




Evaluating the adoption of cybersecurity and its influence on organizational performance

Tahereh Hasani¹  · Norman O'Reilly² · Ali Dehghantanha³ · Davar Rezania¹ · Nadège Levallet²

Received: 14 January 2022 / Accepted: 21 April 2023 / Published online: 27 April 2023
© The Author(s), under exclusive licence to Springer Nature Switzerland AG 2023

Abstract

Cyberattacks negatively impact the performance of enterprises all around the globe. While organizations invest more in cybersecurity to avoid cyberattacks, studies on the factors affecting their overall cybersecurity adoption and awareness are sparse. In this paper, by integrating the diffusion of innovation theory (DOI), technology acceptance model (TAM), and technology-organization-environment (TOE) with the balanced scorecard approach, we propose a comprehensive set of factors that influence cybersecurity adoption and assess the effects of these factors on organizational performance. Data are collected through a survey of IT experts in small and medium-sized enterprises (SMEs) in the United Kingdom, with 147 valid responses. Structural equation modeling based on a statistical package for the social sciences (SPSS) was used to assess the model. The findings identify and confirm the importance of eight factors affecting SMEs' cybersecurity adoption. Moreover, cybersecurity technology adoption is found to positively impacts organizational performance. The proposed framework depicts variables influencing cybersecurity technology adoption and assesses their importance. The outcomes of this study provide a basis for future research and can be adopted by IT and cybersecurity managers to identify the most appropriate cybersecurity technologies that positively impact their company's performance.

Keywords Cybersecurity · Technology-organization-environment · Balanced scorecard · SMEs

✉ Tahereh Hasani
htaahereh@uoguelph.ca

¹ Gordon Lang School of Business and Economics, University of Guelph, Guelph, ON, Canada

² Maine Business School, University of Maine, Orono, ME, USA

³ School of Computer Science, University of Guelph, Guelph, ON, Canada

Introduction

Organizations have benefited from noteworthy progress in digital technologies, gadgets, and interconnectivity in several ways, including enhanced system accessibility, expanded communication speed, improved productivity and decreased operational costs (Park et al. 2017). In turn, organizations can take advantage of new business possibilities and produce higher-quality products by adopting new digital or cyberspace technologies (Reuver et al. 2018). While cyberspace makes information, products, and services more accessible to a broad spectrum of participants, there are growing concerns about protecting the fast-growing cyberspace environment from cyberattacks (Hopkins and Dehghantanha 2016). The increasing risk of cyberattacks negatively impacts companies' digital transformation (Rindasu 2017). Every day, more than 4000 ransomware attacks are reported to the FBI in the United States (FBI 2017), and more than 330,000 malware programs are produced (KasperskyLab 2018). As cyberattacks continue to develop in scale and complexity, these figures are anticipated to worsen (FBI 2017).

The costs and consequences of such attacks on businesses and governments are considerable. Cyberattacks cost organizations over \$5 billion in 2017 and are anticipated to cost over \$6 trillion in 2021 (Morgan 2021). These costs include income and reputation losses, along with the leakage of sensitive information (Nicholson 2019; Pala and Zhuang 2019). According to Gyde (2017), in 2017, 49% of worldwide firms suffered commercial losses due to cyberattacks. In reality, the actual costs of cyberattacks may be higher than reported since numerous organizations may choose not to record cyberattack occurrences in order to prevent reputational harm or humiliation (Pearson 2014).

Cyberattacks are becoming more common, emphasizing the significance of proper cybersecurity. Cybersecurity protects an organization's IT-related assets, such as data, systems, and networks, from digital attacks that might access, delete, or manipulate sensitive data or disrupt company operations (Kim and Solomon 2016). The convergence of people, procedures, and technology to defend businesses, persons, or networks against digital attacks is known as cybersecurity (Li and Liu 2021). Cybersecurity refers to the technological and non-technical measures taken to protect digital assets from unauthorized access or use (Li and Wang 2018). This includes the safety and health of the Internet, including computers, lines of communication, programs, and data that create and support the Internet (Cavelty 2014). Cybersecurity may improve an organization's reputation, core competency, and outstanding organizational performance. Marketers have acknowledged the need to consider issues with cybersecurity risk to carry out marketing activities effectively (Joshi and Gimenez 2014). Businesses relying on digital services regularly raise cybersecurity as a significant challenge for growth and productivity (James 2018). These concerns have increased considerably during the COVID-19 pandemic and are expected to continue post-pandemic (Donthu and Gustafsson 2020). Cybersecurity investments are growing at the pace of 6% per annum globally and are expected to exceed \$1 trillion by 2021 (CISOMAG 2020). However, before adopting any cybersecurity technologies, a

company must be aware of the implications of cyberattacks and commit to avoiding, identifying, and combating them (Hathaway 2013).

Despite the significance of cybersecurity adoption, current assessments of companies' cybersecurity technologies adoption are insufficient and inadequately comprehensive, according to a review of the literature. Previous research on the role of cybersecurity in decreasing threats and attacks has focused on information security management in organizations in terms of investment decision-making (Kong et al. 2012) and administrative information system security innovations (Hsu et al. 2012), but not cybersecurity technologies adoption and its affect on organizational performance. Smith et al. (2010) and Tsou and Hsu (2015) propose that firms may increase their financial returns and reputation by assuring cybersecurity. Furthermore, adherence to cybersecurity policies, standards, and best practices, such as the implementation of new security controls, backup and system recovery solutions, and incident response planning, may influence the firm performance (Daud et al. 2018).

There is also limited empirical work to study the effects of cybersecurity adoption on organizational performance, despite the significance of cybersecurity adoption in enhancing organizational performance. Quigley et al. (2015) indicated that the organization's internal and external environmental elements need to be taken into account when studying the impact of the adoption of cybersecurity technologies. This is an important gap in the literature that is addressed by this research as we seek to understand the broad range of determining factors and assess their influence on the adoption of cybersecurity technologies. In seeking to address this gap, we use three variables—technology, organization, and environment—to identify the factors that affect on cybersecurity adoption (Su 2021). As a group, these factors can provide an organizational-level framework that is comprehensive, robust, and flexible and takes into account both internal and external viewpoints of the organization (Cheng 2021).

As a result, organizations need to understand the factors that impact the successful adoption of cybersecurity technologies. Identifying these factors may reduce the cost of adoption and allow companies to make the most out of their cybersecurity investments. This is especially important for SMEs as they (typically) operate under financial constraints, and a successful cyberattack could lead to the closure of an SME (Lloyd 2020). The maturity of IT infrastructure (Angst et al. 2017), top management support (Hsu et al. 2012), organizational culture (Kraemer et al. 2009), supplier/partner relationships (Smith et al. 2007), collaboration with competitors (Gao and Zhong 2016), industry standards (Njenga and Jordaan 2016), government support (Hwang and Choi 2017), and government regulations (Quigley et al. 2015) have all been studied as factors that improve the cybersecurity posture of companies. Previous researchers have identified factors that impact the usability of cybersecurity technologies (Furnell and Clarke 2012) and the factors that influence the ease of use of cybersecurity products (Church 2008). Despite the common belief that adopting cybersecurity technologies can provide a significant growth advantage for SMEs (Li and Liu 2021), to the best of our knowledge, there is no study on factors impacting the adoption of cybersecurity technologies in organizations. Various theories have been utilized to explain the inclusion of chosen components in prior publications, such as institutional theory, macro-ergonomic theory, and deterrence theory, which include internal organizational aspects

but ignore the external environment (Angst et al. 2017; Hwang and Choi 2017; Wall et al. 2016). A complete collection of elements impacting cybersecurity technologies adoption and a holistic knowledge of their overall impact that spans multiple theories is yet to be realized. Identifying such a collection of variables would also respond to Li et al. (2019) request to identify internal and exterior factors that impact SMEs' adoption of cybersecurity technologies.

To address the knowledge gaps discussed above, different internal and external elements influencing businesses' cybersecurity technologies adoption and their influence on performance ought to be investigated by concurrently employing a more comprehensive framework than those accessible in the present literature. As a result, in this research, we examine the factors that impact cybersecurity technology adoption and provide a comprehensive model to fill in research gaps. Specifically, the following research questions are addressed in this study:

- What are the key factors affecting the cybersecurity technology adoption of organizations?
- How does the cybersecurity technology adoption affect organizational performance from financial, customer, internal process, and earning and growth perspectives?

To address the research questions, we utilize the Technology-Organization-Environment (TOE) framework (DePietro et al. 1990) to synthesize elements influencing companies' cybersecurity technology adoption from the literature. We utilize the TOE framework since it is a comprehensive, adaptable, and robust framework employed to model the adoption of different technologies in different organizations. The TOE framework has significant empirical backing in earlier information systems research (Pan and Jang 2008), and it encompasses practically all components of an organization both internally (i.e., technological characteristics) and externally (i.e., environment pressures). In addition, the TOE framework allows adding other variables to the model and the integration of various hypotheses (Kurnia et al. 2015). To address the second research question, we look at the mediating role of cybersecurity technology adoption on organizational performance. In order to respond to the research questions, we undertake a large-scale survey. The majority of our assumptions are supported, namely that compatibility, perceived usefulness, perceived ease of use, organizational flexibility, top management support, collaborative board oversight, competitive pressure and vendor support affect cybersecurity adoption. Additionally, we find evidence to support the hypotheses that cybersecurity adoption mediates the relationship between technological, organizational, and environmental characteristics and organizational performance as well as the relation between cybersecurity adoption and organizational performance.

