other words, the final predictions for each variable are computed by averaging the corresponding predictions from individual models whereby more likely models receive a greater weight when calculating the average. The best model has the lowest Bayesian Information Criterion (BIC) and the highest posterior probability. For a statistical introduction to BMA, see Hoeting et al. (1999). For introductions with social science examples, see Hinne et al. (2020), Kaplan and Lee (2018), or Vakhitova and Alston-Knox (2018).

We implemented Bayesian Model Averaging using the bic.glm function in the package BMA (Raftery et al., 2022) for R open source software (R Core Team, 2021). This package uses the fast leaps and bounds algorithm to conduct an exhaustive search over the model space and produces summary results that display posterior means (β), standard deviations (SD) and inclusion probabilities for the coefficients associated with each variable, in other words, the probability that the coefficient is not equal to zero ($Pr(\beta \neq 0)$). As advocated by Madigan and Raftery (1994), we take a parsimonious approach to calculating the posterior distribution of coefficients and follow Kaplan and Lee (2018) by setting Occam's window to 20. In short, Occam's window is a method to discard those models that are effectively discredited because they predict the data far less well than the best model (Madigan and Raftery, 1994). Given we were uncertain about the prior probability of each candidate model, the default position of a uniform distribution was used, as recommended by Vakhitova and Alston-Knox (2018).

The BMA method was chosen for the present study to deal with the issue of model uncertainty and because it is particularly suited to exploratory research in new areas where theoretical guidance on variables of interest is limited (Hinne et al., 2020; Vakhitova and Alston-Knox, 2018). As noted in Section 2, there is a dearth of quantitative research on cyber awareness-raising aimed at organizations and on organizational cyber victimization and its impact. BMA can offer a more realistic and less risky approach than traditional GLM methods, with various studies showing this analytic tool to offer greater predictive performance than the single model approach as well as other variable selection methods such as stepwise selection (Hoeting et al., 1999; Kaplan and Lee, 2018; Raftery, 1995; Vakhitova and Alston-Knox, 2018). While it is by no means a panacea, BMA is frequently better than the traditional alternative (Piironen and Vehtari, 2017).

4. Results

4.1. Implementation of cybersecurity recommendations

Table 4 shows the results for BMA analysis in which the binary outcome variable is whether the participant reports having all five Cyber Essentials controls. It displays the posterior mean (β) and standard deviations (SD) for each variable estimated by the BMA technique, in other words, the model averaged coefficients weighted by the posterior model probabilities. The table also details the inclusion probabilities for each variable ($Pr(\beta \neq 0)$), that is to say, the probability that the coefficient is not 0 and, therefore, that the inclusion of the variable explains the outcome variable. In accordance with Viallefont et al. (2001), the rule of thumb for interpreting inclusion probabilities is that below 50 percent indicates there is no evidence the variable is associated with the outcome variable, between 50 percent and 75 percent is weak evidence of an association, between 75 and 95 percent is positive evidence, between 95 and 99 percent is strong evidence, and above 99 percent the evidence is very strong. Furthermore, Table 4 notes the cumulative posterior model probability over the best five models as identified by the BMA algorithm, as well as the posterior model probability and the included variables for each individual model. All results tables include the same information.

As can be observed in Table 4, the top five models have a cumulative posterior probability of over sixty percent, meaning the other models are much less likely. The first model and the second model have very similar individual posterior probability (0.2 and 0.19). In total, there are eight variables, excluding the intercept, for which there is very strong evidence they are associated with implementing all Cyber Essentials controls. Having social media, updating the board on cybersecurity issues more than quarterly, having board members with responsibility for cybersecurity, using an outsourced cybersecurity provider, and having a formal cybersecurity policy are all positively associated with implementing Cyber Essentials. On the other hand, considering cybersecurity a low priority is negatively associated with adopting the required technical controls. Businesses that are in the retail, accommodation and entertainment services sectors are also less likely to have fully implemented Cyber Essentials than the reference category of manufacturing, transport, and construction companies.

Finally, and importantly, there is positive evidence that having heard of Cyber Essentials is positively associated with adopting the controls recommended in the scheme. The posterior mean of 0.25 translates to companies that have heard of the scheme having 28% greater odds of adopting the controls, though it should be noted that the standard deviation is relatively large in comparison to the mean. The implications of the Cyber Essentials findings will be considered in the discussion section since one of the main aims of the Cyber Essentials scheme is to encourage businesses to take simple cybersecurity measures.

Table 5 displays the results of BMA estimated for the outcome variable implementing seven or more of the 10 Steps to Cyber Security. The cumulative posterior probability of the five best models is ninety-three percent, with twelve variables found to predict the outcome variable. Regarding characteristics, medium-sized businesses are more likely to have implemented the majority of the 10 Steps than small businesses, though no evidence of a relationship is found for large businesses. The information, administrative and financial services sectors, and the tech, knowledge, and health sectors are positively associated with 10 Steps in comparison to companies dedicated to manufacturing, transport, and construction. In terms of digital characteristics, we find having social media and holding personal information to be positively related to implementing the 10 Steps, but companies that allow mobile working are less likely to have implemented the measures. In relation to the cybersecurity profile of businesses, having cybersecurity insurance, outsourcing cybersecurity management, and having board members with responsibility for cybersecurity are associated with greater likelihood of complying with the government guidance, while those businesses that stated cybersecurity was a low priority are less likely to follow the 10 Steps. Finally, we find a very strong positive association between awareness of the NCSC cybersecurity programs and implementing the 10 Steps. In both cases, having heard of the schemes is associated with 2.5 times higher odds of following the guidance.

4.2. Cyber victimization of businesses

Having presented the findings regarding the factors that predict the adoption of government-recommended cybersecurity mea-

Table 4
BMA results for implementation of all Cyber Essentials controls.

