Journal of Small Business Management

ISSN: 0047-2778 (Print) 1540-627X (Online) Journal homepage: www.tandfonline.com/journals/ujbm20

Underinvestment in cyber security: Quantifying cyber security behavior in UK businesses

Anna Cartwright & Edward Cartwright

To cite this article: Anna Cartwright & Edward Cartwright (07 Oct 2025): Underinvestment in cyber security: Quantifying cyber security behavior in UK businesses, Journal of Small Business Management, DOI: 10.1080/00472778.2025.2549068

To link to this article: https://doi.org/10.1080/00472778.2025.2549068

JOURNAL OF SMALL BUSINESS MANAGEMENT
https://doi.org/10.1080/00472778.2025.2549068

Underinvestment in cyber security: Quantifying cyber security behavior in UK businesses

Anna Cartwright [a] and Edward Cartwright [b]

[a]Consultant, UK; [b]Department of Accounting, Finance and Economics, De Montfort University, UK

ABSTRACT

Many businesses, particularly small businesses, are underinvesting in cyber security. This exposes them to the risk of costly cyber attack. To address the challenge of cyber security in small businesses a greater understanding is needed of why businesses are underinvesting. To address this challenge, we propose a novel framework to distinguish five behavioral types and quantify the proportion of businesses fitting each type. The types are overconfident, procrastinator, risk accepting, defer responsibility, and optimal. We apply our framework using data from the UK Government's Cyber Security Breaches Survey from 2018–2024. We find that procrastination and overconfidence are the main reasons for underinvestment in cyber security in small businesses. We also find that small businesses with cyber insurance and/or cyber outsourcing are more likely to be classified as optimal. These results can inform policy interventions that better target the root cause of underinvestment in cyber security.

KEYWORDS

Cyber risk assessment; cyber risk analysis; cyber security investment; cyber insurance; IT outsourcing

The use of digital, information, and communication technologies opens up exciting opportunities for businesses to increase productivity, profitability, and growth. Use of these technologies, however, exposes businesses to the evolving threat of cyber attacks. Businesses are, consequently, having to contend with and adapt to increasing cyber security risks (Wall, 2024). The significant costs resulting from cyber attacks and data breaches are well documented (e.g., Anderson et al., 2019; Lagazio et al., 2014; Paoli et al., 2018). For instance, ransomware has caused major disruption to businesses and economies in recent years (Connolly & Wall, 2019; Meurs et al., 2023; Mott et al., 2024). As a specific example, consider the case of KNP, a UK-based transport company that had been in operation for over 150 years. They declared bankruptcy, with over 700 made redundant, following

CONTACT Edward Cartwright edward.cartwright@dmu.ac.uk Department of Accounting, Finance and Economics, De Montfort University, The Gateway, Leicester LE1 9BH, UK

Supplemental data for this article can be accessed online at https://doi.org/10.1080/00472778.2025.2549068

a ransomware attack in 2023 that is thought to have been facilitated by one weak password.[1]

A pressing challenge for the modern business world is how to embrace the opportunities of digital technology while also managing exposure to cyber risk. The cyber security challenge is particularly pronounced in small businesses. Micro and small businesses are increasingly reliant on digital technology for day-to-day operations, whether that be accounting and tax reporting, communicating through email, digital marketing, remote working, or online banking. Indeed, for an increasing number of businesses, digital technology is a key part of business operations (Attaran & Woods, 2019; Papadopoulos et al., 2020; Ritz et al., 2019). Lack of resource and expertise means, however, that many micro and small businesses will inevitably find it challenging to optimally invest time and resources in cyber security (Alahmari & Duncan, 2020; Berry & Berry, 2018; Chidukwani et al., 2022; Osborn & Simpson, 2018; Selznick & LaMacchia, 2017; Tam et al., 2021). For instance, a survey of Australian small and medium businesses by Chidukwani et al. (2024) found lack of funds, lack of knowledge on where to start, and lack of relevant regulations as significant barriers to implementation of appropriate cyber security practices.

Governments and law enforcement, in collaboration with business membership organizations, have been proactive in initiating and promoting a range of campaigns and schemes aimed at raising cyber security awareness in businesses (Bada & Nurse, 2019). In the United Kingdom there is a Cyber Essentials scheme relevant for all sizes of business, a 10 Steps to Cyber Security campaign aimed at large businesses, and a Cyber Aware campaign of relevance to sole-traders, the self-employed, and micro business owners (HM Government, 2022; Kemp, 2023). Consistent evidence, however, would suggest that cyber awareness campaigns are having a limited effect on behavior (Akpan et al., 2022; Bada et al., 2019; Ključnikov et al., 2019; Ponsard et al., 2019; Rupeika-Apoga et al., 2022; Van Steen et al., 2020). It can also be difficult for small businesses to navigate the diverse information on cyber security that is available to them (Cartwright, Cartwright, & Edun, 2023; Khan et al., 2024). Moreover, evidence would suggest that many, if not most, businesses are not implementing basic cyber security recommendations (Dinkova et al., 2023; Hoppe et al., 2021; Wilson et al., 2022).

Fundamental policy and research questions include why small businesses are not implementing basic cyber security measures and how to better target interventions to bring about desirable behavior change (Antunes et al., 2021; Armenia et al., 2021). In answering these questions it is vital to recognize that there are many distinct reasons why businesses are underinvesting in cyber security and a consequent need for tailored policy interventions (Shojaifar & Järvinen, 2021). The Small Business Standards

[1]See https://www.bbc.co.uk/news/articles/cx2gx28815wo.

association in Europe, for example, highlighted that "differentiation is needed to tailor standards and certification schemes to different types and sizes of SMEs" (Small Business Standards, 2020). To inform policy in this area, we introduce a novel framework to identify, distinguish, and quantify different behavioral types of business (with a particular focus on micro- and small businesses). We apply this framework using data from the annual UK government's Cyber Security Breaches Survey to estimate the proportion of businesses of each behavioral type. In total we consider data on 9,412 businesses over the years 2018 to 2024.

Informed by the evidence on behavioral biases in cyber security behaviors, we distinguish five behavioral types of business owners/managers: (a) Risk accepting, or those who knowingly take on cyber security risk; (b) procrastinator, or those who want to act on cyber security but are delaying; (c) overconfident, or those who underestimate the cyber risk and/or overestimate their cyber security; (d) defer responsibility, or those who are aware of risks but expect others (for example, outsourced IT provider) to address the risk; and (e) optimal, or those who are acting according to best practice. The only previous framework of which we are aware that looks to fully classify cyber security types in SMEs is Shojaifar and Järvinen (2021). They also identify five classes of SME and we show that our types align closely with theirs. A crucial innovation in our work is to develop an algorithmic and data analysis framework with which to classify the type of a business based on data in the Cyber Security Breaches Survey. This allows crucial new insight into the reasons why small businesses are not implementing cyber security best practice across a representative sample of UK businesses.

Our primary research questions can be summarized as follows.

RQ 1 What is the distribution of cyber security behavioral types in owners/managers of UK micro- and small businesses. What proportion of businesses are behaving optimally? Is underinvestment in cyber security primarily driven by procrastination, overconfidence, deferring of responsibility, or acceptance of risk?

We find that less than a third of micro- and small businesses are classified as optimal. Of those that are not optimal, most are classified as overconfident or procrastinating. With a focus on understanding the need for tailored policy interventions in cyber security we distinguish characteristics that influence the distribution of behavioral types with a particular focus on sector. We also quantify "how far away from optimal" business owners/managers are, on average, for different behavioral types. This is based on the UK government's set of recommended controls.

RQ 2 What is the distribution of cyber security behavioral types in UK micro and small businesses across sectors. Does the distribution of behavioral types systemtically differ between sectors?

RQ 3 How many of the recommended cyber security controls are being implemented, on average, by micro- and small businesses of each behavioral type?

We demonstrate that our empirical approach can also be used to offer novel insight into topical policy questions. In particular, there has been growing interest in the impact that cyber insurance and cyber outsourcing are having on cyber security behaviors (e.g. Adriko & Nurse, 2024a, 2024b; Arce et al., 2024; Benaroch, 2020; Cartwright, Cartwright, MacColl, et al., 2023; Mott et al., 2023; Romanosky et al., 2019). Cyber insurance companies can potentially improve cyber security behaviors by mandating controls for insured businesses and providing appropriate support and guidance. On the flip side, insurance may lead to moral hazard with insured businesses taking on more risk. Similarly, outsourcing of cyber security can provide businesses with improved access to resources and expertise but also lead to moral hazard.

RQ 4 Does cyber insurance and/or outsourcing of cyber security lead to improved cyber security behaviors?

Applying our approach, we find strong evidence that both cyber insurance and outsourcing are associated with a higher proportion of businesses classified as optimal. This would suggest that insurance and outsourcing are having a positive impact on cyber security behaviors.

A further application of our approach is to trace the distribution of behavioral types over time. We evidence significant changes in the distribution of types over the period 2018–2024. Such changes are driven by push and pull factors. On the one hand, it could be expected that businesses will become more aware of the relevance of cyber security over time (for example, as they hear of cyber attacks in the news or through networks). On the other hand cyber criminals are evolving their techniques and so the optimal cyber security controls change over time. Technological innovation through advances in artificial intelligence (AI), blockchain, cloud computing, quantum computing, and so forth, add additional complexity (Radanliev, 2024a). We discuss in the concluding section how our framework can offer insight into the consequences of emerging technology and to new policy interventions.

We proceed as follows: In section "Behavioral framework" we introduce our five behavioral types and a framework for discerning the type of a business. In Section "Empirical methodology" we outline how we applied our framework to data on UK businesses. In Section "Results," we detail the

distribution of behavioral types over time and sectors. Further results are provided in Section "Insurance and outsourcing" and "Cyber security controls across types." The implications of our results are discussed in Section "Concluding discussion." Additional materials are provided in the supplementary material.

Behavioral framework

A business's optimal investment in cyber security can be determined, in principle, using an economic cost-benefit analysis (Gordon & Loeb, 2002, 2006; Huang et al., 2006). The business needs to optimally trade off the costs of increased investment in cyber security with the benefits from a reduction in expected losses from cyber attack. At the optimum, the marginal gains from increased investment equal the marginal cost, taking into account the budget constraints. In practice, this analysis is inherently complex for a range of reasons, including large uncertainty concerning both the likelihood and the costs of a cyber attack in a fast-changing threat landscape and because of an interdependency between firms' optimal investment. There exist various frameworks to help businesses determine the optimal investment (e.g., Gordon et al., 2020; Huang & Behara, 2013; Nagurney & Shukla, 2017; Tsiodra et al., 2023).

While the optimal investment in cyber security will be specific to each business, there is clear evidence that many businesses are *underinvesting* in cyber security (Arroyabe et al., 2024; Dinkova et al., 2023; Renaud & Weir, 2016). This underinvestment should be interpreted as businesses investing less than optimal, taking into account their financial constraints, and is usually evidenced by businesses failing to implement basic security measures, such as a firewall, malware protection, and software updates, which would almost certainly have a favorable cost–benefit trade-off given that they are low cost and high benefit (Johns & Ell, 2020; Kemp, 2023). Decision-making in a micro- or small business will typically be taken by the owner or senior managers, who are not cyber security experts. Underinvestment, therefore, likely has an underlying behavioral explanation, such as procrastination or lack of understanding (Arroyabe et al., 2024). Lee and Larsen (2009), for instance, have surveyed executives of SMEs and show a link between threat and coping appraisal and adoption of antimalware software. In this paper, we provide a framework with which to model the role behavioral factors play in systematic underinvestment in cyber security.