Literature review

We performed a systematic literature review to identify elements impacting cybersecurity technology adoption. To begin with, researchers conducted searches in Google Scholar and databases such as EBSCO, ProQuest, and Science to identify relevant papers. Cybersecurity, cyber incidents, cyberattacks, information security

management, security performance, adoption, readiness, resilience, TOE framework, organizational and financial performance were all used as search terms.

The topic of cybersecurity has gained prominence due to a widely publicized number of cybercrimes, such as hacking attacks and data breaches. Zimmerman and Renaud (2019) investigated the continuing incidences of attacks used by cybercriminals and theorized that a well-intentioned individual is as essential to cybersecurity as other defense mechanisms, such as firewalls, antivirus software, or analytics. They focused on enhancing the factors that contribute to favorable outcomes and resilience regarding cybersecurity and not relying on technical means to do so. Liu et al. (2020) explained that centralized management leads to a better cybersecurity posture in an organization. Benz and Chatterjee (2020) believed that SMEs are among the most immature and critically vulnerable types of companies. Simola (2019) explained that further investment in cybersecurity technologies is required to mitigate the ever-growing cyber risks for SMEs due to growing cybercrime. He et al. (2017) had a similar outlook to Simola (2019), developed three models for sharing cybersecurity information, and recommended collaboration on a global scale to further reduce the frequencies by which SMEs fall victim to cybercriminals.

To support business operations inside a company, IT infrastructure accessibility and utilization are crucial. Organizations need to take into account IT infrastructure, capacity, and investment when determining IT availability and usage (Hasan et al. 2021). Three studies on the effect of IT infrastructure on information security (Hsu et al. 2012; Kong et al. 2012; Angst et al. 2017) note that having adequate IT resources will enhance information system security and decrease the frequency of security breaches and incidents. Organizational variables, which relate to organizational characteristics, also impact organizational decision-making when it comes to implementing digital innovation. For example, Hsu et al. (2012) and Kraemer et al. (2009) noted that organizational characteristics such as organizational culture, management support, and skills might affect how quickly firms adopt new technologies or digital innovations. Wallace et al. 2020 provided an updated expanded TOE framework that is notably relevant to choices about the adoption of cybersecurity. Under the traditional technology, organization, and environment dimensions, this developed framework contains additional dimensions, practice standards, cyber catalysts, and new variables. Moreover, Hasan et al. (2021) adopted the TOE framework to look at a broad range of variables affecting organizations' readiness for cybersecurity and how these variables affect the organization's financial and non-financial performance.

Theories on the adoption of technology

Adopting a technology or innovation may be clarified using distinctive models that consider the demographic and psychological features of designated adopter groups, whether people or organizations (Oorschot et al. 2018). Many conceptual models and theoretical frameworks have been developed to help understand the relationship between the factors that favor technology adoption (Gangwar et al. 2014; Gounaris and Koritos 2008). Several theories, including innovation theory (Rosenberg 1983), the technology acceptance model (TAM) (Davis 1989; Davis

et al. 1989), the theory of planned behavior (TPB) (Ajzen 1985, 1991), the diffusion of innovation theory (DOI) (Rogers 2003), the unified theory of acceptance and use of technology (UTAUT) (Venkatesh et al. 2003), and the balanced scorecard (Kaplan and Norton 1992), have been utilized to explain the process of technology adoption.

Because TPB, TAM, and UTAUT theories highlight aspects such as individual attitudes and perceptions of consumers, they are frequently employed to explain the adoption of technologies. However, because TOE examines factors related to technology, the organization, and the environment, it is more widely used for analyzing the process of technology adoption (Cao et al. 2018; Gutierrez et al. 2015; Molinillo and Japutra 2017). Several technology adoption studies have utilized and adapted the TOE model, which was proposed by DePietro et al. (1990) since it gives a useful analytical framework for studying the assimilation of diverse sorts of innovation at the organizational level (Oliveira and Martins 2011); including technological, organizational, and environmental factors (Sila 2013).

Technological readiness refers to the characteristics of the technology being evaluated for adoption. On the other hand, organizational readiness focuses on organizational features and resources such as hierarchy, size, structure, business type, and competencies. Environmental readiness, the third component, reflects the environment's exterior qualities, such as government rules, consumers, rivals, and other stakeholders (Awa et al. 2017). In summary, the TOE framework is appropriate for analyzing information technology adoption and may be utilized to research cybersecurity technology adoption across various industries.

The diffusion of innovation (DOI) theory is among IT adoption experts' most utilized study paradigms (Sallehudin et al. 2015; Cegielski et al. 2013). A technique, idea, or object discovered as unique by a group of people or individuals has been classified as an innovation (Rogers 2003). While the innovation definition appears straightforward, the common innovation diffusion paradigm is broad, encompassing theories that address both the genuine innovation and the adopter. Relative advantage, compatibility, complexity, observability, and trialability are some of the aspects that a potential adopter of cybersecurity technology looks for (Rogers 2003). Hence, this study is used as the basis for looking into an organization's desire to adopt cybersecurity technologies. Even though numerous innovative components that promote adoption have been found, previous research has suggested that each setting or situation requires a unique collection of components (Rogers 2003; Hazen and Byrd 2011). As a result, considering the nature of cybersecurity technology, several individual factors such as relative advantage, compatibility, and complexity must be considered. The TAM model (Davis et al. 1989) has been extensively recognized for explaining information technology adoption and usage. This model accounts for a large portion of the variation in users' behavioral intentions towards adopting and using information technology in a range of contexts. TAM forecasts a user's acceptance of technology, its application at work, and the factors influencing user acceptance of the technology (Au and Zafar 2008). TAM aims to explain the link between technological acceptance and adoption and, as a result, behavioral intention to use it, and positions perceived usefulness (PU) and perceived ease of use (PEOU) as major drivers of technology usage (Autry et al. 2010).

The balanced scorecard (BSC) is widely used to study organizational performance changes. The BSC framework provides a set of metrics for senior executives to get a quick and comprehensive view of their business (Kaplan and Norton 1992). The rationale behind this framework is that accounting and traditional financial metrics such as Return on Assets (ROA) and Return on Investment (ROI) provide an incomplete view of an organization's performance, thereby limiting opportunities to create future business value (Wu and Wang 2014). The BSC considers the firm performance in four aspects: customer, financial, learning and growth, and internal processes. The customer perspective examines how a company stands out from rivals and how consumers perceive a company in regard to its client relationships and reputation. Measures like market share, customer retention rate, and customer satisfaction are typically included in this perspective. The financial perspective of the BSC reveals how a company is seen by its shareholders. Measures like sales growth, return on investment, operational income, etc., are included in this perspective. A business may improve its capacity to improve customer service and satisfaction by developing its understanding of the customer needs. Analysis of internal business processes, such as productivity and operational efficiency, is important for attaining shareholder and customer satisfaction. The means by which performance exceptions are achieved are internal business processes.

Integration of TOE–DOI–TAM framework

This research considers three technology adoption models: the TOE framework, DOI model, and the TAM model, which have been frequently adopted in organizational studies (Pejic et al. 2016). Several empirical and conceptual investigations have supported the TOE framework, DOI model, and the TAM model's importance, dominance, and meaningful role in clarifying technology adoption independently, yet the models themselves have limits. TAM's two constructs, PU and PEOU, account for around 40% of technology usage, while additional factors in TAM's expanded models are not yet properly characterized. On the other hand, the TOE framework is overly general and has unclear key constructs. As a result, enhancing the TOE framework by combining it with other models is required to improve the predictive potential of the final model while also overcoming some of its limitations (Qin et al. 2020). To create the integrated model shown in Fig. 1, the researchers used a method that incorporated variables from the TOE, DOI, and TAM models, which were recognized in previous studies and chosen based on the research requirements and the context (Chandra and Kumar 2018; Lai et al. 2018).