Variable	β	SD	Pr($\beta \neq 0$)	Inclusion in Model				
				M1	M2	M3	M4	M5
(Intercept)	−1.06	0.09	100	▲	▲	▲	▲	▲
Business size (ref: small)								
Size (Medium)	0.12	0.24	23.9					
Size (Large)	0.02	0.16	2.8					
Business sector (ref: Manufacturing, transportation, and construction)								
Retail, accommodation, and entertainment services	−0.26	0.09	95.7	▲	▲	▲	▲	▲
Information, administrative and financial services	0	0	0					
Tech, knowledge, and health	0	0	0					
Have social media accounts	0.24	0.06	100	▲	▲	▲	▲	▲
Personal data held electronically	0.14	0.11	70.6	▲	▲			▲
System to pay or order online	0	0	0					
Online banking	0	0	0					
Have industrial control system	0	0	0					
Mobile working	−0.08	0.09	45.7	▲			▲	
Cybersecurity low priority	−0.62	0.08	100	▲	▲	▲	▲	▲
Insurance	0	0	0					
Outsourced cybersecurity	0.45	0.06	100	▲	▲	▲	▲	▲
Board member responsible for cybersecurity	0.42	0.07	100	▲	▲	▲	▲	▲
Sought government information	0	0	0					
Heard of Cyber Aware	0	0	0					
Heard of Cyber Essentials	0.25	0.15	79.1	▲	▲	▲	▲	▲
Heard of 10 Steps	0	0	0					
Board updated cybersecurity at least quarterly	0.59	0.06	100	▲	▲	▲	▲	▲
Have formal cybersecurity policy	0.89	0.07	100	▲	▲	▲	▲	▲
Cumulative posterior model probability over best five models	0.61	Posterior model probability		0.2	0.19	0.1	0.06	0.06
		BIC		−43,367.2	−43,367.2	−43,365.9	−43,364.9	−43,364.7

Table 5
BMA results for implementation of seven or more 10 Steps to Cyber Security.

Variable	β	SD	Pr($\beta \neq 0$)	Inclusion in Model				
				M1	M2	M3	M4	M5
(Intercept)	−2.8	0.13	100	▲	▲	▲	▲	▲
Business size (ref: small)								
Size (Medium)	1.13	0.21	100	▲	▲	▲	▲	▲
Size (Large)	0.44	0.66	35		▲		▲	
Business sector (ref: Manufacturing, transportation, and construction)								
Retail, accommodation, and entertainment services	0	0	0					
Information, administrative and financial services	0.49	0.09	100	▲	▲	▲	▲	▲
Tech, knowledge, and health	0.67	0.08	100	▲	▲	▲	▲	▲
Have social media accounts	0.57	0.07	100	▲	▲	▲	▲	▲
Personal data held electronically	0.47	0.08	100	▲	▲	▲	▲	▲
System to pay or order online	0	0	0					
Online banking	−0.06	0.11	28					
Have industrial control system	0.73	0.19	100	▲	▲	▲	▲	▲
Mobile working	−0.41	0.07	100	▲	▲	▲	▲	▲
Cybersecurity low priority	−1.06	0.12	100	▲	▲	▲	▲	▲
Insurance	0.94	0.07	100	▲	▲	▲	▲	▲
Outsourced cybersecurity	0.61	0.07	100	▲	▲	▲	▲	▲
Board member responsible for cybersecurity	1.05	0.07	100	▲	▲	▲	▲	▲
Sought government information	0.04	0.12	14					
Heard of Cyber Aware	0	0	0					
Heard of Cyber Essentials	0.92	0.1	100	▲	▲	▲	▲	▲
Heard of 10 Steps	0.92	0.09	100	▲	▲	▲	▲	▲
Cumulative posterior model probability over best five models	0.93	Posterior model probability		0.38	0.23	0.17	0.08	0.07
		BIC		−45,001.6	−45,000.6	−45,000	−44,998.5	−44,998.1

sures, this section set outs the results for the factors that predict victimization.

4.2.1. Phishing

The estimation of BMA for the outcome variable phishing produces the results found in Table 6. The cumulative posterior probability of the five best models is fifty-six percent and there is evidence of an association between having suffered phishing attacks and ten predictors. In term of business characteristics, there is positive evidence that medium-sized businesses are more likely to report having experienced phishing attacks than small businesses, though we find no evidence of a relationship regarding large businesses. Very strong evidence is found for greater likelihood of phishing attacks and companies in the information, administrative and financial services sectors. Very strong evidence is also found with regard to phishing attacks and having social media, using online banking, having somebody in the board who is responsible for cybersecurity, and providing a separate Wi-Fi system

Table 6
BMA results for phishing.

Variable	β	SD	Pr($\beta \neq 0$)	Inclusion in Model				
				M1	M2	M3	M4	M5
(Intercept)	−1.73	0.1	100	▲	▲	▲	▲	▲
Business size (ref: small)								
Size (Medium)	0.56	0.24	91.1	▲	▲	▲	▲	▲
Size (Large)	0.17	0.39	18.5					
Business sector (ref: Manufacturing, transportation, and construction)								
Retail, accommodation, and entertainment services	0	0	0					
Information, administrative and financial services	0.39	0.07	100	▲	▲	▲	▲	▲
Tech, knowledge, and health	0	0	0					
Have social media accounts	0.34	0.06	100	▲	▲	▲	▲	▲
Personal data held electronically	0.19	0.09	86.7	▲	▲	▲		▲
System to pay or order online	0	0	0					
Online banking	0.4	0.08	100	▲	▲	▲	▲	▲
Have industrial control system	0	0	0					
Mobile working	0.15	0.09	79.2	▲	▲	▲	▲	▲
Cybersecurity low priority	−0.34	0.08	100	▲	▲	▲	▲	▲
Insurance	0.05	0.09	27.3			▲		
Outsourced cybersecurity	0	0	0					
Board member responsible for cybersecurity	0.35	0.07	100	▲	▲	▲	▲	▲
Separate guest Wi-Fi	0.29	0.06	100	▲	▲	▲	▲	▲
Implemented all Essentials	0	0	0					
Implemented ≥ 7 of 10 Steps	0.12	0.12	56.1	▲			▲	
Cumulative posterior model probability over best five models	0.56	Posterior model probability		0.22	0.11	0.10	0.07	0.06
		BIC		−43,212.9	−43,211.4	−43,211.4	−43,210.6	−43,210.2

for guest users. Furthermore, holding personal information electronically and having workers who work remotely is positively associated with reporting having suffered phishing attacks. Finally, there are two associations that appear counterintuitive: businesses that stated cybersecurity was a low priority are strongly associated with lower probability of suffering phishing attacks, and there is weak evidence that implementing seven or more of the 10 Steps is related to greater likelihood of phishing. With regard to our variable of interest and research question, those companies that have implemented seven or above of the 10 Steps have 12% greater odds of reporting having suffered phishing attacks, though the standard deviation of the posterior mean indicates this relationship is uncertain. The possible explanations for the direction of these relationships are discussed in the Discussion, conclusions and limitations section.