In our framework we distinguish four broad factors that can influence cyber security investment within a micro- or small business: procrastination, risk accepting, overconfidence, and deferral of responsibility. We shall detail and motivate each in turn. Before doing so we briefly note that prior studies on cyber security behavior have primarily focussed on individual security

behavior (for example, clicking on a malicious link) rather than business behavior (for example, instigating an effective management policy). Reviewing such studies, Moustafa et al. (2021) identify four personality traits that impact an individual's compliance with security policy: procrastination, risk taking, impulsivity, and lack of thinking about the future consequences of actions (see also Egelman & Peer, 2015; Moustafa, 2022). Our framework aligns with these findings while changing the focus of analysis to a micro- and small-business context.

Behavioral factors

One behavioral factor evidenced to be of particular importance with regard to cyber security is overconfidence. Specifically, there is evidence that individuals can be overconfident in assessing cyber risk (see e.g., Vetter et al., 2011). In prior work three types of overconfidence are distinguished (Frank, 2020; Moore & Healy, 2008). These can be summarized as (a) when individuals think that they perform better than the average (Ament & Jaeger, 2017); (b) when individuals are overly confident in judging their ability—that is, they perceive more precision in their beliefs than is warranted; and (c) when individuals overrate their ability to resolve a security incident were one to arise. Overconfidence may be amplified within businesses because, for instance, overconfident individuals are more likely to reach senior management roles (Meikle et al., 2016). Overconfidence can lead to underinvestment in cyber security. For instance, overconfident business owners and senior managers may overestimate their business's ability to deter attack and underestimate the potential losses from an attack (Lee & Larsen, 2009). They may also have a bias to believe they are optimally investing in cyber security while actually underinvesting (Renaud & Weir, 2016).

A second behavioral factor evidenced to be of importance with regard to cyber security is procrastination. Procrastination comes from time-inconsistent choices whereby an individual plans to take future actions but subsequently delays those actions, potentially perpetually (Frederick et al., 2002). A tendency to procrastinate is prevalent across diverse populations (Ferrari et al., 2007; Steel, 2007) and can impact team decision-making (Van Hooft & Van Mierlo, 2018). In a cyber security context, procrastination exists if business owners and management identify the need for greater investment in cyber security but delay actions because of, say, other priorities (Renaud & Weir, 2016). Evidence suggests that procrastination is interlinked with stress, including work-related stress (e.g., Beheshtifar et al., 2011), and can be heightened in settings that are complex and ambiguous (Harris & Sutton, 1983). Procrastination can also be interlinked with entrepreneurial risk taking (Soomro & Shah, 2022). Moreover, cyber security can be seen as a low priority because "there is no

deadline" and it typically involves secondary tasks of avoiding a probabilistic loss rather than primary tasks that produce some direct, positive outcome. These are some of the multiple reasons why procrastination may have a significant impact on cyber security investment (Frik et al., 2018).

A third behavioral factor of importance with regard to cyber security is risk acceptance. A business may underinvest in cyber security because the owners and management have evaluated the risks and are knowingly willing to accept additional cyber risk. This would equate to being lax about cyber security in the framework of Renaud and Weir (2016). It may appear optimal from the perspective of risk-accepting owners or managers to invest less in cyber security. However, from a broader perspective, low investment may have negative spillover effects on others, such as employees, shareholders, lenders, or investors. Low investment could, therefore, be nonoptimal for the business even if the owners or managers are willing to accept risk. There is evidence of a significant correlation between passive risk behavior—that is, a willingness to accept risks that result from not implementing an action—and cyber security behavioral intentions and actual behavior (Arend et al., 2020). There is also evidence that entrepreneurs may be willing to take on more risk, particularly, if they have low wealth or are seeking high returns (Stewart & Roth, 2001; Vereshchagina & Hopenhayn, 2009).

The final behavioral factor considered is that of deferring responsibility onto others. For the vast majority of business owners/managers, cyber security is an unwanted distraction from the core activities of the business. Moreover, it is a distraction that results from criminal behavior. Owners and managers may, therefore, believe that it is "somebody else's problem to solve," whether they be law enforcement, government, internet service providers, multinational giants such as Microsoft and Apple, banks, or other. For instance, Wilson and McDonald (2025) find that the SMEs can favor "technical solutions" that rely on others rather than investing in appropriate cyber security training and policy. A particular concern is that businesses who outsource elements of IT may believe that the service provider will cover cyber security (when often they do not) (Cartwright, Cartwright, Edun, et al., 2023; Cezar et al., 2014; Cezar et al., 2017). An additional concern is that interconnected businesses may fail to cooperate in cyber security investments, leading to additional risk exposure within networks and supply chains (Nagurney & Shukla, 2017). Deferring responsibility onto others could be seen as a form of free riding, in which a business expects its risk exposure to be reduced by the actions of other organizations (Huang et al., 2006; Tosh et al., 2015). The notion, however, can be interpreted more generally in terms of encompassing the complex balance of responsibility for dealing with a criminal threat. For instance, the Cyber Perception Gap report produced by the UK government

highlighted the propensity of individuals and businesses to think cyber crime is "someone else's problem" (UK Home Office, 2018).

Behavioral types

In the preceding discussion we identified four behavioral factors that are of relevance in understanding underinvestment in cyber security: overconfidence, procrastination, risk acceptance, and deferring responsibility. We now provide a framework that can be used to classify businesses owners/managers into distinct behavioral types based on their cyber security beliefs, awareness, and actions. The behavioral type of a business is determined by the algorithmic framework depicted in the flow chart in Figure 1. The framework is built around six yes/no questions and can be summarized as follows.

- *Optimal type. This type of business is aware of the cyber threat, aware of cyber security best practice and implementing that best practice*. There is a wealth of trustworthy information available to micro- and small businesses on the cyber security threat and ways to mitigate that threat. For instance, as we shall discuss in more detail below, the UK government operates a Cyber Essentials Scheme that outlines best practice. A business behaving optimally will be aware of the threats to the business and taking appropriate action. Such a business still faces cyber risk and can be the victim of attack but is optimally managing the risk. Ideally, all businesses would be of this type. Underlying our framework is the notion that a business cannot be optimal "by accident" and so the business is knowingly implementing best practice.
- *Risk accepting. This type of business is aware of the cyber threat and aware of advised best practice but is knowingly "underinvesting" in cyber security because of a willingness to accept risk*. The risk-accepting business shares similarities with the optimal type in terms of a good understanding and awareness of the cyber threat. This type, however, is not following best practice.
- *Overconfident. This type of business is not fully aware of the cyber threat but believes best practice is being followed*. As we discussed above, overconfidence can occur for a range of different reasons but ultimately involves an overestimation of one's own capability. Hence, we associate overconfidence with business who believe they are following best practice but are not. A mismatch between beliefs and actions implies decision-makers are also unaware or naive about the cyber threat to the business, leading to the overconfidence.
- *Procrastinator. This type of business know they should be acting on cyber security but are delaying action. Our framework allows for procrastination in seeking information or failing to act on information*. In total there are

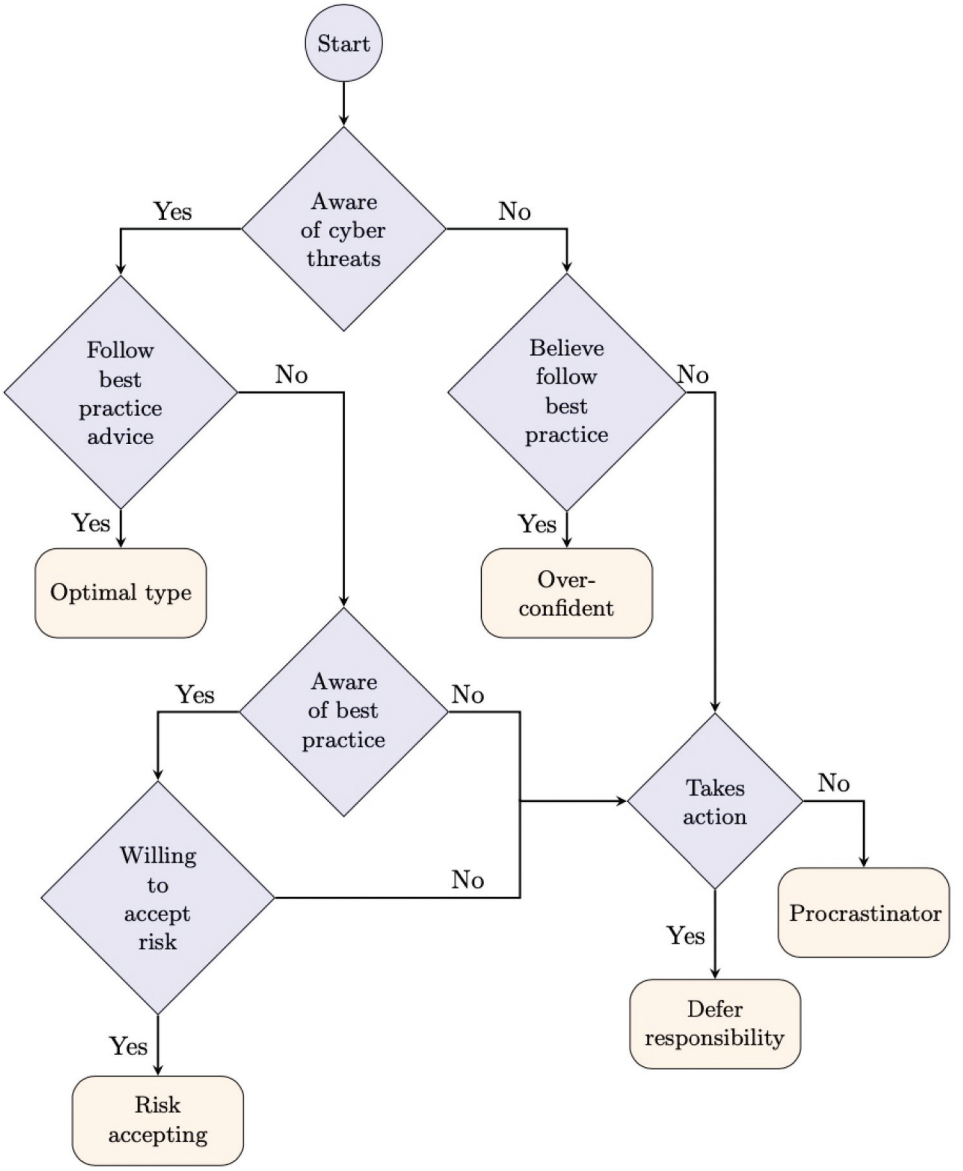

Figure 1. Framework for discerning the main behavioral type of a business.

three possibilities within our framework: (a) The business are not aware of the cyber threat and recognize that they are not following best practice but are delaying to seek information; (b) the business are aware of the cyber threat but not of cyber best practice and are delaying to seek information; (c) the business are aware of the cyber threat and of best practice but not following best practice because they are delaying action. Either way, delay is leading to underinvestment in cyber security.

- *Defer responsibility. This type of business know that action is needed on cyber security but expects or believes others (such as law enforcement or an IT provider) will do it*. As with procrastination, there are three possibilities within our framework: (a) The business are not aware of the cyber threat and recognize that they are not following best practice but are not planning to act; (b) the business owners/managers are aware of the cyber threat but not of cyber best practice and are not planning to act; (c) the business owners/managers are aware of the cyber threat and of best practice but are not following best practice and do not plan to act. The key distinction with procrastination is whether the business wants to act.