Organizations encounter a variety of obstacles when adopting cybersecurity technologies, which can be divided into three categories. The first challenge is one of the technological aspects, in which the DOI model's major constructs of compatibility, trialability, and observability, and the TAM model's major constructs, such as perceived usefulness and ease of use, are addressed. The second challenge is with organizational aspects of adoption. When a company adopts a technology, senior management ought to endeavor to access and analyze potential changes within the company's structure and culture, operational procedures, and work relationships (Alshamaila et al. 2013). In this regard, senior

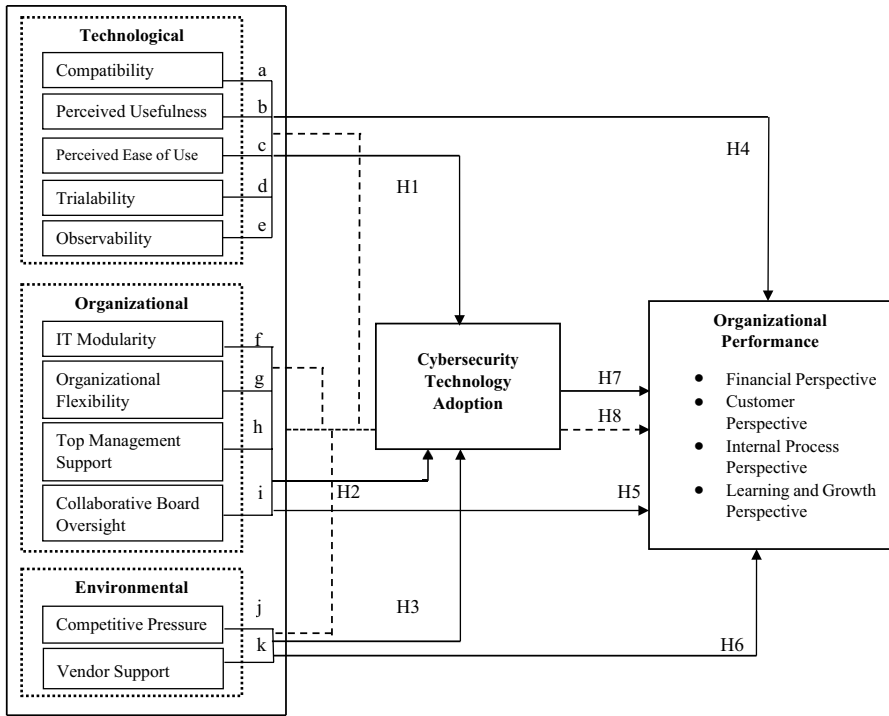


Fig. 1 Proposed cybersecurity technology adoption model

management’s willingness to recognize the benefits of cybersecurity technology adoption and implement it in the organization is primarily tied to IT modularity, organizational flexibility, and collaborative board oversight. The third challenge affects both competitive pressure and vendor support. According to Hsu et al. (2014), a firm under tremendous external pressure, such as pressure from trading partners and government policies, seems more likely to adopt new technologies.

Factors influencing an organization to adopt cybersecurity technologies

Eleven components impacting organizations’ intent to adopt cybersecurity technologies based on the numerous theories are outlined above: (1) compatibility, (2) perceived usefulness, (3) perceived ease of use, (4) trialability, (5) observability, (6) IT modularity, (7) organizational flexibility, (8) top management support, (9) collaborative board oversight, (10) competitive pressure, and (11) vendor support (see Table 1). Based on the TOE framework, we divide these components into three groups. Each of the eleven factors is briefly explained in “Research model and hypotheses development”.

Research model and hypotheses development

We create a cybersecurity technology adoption model (see Fig. 1) that includes eleven factors hypothesized to impact an organization's cybersecurity adoption in the TOE framework's technological, organizational, and environmental contexts. Under the holistic TOE framework, two complementary theories are used in this study to give a complete knowledge of the elements impacting an organization's cybersecurity technology adoption. This study applies DOI theory to the TOE framework's technological contexts to better understand the impact of compatibility, trialability, and observability on an organization's cybersecurity technology adoption. This study employs TAM within the technological context of the TOE framework to comprehend the impact of perceived usefulness and perceived ease of use on an organization's cybersecurity technology adoption. Institutional theory is also used inside the TOE framework's organizational context to explain the impact of top management support on an organization's cybersecurity technology adoption. Improving an organization's cybersecurity might substantially impact its overall performance (Suroso et al. 2019). Financial, customer, internal process, and learning and growth perspectives are used aspects of performance in the literature, and the items used to assess these dimensions are well-known and verified (Tsou and Hsu 2015).

Technological characteristics

San-Martna and López-Catalánb (2016) argue that technological characteristics are critical in adopting emerging technologies. Hasani and O'Reilly (2021) cite previous research demonstrating the significance of technological orientation in adopting eCRM (electronic customer relationship management) and social customer relationship management technologies.

Potential adopters' expectations of a technology's advantages, its consistency with current market processes, the technology's observability, and its trialability have been identified as significant factors impacting emerging technology adoption and are thus introduced as constructs in the technological characteristics aspect of this review. Compatibility and observability are adopted from DOI theory, while perceived usefulness is borrowed from TAM.

Compatibility

The degree of compatibility of new technology or innovation with existing technology reflects the assumption of compatibility with new technology (Charlton and Cornwell 2019). Adopting any new technology would change the business processes and practices that could cause adoption resistance among business employees (Hasani et al. 2017). According to Wang et al. (2016), there is a link between the compatibility of mobile reservation systems and their adoption in the travel industry (Wang et al. 2016). Awa et al. (2015) reported a positive

Table 1 Operationalization of key constructs

Variables	Measures (7-point Likert scale)	Source of measures
Compatibility (COMP)	<ol style="list-style-type: none"> 1. Cybersecurity technologies are compatible with a majority of my company's functions 2. Cybersecurity technologies are required or integrated into my company's working style 3. I think cybersecurity technologies are compatible with existing technologies in my company 	(Wang et al. 2016); (Yang et al. 2015)
Perceived usefulness (PU)	<ol style="list-style-type: none"> 1. Adopting cybersecurity technologies enables me to accomplish tasks with more reliability 2. Adopting cybersecurity technologies enhances the robustness of my activities 3. Adopting cybersecurity technologies improve the trustworthiness of my activities 	(Plewa et al. 2012)
Perceived ease of use (PEOU)	<ol style="list-style-type: none"> 1. I find it easy to understand cybersecurity technologies required in my work 2. Cybersecurity systems provide clear and understandable instructions to deploy and use them 3. I find it relatively easy to adopt cybersecurity technologies in my day-to-day activities 	(Plewa et al. 2012)
Observability (OBSR)	<ol style="list-style-type: none"> 1. I think other companies widely use cybersecurity technologies 2. I think my competitors have already adopted cybersecurity technologies 3. I know experts or companies in cybersecurity that can be acquired/hired as needed 	(Wang et al. 2016)
Trialability (TRL)	<ol style="list-style-type: none"> 1. I have the chance to test and try cybersecurity technologies before deciding to adopt them or not 2. I am allowed to try cybersecurity technologies for a long enough time before deciding to adopt them or not 3. I believe there are enough people in my company to help try various aspects of cybersecurity technologies 	(Wang et al. 2016)
IT modularity (IT)	<ol style="list-style-type: none"> 1. Different IT functions of my firm are highly independent 2. Most IT technologies in my firm interact through standardized interfaces 3. IT technologies adopted in my firm are highly interoperable 	(Tiwana and Konsynski 2010)
Organizational flexibility (OFX)	<ol style="list-style-type: none"> 1. We value openness and responsiveness in our firm 2. We place a great value on being flexible in our approach to problems in our firm 3. A willingness to show flexibility and openness is valued within our firm 	(Shee et al. 2018)

Table 1 (continued)

Variables	Measures (7-point Likert scale)	Source of measures
Top management support (TMS)	<ol style="list-style-type: none"> 1. My company's top management is likely to invest in adopting cybersecurity technologies in the near future 2. My company's top management is willing to take risks involved in adopting cybersecurity technologies 3. My company's top management is likely to be interested in adopting cybersecurity technologies to gain a competitive advantage 	(Wang et al. 2016); (Yang et al. 2015)
Collaborative board oversight (CBO)	<ol style="list-style-type: none"> 1. In our organization, the board of directors is aware of the cybersecurity trends and understands current cybersecurity technologies 2. The board of directors collaborate with external resources to increase their awareness of required cybersecurity technologies in our organization 3. In our organization, the board of directors understands the impact of the adoption of cybersecurity technology on the organization's risk appetite and collaborate with the operational managers to balance associated risks 	(Prasad and Green 2015)
Competitive pressure (CP)	<ol style="list-style-type: none"> 1. My company experienced competitive pressures to adopt cybersecurity technologies 2. I believe that my company will lose customers to our competitors if we do not adopt cybersecurity technologies 3. I feel that it is a strategic necessity to introduce cybersecurity technologies to compete in the existing marketplace 	(Wang et al. 2016); (Yang et al. 2015)
Vendor support (VS)	<ol style="list-style-type: none"> 1. For our company quality of cybersecurity vendors' technical support is essential 2. For our company amount of cybersecurity technologies training provided by the vendors is important 	(Wang et al. 2016); (Yang et al. 2015)
Learning and growth (LaG)	<ol style="list-style-type: none"> 1. Cybersecurity technology adoption improved the reliability of information exchange between employees in our company 2. Cybersecurity technology adoption improved the work efficiency of employees 3. Cybersecurity technology adoption improved the productivity of different departments 	(Wu and Chen 2014)

Table 1 (continued)

Variables	Measures (7-point Likert scale)	Source of measures
Internal process (IP)	<ol style="list-style-type: none"> 1. Cybersecurity technology adoption improved the efficiency of working processes 2. Cybersecurity technology adoption helped to reduce our working complexity 3. Cybersecurity technology adoption helped to improve interactions between different departments 	(Wu and Chen 2014)
Customer (CUST)	<ol style="list-style-type: none"> 1. Cybersecurity technology adoption helped to improve the reliability of communications with customers 2. Cybersecurity technology adoption helped to improve customer satisfaction 3. Cybersecurity technology adoption helped to improve customer trust in the company 	(Wu and Chen 2014)
Financial (FINC)	<ol style="list-style-type: none"> 1. Cybersecurity technology adoption helped build reliable remote working stations that reduced the space cost of the company 2. Cybersecurity technology adoptions helped to organize reliable remote meetings that reduce the cost of business travel 3. Cybersecurity technology adoption helped reduce the cost of reliable and trustable information processing 	(Wu and Chen 2014)
Cybersecurity technology adoption (CSA)	<ol style="list-style-type: none"> 1. Adopting cybersecurity technologies enable reliable access to data 2. Cybersecurity technologies adoption improves data accuracy 3. Adopting cybersecurity technologies develop new business opportunities 4.4. Cybersecurity technologies' adoption will improve organizational structure and processes 5. Cybersecurity technologies adoption creates a competitive advantage 	(Raguseo and Vitari 2018)

relationship between enterprise resource planning (ERP) software compatibility and its adoption in SMEs. SMEs are more likely to adopt cybersecurity technologies if they are perceived compatible, aligned with technical dimensions of the company, such as IT infrastructure, and offer a good fit to their style of work. Consequently, the following hypotheses are proposed in this study:

H1a. The compatibility of cybersecurity technologies is positively correlated with cybersecurity technology adoption.