4.2.2. Identity theft

As can be observed in Table 7, none of the five best models for identity theft have a high posterior probability. The result for Model 1 is 0.12, which means there is large amount of model uncertainty. As such, the cumulative posterior probability over the best five models is lower (0.46) than in the other analyses conducted thus far. Regarding business characteristics, size and sector are related to the outcome variable: medium and large companies are more likely to report having suffered identity theft, while retail, accommodation, and entertainment companies are less likely to suffer identity theft than the reference category of manufacturing, transport, and construction. There is very strong evidence using social media and having separate guest Wi-Fi are positively associated with identity theft, positive evidence that mobile working is related, and weak evidence that having outsourced cybersecurity explains the outcome variable. Finally, we again find unexpected results regarding priority and adhering to the 10 Steps, as there is weak evidence that considering cybersecurity a low priority is associated with lower likelihood of identity theft and, inversely, that having seven or more of the 10 Steps increases the likelihood. Finally, in the case of identity theft, the posterior mean translates to 20% greater odds of victimization for those companies who have implemented over six 10 Steps, although the relatively large standard deviation indicates uncertainty in this relationship.

4.2.3. Malware

Table 8 displays the results for the BMA analysis with regards to malware victimization. Similar to the identity theft analysis, the posterior probabilities of the five best models are quite low, therefore, so is the cumulative posterior probability (0.43). The results find no evidence of an association between suffering malware victimization and most of the predictor variables. Regarding businesses activities, only using social media and allowing mobile working are associated with being infected by malware. In terms of cybersecurity practices, companies that outsource cybersecurity management and provide a separate Wi-Fi system for guest users are more likely to report suffering malware incidents. We find no evidence of a relationship between the Cyber Essentials and 10 Steps programs and suffering malware. This is despite All Cyber Essentials being found to be significant in 3 of the five best models.

4.2.4. Hacking

The final type of cybersecurity incident that was analyzed was hacking. As shown in Table 9, the three best models each have a posterior model probability of 0.07, meaning the cumulative posterior probability is very low (0.31) and, therefore, the data explain little of the variance in the outcome variable. With regard to business characteristics, the analysis finds strong evidence of a relationship between using social media and suffering hacking. There is also positive evidence that companies in which employees work using personal devices are more likely to have suffered hacking, while firms in which cybersecurity is a low priority are less likely to report experiencing this type of incident.

4.3. Outcome and impact of cybersecurity incidents

Table 10 details the results of the BMA analysis to respond to the third research question on the relationship between businesses' characteristics, activities, whether they have implemented

Table 7
BMA results for identity theft.

Variable	β	SD	Pr($\beta \neq 0$)	Inclusion in Model				
				M1	M2	M3	M4	M5
(Intercept)	−2.89	0.16	100	▲	▲	▲	▲	▲
Business size (ref: small)								
Size (Medium)	1.14	0.19	100	▲	▲	▲	▲	▲
Size (Large)	1.47	0.41	98.5	▲	▲	▲	▲	▲
Business sector (ref: Manufacturing, transportation, and construction)								
Retail, accommodation, and entertainment services	−0.48	0.12	100	▲	▲	▲	▲	▲
Information, administrative and financial services	0.01	0.06	6.5					
Tech, knowledge, and health	−0.02	0.08	10.5					
Have social media accounts	0.68	0.1	100	▲	▲	▲	▲	▲
Personal data held electronically	0	0	0					
System to pay or order online	0	0	0					
Online banking	0	0	0					
Have industrial control system	0	0	0					
Mobile working	0.24	0.13	83.7	▲	▲	▲	▲	▲
Cybersecurity low priority	−0.33	0.22	75.1	▲	▲		▲	▲
Insurance	0.01	0.04	2.8					
Outsourced cybersecurity	0.19	0.15	68.1	▲		▲	▲	▲
Board member responsible for cybersecurity	0.06	0.12	25.1					▲
Separate guest Wi-Fi	0.45	0.09	100	▲	▲	▲	▲	▲
Implemented all Essentials	0	0	0					
Implemented ≥ 7 of 10 Steps	0.19	0.17	60.2	▲	▲	▲		
Cumulative posterior model probability over best five models	0.46	Posterior model probability		0.12	0.12	0.09	0.08	0.06
		BIC		−46,387.9	−46,387.9	−46,387.5	−46,387	−46,386.6

Table 8
BMA results for malware.

Variable	β	SD	Pr($\beta \neq 0$)	Inclusion in Model				
				M1	M2	M3	M4	M5
(Intercept)	−2.96	0.14	100	▲	▲	▲	▲	▲
Business size (ref: small)								
Size (Medium)	0.21	0.32	33.6					▲
Size (Large)	0.01	0.12	1.8					
Business sector (ref: Manufacturing, transportation, and construction)								
Retail, accommodation, and entertainment services	−0.02	0.08	8.5					
Information, administrative and financial services	0	0	0					
Tech, knowledge, and health	0	0	0					
Have social media accounts	0.3	0.14	90.1	▲	▲	▲	▲	▲
Personal data held electronically	0	0	0					
System to pay or order online	0	0	0					
Online banking	0.01	0.04	2.3					
Have industrial control system	0	0	0					
Mobile working	0.16	0.15	57.5		▲	▲	▲	▲
Cybersecurity low priority	0	0	0					
Insurance	0	0.02	1.2					
Outsourced cybersecurity	0.53	0.09	100	▲	▲	▲	▲	▲
Board member responsible for cybersecurity	0	0	0					
Separate guest Wi-Fi	0.22	0.17	70	▲	▲	▲		
Implemented all Essentials	0.14	0.16	47.9			▲	▲	▲
Implemented ≥ 7 of 10 Steps	0.00	0.02	0.6					
Cumulative posterior model probability over best five models	0.43	Posterior model probability		0.11	0.11	0.08	0.07	0.06
		BIC		−46,740	−46,740	−46,739.4	−46,739.3	−46,738.8

the Government-recommended cybersecurity measures and the outcome from cybercrime victimization. The best model has a notably larger posterior model probability than the others (0.20), and it finds evidence that eight predictor variables explain the likelihood of suffering a negative outcome from a cybersecurity incident. Firstly, there is weak, positive, and very strong evidence, respectively, that allowing mobile working, providing a separate guest Wi-Fi system, and outsourcing cybersecurity management are associated with greater likelihood of experiencing one of the negative outcomes. Secondly, as may be expected, the type of incidents suffered is relevant to the outcome. In this sense, there is very strong evidence that all incident types are more likely to produce a negative outcome than experiencing phishing. Finally, the analysis finds that suffering more than one cybersecurity incident is associated with lower likelihood of being affected by a negative outcome.