To further motivate our framework we relate it to the work of Shojaifar and Järvinen (2021). Their framework identifies five classes of SME based on the businesses characteristics: (a) "cyber security abandoned SMEs" that lack skills and resources and do not see the need for security measures, (b) "cyber security unskilled SMEs" that have a partial cyber security policy and want to act but lack skills and resources, (c) "cyber security expert-connected SMEs" with a partial policy but dependency on third parties and/or network connections and without adequately skilled employees, (d) cyber security capable SMEs and (e) cyber security provider SMEs. Our classification naturally aligns with Shojaifar and Järvinen if we equate cyber security abandoned SMEs with overconfident, cyber security unskilled SMEs with procrastinator, cyber security expert-connected SMEs with defer responsibility, and cyber security capable SMEs with optimal. An innovation in our framework is to provide the algorithmic framework in Figure 1 that allows us to systematically classify businesses.

To apply our framework we need an approach to evaluate each of the six questions in the framework, for a particular business, based on available data. We can then determine the type of a business and consequently analyze the distribution of behavioral types. In the following section we set out the methodology we used.[2]

Empirical methodology

We apply our behavioral framework to analyze data from the annual UK Cyber Security Breaches Survey (CSBS). The CSBS is conducted on behalf of the UK government (DCMS, 2024). The survey samples around 1,500–2,000 organizations each year, asking a wide range of questions about their cyber

[2]We recognize that a business may fall across different types. For instance, a business may display a mix of overconfidence and procrastination, say overconfident on the security of a supply chain and procrastinating on the implementation of network controls. We could, therefore, distinguish types based on particular aspects of cyber security, or associate a type that best fits the business when viewed across all aspects. We focus on the latter in this paper.

Table 1. Number of businesses in the CSBS by year and size of business that we analyzed.

	2018	2019	2020	2021	2022	2023	2024	Total
Micro-	655	770	644	746	698	685	526	4724
Small	349	330	286	275	272	239	243	1994
Medium	263	301	223	219	154	152	129	1441
Large	252	214	221	208	141	132	85	1253
Total	1,519	1,615	1,374	1,448	1,265	1208	983	9412

security practice, including current controls and policies and whether they were attacked in the last 12 months. We use the survey questions to categorize businesses according to our framework with data from the 2018–2024 surveys.[3] The data were accessed from the UK Data Service (https://ukdataservice.ac.uk/) which offers it cost-free to registered users.

In the remainder of the section we set out the main details of our analytical approach. For those interested in further details, particularly with an objective of replicating our work or applying our framework in their own research, please see the supplementary material. In Table 1 we summarize the number of businesses for which we had complete data for our analysis, distinguishing micro- (fewer than 10 employees), small (10–49 employees), medium (50–249 employees), and large (more than 250 employees) businesses. We analyze a total of 9,412 observations of which 6,718 are micro- or small businesses.

The CSBS has the advantage of providing a large number of observations over several years for micro- and small businesses. To apply our framework using data from the CSBS we created a range of measures and proxies for each of the six questions needed to characterize a business using our framework (see Figure 1). In identifying these measures we first discerned variables from the CSBS that were in scope in the sense that (a) there was consistency of data across the 7 years of analysis with (b) relatively few missing observations. We subsequently identified the most relevant variables to judge each of the six questions in our framework.

Measures of business practice

We now outline the measures used for each of the six questions in our framework. On the basis that there is no "perfect measure" we provide multiple measures for each question in the framework. This, as we shall discuss, allows us to check the robustness of our results and analysis to different formulations. The measures are also designed to provide upper and lower bounds on the likely "true" value. The measures we use are summarized in Table 2 and can be motivated as follows.

Is the business aware of cyber threats? The focus with this question is whether the organization recognizes the importance of cyber security,

[3]Data for 2017 and 2015 is available but the Survey was radically changed in 2018 and so we have omitted earlier years.

Table 2. The measures we use from the CSBS to evaluate the six questions in our framework.

Question		Measure
Aware of cyber threats?	AT1	Have looked up information on cyber security in the last 12 months or experienced a cyber attack in the last 12 months.
	AT2	Have looked up information on cyber security in the last 12 months and say that cyber security is a high priority.
	AT3	Have looked up information on cyber security in the last 12 months and say that cyber security is a high priority and have senior management responsibility for cyber security.
	AT4	Satisfy (AT3) or have experienced a cyber attack in the last 12 months.
Following best practice?	BP1	Implementing all the technical controls of Cyber Essentials.
	BP2	Implementing all the technical controls of the NCSC 10 Steps to Cyber Security.
	BP3	Implementing the technical controls of Cyber Essentials and have secure backups.
	BP4	Implementing the technical controls of Cyber Essentials and have secure backups and some management practices in place.
Aware of best practice?	ABP1	Heard of Cyber Aware or Cyber Essentials or 10 Steps to Cyber Security.
	ABP2	Satisfy (ABP1) and have accessed information on cyber security in the last 12 months.
	ABP3	Heard of Cyber Essentials or 10 Steps to Cyber Security.
Willing to accept risk?	AR1	There is a risk management process in place.
	AR2*	Say they do not have cyber insurance because either "have not prioritised it," "existing measures are good enough," "costs too much," or "cannot see the benefits/don't see the need."
Believe following best practice?	BBP1*	Agree that they have enough people dealing with cyber security to effectively manage the risks.
	BBP2*	Satisfy (BBP1) and agree that the people dealing with cyber security have the right skills.
	BBP3	Consider cyber security a priority.
Delaying action?	DA1	Have undertaken an internal audit, health check, risk assessment, and/or threat intelligence to identify cyber risks.
	DA2	Have undertaken some cyber security training and awareness within the business (either internally or externally).

*Indicates this measure is only available for the 2018-2019 data.

rather than whether they know how to deal with that threat. We compare and contrast four different measures (AT1–AT4 in Table 2) that are based on the businesses' experience, namely whether they have experienced a cyber attack in the last 12 months, and/or their actions, namely looking up information, treating cyber security as a priority and having senior management responsibility for cyber security. In interpretation we would say that a business that has, for example, been attacked in the last 12 months and/or has looked up information on cyber security shows an awareness of the cyber threat.

Is the business following best practice advice? There are two sources of best practice advice that we focus on. The UK government's Cyber Essentials Scheme, built around five technical controls, provides a minimum standard that all businesses (including micro- and small businesses) should satisfy (BP1). The NCSC 10 Steps to Cyber Security provides a more comprehensive set of controls covering policy and management processes. Compliance with the 10 Steps can be seen as the "gold standard" of best practice (BP2). The 10 Steps may be excessive for a micro- or small business and so we considered two intermediate measures consisting of Cyber Essentials and secure backups

(BP3) and management practices (BP4). We highlight that the guidance in Cyber Essentials and the NSCS 10 Steps has evolved during 2018–2024 to reflect the changing cyber-threat landscape. Our approach is to categorize businesses based on whether they were following the advice available at the time.

Is the business aware of best practice advice? In our framework, this question is asked only of businesses that are not following best practice. The focus is, thus, on whether a business that is not following advice is, at least, aware of that advice. The UK government oversees the previously mentioned Cyber Essentials and 10 Steps to Cyber Security. It also oversees a Cyber Aware campaign that is aimed more at individuals but is also relevant for sole traders and self-employed persons. These three schemes/campaigns are very widely advertised in the UK, including by industry bodies and business membership organizations. It would be expected, therefore, that a business owner/manager is aware of best practice should have heard of at least one of these schemes. This motivates our three measures (ABP1–ABP3).[4]

Is the business willing to accept cyber risk? In our framework, this question is asked of businesses who are not following best practice advice but are aware of that advice. Our focus is, therefore, on whether they have processes in place to manage risk and/or are knowingly willing to accept risk. We considered two measures to capture these two aspects— managing risk (AR1) and taking risk (AR2). Measure (AR1) is available across our full data set. Measure (AR2) captures risk taking but is available only in 2018–2019. It is, therefore, primarily used as a robustness check of the results obtained with measure (AR1).

Do the business owners/managers believe they are following best practice? In the 2018–2019 CSBS there were two survey questions that directly probed a business about cyber security skills. These provide our first two measures of belief in following best practice (BBP1–BBP2). Unfortunately, from 2020 onward these questions were dropped and there has been an absence of questions on skills. For the overall data set we, therefore, use a generic measure of prioritization (BBP3) that we identified as being highly correlated with attitudes toward skills in the 2018–2019 data sets.

Is the business taking (delaying) action on cyber security? In our framework, this question is asked of businesses that are not following best practice advice. We, therefore, focus on actions short of best practice that indicate that positive actions are being taken by the business. We consider two different measures capturing either actions to identify risks (DA1) or training and awareness in the business (DA2).

[4]Measure ABP3, which excludes Cyber Aware, recognizes that some respondents may have heard of Cyber Aware from their personal life (e.g. personal banking) but not know how to apply its guidance in a business context.

Classifying businesses by type

Focusing on our full (2018–2024) data set, as summarized in Table 2, we consider four measures of awareness of cyber threat, four measures of whether the business is following best practice, three measures of awareness of best practice, one measure of willingness to take risk, one measure of whether the business owners/managers believe they are following best practice and two measures of delaying action. If we fix a measure for each of the six questions then we can apply our framework and determine the classified behavioral type of any business. We can then estimate the proportion of businesses classified as each behavioral type. If we consider all possible permutations of our measures we have $4 \times 4 \times 3 \times 1 \times 1 \times 2 = 96$ different ways of classifying type. By estimating the proportion of businesses of each behavioral type across all these different permutations we are able to check the robustness of our results.

For each particular business we also obtain a nondiscrete measure of businesses type. To illustrate, consider two examples from our data set: (a) A micro business with two employees in the "professional, scientific or technical sector" that in all 96 permutations was classified as a procrastinator; (b) a small business with 13 employees from the "food and hospitality sector" that in 54 permutations (56.3 percent) was classified as optimal, in 24 permutations (25 percent) as overconfident, in 12 permutations (12.5 percent) as risk accepting, in three permutations (3.1 percent) as defer responsibility, and in three permutations (3.1 percent) as procrastinator. As you can see, our framework and empirical methodology allow us to determine type and uncertainty over type. In example (a) we can say with confidence the business is classified as a procrastinator whereas in example (b) we find evidence that the business is optimal but recognize uncertainty over that classification.

We performed a range of analyses to check that our framework is robust and producing reliable results. For instance, for the 2018–2019 data we have $4 \times 4 \times 3 \times 2 \times 3 \times 2 = 576$ different ways of classifying the type of a business. We demonstrate that we obtain similar results using this richer set of measures compared to the 96 measures we use for the full data set. We also demonstrate that for the majority of businesses in our sample, our method strongly identifies one behavioral type. Specifically, for around a third of businesses every permutation of our model identifies the same behavioral type (that is, 96 out of 96 or 576 out of 576 permutations give the same classification for that business). For another third of businesses, more than 70 percent of the permutations yield the same behavioral type (that is, 70 or more out of 96 or 404 or more out of 576 permutations give the same classification).

Results

Distribution of types

We begin our analysis of the results by summarizing the estimated distribution of behavioral types across businesses. In Table 3 we report, for comparison, three contrasting ways to summarize the distribution: mean, median, and modal. The entries under "mean" are calculated by averaging the estimated proportion of businesses of each behavioral type across all 96 permutations in our approach. The entries under "median" are calculated by finding the median proportion across permutations.[5] Finally, the entries under "modal" are calculated by assigning the modal type of each business, across all permutations; once the modal type of each business is assigned then the distribution across all businesses can be determined.

We see in Table 3 that the estimated proportion of optimal type is, as we would expect, strongly increasing in business size ($p < 0.0001$ proportions test based on modal classification). Less than one in five micro-businesses are estimated to be behaving optimally compared to around a half of large businesses. We remind the reader that our measures of whether a business is following cyber security best practice are primarily based around the five basic controls of Cyber Essentials, plus back-ups and management practices.[6] These are controls that every business, irrespective of size, should be implementing.

Table 3. Proportion (percentage) of businesses of each behavioral type by business size across three different ways of summarizing the distribution.