H4a. The compatibility of cybersecurity technologies is positively correlated with the organizational performance of SMEs.

Perceived usefulness

The degree to which a person finds a new technology useful in enhancing their performance is perceived usefulness (Davis 1989). The perceived usefulness of technology directly impacts adopters' intention to use the technology (Grover et al. 2019). Prospective technology adopters evaluate the implications of their adoption actions based on the continuous desirability and effectiveness of the technology (Caffaro et al. 2020). In reality, technologies that do not help individuals perform their jobs are not favorably received (Mican et al. 2020). Although not yet verified, it can be hypothesized that if a cybersecurity technology is found beneficial, for instance, by expanding efficacy or quality of activities, a more favorable attitude may be anticipated towards its adoption. For example, cybersecurity technologies required for compliance purposes are believed to achieve higher adoption. Thus:

H1b. Perceived usefulness is positively correlated with cybersecurity technology adoption in SMEs.

H4b. The perceived usefulness of cybersecurity technology is positively correlated with the organizational performance of SMEs.

Perceived ease of use

Perceived ease of use is an individual's perception of how easy it is to use a specific technology (Mohd Amir et al. 2020). Perceived ease of use can lead to successful technology adoption, whereas lack of it may lead to dissatisfaction and hinder acceptance of technology (Izuagbe et al. 2019). Moreover, Ashraf et al. reported perceived ease of use as an essential factor impacting the attractiveness of a website to users who like to make an online order (Ashraf et al. 2016). Hence, it can be hypothesized that perceived ease of use may impact cybersecurity technology adoption as below:

H1c. Perceived ease of use is positively correlated with cybersecurity technology adoption.

H4c. Perceived ease of use of cybersecurity technology is positively correlated with the organizational performance of SMEs.

Trialability

Any emerging technology is followed by a certain complexity, affecting how widely it is adopted (Laurell et al. 2019; He et al. 2017). Trialability allows customers to test whether technology can function successfully in their environment. Cloud technologies (Lin and Chen 2012), Web technology (Hussein and Mourad 2014), and e-government schemes have all benefited from trialability (Ji and Liang 2016). Besides that, the trialability of eCRM applications and tools has been cited as a significant factor influencing adoption (Sophonthummapharn 2009).

On the other hand, others identified negative or negligible associations among trialability and the desire to adopt advanced technologies (Wu and Wang 2014). In view of the conflicting findings in the connection among both trialability and advanced technology adoption in the literature, the subsequent hypotheses have been developed:

H1d. The trialability of cybersecurity technology positively correlates to cybersecurity application adoption in SMEs.

H4d. The trialability of cybersecurity technology is positively correlated to the organizational performance of SMEs.

Observability

In accordance with observability, when a technology is more visible to end-users or consumers, individuals and businesses seem more willing to adopt and use it (Ramdani et al. 2013). According to several reports, there are many opportunities to adopt information technologies (IT) that are more noticeable (Ouiridi et al. 2016). In SMEs, the visibility of e-technologies and IT has strongly influenced the adoption of eCRM (Awa et al. 2015). Furthermore, the low visibility of cloud technology has been identified to be an obstacle to cloud-based e-commerce adoption (Rahayu and Day 2015). Increased visibility of mobile technologies, including advanced mobile phones and typical applications, has led to the adoption of mCRM technologies in numerous businesses (Rodriguez and Trainor 2016). Cybersecurity technologies tend to be less visible and mainly support back-office operations. Hence, it is interesting to explore the impact of observability on cybersecurity technology adoption as follows:

H1e. The observability of cybersecurity technology is positively correlated to Cybersecurity applications adoption.

H4e. The observability of cybersecurity technology is positively correlated to the organizational performance of SMEs.

Organizational characteristics

A company's environment and organizational structure play a critical role in adopting technology. Flexible and creative SMEs may find innovative ways to adopt innovative technologies quickly. SMEs with pro-innovation culture and those who feel external pressures are mostly early adopters of new technologies (Yun 2020).

Different organizational characteristics such as IT environment, top management technology awareness, size, and age of business, and even business flexibility are essential factors affecting SMEs' digital technology adoption (Lu et al. 2019). This section hypothesizes the impacts of organizational characteristics such as IT modularity, organizational flexibility, top management support, and collaborative board oversight on cybersecurity technology adoption in SMEs.

IT modularity

IT modularity refers to "the degree of decomposition of an organization's IT portfolio into loosely coupled subsystems that communicate through standardized interfaces" (Elia et al. 2019). The internal IT project portfolio must be flexible to adapt to technological changes. Suppose the subsystems of a company, like its programs and information system (IS) elements, are tightly coupled. In that case, they can operate in different IT environments without needing a complicated reconfiguration. Nevertheless, when linking an existing subsystem to new systems, a strongly coupled device of non-standardized interfaces presents an obstacle. Hence, IT modularity refers to tight coupling within different IT subsystems that allows them to work independently while offering a variety of interfaces that enable easy integration of various sub-systems. IT modularity is a crucial element in IT infrastructure flexibility which helps to gain and recover valuable knowledge and increases absorption ability by improving knowledge scope and resources. A flexible IT infrastructure facilitates the accelerated transformation of existing IT products to satisfy customer needs. According to Hsu et al. (2012) and Angst et al. (2017), the availability and use of IT inside an organization impact cybersecurity. Cybersecurity vulnerabilities and cybersecurity incidents are decreased by the availability and effective use of IT infrastructure, comprising IT resources and technical support for cybersecurity (Angst et al. 2017). Modular IT infrastructure reduces the mean time to respond to cyber incidents and increases the organization's robustness by limiting cyber incidents' impacts. Because IT systems and resources may support security controls and measures, Chang and Ho (2006) show a positive correlation between IT capabilities and the implementation of information security management in enterprises. These earlier studies highlight the significance of the availability and use of IT in supporting companies to manage cybersecurity and defend against cyberattacks. Hence, the IT modularity may offer a versatile and adaptive environment for adopting new cyber technology.

H2af. IT modularity positively affects cybersecurity technology adoption.

H5af. IT modularity positively affects on organizational performance of SMEs.

Organizational flexibility

The capacity of people, organizations, or communities to cope with, adapt to, and recover from a disastrous occurrence has often been viewed as a sign of flexibility (Riulli and Savicki 2003). Increased flexibility helps a company weather routine business challenges and crisis events and gives it an advantage in the competitive

marketplace (McManus et al. 2008). A company's ability to maneuver may be enhanced through organizational flexibility, and it is advantageous to modify current systems and procedures to account for changing environmental conditions (Lim et al. 2011). In complex infrastructure projects, time performance is improved by project management techniques emphasizing flexibility based on cooperation, exploratory learning, and adaptation (Eriksson et al. 2017). The existence of organizational flexibility involves the rapid adoption of new technologies and represents the willingness of businesses to innovate and introduce new technologies (Elia et al. 2019). Previous works have shown that organizational flexibility is essential for achieving long-term sustainability (Loi et al. 2019). Flexible adoption and application of external knowledge will affect the creativity and efficiency of a company and the implementation of new technologies. It is therefore hypothesized that:

H2g. Organizational flexibility positively affects cybersecurity technology adoption.

H5g. Organizational flexibility positively affects the organizational performance of SMEs.

Top management support

Top management plays a significant role in bringing innovative technology to firms (Shen et al. 2020). Top management support is vital for adopting new technologies as top management makes decisions on crucial changes in every organization (Singh et al. 2019). The positive effect of top management support and technology adoption on mobile reservation systems was confirmed by Wang et al. (2016). Arguably, top managers always play a leading role in accepting and disseminating new technologies. Therefore, SMEs may adopt cybersecurity technologies if it is among the priorities of top management, and the following hypothesis can be suggested:

H2h. Top management support poses a positive relationship towards the adoption of cybersecurity technologies.

H5h. Top management support poses a positive relationship with the organizational performance of SMEs.