The results with respect to experiencing one of the impacts are similar to those for the negative outcomes, though in this case there are seven significant predictor variables, and no model is clearly better than the others. Regarding organizational practices, we find weak evidence that mobile working is associated with impact from cybersecurity incidents and very strong evidence about having a separate guest Wi-Fi system. All incident types are again more likely than phishing to produce an impact. However, there is a notable difference with regard to the previous model: having implemented seven or more of the 10 Steps is very strongly asso-

Table 9
BMA results for hacking.

Variable	β	SD	Pr($\beta \neq 0$)	Inclusion in Model				
				M1	M2	M3	M4	M5
(Intercept)	−3.36	0.25	100	▲	▲	▲	▲	▲
Business size (ref: small)								
Size (Medium)	0	0	0					▲
Size (Large)	0	0	0					
Business sector (ref: Manufacturing, transportation, and construction)								
Retail, accommodation, and entertainment services	−0.01	0.05	2.1					
Information, administrative and financial services	0.22	0.21	56.7	▲			▲	
Tech, knowledge, and health	0	0	0					
Have social media accounts	0.44	0.15	96.6	▲	▲	▲	▲	▲
Personal data held electronically	0	0	0					
System to pay or order online	0.22	0.21	57.5	▲	▲			
Online banking	0.17	0.23	39.5					▲
Have industrial control system	0	0	0					
Mobile working	0.28	0.18	76.8	▲	▲	▲	▲	▲
Cybersecurity low priority	−0.48	0.25	85.8	▲	▲	▲	▲	▲
Insurance	−0.02	0.07	6.2					
Outsourced cybersecurity	0.04	0.11	13.8					
Board member responsible for cybersecurity	0	0	0					
Separate guest Wi-Fi	0.03	0.1	11.4					
Implemented all Essentials	0	0	0					
Implemented ≥ 7 of 10 Steps	0	0	0					
Cumulative posterior model probability over best five models	0.31	Posterior model probability		0.07	0.07	0.07	0.06	0.04
		BIC		−47,713.2	−47,713.1	−47,713	−47,712.7	−47,712.1

Table 10
BMA results for outcome.

Variable	β	SD	Pr($\beta \neq 0$)	Inclusion in Model				
				M1	M2	M3	M4	M5
(Intercept)	−2.37	0.2	100	▲	▲	▲	▲	▲
Business size (ref: small)								
Size (Medium)	0	0	0					
Size (Large)	0	0	0					
Business sector (ref: Manufacturing, transportation, and construction)								
Retail, accommodation, and entertainment services	0	0	0					
Information, administrative and financial services	0	0	0					
Tech, knowledge, and health	0.06	0.13	19.5					▲
Have social media accounts	0	0	0					
Personal data held electronically	0.02	0.08	9.3					
System to pay or order online	0.05	0.12	16.7					
Online banking	0	0	0					
Have industrial control system	0	0	0					
Mobile working	0.18	0.18	54.9	▲		▲		▲
Cybersecurity low priority	0	0	0					
Insurance	−0.07	0.14	22.5			▲	▲	
Outsourced cybersecurity	0.57	0.11	100	▲	▲	▲	▲	▲
Board member responsible for cybersecurity	0	0	0					
Separate guest Wi-Fi	0.3	0.18	80.6	▲	▲	▲	▲	▲
Crime type (ref: Phishing)								
Identity theft	1.07	0.17	100	▲	▲	▲	▲	▲
Malware	2.74	0.16	100	▲	▲	▲	▲	▲
Hacking	2.66	0.19	100	▲	▲	▲	▲	▲
Other attack	2.29	0.17	100	▲	▲	▲	▲	▲
Implemented all Essentials	0	0	0					
Implemented ≥ 7 of 10 Steps	0	0	0					
Suffered >1 attack	−0.56	0.12	100	▲	▲	▲	▲	▲
Cumulative posterior model probability over best five models	0.53	Posterior model probability		0.20	0.14	0.07	0.05	0.05
		BIC		−19,455.7	−19,455	−19,453.6	−19,453.1	−19,453.1

ciated with being more likely to have experienced an impact from cyber victimization. The implications of this finding and the other results are discussed in the next section. Table 11

5. Discussion, conclusions and limitations

There is a distinct lack of research on the effectiveness of cybercrime prevention policy initiatives (Brewer et al., 2019), which is a notable gap in the literature given the extent of victimization and the fact that evaluations are essential to understanding what works to reduce cyber incidents and their impact (Maimon, 2020). As Dupont states (2019:513):

> "Given the considerable investments being made by governments and organizations to improve cybersecurity, it is concerning that there are not more scientifically rigorous efforts being undertaken to establish which policies and programs are

Table 11
BMA results for impact.

Variable	β	SD	Pr($\beta \neq 0$)	Inclusion in Model				
				M1	M2	M3	M4	M5
(Intercept)	−1.33	0.2	100	▲	▲	▲	▲	▲
Business size (ref: small)								
Size (Medium)	0	0	0					
Size (Large)	0	0	0					
Business sector (ref: Manufacturing, transportation, and construction)								
Retail, accommodation, and entertainment services	0	0	0					
Information, administrative and financial services	0	0	0					
Tech, knowledge, and health	0	0	0					
Have social media accounts	0.01	0.04	4					
Personal data held electronically	0.01	0.04	4.3					
System to pay or order online	0	0	0					
Online banking	0.01	0.05	3.8					
Have industrial control system	0	0	0					
Mobile working	0.14	0.15	53.4	▲		▲		▲
Cybersecurity low priority	0	0	0					
Insurance	0	0	0					
Outsourced cybersecurity	0.07	0.12	30.8					▲
Board member responsible for cybersecurity	0.03	0.08	12.8					
Separate guest Wi-Fi	0.45	0.1	100	▲	▲	▲	▲	▲
Crime type (ref: Phishing)								
Identity theft	0.95	0.14	100	▲	▲	▲	▲	▲
Malware	1.96	0.16	100	▲	▲	▲	▲	▲
Hacking	1.84	0.2	100	▲	▲	▲	▲	▲
Other attack	1.42	0.15	100	▲	▲	▲	▲	▲
Implemented all Essentials	0	0	0					
Implemented ≥7 of 10 Steps	0.55	0.1	100	▲	▲	▲	▲	▲
Suffered >1 attack	−0.14	0.17	45.3			▲	▲	
Cumulative posterior model probability over best five models	0.58	Posterior model probability		0.14	0.13	0.12	0.10	0.09
		BIC		−18,712.6	−18,712.4	−18,712.3	−18,711.9	−18,711.7

delivering measurable improvements to the safety of our digital ecosystem"

In particular, the empirical literature on the effectiveness of government cybersecurity schemes and organizational prevention strategies is virtually non-existent. Thus, the main contribution of the present article is that it begins to fill these salient lacunas and to do so, employs an original quantitative method that is underused in social sciences.