	Micro-	Small	Medium	Large
Mean				
Optimal	15.9	27.1	40.1	49.4
Overconfident	30.7	29.1	23.7	22.0
Procrastinator	36.1	23.3	13.5	7.6
Defer responsibility	12.0	12.5	11.5	10.3
Risk accepting	5.3	7.9	11.2	10.8
Median				
Optimal	18.5	32.5	48.3	55.6
Overconfident	27.3	24.7	18.6	17.1
Procrastinator	31.9	19.8	10.9	5.9
Defer responsibility	9.6	10.4	10.7	9.7
Risk accepting	4.7	6.7	8.4	8.1
Modal				
Optimal	18.5	32.4	48.3	58.3
Overconfident	38.5	34.5	26.7	22.6
Procrastinator	36.2	22.8	13.5	6.9
Defer responsibility	2.6	4.0	3.8	4.6
Risk accepting	4.2	6.4	7.6	7.6

[5]The proportions in the median measure, unlike the mean and modal, need not add to 100 percent.
[6]The "mean" measure also reflects our stricter measures based around the 10 Steps and hence gives a lower estimate than the "median" or "mode."

It is, therefore, concerning that so few businesses, including large businesses, are classified as optimal. This is our first key finding.

Result 1. Relatively few businesses are classified as behaving optimally. Only 15 percent to 19 percent of micro-businesses, 27 percent to 33 percent of small businesses, 40 percent to 48 percent of medium businesses, and 49 percent to 59 percent of large businesses are classified as optimal.

The data recorded in Table 3 show that of the four nonoptimal types the two that appear to be most prevalent are overconfident and procrastinator. Interestingly, overconfident type declines with business size but only marginally, with around one in three micro-businesses and one in five large businesses being classified as overconfident. Procrastination, by contrast, appears to be more of a problem for micro- and small businesses, with around one in three micro businesses, but fewer than one in ten large businesses classified as Procrastinator ($p < 0.0001$ proportions test based on modal classification). This would be consistent with micro- and small businesses having limited resources and competing (non–cyber related) pressures that are barriers to action.

Result 2. Among micro-businesses we find that overconfident and procrastinator are the most common types. The estimated proportion of overconfident type is marginally decreasing with business size, ranging from 27 percent to 39 percernt in micro-businesses to 17 percent to 23 percent in large businesses. The estimated proportion of procrastinator type is strongly decreasing in business size, ranging from 31 percent to 37 percent in micro-businesses to 5 percent to 8 percent in large businesses.

The data recorded in Table 3 show that the least prevalent types are defers responsibility and risk accepting. Defers responsibility characterizes around one in ten businesses, of all sizes, using the mean and median measure. Risk accepting is increasing with business size, from around one in 20 micro-businesses and around one in ten medium and large businesses ($p < 0.0001$ proportions test based on modal classification). The higher proportion of risk accepting type in large and medium businesses, combined with Result 1, reinforces the notion that medium and large businesses are more likely to be managing cyber risk (than micro- or small businesses).

Result 3. Defer responsibility and risk accepting are the least common types with the estimated proportion below 12 percent across all business sizes. The proportion of defer responsibility type is similar across business size. The proportion of risk accepting is lowest for micro-businesses and highest for medium and large businesses.

Distribution of types over time

Recall that we apply our classification method to CSBS data over a 7-year period from 2018 to 2024. This allows us to analyze the change in the

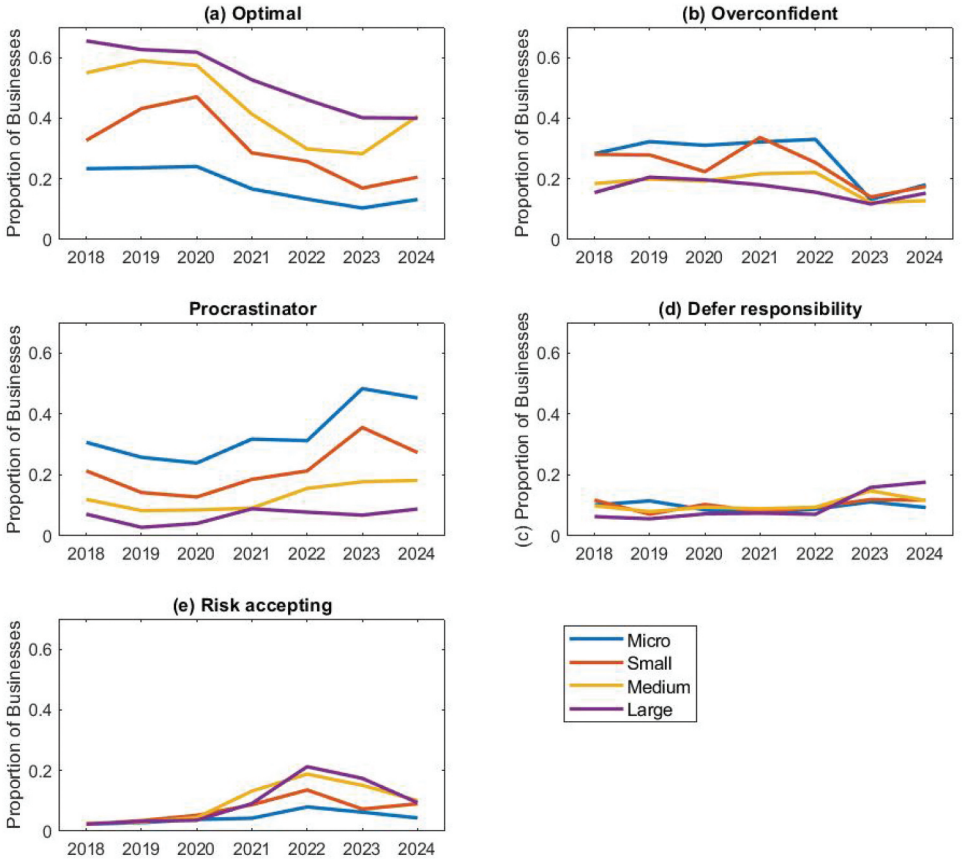

Figure 2. Proportion of businesses of each behavioral type over the period 2018 to 2024.

distribution of types over time. In Figure 2 we detail the proportion of businesses of each type by year and size of business. This is based on the median measure of the distribution.

We see in Figure 2 that the estimated proportion of businesses classified as optimal has primarily declined from 2018 to 2024 with the drop most pronounced in large businesses ($p = 0.001, 0.0017, 0.015, 0.0001$ proportions test of 2018 compared to 2024 for micro-, small, medium, and large businesses, respectively). In interpreting this finding we reiterate that the CSBS measures have changed during this time to reflect the evolving, and stricter, criteria for Cyber Essentials and the NCSC 10 Steps. Those stricter criteria, in turn, reflect changes in the threat landscape and the cyber security tools available to businesses, such as can be expected through, for example, AI innovations and greater use of cloud computing. Thus, we see that the proportion of businesses classified as optimal falls relative to accepted best practice of the time.

The decline in the proportion of optimal type has primarily been mirrored by a rise in procrastinator type for micro-businesses ($p = 0.005, 0.11, 0.12, 0.93$

proportions test of 2018 compared to 2024 for micro-, small, medium and large businesses, respectively) and risk accepting type for small, medium, and large businesses ($p = 0.09, 0.0005, 0.004, 0.013$). There is also a slight rise in the proportion of defer responsibility type for large businesses ($p = 0.004$) and a decline in overconfident type for micro- and small businesses ($p = 0.001, 0.003$, respectively). In interpretation, this would suggest a growing understanding and awareness of the cyber threat but challenges in converting that into positive action. One explanation could be that businesses during the period of study faced a number of challenges, including the COVID-19 pandemic, the UK's exit from the European Union and single market, and a period of high inflation. Cyber security may not have been seen as a priority during this period, particularly for micro- and small businesses.

Result 4. Over the period 2018 to 2024 we observe a significant decline in the proportion of businesses classified as optimal across all business sizes. For micro- and small businesses we also observe a decline in the proportion of overconfident type. For micro-businesses we see a counteracting rise in the proportion of procrastinator type. For small and medium businesses we see a counteracting rise in the proportion of risk accepting. For large businesses we see a counteracting rise in the proportion of risk accepting and defer responsibility types.

Sector

We next turn our attention to sector. For our full sample the CSBS categorizes businesses according to 12 sectors: administration or real estate (SIC L or N); construction (SIC F); education (SIC P); entertainment, service or membership organizations (SIC R or S); finance or insurance (SIC K); food or hospitality (SIC I); health, social care or social work (SIC P or Q); information or communication (SIC J); professional, scientific or technical (SIC M); retail or wholesale (SIC G); transport or storage (SIC H); and utilities or production (SIC B, C, D or E).[7] In Figure 3 we detail our estimated proportion of businesses of each behavioral type by sector, distinguishing (a) micro-businesses, (b) small businesses, and (c) medium and large businesses.[8]

We see in Figure 3 that the estimated proportion of the optimal type varies considerably across sectors. For example, in "finance or insurance" around 30 percent of micro businesses, 50 percent of small businesses, and 60 percent of medium and large businesses are identified as optimal, compared with only 10 percent, 10 percent, and 30 percent, respectively, in "food or hospitality." In each of the three subfigures, we have ordered the sectors according to the proportion of businesses classified as optimal. The ordering is identical for micro-businesses

[7] In 2022, agriculture, forestry or fishing (SIC A) was also added but we have omitted it from our analysis given the smaller number of observations.

[8] We combine medium and large businesses due to space considerations and our focus on micro and small businesses. Results are similar comparing medium and large businesses.

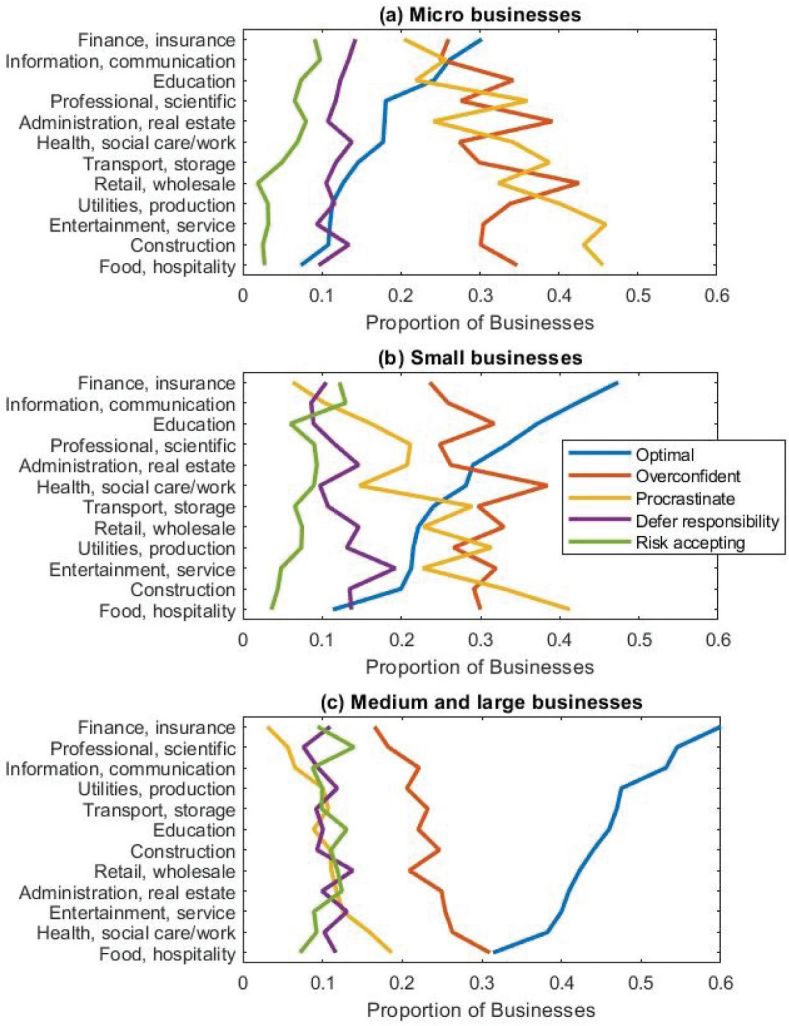

Figure 3. Proportion of businesses of each behavioral type by sector for micro-, small, and medium and large businesses.

and small businesses. There are, though, some interesting differences in the relative ordering of micro- and small businesses compared with medium and large businesses. For instance, in the "health, social care or social work" sector, micro- and small businesses are performing relatively well (4th out of 12 sectors), whereas, medium and large businesses are performing relatively poorly (11th out of 12). However, the "finance or insurance," "information or communication," and "professional, scientific and technical" sectors show a relatively high proportion of optimal type across all business sizes. "Food or hospitality" stands out as the sector with the lowest proportion of optimal type.