Collaborative board oversight

The governance of IT resources at the board level refers to the actions of the board members to ensure that the IT functions support and expand the business strategies and objectives (Turel and Bart 2014). Board-level governance imitates an organization's competence within the resource-centric lens, bringing value to the organization (de Man and Luvison 2019). Board-based governance promotes strategic leadership, provides guidance to the executive management team, creates management structures to defend stakeholder interests, and allows access to external resources (Hermanson et al. 2020). The board's knowledge of cybersecurity may assist in managing risks and balancing the advantages of cybersecurity technologies with associated costs (COSO 2012). This would help organize and make reasoned decisions

about adopting and applying cybersecurity technologies. Accordingly, the following hypotheses are suggested:

H2i: Collaborative oversight from organizations' boards of directors will positively link cybersecurity technology adoption.

H5i: Collaborative oversight of CCS from the board of directors of organizations will be positively linked to the organizational performance of SMEs.

Environmental characteristics

Environmental context refers to the factors that affect companies because of their operating situation. Companies optimizing existing technologies would perform better in rapidly changing and turbulent environments (Yuan and Yi 2011). Rodriguez and Trainor (2016) found that environmental pressures are the main factors that push companies to adopt new business-to-customer (B2C) technologies. Ramdani and Williams (2013) reported environmental factors such as competitive pressure, customer pressure, industry pressure, and governmental support for new technology adoption in SMEs. Ahmadi et al. (2017) reported the direct impact of vendor support as an environmental characteristic on hospitals' information systems adoption. This study analyzes the effects of competitive pressure and vendor support as environmental factors impacting cybersecurity technology adoption.

Competitive pressure

Competitive pressure refers to the degree of competition an organization faces when competing against other companies close to its market (Yenipazarli 2019). Companies feel more pressure to innovate and survive in a more competitive market, which could be considered a driving force for companies (Yenipazarli 2019). Companies facing competitive pressures are obliged to adopt new technologies faster. Chiu and Chen (2017) showed that competitive pressure made companies adopt broadband mobile technologies. If SMEs feel pressure from their rivals and are conscious of their competitors, they may adopt cybersecurity technologies. Hence, this research suggests the following hypothesis:

H3j. Competitive pressure poses a positive relationship toward cybersecurity technology adoption.

H6j. Competitive pressure poses a positive relationship with the organizational performance of SMEs.

Vendor support

Vendor support involves technology training, assistance during adoption, or system updates through vendors or consultants (Chatzoglou et al. 2017). Several recent research, including research on ERP implementation (Chatzoglou et al. 2017), research on private cloud services adoption (Chang et al. 2016), and the adoption of cloud-based human resource management systems (Johnson and Diman 2017), have indicated a positive correlation between vendor support and technology adoption. In

this sense, SMEs may adopt cybersecurity technologies because they assume that vendors offer enough support for their technologies both in-between and after adoption. Hence, the following hypothesis can be posited:

H3k. Vendor support poses a positive relationship toward cybersecurity technology adoption.

H6k. Vendor support poses a positive relationship with the organizational performance of SMEs.

Organizational performance

Organizational performance is regarded as the dependent variable in the proposed model. This variable's relationship to an organization's cybersecurity adoption is also looked at. The BSC method identified four performance indicators, product leadership, financial achievement, customer intimacy, and operational excellence, for evaluating organizational performance based on the four identified perspectives, internal process, learning and growth, customer, and finance (Rai et al. 2006). Additionally, Zhu and Kraemer (2005) suggested that evaluating the effectiveness of an organization's internal processes is a crucial component of evaluating organizational success. Additionally, Tsou and Hsu (2015) identified excellent reputation as a crucial factor in evaluating organizational performance. Angst et al. (2017) emphasizes that if a company raises its readiness to combat cyberattacks by investing in IT security, it may achieve higher performance, as evaluated by the decrease in data breaches over time. As previously stated, cybersecurity adoption seems important for decreasing cyberattacks and influencing organizational performance. Consequently, the seventh hypothesis is as follows:

H7: The greater the adoption of an organization to combat cyberattacks, the higher the organization's performance.

Cybersecurity technology adoption as a mediator

Improving organizational performance is among the primary concerns of any company's management (Gavrea et al. 2011). Technology adoption appears to positively impact organizational performance (Martin-Rojas et al. 2019). For instance, research on business intelligence systems in banks (Owusu 2017) and knowledge management systems (Valmohammadi and Ahmadi 2015) point to the generally positive impact of technology adoption and use on organizational performance. We use Kaplan and Norton's (1992) BSC framework to measure organizational performance across four criteria: financial perspective, internal processes perspective, learning and growth perspective, and consumer perspective. Cybersecurity technology adoption may increase customer satisfaction and enhance brand marketing and business credibility. Cybersecurity technology adoption may lead to higher assets, business investment, profit margins, and market share from a financial perspective. Cybersecurity technology adoption poses a positive relationship with the organizational performance of SMEs. Adopting cybersecurity can help SMEs improve their inner processes in the context of operating and working modalities. Hence, the final

hypothesis of this research investigates the mediating role of cybersecurity technology adoption in the relation between independent constructs of this research and the organizational performance of SMEs as follows:

H8. Cybersecurity technology adoption mediates the relationship between technological, organizational, environmental, and organizational performance.

Methodology

This research examines the adoption of cybersecurity technology. A quantitative survey was undertaken to explore organizational readiness to battle cyberattacks and the links between the model elements and experimentally evaluate the model hypotheses. To guarantee the highest possible reliability and validity of the items, the construct items were built using existing construct items from prior research whenever possible. In addition, some new items were created based on the descriptions of the model structures and concurrent conversations with three experienced academics who specialize in cybersecurity. Table 4 lists all constructs and the quantity and sources of measurement elements.

The construct items were measured on a seven-point Likert scale (from 1 = 'strongly disagree' to 7 = 'strongly agree'). In addition, respondents were requested to submit demographic information about their companies. Similar to previous works, we included a validation question about the SMEs' intention to adopt cybersecurity technologies. This study did not include responses from participants who had no intention to adopt a cybersecurity technology.

The completed survey was distributed to roughly 190 IT experts from various UK organizations who were chosen randomly. Because not all businesses have cybersecurity professionals, this respondent pool was selected as the most informed about information security in organizations. The survey was delivered in electronic format. Soft copies were created with Google Forms and distributed via email invitations, including a link to the Google Form. As the questionnaire was administered through Google Forms, it was only possible to submit it when all required fields were appropriately completed, so there was no possibility of obtaining an incorrect or inappropriate response. A total of 147 replies were received, with a response rate of 77%. It is commonly agreed that bigger samples result in more accurate results, which are even more important when researchers use the SEM technique (Hair et al. 2010). It is challenging to utilize SEM with fewer than 100 samples, and a minimum sample size of 150 is usually suggested (Guadagnoli & Velicer (1988)). The organizations the respondents worked for varied in years of operation, sector, and size (based on the number of employees) see Table 2.

Data analysis

We used SPSS version 21 and AMOS 22 for the Confirmatory Factor Analysis (CFA) and Structural equation modeling (SEM). SEM is best suited for this study as it comprehensively analyzes different independent and dependent variables and

tests mediator relations. The demographics of all those who participated throughout the survey are presented in Table 2.

Table 3 displays alpha values, means and standard deviations, Skewness, and Kurtosis. The alpha values range from 0.78 to 0.94, above the recommended value of 0.70 and considered high. Moreover, the means and standard deviations reflect general descriptive statistics for each variable. Perceived ease of use and perceived usefulness had the highest mean scores of 4.122 and 4.102 respectively. The lowest mean score belonged to trialability (1.673). Vendor support had the highest standard deviation of 2.334, while trialability had the lowest standard deviation of 0.563.

An examination of the correlation coefficients between the research variables in Table 4 shows that, except for the three variables: IT modularity, observability, and trialability, other variables are strongly associated with cybersecurity and performance factors such as finance, consumer, learning, except internal processes. Concerning internal processes, all variables except trialability are highly correlated.

Construct validity can be examined by assessing convergent validity, discriminant validity, and nomological validity. Standard factor loadings of the construct, Average Variance Extracted (AVE), and Construct Reliability (CR) estimation are factors for assessing convergent validity. For each construct, the minimum cut-off point for standard factor loading is 0.7, AVE is 0.5, and CR is 0.7 to reflect an adequate level of convergent validity. The value of Cronbach's Alpha can range from zero to 1, with higher values (closer to 1) indicating greater measuring instrument reliability. Cronbach's Alpha of 0.7 or more is considered good and acceptable for measurement as a rule of thumb. As shown in Table 3, for all multi-item scales in this research, Cronbach's alpha became greater than 0.70, indicating that our research scales are reliable (Bujang et al. 2018). Moreover,

Table 2 Demographic data of responders

	Option	Percentage
Total year(s) of operation	≤ 5	21.94
	6–10	32.45
	11–20	29.78
	21 ≤	15.83
Types of sectors	Business activities	29.36
	Construction	15.47
	Transport, storage, and communication	13.68
	Wholesale and retail trade	12.75
	Health, social and personal services activities	12.43
	Manufacturing	11.27
	Others	5.04
Number of employees	≤ 9	35.66
	10–49	34.90
	50–249	29.44