Our first research question examined the relationship between businesses' awareness of Government schemes that aim to promote adoption of cybersecurity measures and the reported implementation of these recommended measures. In this regard, Bayesian model averaging estimated on a representative sample of United Kingdom businesses found positive evidence that firms that had heard of the National Cyber Security Centre's Cyber Essentials program were more likely to have implemented the five recommended technical controls. Similarly, results showed that those firms that had heard of NCSC's 10 Steps to Cyber Security program were more likely to have adopted seven or more of the 10 Steps. A prior review of Cyber Essentials found lack of awareness of the scheme to be an impediment to it successfully fostering cybersecurity practices (Britain Thinks, 2021) and the evidence herein suggests that improving awareness of Government programs could indeed increase adoption of basic cybersecurity controls. This relationship may seem obvious, but, in fact, providing cybersecurity advice does not necessarily promote organizational behavior change (Bada and Nurse, 2019; Renaud and Ophoff, 2021). Moreover, the extensive cybersecurity literature grounded on Protection Motivation Theory has demonstrated the complexity of the link between knowledge of threats and responses and changes in behavior (Hanus and Wu, 2016; van Bavel et al., 2019).

However, while these findings provide original evidence of a relationship between awareness of government schemes for businesses and the adoption of more secure practices, it is important to note that we provide no evidence of a causal effect. In fact, the relationship is likely very complex given that other factors in our analysis were also associated with complying with the Government recommendations, such as the priority given to cybersecurity or having board members responsible for cybersecurity. It is probable that those companies that consider cybersecurity a high priority are more likely to have board members responsible for cybersecurity, are more likely to have adopted security controls and at the same time, are also more likely to have heard of the Government schemes. Thus, future research should aim to delve further into the causal effect of government cybersecurity schemes on organizational behavior change and the factors that may influence their impact.

The second research question inquired about the relationship between following Government schemes and suffering cyber incidents (phishing, malware, identity theft and hacking). This question is particularly relevant to evaluating Cyber Essentials, which affirms "Cyber Essentials is an effective, Government backed scheme that will help you to protect your organization, whatever its size, against a whole range of the most common cyber attacks". Likewise, the 10 Steps to Cyber Security guidance asserts it "reduces the likelihood of cyber attacks occurring". Our results do not provide evidence to support these claims and in some cases even point to companies following the scheme being more likely to suffer attacks, which is similar to previous studies on organizations and cyber incidents (Angst et al., 2017; Buil-Gil et al., 2021; Sen and Borle, 2015).

There are several possible explanations for this. Firstly, it may be that businesses that are inherently more likely to suffer cyberattacks are aware of their attractiveness as a target and are therefore more likely to invest in control measures and policies (Rakes et al., 2012). This may reduce the likelihood of attack for these companies in comparison to themselves prior to investments but not in comparison to other companies that, due to factors such as size,

sector, or business routine activities, are already inherently less likely to be attacked. Cross-sectional surveys such as the Cyber Security Breaches Survey cannot be used for before and after treatment comparisons, hence, future research should aim to employ methods that permit pre and post analysis to identify whether the adoption of protective measures reduces the number of incidents suffered.

A second plausible explanation is that those companies with more developed cybersecurity strategies also have increased ability to detect cyber incidents (Buil-Gil et al., 2021). Consequently, our results based on survey measures may be identifying that companies with more technical controls and cybersecurity policies have a greater capacity to detect cyberattacks, as opposed to being equally or less susceptible to attacks. Thirdly, information security studies have concluded that organizations that invest more in security might in fact be publicizing their increased value as targets, thereby making themselves more attractive to offenders (Angst et al., 2017; Gupta et al., 2020). This may explain the greater likelihood of suffering phishing or identity theft for those companies that have implemented seven or more of the 10 Steps. Along similar lines, Vasek and Moore (2014) found that outdated insecure webservers were not the most likely to be hacked, but rather, newer versions are more attractive to offenders.

Finally, the simplicity of many of the controls and policy elements included in the NCSC schemes and the strongly optimistic messaging regarding their effectiveness could lead organizations and their members to be over-confident about cyber risks and therefore less vigilant. Previous research on individuals has indeed found that increased awareness about online risks and safety can be associated with feeling less vulnerable and being susceptible to optimism bias with regard to mitigating threats (De Kimpe et al., 2021; Martens et al., 2019). As one of the first empirical studies on the cyber victimization of businesses, it is beyond the scope of this paper to test the reasons for the lack of positive evidence regarding the effectiveness of the Government schemes, but future research should aim to do so. This requires complimenting cross-sectional survey-based research with more innovative data sources, such as honeypots (Maimon et al., 2014) or data from intrusion protection systems (Maimon et al., 2013), and promoting the collection of longitudinal data that allows testing of causal mechanisms (Howell and Burruss, 2020).

With respect to victimization and theoretical debates, it should also be noted that we find evidence of a correlation between certain business routine activities and victimization. Having company social media accounts and employees using personally owned devices for work are both related with an increased chance of targeting or victimization by phishing, identity theft, malware and hacking, which suggests that companies carrying out these activities should ensure their cybersecurity strategies take this into account.

The third research question focused on the relationship between adopting the measures advocated for in the Government schemes and the outcome and impact of suffering cyberattacks. The results regarding negative outcomes were similar to those for victimization: we did not find evidence of lower likelihood of negative consequences for those companies that had implemented Cyber Essentials or the majority of the 10 Steps. Prior studies have postulated that findings of this type may be the result of an inability to fully control for differences in the level of threats faced by different organizations. For instance, a simulation conducted by Woods and Bohme (2021) found that in general, higher security was associated with greater harm, but when focusing on only high-threat organizations, the relationship was inverse and more security was related with less harm.