Result 5. There are large sector differences in the proportion of businesses classified as optimal. Differences range from 10 percent to 30 percent of micro-businesses, 10 percent to 50 percent of small businesses, and 30 percent to 60 percent of medium and large businesses. The "finance or insurance" sector has the highest proportion of businesses classified as optimal and the "food or hospitality" sector, the lowest.

For micro-businesses and, especially, small businesses we can see in Figure 3(a) and (b) that differences in the proportion of businesses classified as optimal across sectors are largely mirrored by differences in the proportion classified as procrastinator. In "finance or insurance," for instance, we find a relatively high proportion of optimal, or risk accepting (relative to other sectors) but a low proportion of procrastinator. In the "food or hospitality" sector, by contrast we find a low proportion of optimal, or risk accepting and a high proportion of procrastinator. Overconfident is between 25 percent and 40 percent across all sectors. By interpretation, therefore, our analysis shows that differences between, say, "finance or insurance" compared with "food or hospitality" are driven more by delays in acting than by differences in awareness or understanding. This may reflect different priorities and/or legislative and regulatory frameworks.

For medium and large businesses differences in the proportion of businesses classified as optimal are largely mirrored by differences in procrastinator and overconfident (Figure 3(c)). In "finance or insurance," for instance, we find a relatively high proportion of optimal and a low proportion of procrastinator and overconfident. In the "food or hospitality" sector, by contrast, we find a low proportion of optimal and a higher proportion of procrastinator and overconfident (compared to other sectors). Consistent with Result 2, across all sectors and all sizes of business, overconfidence is a problem for an estimated 20 percent to 40 percent of businesses.

Result 6. For micro- and small businesses there is an inverse relationship between the proportion of businesses in the sector classified as optimal and those classified as procrastinator. In medium and large businesses there is an inverse relationship between those classified as optimal and those classified as procrastinator and overconfident.

Insurance and outsourcing

As we mentioned earlier, there has been growing interest in the impact that cyber insurance and, to a lesser extent, cyber outsourcing has on cyber security behaviors within businesses (e.g. Adriko and Nurse, 2024a, 2024b; Arce et al., 2024; Benaroch, 2020; Cartwright, Cartwright, MacColl, et al., 2023; Cezar et al., 2014, 2017; Mott et al., 2023; Romanosky et al., 2019; Wu et al., 2021). Both insurance and outsourcing can have a positive impact on cyber security behaviors, for example access to appropriate support and guidance, but also potential

negative consequences, for example moral hazard by organizations taking on excess risk. There is, thus, a keen interest in whether the net impact of insurance and/or outsourcing is positive. In this section we demonstrate that our framework and empirical methodology can be used to address this applied question.

In Figure 4 we detail the estimated distribution of types by business size, distinguishing between businesses with and without cyber insurance. The proportion of businesses with cyber insurance is detailed in the title of the subplot (for example, 7% of micro-businesses have cyber insurance). As you can see in Figure 4, businesses with cyber insurance are more likely to be classified as optimal than those without, for all sizes of business ($p < 0.0001$ proportions test for micro-, small, medium, and large businesses). This difference is particularly pronounced for micro- and small businesses. Note, however, that only an estimated 35 percent of micro-businesses and 50 percent of small businesses are optimal even if they have cyber insurance. This suggests that cyber insurance has a positive impact, but there is still a large proportion of businesses with insurance that are not optimal. In micro- and small businesses we see that those without insurance are proportionally more likely to be classified as procrastinator.

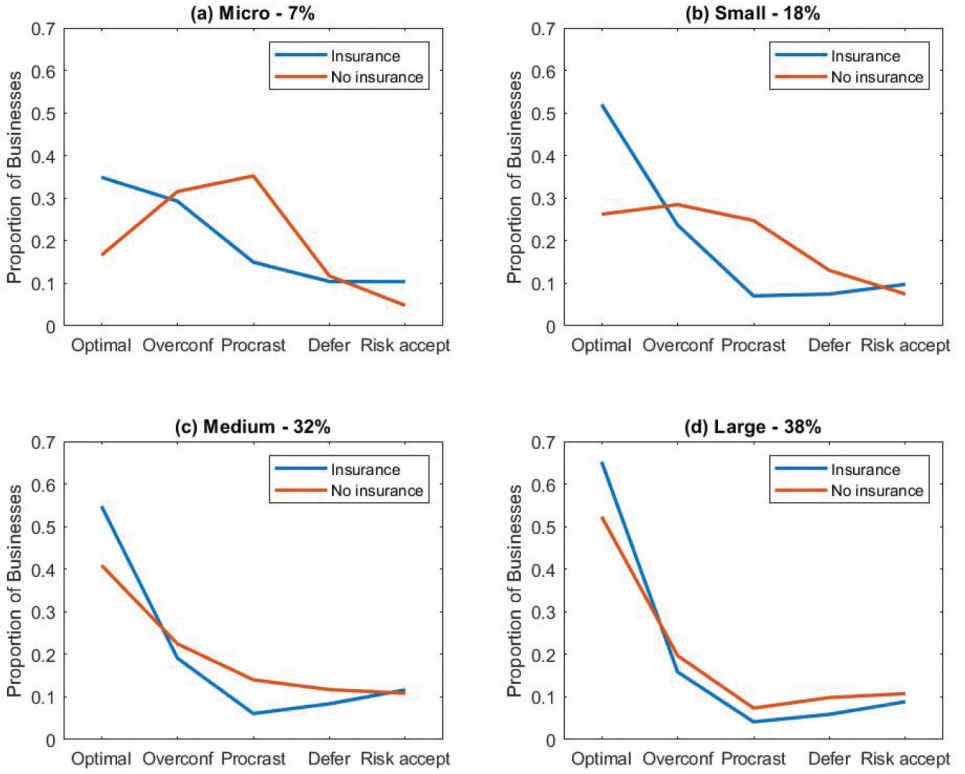

Figure 4. Distribution of types by business size distinguishing between businesses with and without cyber insurance.

In Figure 5 we detail the distribution of types by business size, distinguishing between businesses that outsource cyber security to a third-party provider. The proportion of businesses that outsource is detailed in the title of the subplot (for example, 38 percent of micro-businesses outsource). As you can see in Figure 5, micro- and small businesses who outsource are more likely to be classified as optimal ($p < 0.0001$ proportions test for micro- and small businesses, $p = 0.103, 0.125$ for medium and large, respectively). This suggests that outsourcing, like insurance, is associated with a positive impact on cyber security. However, well over half of micro- and small businesses that outsource are not classified as optimal. For micro- and small businesses that are not outsourcing we see a relatively high proportion of businesses classified as procrastinator.

Regression analysis

Insurance, outsourcing, and sector are all correlated. For example, in the "finance or insurance" sector, 21 percent of micro-businesses have cyber insurance and 65 percent outsource cyber security, while in the "food or hospitality" sector the respective proportions are 3 percent and 27 percent.

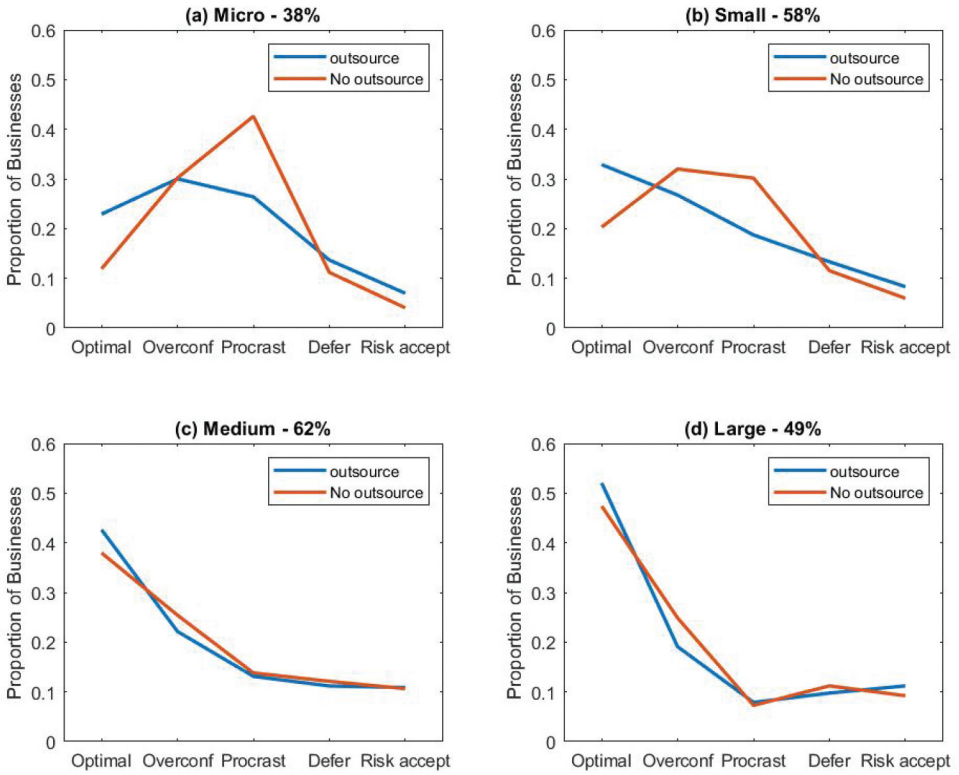

Figure 5. Distribution of types by business size, distinguishing between businesses with and without an outsourced cyber provider.

It is important, therefore, to evaluate the statistical significance of insurance and outsourcing, controlling for sector. To do so, we performed a regression analysis. We used a probit regression where the dependent variable is set to 1 if the business is classified as type optimal and 0 otherwise. The independent variables are dummy variables for insurance (whether the business has cyber-specific insurance), outsourcing (whether the business outsources cyber security to a third party), and individual sectors, using the "retail or wholesale" sector as the baseline for comparison.[9] We performed a separate regression analysis for micro-, small, and medium and large businesses to control for firm size. The results are presented in Table 4.

The regression results in Table 4 show that businesses with cyber insurance and businesses that outsource cyber security are significantly more likely to be classified as optimal, even when we control for sector. This holds for micro-, small, medium, and large businesses. To illustrate how to interpret these results, consider a micro-business in the "retail or wholesale" sector. A micro-business with no cyber insurance or outsourcing is estimated to have a 0.1 probability of being optimal.[10] A micro-business with cyber insurance is estimated to have a 0.19 probability of being optimal, a micro-business with outsourcing has a 0.21 probability, and a micro-business with cyber insurance and outsourcing, a 0.35 probability. These results reinforce the positive influence of insurance and outsourcing.

Result 7. Across all sizes of business we find that businesses with insurance and/or businesses that outsource cyber security are significantly more likely to be classified as optimal.