Table 3 Central and dispersion statistic for research variables

Variable	Min	Max	Mean	Std Deviation	Skewness		Kurtosis	
					Statistic	Std. Error	Statistic	Std. Error
Compatibility	1	7	4.007	2.012	0.067	0.231	- 1.348	0.397
P. usefulness	1	7	4.102	1.992	0.047	0.216	- 1.369	0.214
P. ease of use	1	7	4.122	1.809	0.103	0.118	- 1.017	0.308
Observability	1	5	2.082	0.864	0.745	1.246	0.765	1.084
Trainability	0	3	1.673	0.563	- 0.136	0.987	- 0.361	0.421
IT modularity	1	5	2.156	0.919	0.434	1.145	- 0.121	1.309
Organizational flexibility	0	7	3.728	2.241	- 0.039	1.876	- 1.435	0.368
Top management support	0	7	3.735	2.312	0.072	0.516	- 1.619	0.327
Collaborative board	1	7	4.068	2.163	- 0.035	1.530	- 1.555	0.018
Competitive pressure	0	7	3.741	2.246	- 0.054	1.819	- 1.446	0.697
Vendor support	0	7	3.803	2.334	- 0.007	0.418	- 1.670	1.047
Cybersecurity	1	7	3.906	1.870	0.058	0.261	- 1.767	0.641
Financial	1	7	4.068	2.106	- 0.015	2.147	- 1.468	0.645
Customer	0	7	3.891	2.291	0.035	0.717	- 1.481	1.213
Learning	1	7	3.891	2.206	0.101	0.632	- 1.453	0.322
Processes	0	7	3.844	2.287	- 0.004	0.395	- 1.455	0.775

Table 4 Correlation coefficients between research variables

Variable	Cybersecurity	Finance	Customer	Learning	Processes
Compatibility	0.848**	0.734**	0.774**	0.760**	0.777**
P. usefulness	0.863**	0.749**	0.792**	0.812**	0.742**
P. ease of use	0.842**	0.717**	0.749**	0.760**	0.723**
Observability	0.140	0.215**	0.157	0.148	0.142
Trialability	0.145	0.175*	0.126	0.175*	0.120
IT modularity	0.044	0.147	0.054	0.059	0.064
Flexibility	0.826**	0.814**	0.769**	0.733**	0.788**
Top management support	0.880**	0.821**	0.768**	0.769**	0.762**
Collaborative board	0.899**	0.820**	0.825**	0.790**	0.819**
Competitive pressure	0.869**	0.827**	0.796**	0.760**	0.810**
Vendor support	0.908**	0.847**	0.798**	0.795**	0.795**
Cybersecurity	1.000	0.856**	0.868**	0.860**	0.856**
Finance	0.856**	1.000	0.792**	0.782**	0.796**
Customer	0.868**	0.792**	1.000	0.856**	0.875**
Learning	0.856**	0.796**	0.875**	1.000	0.847**
Processes	0.860**	0.782**	0.856**	0.847**	1.000

*Correlation is significant at the 0.05 level (2-tailed)

**Correlation is significant at the 0.01 level (2-tailed)

for all constructs, standard factor loading (standard regression weight) was above 0.7, AVE became greater than 0.5, and CR became higher than 0.7. Further, the critical ratios (t-values) became above 1.96 ($p < 0.001$) can be seen in Table 5.

Discriminate validity occurs when the shared variance between a construct and any other construct is less than the shared variance between the construct and its indicators (Hair et al. 2010). Discriminate validity is supported where the AVE estimation of a construct becomes continuously greater than the Squared Inter-construct Correlation (SIC) estimate. As shown in Table 6, the AVE estimate for each construct in this research is higher than the SIC estimate, suggesting that discriminate validity occurs in each construct.

Structural model and hypotheses testing

This section demonstrates the path analysis process for investigating mediation and direct and indirect structural relationships among research variables. Moreover, an analysis of cybersecurity technology adoption impact as a mediator between predictor variables and organizational performance is presented. This study's theoretical model hypothesized the relationship between eleven predictor variables: compatibility, perceived ease of use, perceived usefulness, observability, trialability with cybersecurity technology adoption, and organizational performance of SMEs. The structural model shown in Fig. 2 was examined to evaluate the proposed hypotheses.

Estimates of the goodness of fit indices and other parameters indicate that seventeen out of twenty-three hypothesized paths were significant. All relations with a

Table 5 Convergent validity

Variable	AVE (<0.5)	Cronbachs alpha	Composite reliability (<0.7)
Compatibility	0.752	0.772	0.855
Perceived usefulness	0.810	0.752	0.861
Perceived ease of use	0.724	0.798	0.883
Observability	0.582	0.713	0.757
Trialability	0.513	0.721	0.724
IT modularity	0.583	0.709	0.711
Organizational flexibility	0.950	0.891	0.974
Top management support	0.948	0.973	0.764
Collaborative board	0.947	0.972	0.982
Competitive pressure	0.727	0.711	0.868
Vendor support	0.954	0.976	0.814
Cybersecurity	0.777	0.833	0.923
Finance	0.615	0.700	0.702
Customer	0.671	0.718	0.743
Learning	0.616	0.715	0.708
Processes	0.597	0.706	0.782

Table 6 Discriminant validity

Variable	COMP	PU	PEOU	OBSR	TRI	ITM	OFX	TMS	CBO	CP	VS	CSA	FINC	CUST	LaG	IP
COMP	0.84															
PU	0.61	0.76														
PEOU	0.63	0.64	0.71													
OBSR	0.63	0.52	0.34	0.68												
TRI	0.48	0.32	0.25	0.43	0.70											
ITM	0.23	0.53	0.12	0.18	0.47	0.55										
OFX	0.15	0.47	0.41	0.11	0.27	0.41	0.63									
TMS	0.54	0.52	0.46	0.44	0.06	0.46	0.18	0.59								
CBO	0.43	0.43	0.32	0.53	0.09	0.32	0.35	0.16	0.64							
CP	0.56	0.48	0.36	0.26	0.21	0.09	0.37	0.07	0.15	0.77						
VS	0.57	0.32	0.27	0.29	0.41	0.17	0.32	0.20	0.37	0.51	0.69					
CSA	0.65	0.25	0.41	0.19	0.56	0.28	0.21	0.17	0.38	0.63	0.27	0.81				
FINC	0.51	0.19	0.33	0.08	0.41	0.23	0.27	0.35	0.41	0.43	0.43	0.17	0.68			
CUST	0.32	0.31	0.26	0.27	0.23	0.21	0.11	0.33	0.45	0.25	0.32	0.53	0.34	0.85		
LaG	0.38	0.23	0.17	0.19	0.25	0.07	0.08	0.41	0.28	0.19	0.27	0.46	0.29	0.19	0.56	
IP	0.43	0.41	0.15	0.35	0.07	0.31	0.19	0.26	0.34	0.27	0.21	0.55	0.23	0.31	0.09	0.66

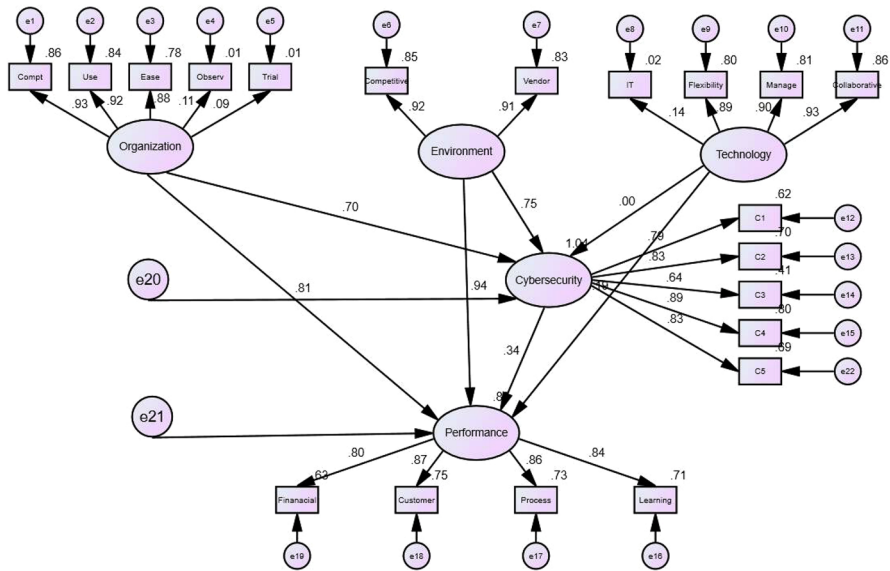


Fig. 2 Structural equation model for the prediction of organizational performance

Table 7 Structural model fit indices for SEM model

Model	Chi- Square	Df	X ² /df	RMSEA	GFI	NFI	IFI	TLI	PGFI
SEM	345.236	164	1.905	0.082	0.925	0.867	0.975	0.784	0.578

χ^2 =Chi-square, DF=Degree of Freedom, GFI=Goodness of Fit Index, RMSEA=Root Mean Square Error of Approximation, NFI=Normed Fit Index, IFI=Increment Fit Index, PGFI=Parsimony Goodness-of-Fit Index (PGFI), TLI=Tucker-Lewis Index (TLI)

factor loading of less than 0.05 should be excluded as a rule. As shown in Table 7, most fit measures of data were acceptable. Root Mean Square Error of Approximation (RMSEA) was 0.081, chi-square ($\chi^2=345.236$; $df=164$; $p=0.000$) was significant ($p<0.001$), and all incremental fit measures, namely Normed Fit Index (NFI), Tucker-Lewis Index (TLI), and Increment Fit Index (IFI), were above minimum requirements, AGFI (Adjusted Goodness-of-Fit Index) was above 0.8 cut-off point, and the X²/df was 1.905 which is within the threshold of 1.0 to 3.0. Despite the outrages of GFI values, all of this represents an adequate fit. The effect of GFI can be ignored because of its sensitivity to the sample size.