On the other hand, our results show that companies who had adopted seven or more of the 10 Steps to Cyber Security were more likely to have suffered an impact from cyber incidents. One potential explanation for this finding resides in the fact that some of the impacts included in the survey are expected for those companies with more developed cybersecurity policies. For example, the introduction of new measures or staff time to deal with the incident. A company with a substantive cybersecurity policy will have set out reaction procedures that include assigning extra resources as well as learning and adapting from attacks. Overall, the findings herein with respect to negative outcomes and impacts underscore the difficulties to provide reliable measures of the costs of cybercrime, which has been noted in previous research (Anderson et al., 2019; Paoli et al., 2018).

By answering the three research questions, the present paper has begun to provide an evidence base for government policies related to cybercrime against businesses, which is a particularly pressing issue in modern society. However, it should be noted that the findings may be susceptible to the limitations that can affect all survey work, notably, response bias. Businesses are concerned about the possible reputational impact of having suffered cyber incidents, thus, they may be reticent to share this information, even in an anonymous survey (Kemp, et al., 2021a). For this reason, the present article constitutes only an initial step towards understanding the effectiveness of public policies that aim to strengthen organizational resilience to threats in the digital era. To gain deeper comprehension of responses to crime against businesses in the twenty-first century, concerted efforts need to be made to improve data collection.

Credit author statement

Steven Kemp: all contributions to the paper have been performed by the sole author.

Funding

This work was supported by the Spanish State Research Agency [grant number: FJC2020–042884-I, PID2019-105042RB-I00]

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., Upton, D., 2018. A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. J. Cybersecur. 4 (1), tyy006. doi:10.1093/cybsec/tyy006.

Anderson, R., Barton, C., Boehme, R., Clayton, R., Ganan, C., Grasso, T., Levi, M., Moore, T., Savage, S., Vasek, M., 2019. Measuring the changing cost of cybercrime. In: The 18th annual workshop on the economics of information security, p. 32.

Ando, T., 2010. Bayesian Model Selection and Statistical Modeling. Chapman and Hall/CRC doi:10.1201/EBK1439836149.

Angst, C.M., Block, E.S., D'Arcy, J., Kelley, K, 2017. When do it security investments matter? accounting for the influence of institutional factors in the context of healthcare data breaches. MIS Quarterly 41 (3), 893–916. doi:10.25300/MISQ/2017/41.3.10.

Bada, M., Nurse, J.R.C., 2019. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Inf. Comput. Secur. 27 (3), 393–410. doi:10.1108/ICS-07-2018-0080.

Bilodeau, H., Mohammad, L., Uhrbach, M., 2019. Cyber security and cybercrime challenges of Canadian businesses, 2017. Statistics Canada. https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00006-eng.htm.

Blythe, J.M., Coventry, L., 2018. Costly but effective: comparing the factors that influence employee anti-malware behaviours. Comput. Human Behav. 87, 87–97. doi:10.1016/j.chb.2018.05.023.

Brewer, R., Vel-Palumbo, M.D., Hutchings, A., Holt, T.J., Goldsmith, A., Maimon, D., 2019. Cybercrime Prevention: Theory and Applications. Palgrave Pivot doi:10.1007/978-3-030-31069-1.

Britain Thinks, 2021. Review of Cyber Essentials Influence On Cyber Security Attitudes and Behaviours in UK Organisations. National Cyber Security Centre https://www.ncsc.gov.uk/information/setting-baseline-ce-prior-to-iasme.

Buil-Gil, D., Lord, N., Barrett, E., 2021. The dynamics of business, cybersecurity and cyber-victimization: foregrounding the internal guardian in prevention. Vict. Offender 16 (3), 286–315. doi:10.1080/15564886.2020.1814468.

Button, M., 2020. The "new" private security industry, the private policing of cyberspace and the regulatory questions. J. Contemp. Crim. Justice 36 (1), 39–55. doi:10.1177/1043986219890194.

Clubb, A.C., Hinkle, J.C., 2015. Protection motivation theory as a theoretical framework for understanding the use of protective measures. Crim. Justice Stud. 28 (3), 336–355. doi:10.1080/1478601X.2015.1050590.

Cohen, L.E., Felson, M., 1979. Social change and crime rate trends: a routine activity approach. Am. Sociol. Rev. 44 (4), 588–608. doi:10.2307/2094589, JSTOR.

Connolly, L.Y., Wall, D.S., Lang, M., Oddson, B., 2020. An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. J. Cybersecur. 6 (1), tyaa023. doi:10.1093/cybsec/tyaa023.

Dang-Pham, D., Pittayachawan, S., 2015. Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: a protection motivation theory approach. Comput. Secur. 48, 281–297. doi:10.1016/j.cose.2014.11.002.

Dash, D., Cooper, G.F., 2004. Model Averaging for prediction with discrete Bayesian networks. J. Mach. Learn. Res. 5, 1177–1203.

De Kimpe, L., Walrave, M., Verdegem, P., Ponnet, K., 2021. What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behav. Inf. Technol. 0 (0), 1–13. doi:10.1080/0144929X.2021.1905066.

Department for Business, Energy & Industrial Strategy, 2020. Business Population Estimates 2020. Department for Business, Energy & Industrial Strategy https://www.gov.uk/government/statistics/business-population-estimates-2020.

Department of Digital, Culture, Media & Sport, 2021a. *Cyber Security Breaches Survey 2021: Statistical Release* (Cyber Security Breaches Survey, p. 66). Department of Digital, Culture, Media & Sport.

Department of Digital, Culture, Media & Sport. (2021b). *Cyber Security Sectoral Analysis 2021*. https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2021

Drew, J.M., Farrell, L., 2018. Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs. Police. Pract. Res. 19 (6), 537–549. doi:10.1080/15614263.2018.1507890.

Dupont, B., 2019. Enhancing the effectiveness of cybercrime prevention through policy monitoring. J. Crime Justice 42 (5), 500–515. doi:10.1080/0735648X.2019.1691855.

ENISA. (n.d.). *Tools*. retrieved 5/3/2022, from https://www.enisa.europa.eu/tools

Fragoso, T.M., Bertoli, W., Louzada, F., 2018. Bayesian model averaging: a systematic review and conceptual classification. Int. Stat. Rev. 86 (1), 1–28. doi:10.1111/insr.12243.

Furnell, S., Heyburn, H., Whitehead, A., Shah, J.N., 2020. Understanding the full cost of cyber security breaches. Comput. Fraud Secur. 2020 (12), 6–12. doi:10.1016/S1361-3723(20)30127-5.