The regression results in Table 4 also reinforce Result 5, with the "finance or insurance" sector showing a high probability of businesses being optimal and the "food or hospitality" sector, a low probability. The "information or communication" sector also shows a relatively high probability of businesses being optimal.

Cyber security controls across types

We finish our analysis by exploring how the adoption of cyber security controls varies across behavioral types. This will allow us to explore not only whether a business is classified as optimal but also how far they are away from being classified as optimal. Recall that the NSCS 10 Steps to Cyber Security provides a comprehensive set of controls for all

[9]We chose the "retail or wholesale" sector as the baseline because this sector has the most number of observations in our data set (1302 observations) and also has good balance across the four business sizes under consideration.

[10]The baseline probability of being Optimal is given by $\Phi(-1.294)$ where Φ is the normal cumulative distribution function with mean 0 and standard deviation 1, and -1.294 is the constant term of the regression. The probability of being optimal with insurance is $\Phi(-1.294 + 0.408)$ etc.

Table 4. Results of probit regression with dependent variable representing whether the business is classified as type optimal. Independent variables represent whether the business has cyber-specific insurance, whether the business outsources, and what sector the business is in.

	Micro-	Small	Medium and Large
Insurance	0.408***	0.503***	0.370***
	(0.088)	(0.093)	(0.067)
Outsource	0.492***	0.438***	0.164***
	(0.052)	(0.075)	(0.063)
Sectors			
Administration or real estate	0.374***	0.323**	−0.086
	(0.098)	(0.149)	(0.110)
Construction	−0.018	0.064	0.090
	(0.103)	(0.158)	(0.145)
Education	0.560***	0.334*	−0.001
	(0.157)	(0.198)	(0.179)
Entertainment, service or memb. org.	0.308***	0.036	0.114
	(0.113)	(0.206)	(0.162)
Finance or insurance	0.653***	0.782***	0.252*
	(0.110)	(0.151)	(0.140)
Food or hospitality	−0.259*	−0.260	−0.164
	(0.139)	(0.171)	(0.134)
Health, social care or social work	0.326***	0.136	−0.307**
	(0.126)	(0.151)	(0.136)
Information or communication	0.756***	0.834***	0.170
	(0.097)	(0.170)	(0.160)
Professional, scientific or technical	0.283***	0.420***	0.364***
	(0.094)	(0.155)	(0.131)
Transport or storage	0.027	0.034	−0.044
	(0.149)	(0.206)	(0.143)
Utilities or production	−0.001	0.097	0.149
	(0.122)	(0.156)	(0.120)
Constant	−1.294***	−0.929***	0.023
	(0.069)	(0.113)	(0.084)
Observations	3,446	1,371	1,723
Log Likelihood	−1,633.204	−815.815	−1,118.190
Akaike Inf. Crit.	3,294.408	1,659.631	2,264.381

*$p < 0.1$; **$p < 0.05$; ***$p < 0.01$.

businesses to follow. Ideally a business would satisfy all 10 of the steps although there is a recognition that some of the steps may not be critical for a micro- or small business. The Cyber Essentials minimum standard can be seen to cover five of the most basic controls (of the 10 Steps).[11] In our methodology we suggested (see Table 2) that secure back-ups and basic management practices complement Cyber Essentials. This implies that a minimum of 7 steps are recommended (the five of Cyber Essentials plus secure back-ups and management practice). A priori, therefore, we expected optimal to be somewhere between 7 and 10 steps.

In Figure 6 we plot the average number of the 10 steps that businesses implemented (as measured on the CSBS), distinguishing business size and

[11]The NSCS 10 Steps is distinct from Cyber Essentials and so there is not a perfect one-to-one mapping. For the purposes of our analysis, however, the overlap is large enough that we do not take account here of the small nuances.

their classified behavioral type. We observe that micro-businesses classified as optimal were implementing an average of 7.4 steps and small businesses, an average of 8.2 steps. For comparison, medium and large businesses satisfy an average of, respectively, 8.6 and 8.9 steps. It is natural that micro- and small businesses would optimally implement fewer steps than medium and large businesses (because of the smaller businesses' more-limited operations). It is reassuring that our framework permits and captures this (as evidenced by optimal micro-businesses implementing fewer steps than optimal large businesses). The number of steps implemented by businesses classified as optimal provides a benchmark for comparison against which we can evaluate the cyber security controls of other types.

When we look at nonoptimal types in Figure 6 we see, as would be expected, a lower average number of steps implemented compared to optimal. Interestingly, businesses classified as risk accepting are closest to optimal. This is consistent with the notion that businesses classified as risk accepting are only accepting a "small" amount of extra risk. In specific terms they are, on average, performing around one step fewer than optimal. Businesses may argue that this represents a reasonable transfer of risk dependent on their circumstances or risk preferences. Note, however, that the average number of steps implemented by micro-businesses falls bellow our suggested minimum of 7, and so it is questionable whether this could be classified as a reasonable level of risk.

Businesses classified as defer responsibility are, on average, implement around 1.5 to two steps fewer than optimal. With overconfident and procrastinator we see a more pronounced gap relative to optimal; micro- and small businesses that are classified as overconfident are around three steps below

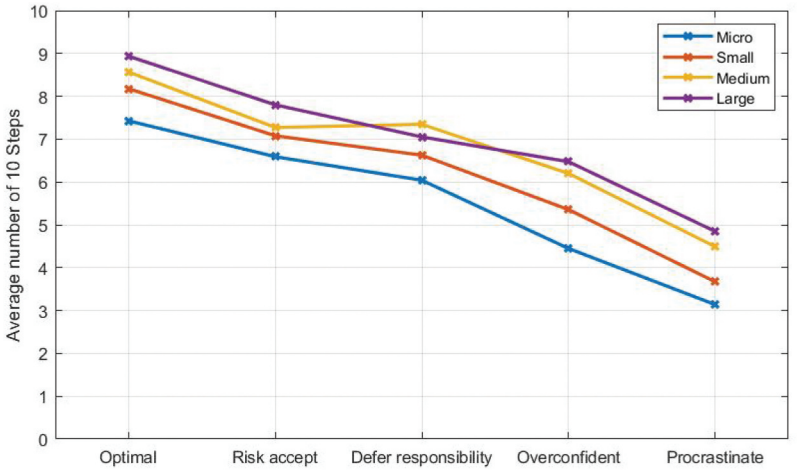

Figure 6. The average number of the 10 Steps to Cyber Security that businesses are implementing by size of business and behavioral type.

optimal; whereas, those classified as procrastinator are implementing over four steps fewer than optimal. We also see that the number of steps implemented drops below five for micro-businesses and, in the case of procrastinator, drops below five even for large businesses. This indicates that businesses classified as overconfident or procrastinator appear to be well below the level of cyber security controls advised by the UK government, exposing them to excess cyber security risks and losses. Recall (see Result 2) that overconfident and procrastinator are the most commonly observed types, especially for micro- and small businesses.

Result 8. Businesses classified as overconfident or procrastinator are implementing only around half as many cyber security controls as those classified as optimal and fall below the minimum level advised by the UK government. Those classified as procrastinator are implementing the fewest controls.

Concluding discussion

Digitalization means that cyber security is an active and growing threat to businesses. This threat is particularly relevant for small business owners/managers who are increasingly reliant on digital technology but lack resources and expertise to implement cyber security controls (Berry & Berry, 2018; Ključnikov et al., 2019; Selznick & LaMacchia, 2017; Tam et al., 2021). Evidence suggests that most small businesses are not implementing basic recommended security controls (e.g, DCMS, 2024; Hoppe et al., 2021; Wilson & McDonald, 2025; Wilson et al., 2022). This puts small businesses at risk of costly and damaging cyber attack. To improve cyber security resilience in small businesses is, therefore, a significant challenge faced by modern society. To address this challenge it is vital to understand why businesses are underinvesting in cyber security and to quantify the different barriers to investment.

In this paper we propose a behavioral framework with which to quantify the reasons for small business underinvestment in cyber security. In doing so we identified five broad behavioral types: (a) risk accepting, knowingly underinvests in cyber security; (b) procrastinator, wants to invest but delays action; (c) overconfident, believes they are investing optimally; (d) defer responsibility, expects others (for example, managed service providers) to invest; and (e) optimal, investing optimally. We argue that these five types capture, in a stylized way, the different approaches businesses are taking to cyber security. We then proposed an empirical approach to analyze data from the UK government's annual Cyber Security Breaches Survey (2018–2024) to estimate the distribution of businesses across behavioral types. We demonstrate that our empirical approach produces robust estimates, not only of the proportion of businesses of each type, but also of uncertainty over type.

One of our main findings is that procrastination and overconfidence appear to be the main reasons for underinvestment in cyber security by micro- and small businesses in the United Kingdom. We find relatively little evidence of risk acceptance or deferring responsibility. Moreover, we find that businesses classified as procrastinator or overconfident are implementing only around half as many of the cyber security controls as businesses of the optimal type, which falls below the minimum number of controls advised by the UK government. We find large sectoral differences in the proportion of businesses classified as procrastinator, with businesses in "food and hospitality" four times as likely to be classified as procrastinator as those in "finance and insurance." We also see an increase in the proportion of businesses classified as procrastinator over time. This may reflect a trend toward increased awareness of the cyber security threat but procrastination in addressing that threat.

Implications

Our work offers valuable insights to policymakers, law enforcement, and business membership organizations (for example, the Federation of Small Businesses) on improving cyber security guidance for small businesses. In particular, this research can help guide more-targeted cyber security interventions. Most current policy initiatives are aimed at improving awareness of the cyber security threat (Van Steen et al., 2020). If, however, procrastination is a main barrier for many businesses to implement cyber best practice then policy initiatives focused on raising awareness will not be fully effective. Specifically, if businesses are procrastinating then awareness is not the problem; instead we need mechanisms that make businesses take action.

To illustrate this point and the value of our framework for policymakers, we provide in Figure 7 the flow of micro- and small businesses through our algorithmic framework (based on responses in the CSBS).[12] The top number is the proportion of micro-businesses along each branch and the bottom number is the corresponding proportion of small businesses. At the first decision node you can see that an estimated 52.3 percent of micro-businesses and 61.3 percent of small businesses are aware of cyber threats and 47.7 percent and 38.8 percent, respectively, are not. This finding is similar to the analogous estimate of Renaud and Weir (2016), who surveyed UK small businesses. Thus, at least half of micro- and small businesses are aware of the generic cyber threat.

If we follow through the flowchart, those businesses that are aware of the cyber threat, we see there are an estimated 36.5 percent of micro-businesses and 34.1 percent of small businesses not classified as optimal. This includes 24.8 percent and 21.1 percent of businesses, respectively, that are not aware of best

[12]This is based on the mean method for classifying types.