Table 8 shows the parameter estimates utilized to develop the estimated population covariance matrix of the structural model. A parameter estimate is significant at the 0.05 level when its critical ratio (CR) is more than 1.96. Seventeen (17) out of twenty-three (23) who examined the hypothesis of this research had t-values greater than 1.96 at the significant level of less than $p<0.05$ and hence supported. In the technological dimension, it was found that the direct effect of compatibility (C.R=6.181, $***p<0.000$), perceived usefulness (C.R=9.291, $***p<0.000$), and

perceived ease of use ($C.R=6.781, ***p<0.000$), on cybersecurity technologies adoption was significant, which leads to accepting H1a, H1b, and H1c. However, trialability ($C.R=0.513, p=0.608$) and observability ($C.R=0.302, p=0.763$), on cybersecurity technologies adoption was not significant, so H1d, and H1e are rejected. Additionally, it is found that compatibility ($C.R=2.380, p=0.017$), perceived usefulness ($C.R=17.912, ***p<0.000$), and perceived ease of use ($C.R=11.554, ***p<0.000$), have a direct, positive and significant impact on organizational performance which allows to accept H4a, H4b, and H4c. Finally, the direct effect of trialability ($C.R=0.403, p=0.687$) and observability ($C.R=1.009, p=0.313$) on organizational performance were not significant, so H4d and H4e were rejected.

When analyzing mediation, as shown in Table 9, it was found that the indirect effect of trialability ($\beta=0.076; S.E=0.188$) and observability ($\beta=0.121; S.E=0.120$) on organizational performance through cybersecurity technologies adoption has a negative effect, in such a way that no mediation is found, which rejects

Table 8 Structural path analysis result

Dependent variables	←	Independent variables	Estimate	S.E	C.R	P
Cybersecurity	←	Compatibility	0.118	0.019	6.181	***
Cybersecurity	←	Usefulness	0.197	0.021	9.291	***
Cybersecurity	←	Ease of use	0.147	0.022	6.781	***
Cybersecurity	←	Observability	0.013	0.042	.302	0.763
Cybersecurity	←	Trialability	0.033	0.064	.513	0.608
Cybersecurity	←	Competitive pressure	0.256	0.022	11.905	***
Cybersecurity	←	Vendor support	0.401	0.027	14.763	***
Cybersecurity	←	IT modularity	0.004	0.039	.114	0.909
Cybersecurity	←	Organizational flexibility	0.981	0.052	18.843	***
Cybersecurity	←	Top management support	0.218	0.020	10.996	***
Cybersecurity	←	Collaborative board oversight	0.861	0.050	17.166	***
Performance	←	Cybersecurity adoption	0.145	0.048	3.042	0.002
Performance	←	Compatibility	0.097	0.041	2.380	0.017
Performance	←	Usefulness	0.979	0.055	17.912	***
Performance	←	Ease of use	0.424	0.037	11.554	***
Performance	←	Observability	0.121	0.120	1.009	0.313
Performance	←	Trialability	0.076	0.188	.403	0.687
Performance	←	Competitive pressure	1.165	0.107	10.878	***
Performance	←	Vendor support	0.974	0.126	7.716	***
Performance	←	IT modularity	0.112	0.111	1.006	0.314
Performance	←	Organizational flexibility	0.218	0.061	3.546	***
Performance	←	Top management support	0.844	0.080	10.569	***
Performance	←	Collaborative board oversight	1.048	0.080	13.065	***

Source: Survey

*** $p<0.000$, ** $p<0.01$, * $p<0.05$; *S.E* standard error, *C.R* critical ratio

hypothesis H8d, and H8e. However, the influence of compatibility, perceived usefulness, and perceived ease of use on organizational performance through cybersecurity technologies adoption are positive and significant, which leads to identifying partial mediation and supporting H8a, b, c.

In the organizational dimension, it was found that the relationship between organizational flexibility (C. R=18.843, *** $p < 0.000$), top management support (C.R=10.996, *** $p < 0.000$), and collaborative board oversight (C.R=17.166, *** $p < 0.000$) and cybersecurity technologies adoption have a positive and significant effect, which allows to accept H2g, H2h, and H2i. The direct effect of IT modularity on adoption was not significant (C.R=0.114, $p=0.909$) so H2f is rejected. Regarding the direct effect of organizational flexibility (C.R=3.546, *** $p < 0.000$), top management support (C. R=10.569, *** $p < 0.000$), and collaborative board oversight (C. R=13.065, *** $p < 0.000$), it was found that they have a significant relationship with organizational performance, which allows to accept H5g, H5h, and H5i. The direct effect of IT modularity on organizational performance was not significant (C.R=1.006, $p=0.314$), so H5f is rejected. When mediation is analyzed, it is observed that the influence of IT modularity on organizational performance

Table 9 Summary of significant paths for mediation hypotheses

Independent variables	Path c		Path a		Path b		Path c'		Findings
	β	S.E	β	S.E	β	S.E	β	S.E	
Compatibility	0.145***	0.032	0.119 ***	0.018	1.142***	0.084	0.359**	0.160	Partial Mediation
Usefulness	0.239***	0.033	0.201***	0.020	1.142***	0.084	0.298**	0.135	Partial Mediation
Ease of use	0.087**	0.035	0.127***	0.022	1.142***	0.084	0.276***	0.044	Partial Mediation
Trialability	0.172	0.112	0.068	0.062	1.142***	0.084	0.076	0.188	No Mediation
Observability	0.237	0.398	0.050	0.041	1.142***	0.084	0.121	0.120	No Mediation
Competitive pressure	0.256 ***	0.029	0.248***	0.020	1.142***	0.084	0.360***	0.044	Partial Mediation
Vendor support	0.685***	0.033	0.454***	0.027	1.142***	0.084	0.258***	0.049	Partial Mediation
IT modularity	0.103	0.069	0.021	0.038	1.142***	0.084	0.112	0.111	No Mediation
Flexibility	0.135***	0.028	0.132***	0.046	1.142***	0.084	0.218***	0.061	Partial mediation
Management support	0.597	0.032	0.300***	0.021	1.142***	0.084	0.757***	0.050	Partial mediation
Collaborative board	0.842	0.399	0.454***	0.054	1.142***	0.084	0.687***	0.053	Partial mediation

Source: Survey

*** $p < 0.000$, ** $p < 0.01$, * $p < 0.05$; β = Path coefficients; S.E= Standard Error

through cybersecurity technologies adoption ($\beta=0.112$; S. E=0.111) is negative, in such a way that no mediation is found, which rejects hypothesis H8f. However, the influence of OFX, TMS, and CBO on organizational performance through cybersecurity technologies adoption is positive and significant, which leads to identifying partial mediation and supporting H8g, H8h, and H8i.

In the environment dimension, it was obtained that the direct effect of competitive pressure (C. R=11.905, $***p<0.000$) and vendor support (C. R=14.763, $***p<0.000$) on adoption was significant, which supports hypotheses H3j and H3k. It was found that the direct effect of competitive pressure (C. R=10.878, $***p<0.000$) and vendor support (C. R=7.716, $***p<0.000$) on organizational performance were significant, so H6j and H6k are supported. When analyzing mediation, it was found that competitive pressure ($\beta=0.360$; S. E=0.044) and vendor support ($\beta=0.258$; S. E=0.049) through OP have a positive and significant effect on cybersecurity technologies adoption; this result confirms a partial mediation and supports hypothesis H8j, H8k.

As shown in Fig. 2, complete hypotheses testing was conducted using structural equation modeling. The structural model fit was used afterward to quantify each hypothesis, as shown in (Table 8). P-values for all hypotheses were determined at the alpha level of 0.05 to measure the significance of each correlation.

Discussion

The TOE framework was used to investigate the influence of technological, organizational, and environmental aspects on organizations' cybersecurity adoption in order to answer the research question. The technological factors (compatibility, triability, observability, perceived ease of use, and perceived usefulness), organizational factors (IT modularity, top management support, organizational flexibility, and collaborative board oversight), and environmental factors (competitive pressure, and vendor support) all had significant positive effects on the level of cybersecurity technologies adoption. To address the second research question, this study looked at the influence of cybersecurity technology adoption on companies' performance, specifically on the business's financial and non-financial performance. The outcomes of this investigation corroborated these linkages. These findings are expanded in the following subsections, drawing on past research to emphasize the study's contributions.