Gupta, R., Biswas, B., Biswas, I., Sana, S.S., 2020. Firm investment decisions for information security under a fuzzy environment: a game-theoretic approach. Inf. Comput. Secur. 29 (1), 73–104. doi:10.1108/ICS-02-2020-0028.

Hanus, B., Wu, Y."Andy", 2016. Impact of users' security awareness on desktop security behavior: a protection motivation theory perspective. Inf. Syst. Manage. 33 (1), 2–16. doi:10.1080/10580530.2015.1117842.

Heidt, M., Gerlach, J.P., Buxmann, P., 2019. Investigating the security divide between SME and large companies: how SME characteristics influence organizational IT security investments. Inf. Syst. Front. 21 (6), 1285–1305. doi:10.1007/s10796-019-09959-1.

Herath, T.C., Herath, H.S.B., D'Arcy, J., 2020. Organizational Adoption of Information Security Solutions: An Integrative Lens Based on Innovation Adoption and the Technology- Organization- Environment Framework'. *ACM SIGMIS Database*. The DATABASE for Advances in Information Systems 51 (2), 12–35. doi:10.1145/3400043.3400046.

Hinne, M., Gronau, Q.F., van den Bergh, D., Wagenmakers, E.J., 2020. A conceptual introduction to Bayesian model averaging. Adv. Methods Pract. Psychol. Sci 3 (2), 200–215. doi:10.1177/2515245919898657.

Hiscox, 2021. The Hiscox Cyber Readiness Report 2021. Hiscox https://www.hiscox.co.uk/cyberreadiness.

Ho, H.T.N., Luong, H.T., 2022. Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis. Glas. Zemaljskog Muz. Bosne Hercegovine Sarajevu: Prir. Nauke 2 (1), 4. doi:10.1007/s43545-021-00305-4.

Hoeting, J.A., Madigan, D., Raftery, A.E., Volinsky, C.T., 1999. Bayesian model averaging: a tutorial. Stat. Sci. 14 (4), 382–401.

Howell, C.J., Burruss, G.W., 2020. Datasets for Analysis of Cybercrime. In: Holt, T.J., Bossler, A.M. (Eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance. Springer International Publishing, pp. 207–219. doi:10.1007/978-3-319-78440-3_15.

Hsu, C., Lee, J.N., Straub, D.W., 2012. Institutional influences on information systems security innovations. Inf. Syst. Res. 23 (3–part–2), 918–939. doi:10.1287/isre.1110.0393.

Kaplan, D., Lee, C., 2018. Optimizing prediction using bayesian model averaging: examples using large-scale educational assessments. Eval. Rev. 42 (4), 423–457. doi:10.1177/0193841X18761421.

Kemp, S., Buil-Gil, D., Miró-Llinares, F., Lord, N., 2021a. When do businesses report cybercrime? Findings from a UK study. Criminol. Criminal Justice 17488958211062360. doi:10.1177/17488958211062359.

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., Díaz-Castaño, N., 2021b. Empty streets, busy internet: a time-series analysis of cybercrime and fraud trends during COVID-19. J. Contemp. Crim. Justice 37 (4), 480–501. doi:10.1177/10439862211027986.

Khando, K., Gao, S., Islam, S.M., Salman, A., 2021. Enhancing employees information security awareness in private and public organisations: a systematic literature review. Comput. Secur. 106, 102267. doi:10.1016/j.cose.2021.102267.

Maddux, J.E., Rogers, R.W., 1983. Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change. J. Exp. Soc. Psychol. 19 (5), 469–479. doi:10.1016/0022-1031(83)90023-9.

Madigan, D., Raftery, A.E., 1994. Model selection and accounting for model uncertainty in graphical models using occam's window. J. Am. Stat. Assoc. 89 (428), 1535–1546. doi:10.2307/2291017.

Maimon, D, 2020. Relevance of Evidence-Based Cybersecurity in Guiding the Financial Sector's and Efforts in Fighting Cybercrime. In: Pomerleau, P.-L., Lowery, D.L. (Eds.), Countering Cyber Threats to Financial Institutions: A Private and Public Partnership Approach to Critical Infrastructure Protection. Springer International Publishing, pp. 9–28. doi:10.1007/978-3-030-54054-8_2.

Maimon, D., Alper, M., Sobesto, B., Cukier, M., 2014. Restrictive deterrent effects of a warning banner in an attacked computer system. Criminology 52 (1), 33–59. doi:10.1111/1745-9125.12028.

Maimon, D., Kamerdze, A., Cukier, M., Sobesto, B., 2013. Daily trends and origin of computer-focused crimes against a large university computer network: an application of the routine-activities and lifestyle perspective. Br. J. Criminol. 53 (2), 319–343. doi:10.1093/bjc/azs067.

Maimon, D., Louderback, E.R., 2019. Cyber-dependent crimes: an interdisciplinary review. Annu. Rev. Criminol. 2 (1), 191–216. doi:10.1146/annurev-criminol-032317-092057.

Martens, M., De Wolf, R., De Marez, L., 2019. Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. Comput. Human Behav. 92, 139–150. doi:10.1016/j.chb.2018.11.002.

NCSC, 2020. Cyber Security Small Business Guide. National Cyber Security Centre https://www.ncsc.gov.uk/files/NCSC_A5_Small_Business_Guide_v4_OCT20.pdf.

NCSC. (n.d.-a). *10 Steps to cyber security*. retrieved 5/3/2022, from https://www.ncsc.gov.uk/collection/10-steps

NCSC. (n.d.-b). *About cyber essentials*. retrieved 5/3/2022, from https://www.ncsc.gov.uk/cyberessentials/overview

Niemimaa, E., Niemimaa, M., 2017. Information systems security policy implementation in practice: from best practices to situated practices. Eur. J. Inf. Syst. 26 (1), 1–20. doi:10.1057/s41303-016-0025-y.

NIST. (n.d.). *Small business cybersecurity corner*. retrieved 5/3/2022, from https://www.nist.gov/itl/smallbusinesscyber

Okutan, A., Werner, G., Yang, S.J., McConky, K., 2018. Forecasting cyberattacks with incomplete, imbalanced, and insignificant data. cybersecur. 1 (1), 15. doi:10.1186/s42400-018-0016-5.

Osborn, E., Simpson, A., 2017. On small-scale IT users' system architectures and cyber security: a UK case study. Comput. Secur. 70, 27–50. doi:10.1016/j.cose.2017.05.001.

Paoli, L., Visschers, J., Verstraete, C., 2018. The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium. Crime Law Soc. Change 70 (4), 397–420. doi:10.1007/s10611-018-9774-y.