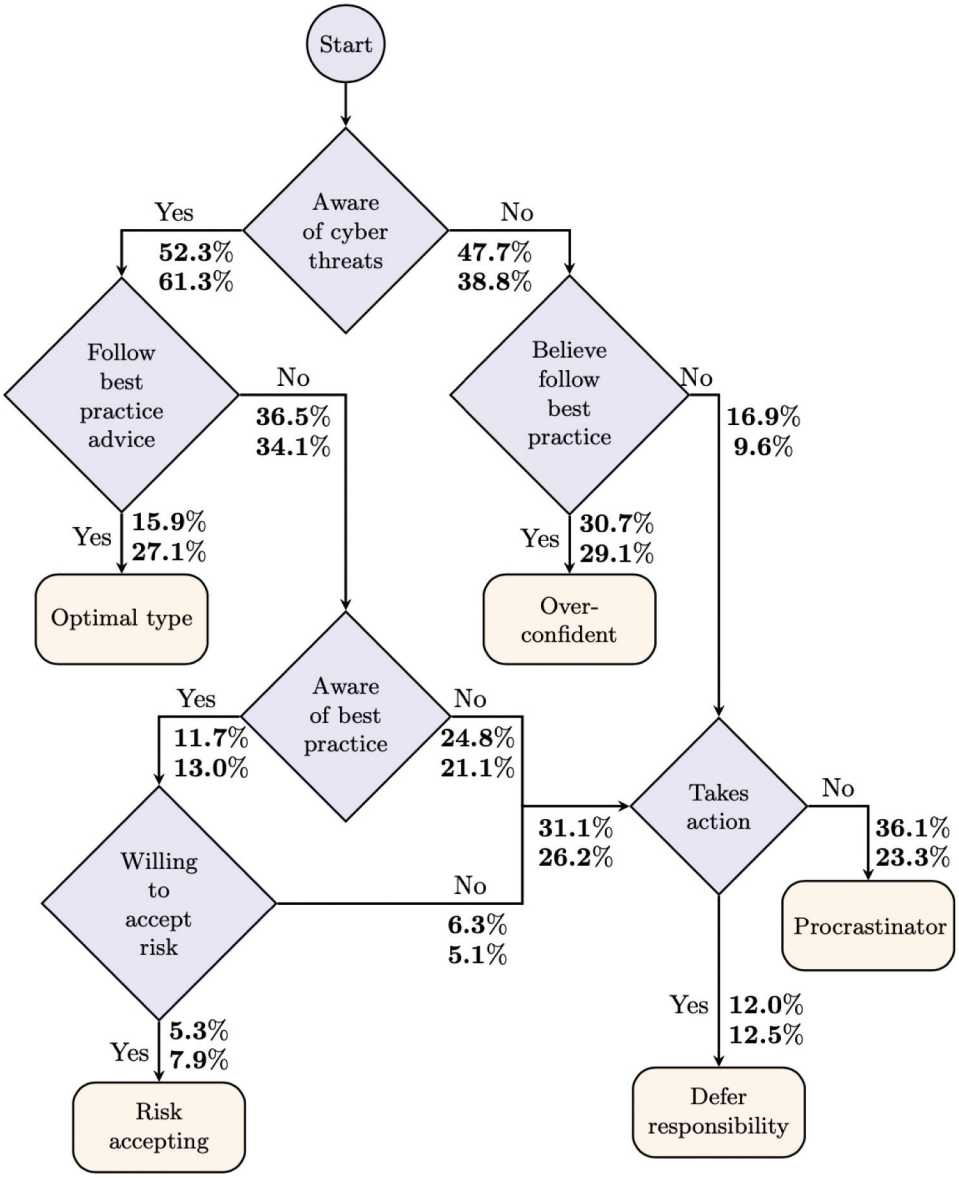

Figure 7. The proportion of micro- (top number as a percentage) and small businesses (bottom number) along each route in the framework for discerning the behavioral type of a business.

practice. These businesses are procrastinating or deferring responsibility at the level of finding out how to protect their business. This could, for instance, reflect overreliance in outsourcing cyber security (Wilson & McDonald, 2025). There are a further 6.3 percent of micro-businesses and 5.1 percent of small businesses that are aware of best practice and not willing to accept risk but still not implementing best practice. This could, for instance, reflect a lack of incentives to act, given competing demands on time and resources (Arroyabe et al., 2024).

For those businesses that are aware of the cyber threat but not implementing best practice there need to be incentives to action to address market failures (Arroyabe et al., 2024) This could come, for instance, in the form of financial incentives and/or support to implement cyber security controls (such as Cyber Essentials in the UK). Or, it could come in the form of regulations that require controls to be implemented. (This approach is already adopted to some extent in the UK with Cyber Essentials becoming required to secure government contracts.) Financial support, or regulation, can work because it makes cyber security more of a priority. In more-regulated sectors, such as finance and insurance, where cyber security is a higher priority, we found lower levels of the procrastinator type.

Our results show that procrastination is not the only barrier to action. Indeed, Figure 7 reiterates that an estimated 30.7 percent of micro-businesses and 29.1 percent of small businesses are underinvesting in cyber security because of overconfidence. This highlights the need for a diverse policy approach that is not based on "one size fits all." For some businesses awareness raising is still vital. Note, however, that policy needs to be "joined up" to reflect the journey that a business may transition through. We remind the reader that the majority of micro-business owners/managers that are aware of cyber threats are still not behaving optimally. If, therefore, awareness campaigns "convert" a business from overconfident to procrastinator or defer responsibility, future policy needs to effectively combine awareness campaigns with additional mechanisms that incentivize businesses to take action. This would enable the full transition from overconfident to optimal.

In summary, our results demonstrate the need for cyber security policy to recognize (a) the heterogeneity of micro- and small businesses in their cyber security behavior, (b) the need for diverse policy levers, including but not limited to awareness campaigns, to incentivize actions, (c) the need for joined-up policy that can "transition" a business toward optimal behavior, recognizing that this will likely be a process rather than a one-off transition, and (d) the need for targeted policy that reflects, for instance, wide differences across sectors. A key advantage of our framework is that it allows quantification of behavioral types that can be traced over time. For instance, we observed a drop in overconfidence and an increase in procrastination in recent years. This can be used to evaluate the effectiveness of policy initiatives.

Our framework can also be used to evaluate changes in the cyber security threat landscape. Most notably, advances in artificial intelligence (AI) are rapidly changing the cyber security landscape for both businesses and cyber criminals (Radanliev, 2024b). For instance, AI is facilitating more-sophisticated social engineering attacks that use, for example, deepfakes (Treleaven et al., 2023). Use of AI software is also exposing businesses to new sources of data loss. On the positive side, AI

can be used to provide more-enhanced cyber security solutions that are affordable to micro- and small businesses (Biswas et al., 2024; Nadella et al., 2024). Our framework provides a way to map the consequences of innovations such as AI. For example, future research could investigate whether wider adoption of AI leads to more optimal behavior or, say, more deferring of responsibility. It could also investigate whether adoption of AI by cyber criminals leads to increases in overconfidence because businesses are not updating their understanding of the threat landscape. Other applied issues that could be evaluated in this way include use of blockchain technology and cloud computing alongside AI (Radanliev, 2024a).

Limitations

There are many limitations to our approach that future work could explore. Our empirical approach is limited by the questions asked on the Cyber Security Breaches Survey. We are particularly constrained in our ability to measure willingness to take risk and delay action. We demonstrated, however, that our results are robust to diverse ways of measuring behavioral type. A comparison of findings from the Cyber Security Breaches Survey with findings from other data sources would be useful to further validate our approach. Our approach can also be applied to consider a range of further questions, such as how behavioral type correlates with prevalence of cyber attack and willingness to report cyber attack.

Another limitation of our work is that we abstract away from studying resource constraints. Evidence suggests that financial and skill constraints are a key reason why businesses underinvest in cyber security (e.g., Arroyabe et al., 2024; Shojaifar & Järvinen, 2021). In our framework we focus on basic cyber security controls (such as those in Cyber Essentials) that all businesses should be taking given the favorable cost–benefit trade-off. Even so, it would be valuable to explore how resource constraints interact with behavioral types. This would allow a closer comparison of our classification (which focuses on behavioral types) and that of Shojaifar and Järvinen (2021) (which is slightly more focused on resource and skill characteristics). Unfortunately, the CSBS does not contain data with which one could evaluate the resource constraints of businesses. An alternative data source would, therefore, be needed to explore this issue.

Authors' contributions

Both authors contributed equally to this work.

Availability of data and materials

The data used for analysis are available on the UK Data Archive for registered users. The code used in the research will be made available on a university repository on publication of the paper.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Ethics approval

No ethical approval was necessary. Analysis of secondary data were deposited in the UK Data Archive.

Funding

The authors reported that there is no funding associated with the work featured in this article.

ORCID

Anna Cartwright http://orcid.org/0000-0003-0194-9368
Edward Cartwright http://orcid.org/0000-0003-1965-842X

References

Adriko, R., & Nurse, J. R. (2024a). *Cybersecurity, cyber insurance and small-to-medium-sized enterprises: A systematic review*. Information & Computer Security.

Adriko, R., & Nurse, J. R. (2024b). Does cyber insurance promote cyber security best practice? An analysis based on insurance application forms. *Digital Threats: Research and Practice*, *5* (3), 1–39. https://doi.org/10.1145/3676283

Akpan, I. J., Udoh, E. A. P., & Adebisi, B. (2022). Small business awareness and adoption of state-of-the-art technologies in emerging and developing markets, and lessons from the COVID-19 pandemic. *Journal of Small Business & Entrepreneurship*, *34*(2), 123–140. https://doi.org/10.1080/08276331.2020.1820185

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. 2020 International conference on cyber situational awareness, data analytics and assessment (CyberSA), Dublin, Ireland (pp. 1–5).

Ament, C., & Jaeger, L. (2017). Unconscious on their own ignorance: Overconfidence in information security. Pacific Asia Conference on Information Systems (PACIS), Langkawi, Malaysia.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganán, C., Grasso, T., & Vasek, M. (2019). Measuring the changing cost of cybercrime. The 18th Annual Workshop on the Economics of Information Security (WEIS 2019), Boston, MA.

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, *1*(2), 219–238. https://doi.org/10.3390/jcp1020012

Arce, D., Woods, D. W., & Böhme, R. (2024). Economics of incident response panels in cyber insurance. *Computers & Security*, *140*, 103742. https://doi.org/10.1016/j.cose.2024.103742

Arend, I., Shabtai, A., Idan, T., Keinan, R., & Bereby-Meyer, Y. (2020). Passive-and not active-risk tendencies predict cyber security behavior. *Computers & Security*, *97*, 101964. https://doi.org/10.1016/j.cose.2020.101964

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580. https://doi.org/10.1016/j.dss.2021.113580

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*, *78*, 102670. https://doi.org/10.1016/j.techsoc.2024.102670

Attaran, M., & Woods, J. (2019). Cloud computing technology: Improving small business performance using the internet. *Journal of Small Business & Entrepreneurship*, *31*(6), 495–519. https://doi.org/10.1080/08276331.2018.1466850

Bada, M., & Nurse, J. R. (2019). *Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs)*. Information & Computer Security.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *ArXiv preprint arXiv: 1901*, 02672.

Beheshtifar, M., Hoseinifar, H., & Moghadam, M. (2011). Effect procrastination on work-related stress. *European Journal of Economics, Finance and Administrative Sciences*, *38*(38), 59–64.

Benaroch, M. (2020). Cybersecurity risk in IT outsourcing-challenges and emerging realities. *Information Systems Outsourcing: The Era of Digital Transformation*, 313–334. https://doi.org/10.1007/978-3-030-45819-5_13

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 1–10. https://doi.org/10.1504/IJBCRM.2018.090580

Biswas, B., Mukhopadhyay, A., Kumar, A., & Delen, D. (2024). A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks. *Decision Support Systems*, *177*, 114102. https://doi.org/10.1016/j.dss.2023.114102

Cartwright, A., Cartwright, E., & Edun, E. S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. *Computers & Security*, *131*, 103288. https://doi.org/10.1016/j.cose.2023.103288

Cartwright, A., Cartwright, E., MacColl, J., Mott, G., Turner, S., Sullivan, J., & Nurse, J. R. (2023). How cyber insurance influences the ransomware payment decision: Theory and evidence. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *48*(2), 300–331. https://doi.org/10.1057/s41288-023-00288-8

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2014). Outsourcing information security: Contracting issues and security implications. *Management Science*, *60*(3), 638–657. https://doi.org/10.1287/mnsc.2013.1763

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2017). Sourcing information security operations: The role of risk interdependency and competitive externality in outsourcing decisions. *Production & Operations Management*, *26*(5), 860–879. https://doi.org/10.1111/poms.12681

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access*, *10*, 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899

Chidukwani, A., Zander, S., & Koutsakis, P. (2024). Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications. *Computers & Security*, *145*, 104026. https://doi.org/10.1016/j.cose.2024.104026

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security*, *87*, 101568. https://doi.org/10.1016/j.cose.2019.101568

DCMS. (2024). Cyber security breaches survey 2024. Department for Digital Culture Media and Sport. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

Dinkova, M., El-Dardiry, R., & Overvest, B. (2023). Should firms invest more in cybersecurity? *Small Business Economics*, *63*(1), 21–50. https://doi.org/10.1007/s11187-023-00803-0

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (SeBIS). Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, South Korea (pp. 2873–2882).

Ferrari, J. R., Diaz-Morales, J. F., O'Callaghan, J., Diaz, K., & Argumedo, D. (2007). Frequent behavioral delay tendencies by adults: International prevalence rates of chronic procrastination. *Journal of Cross-Cultural Psychology*, *38*(4), 458–464. https://doi.org/10.1177/0022022107302314

Frank, M. (2020). Using calibration to help overcome information security overconfidence. Proceedings of the 42nd International Conference on Information Systems (ICIS), India.

Frederick, S., Loewenstein, G., & O'donoghue, T. (2002). Time discounting and time preference: A critical review. *Journal of Economic Literature*, *40*(2), 351–401. https://doi.org/10.1257/jel.40.2.351

Frik, A., Egelman, S., Harbach, M., Malkin, N., & Peer, E. (2018). Better late(r) than never: Increasing cyber-security compliance by reducing present bias. Symposium on usable privacy and security, Baltimore, MD (pp. 12–14).

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274

Gordon, L. A., & Loeb, M. P. (2006). Economic aspects of information security: An emerging field of research. *Information Systems Frontiers*, *8*(5), 335–337. https://doi.org/10.1007/s10796-006-9010-7

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost-benefit analysis into the NIST cybersecurity framework via the Gordon-Loeb model. *Journal of Cybersecurity*, *6*(1), tyaa005. https://doi.org/10.1093/cybsec/tyaa005

Harris, N. N., & Sutton, R. I. (1983). Task procrastination in organizations: A framework for research. *Human Relations*, *36*(11), 987–995. https://doi.org/10.1177/001872678303601102

HM Government. (2022). National cyber strategy 2022: Pioneering a cyber future with the whole of the UK. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachmentdata/file/1053023/national-cyber-strategy-amend.pdf

Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: Insights from industry surveys. *Journal of Risk Finance*, *22*(3/4), 240–260. https://doi.org/10.1108/JRF-02-2020-0024

Huang, C. D., & Behara, R. S. (2013). Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. *International Journal of Production Economics*, *141*(1), 255–268. https://doi.org/10.1016/j.ijpe.2012.06.022

Huang, C. D., Hu, Q., & Behara, R. S. (2006, June). Economics of information security investment in the case of simultaneous attacks. *The 5th Annual Workshop on the Economics of Information Security (WEIS)*.

Johns, E., & Ell, M. (2020). Cyber security breaches survey 2020. *London: Department for Digital, Culture, Media & Sport*, *4*(1), 1–4.

Kemp, S. (2023). Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach. *Computers & Security*, *127*, 103089. https://doi.org/10.1016/j.cose.2022.103089

Khan, N., Furnell, S., Bada, M., Nurse, J. R., & Rand, M. (2024). Assessing cyber security support for small and medium-sized enterprises. International symposium on human aspects of information security and assurance, Skövde, Sweden (pp. 148–162).

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: Factors of success. *Entrepreneurship & Sustainability Issues*, *6*(4), 2081.2081–2094. https://doi.org/10.9770/jesi.2019.6.4(37)

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*, 58–74. https://doi.org/10.1016/j.cose.2014.05.006

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177–187. https://doi.org/10.1057/ejis.2009.11

Meikle, N. L., Tenney, E. R., & Moore, D. A. (2016). Overconfidence at work: Does overconfidence survive the checks and balances of organizational life? *Research in Organizational Behavior*, *36*, 121–134. https://doi.org/10.1016/j.riob.2016.11.005

Meurs, T., Cartwright, E., Cartwright, A., Junger, M., Hoheisel, R., Tews, E., & Abhishta, A. (2023). Ransomware economics: A two-step approach to model ransom paid. 2023 APWG Symposium on Electronic Crime Research (eCrime), Barcelona, Spain (pp. 1–13).

Moore, D. A., & Healy, P. J. (2008). The trouble with overconfidence. *Psychological Review*, *115*(2), 502. https://doi.org/10.1037/0033-295X.115.2.502

Mott, G., Turner, S., Nurse, J. R., MacColl, J., Sullivan, J., Cartwright, A., & Cartwright, E. (2023). Between a rock and a hard (ening) place: Cyber insurance in the ransomware era. *Computers & Security*, *128*, 103162. https://doi.org/10.1016/j.cose.2023.103162

Mott, G., Turner, S., Nurse, J. R., Pattnaik, N., MacColl, J., Huesch, P., & Sullivan, J. (2024). 'There was a bit of PTSD every time I walked through the office door': Ransomware harms and the factors that influence the victim organization's experience. *Journal of Cybersecurity*, *10*(1), tyae013. https://doi.org/10.1093/cybsec/tyae013

Moustafa, A. A. (2022). *Cybersecurity and cognitive science*. Academic Press.

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, *12*, 561011. https://doi.org/10.3389/fpsyg.2021.561011

Nadella, G. S., Gonaygunta, H., Kumar, D., & Pawar, P. P. (2024). Exploring the impact of AI-driven solutions on cybersecurity adoption in small and medium enterprises. *World Journal of Advanced Research & Reviews*, *22*(1), 1199–1197. https://doi.org/10.30574/wjarr.2024.22.1.1185

Nagurney, A., & Shukla, S. (2017). Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, *260*(2), 588–600. https://doi.org/10.1016/j.ejor.2016.12.034

Osborn, E., & Simpson, A. (2018). Risk and the small-scale cyber security decision making dialogue - a UK case study. *The Computer Journal*, *61*(4), 472–495. https://doi.org/10.1093/comjnl/bxx093

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

Papadopoulos, T., Baltas, K. N., & Balta, M. E. (2020). The use of digital technologies by small and medium enterprises during COVID-19: Implications for theory and practice. *International Journal of Information Management*, *55*, 102192. https://doi.org/10.1016/j.ijinfomgt.2020.102192

Ponsard, C., Grandclaudon, J., & Bal, S. (2019). Survey and lessons learned on raising SME awareness about cybersecurity. *ICISSP*, 558–563. https://doi.org/10.5220/0007574305580563

Radanliev, P. (2024a). Digital security by design. *Security Journal*, *37*(4), 1640–1679. https://doi.org/10.1057/s41284-024-00435-3

Radanliev, P. (2024b). Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing. *Frontiers in Blockchain*, *7*, 1359130. https://doi.org/10.3389/fbloc.2024.1359130

Renaud, K., & Weir, G. R. (2016). Cybersecurity and the unbearability of uncertainty. 2016 cybersecurity and cyberforensics conference (CCC), Amman, Jordan (pp. 137–143).

Ritz, W., Wolf, M., & McQuitty, S. (2019). Digital marketing adoption and success for small businesses: The application of the do-it-yourself and technology acceptance models. *Journal of Research in Interactive Marketing*, *13*(2), 179–203. https://doi.org/10.1108/JRIM-04-2018-0062

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, *5*(1), tyz002. https://doi.org/10.1093/cybsec/tyz002

Rupeika-Apoga, R., Bule, L., & Petrovska, K. (2022). Digital transformation of small and medium enterprises: Aspects of public support. *Journal of Risk and Financial Management*, *15*(2), 45. https://doi.org/10.3390/jrfm15020045

Selznick, L. F., & LaMacchia, C. (2017). Cybersecurity liability: How technically savvy can we expect small business owners to be. *Journal Business & Technology Law*, *13*, 217. https://heinonline.org/HOL/P?h=hein.journals/jobtela13&i=233

Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for approaching cybersecurity competence and awareness. Proceedings of the 16th international conference on availability, reliability and security, Vienna, Austria (pp. 1–7).

Small Business Standards. (2020). Eu cybersecurity act and the role of standards for SMEs. *Small business standards position paper*.

Soomro, B. A., & Shah, N. (2022). Is procrastination a "friend or foe"? Building the relationship between fear of the failure and entrepreneurs' well-being. *Journal of Entrepreneurship in Emerging Economies*, *14*(6), 1054–1071. https://doi.org/10.1108/JEEE-12-2019-0191

Steel, P. (2007). The nature of procrastination: A meta-analytic and theoretical review of quintessential self-regulatory failure. *Psychological Bulletin*, *133*(1), 65. https://doi.org/10.1037/0033-2909.133.1.65

Stewart, W. H., Jr., & Roth, P. L. (2001). Risk propensity differences between entrepreneurs and managers: A meta-analytic review. *Journal of Applied Psychology*, *86*(1), 145. https://doi.org/10.1037/0021-9010.86.1.145

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. *Computers & Security*, *109*, 102385. https://doi.org/10.1016/j.cose.2021.102385

Tosh, D. K., Molloy, M., Sengupta, S., Kamhoua, C. A., & Kwiat, K. A. (2015). Cyber-investment and cyber-information exchange decision modeling. Proceedings of the 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, New York (pp. 1219–1224).

Treleaven, P., Barnett, J., Brown, D., Bud, A., Fenoglio, E., Kerrigan, C., & Schoernig, M. (2023). The future of cybercrime: AI and emerging technologies are creating a cybercrime tsunami. *Available at SSRN 4507244*. https://doi.org/10.2139/ssrn.4507244

Tsiodra, M., Panda, S., Chronopoulos, M., & Panaousis, E. (2023). Cyber risk assessment and optimization: A small business case study. *IEEE Access*, *11*, 44467–44481. https://doi.org/10.1109/ACCESS.2023.3272670

UK Home Office. (2018). A call to action: The cyber aware perception gap. https://www.gov.uk/government/publications/cyber-aware-perception-gap-report

Van Hooft, E. A., & Van Mierlo, H. (2018). When teams fail to self-regulate: Predictors and outcomes of team procrastination among debating teams. *Frontiers in Psychology*, *9*, 464. https://doi.org/10.3389/fpsyg.2018.00464

Van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity*, *6*(1), tyaa019. https://doi.org/10.1093/cybsec/tyaa019

Vereshchagina, G., & Hopenhayn, H. A. (2009). Risk taking by entrepreneurs. *The American Economic Review*, *99*(5), 1808–1830. https://doi.org/10.1257/aer.99.5.1808

Vetter, J., Benlian, A., & Hess, T. (2011). Overconfidence in IT investment decisions: Why knowledge can be a boon and bane at the same time. Proceedings of the 32nd International Conference on Information Systems (ICIS 2011), Shanghai, China.

Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age*. John Wiley & Sons.

Wilson, M., & McDonald, S. (2025). One size does not fit all: Exploring the cybersecurity perspectives and engagement preferences of UK-based small businesses. *Information Security Journal: A Global Perspective*, *34*(1), 15–49. https://doi.org/10.1080/19393555.2024.2357310

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2022). It won't happen to me: Surveying SME attitudes to cyber-security. *Journal of Computer Information Systems*, *63*(2), 397–409. https://doi.org/10.1080/08874417.2022.2067791

Wu, Y., Tayi, G. K., Feng, G., & Fung, R. Y. (2021). Managing information security outsourcing in a dynamic cooperation environment. *Journal of the Association for Information Systems*, *22*(3), 827–850. https://doi.org/10.17705/1jais.00681