Piironen, J., Vehtari, A., 2017. Comparison of Bayesian predictive methods for model selection. Stat. Comput. 27 (3), 711–735. doi:10.1007/s11222-016-9649-y.

R Core Team. (2021). *R: a language and environment for statistical computing* (3.6.1.). https://www.r-project.org/

Raftery, A.E., 1995. Bayesian model selection in social research. Sociol. Methodol. 25, 111–163. doi:10.2307/271063.

Raftery, A., Hoeting, J., Volinsky, C., Painter, I., Yeung, K.Y.. BMA: Bayesian Model Averaging. R package version 3.18.17.

Raftery, A.E., Painter, I., Volinsky, C.T., 2005. BMA: an R package for Bayesian model averaging. R. News 5 (2), 2–8.

Rakes, T.R., Deane, J.K., Paul Rees, L., 2012. IT security planning under uncertainty for high-impact events. Omega (Westport) 40 (1), 79–88. doi:10.1016/j.omega.2011.03.008.

Rantala, R., 2008. *Cybercrime Against Businesses, 2005* (p.20). U.S. Department of Justice.

Renaud, K., Ophoff, J., 2021. A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. Organiz. Cybersecur J: Practice Process People 1 (1), 24–46. doi:10.1108/OCJ-03-2021-0004.

Richards, K., 2009. The Australian Business Assessment of Computer User Security: A national Survey. Australian Institute of Criminology.

Rodriguez, T., & Witherell, D. (2021). *Iterake: tools for iterative raking. R package version 0.0.93*. (0.0.93). https://github.com/ttrodrigz/iterake

Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change1. J. Psychol. 91 (1), 93–114. doi:10.1080/00223980.1975.9915803.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A., Herawan, T., 2015. Information security conscious care behaviour formation in organizations. Comput. Secur. 53, 65–78. doi:10.1016/j.cose.2015.05.012.

Sarabi, A., Naghizadeh, P., Liu, Y., Liu, M., 2016. Risky business: fine-grained data

breach prediction using business profiles. J. Cybersecur. 2 (1), 15–28. doi:10.1093/cybsec/tyw004.
Sen, R., Borle, S., 2015. Estimating the contextual risk of data breach: an empirical approach. J. Manage. Inf. Syst. 32 (2), 314–341. doi:10.1080/07421222.2015.1063315.
Sloughter, J.M., Gneiting, T., Raftery, A.E., 2013. Probabilistic wind vector forecasting using ensembles and Bayesian model averaging. Mon. Weather Rev. 141 (6), 2107–2119. doi:10.1175/MWR-D-12-00002.1.
Steel, M.F.J., 2020. Model averaging and its use in economics. J. Econ. Lit. 58 (3), 644–719. doi:10.1257/jel.20191385.
Tam, T., Rao, A., Hall, J., 2021. The good, the bad and the missing: a Narrative review of cyber-security implications for australian small businesses. Comput. Secur. 109, 102385. doi:10.1016/j.cose.2021.102385.
UK Government, 2015. National Security Strategy and Strategic Defence and Security Review 2015. HM Government https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015.
UK Government. (2016). *National Cyber Security Strategy 2016-2021* (p.80).
UK Government, 2021. National Cyber Strategy 2022. UK Government, p. 130.
Vakhitova, Z.I., Alston-Knox, C.L., 2018. Non-significant p-values? Strategies to understand and better determine the importance of effects and interactions in logistic regression. PLoS One 13 (11), e0205076. doi:10.1371/journal.pone.0205076.
van Bavel, R., Rodríguez-Priego, N., Vila, J., Briggs, P., 2019. Using protection motivation theory in the design of nudges to improve online security behavior. Int. J. Hum. Comput. Stud. 123, 29–39. doi:10.1016/j.ijhcs.2018.11.003.
van de Weijer, S.G.A., Leukfeldt, R., van der Zee, S., 2021. Cybercrime Reporting Behaviors Among Small- and Medium-Sized Enterprises in the Netherlands. In: Weulen Kranenbarg, M., Leukfeldt, R. (Eds.), Cybercrime in Context: The human Factor in victimization, offending, and Policing. Springer International Publishing, pp. 303–325. doi:10.1007/978-3-030-60527-8_17.
Vasek, M., Moore, T., 2014. *Identifying risk factors for webserver compromise* [Proceedings paper]. In: Financial Cryptography and Data Security. In: (Proceedings) Financial Cryptography and Data Security. Springer. Springer.
Viallefont, V., Raftery, A.E., Richardson, S., 2001. Variable selection and Bayesian model averaging in case-control studies. Stat Med 20 (21), 3215–3230. doi:10.1002/sim.976.
Vrhovec, S., Mihelič, A., 2021. Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. Comput. Secur. 106, 102309. doi:10.1016/j.cose.2021.102309.
Wall, D.S., 2021. The transnational cybercrime extortion landscape and the pandemic. Eur. Law Enforce. Res. Bull. SCE 5. doi:10.7725/eulerb.v0iSCE, Article SCE 5.
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 Behav. 40 (9), 1119–1131. doi:10.1080/01639625.2018.1461786.
Workman, M., Bommer, W.H., Straub, D., 2008. Security lapses and the omission of information security measures: a threat control model and empirical test. Comput. Human Behav. 24 (6), 2799–2816. doi:10.1016/j.chb.2008.04.005.
Woods, D.W., Böhme, R., 2021. SoK: Quantifying cyber risk. IEEE Symposium on Security and Privacy (SP). 211-228. doi:10.1109/SP40001.2021.00053

Dr. Steven Kemp is Postdoctoral Research Fellow in Criminology at Pompeu Fabra University, Barcelona, Spain. He is a recipient of the Spanish national Juan de la Cierva Postdoctoral Grant. His-main research interests are cybercrime and fraud victimization, reporting, and the evaluation of security public policy. His-recent research has been published in Crime Science, Criminology & Criminal Justice, the Journal of Contemporary Criminal Justice, and the European Journal of Criminology, amongst others. **Selected recent publications** – Kemp, S., Buil-Gil, D., Miró-Llinares, F., & Lord, N. (2021). When do businesses report cybercrime? Findings from a UK study. *Criminology & Criminal Justice*. – Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. *Journal of Contemporary Criminal Justice, 37*(4), 480–501. – Kemp, S. (2020). Fraud reporting in Catalonia in the Internet era: Determinants and motives. *European Journal of Criminology*.