Technological characteristics

The findings demonstrate that compatibility is an important component in the adoption of cybersecurity technologies. This conclusion is consistent with prior research (Johansson and Ruivo 2013), which found that 55 percent of experts agreed that compatibility is essential in the adoption of SAS (Software as a Service). Prior CRM and IT/IS adoption studies in SMEs have found similar results in the adoption of social customer relationship management technologies (Hasani et al. 2017; Ainin

et al. 2015). The observability of the technology is proven to be an influencing component for cybersecurity technology adoption. This finding is consistent with a prior study that inferred that success stories and case studies on cloud computing technologies might boost adoption (Lin and Chen 2012).

The trialability of cybersecurity technologies was an important component in their adoption. This is consistent with the findings of a previous study, which found that adopters are enticed to test out trial versions of applications before committing to a full adoption (Alshamaila et al. 2013). This research indicates that SaaS adopters prefer to utilize the program separately (informally) without the expense of deciding about the registration of paid versions.

According to the findings, PEOU influences the desire to adopt cybersecurity technologies. According to Yi et al. (2006), a substantial component of the usefulness that a professional individual obtains through utilizing an innovation is the decrease in work (Boateng et al. 2016). Firms' adoption of 3D design digital technologies (3DDT) is impacted by their perceptions of the technology's usefulness in improving business efficiency, business operations, task organization, operational quality, competitiveness, and simplicity of use for regular activities (Oh et al. 2009). Users perceive technology to be useful once it leads to improved outcomes, increased efficiency in internal operations, increased staff productivity, improved customer service, reduced stock costs, and enhanced collaboration with business partners (Gangwar et al. 2015). Faced with increased competition from a wide range of businesses, corporations ought to assess the usefulness of a new technology before adopting or using it broadly (Gangwar et al. 2015). Previous research on organizations' adoption of new technological innovations, such as Maduku et al. (2016), and Tsai et al. (2010), has indicated a substantial association between PU and the desire to adopt 3DDT.

Organizational characteristics

Organizational characteristics impact a firm's readiness to protect its assets against cyberattacks. According to this study, these characteristics include top management support, IT modularity, organizational flexibility, and collaborative board. The findings revealed that top management support has a considerable beneficial influence on cybersecurity technology adoption. Previous research by Hsu et al. (2012), and Daud et al. (2018), looked at the impacts of top management support on cybersecurity innovation, effectiveness, and compliance and found that firms should pay close attention to top management's commitment to supporting cybersecurity technologies adoption. Top management must be given a supporting role in establishing cybersecurity policies, plans, rules, strategies, and standards to improve businesses' readiness to combat cyberattacks. Furthermore, top management may show accountability for cybersecurity performance by being directly engaged throughout all discussions regarding cybersecurity inside the firm and committing to sponsoring any cybersecurity initiatives. Lastly, top management ought to outline a vision for the future of the company's cybersecurity strategy.

This study advocates mature IT modularity as a technological component influencing an organization's readiness to adopt cybersecurity technologies. The findings demonstrated that having a more mature IT modularity significantly enhances technology adoption to combat cyberattacks. Furthermore, IT modularity allows businesses to make the most meaningful use of IT resources to combat cyberattacks. This conclusion backs with the findings of Kong et al. (Kong et al. 2012), who looked at cybersecurity investments rather than technology adoption and demonstrated that the chances of investment in cybersecurity technologies are higher in businesses with a modular IT infrastructure.

Moreover, this study's findings align with Lim et al. (2011) in that organizational flexibility is a reliable predictor of technology adoption. By quickly absorbing changes, integrating them, and developing and restructuring resources and capabilities, flexible organizations can respond to cyberattacks and uncertainties in a way that helps them successfully navigate crisis situations. In line with other research on technology adoption by Smith et al. (2007), and Venkatesh and Bala (2012), this study discovered that collaborative board oversight is a significant predictor of cybersecurity technologies adoption. How the board engages with IT security governance procedures, how much capital is invested in IT, and the unique circumstances of the firm impact cybersecurity technology adoption. Our findings suggest that the board's IT governance activity should be intensified when the company prepares to adopt cybersecurity technology. Board-level governance of IT resources involves ensuring that the organization's IT sustains and extends its strategies and objectives. Within the resource-centric lens, board-level IT governance emulates an organization's competency that can add value to the organization. Turel and Bart (2014) suggest that broad-level IT governance can facilitate strategic leadership, establish control mechanisms to protect the stakeholders' interests from self-interest actions of the executive management team, and enable access to external resources. Essentially, this form of relational governance would entail the creation of a collaborative perception of IT governance that would benefit both the organization and the external stakeholders. This understanding helps management to balance cyber risks with benefits and agree on appropriate technology adoption (COSO 2012).

Environmental characteristics

Environmental characteristics influencing firms' readiness to secure their IT infrastructure and services include competitive pressure and vendor support. The need for external vendor support in the adoption of the innovation may be low if incumbent technical expertise in the companies is deemed to be high. The findings show that in the entire sample, external vendor support is positively and significantly linked with cybersecurity technologies adoption, confirming prior findings (Ramayah et al. 2016).

Previous research has found that the threat of competition is the primary motivator for SMEs to strategically adopt any technological innovation (Ghobakhloo et al. 2012). Competitive pressure was the second most significant component in companies' decision to adopt cloud computing solutions behind relative advantage,

confirming that competitive pressure triggers innovation adoption in enterprises (Senyo et al. 2016). We also find that competitive pressure substantially impacts the choice to adopt cybersecurity technologies. This might be due to rivals using the maturity of their cybersecurity program to assure clients about their data security, gain a competitive advantage through lower cyber insurance costs, and reap the financial benefits of loyal customers.

Cybersecurity adoption and organizational performance

In accordance with the findings of this study, cybersecurity adoption has a significant impact on SME performance, correlating with the findings of Angst et al. (Angst et al. 2017). This finding implies that cybersecurity technology adoption improves SMEs' performance over time by reducing data breaches, enhancing the security of internal processes, developing reliable systems with adequate capabilities for information processing, and establishing a legitimate security reputation. Our results indicate the significant perceived impact of cybersecurity technologies adoption on both financial and non-financial performance of SMEs. Improving the cybersecurity posture of an SME leads to higher revenue and profit margin that improves financial performance. Moreover, cybersecurity technology adoption enhances customer satisfaction and increases client retention as non-financial benefits.

Study implications

This study advances knowledge in various ways by proposing a comprehensive, multi-theoretical framework for adopting cybersecurity technologies in SMEs. Our proposed framework combines multiple theories to identify crucial components impacting organizational readiness to adopt cybersecurity technologies. Previous studies have looked at any of these components separately, leading to fragmentation, a lack of comprehensive awareness of the overall influence of these components on SMEs and their relative significance, and a lack of cybersecurity research integration. By examining all potential factors impacting cybersecurity technologies adoption in one research, we can distinguish their impacts and pinpoint the most important factors. This study identifies organizational flexibility as the most significant factor influencing cybersecurity technologies adoption, followed by collaborative board oversight and vendor support. Since each of these factors involves active management, partnerships and requires the engagement of critical stakeholders, the importance of top-management full support for the adoption of cybersecurity technologies is emphasized.

This study aids researchers in better understanding the relationship between cybersecurity technologies adoption and organizational performance. Previous research, such as Daud et al. (2018), has not tested the influence of cybersecurity on organizational performance experimentally. Our research adds to earlier studies by demonstrating how cybersecurity adoption may lead to higher performance in four aspects (financial, customer, internal process, and learning and growth perspectives). This research

also contributes by emphasizing the significance of eleven components that have been empirically proven to improve organizational cybersecurity technology adoption.

In particular, organizations should ensure that their senior executives are supportive of establishing an appropriate organizational culture that increases their ability to protect digital assets and combat cyberattacks to minimize their negative impacts on overall organizational performance. With top management support, SMEs can build and develop appropriate strategies and guidelines to regulate cybersecurity practices. Furthermore, influential SMEs within the industry should be proactive in motivating regulators and governments to establish applicable standards to protect the industry from cyberattacks. Finally, by illuminating the connections between cybersecurity adoption, and organizational performance, this study can assist businesses in stimulating the creation of mechanisms to enhance cybersecurity to obtain optimal performance. This study can help SMEs understand the linkages between cybersecurity adoption and their business's financial and non-financial performance, thereby motivating the development of mechanisms to adopt the latest cybersecurity technologies and achieve superior performance.

Limitations and future works

The results obtained should be interpreted with caution. This study has limitations that may be considered in subsequent studies. First, the survey is focused solely on a sample of UK SMEs. Thus, extra care is needed when generalizing findings to SMEs located in other countries. Second, in terms of participating SMEs, the research was undertaken voluntarily. As such, results are not generalizable to the mandatory settings, recognizing that the sample may not fully represent the population of SMEs in the UK. Fourth, this research measures cybersecurity technology adoption in general and is not focused on a specific type of cybersecurity technology or application. As a result, since different types of cybersecurity applications could differ in their adoption processes, results should be interpreted to consider cybersecurity technology in general only.

Moreover, since the data are gathered in a cross-sectional manner, and all the hypotheses were tested at a single point, a future longitudinal study is needed to validate the factors influencing cybersecurity technology adoption and SMEs' organizational performance. Finally, this study used a quantitative method that relied on survey-based data collection. To get a deeper knowledge of how various variables impact adoption and performance, future qualitative research, including focus groups, individual interviews, and observations, might be valuable. Future studies addressing these limitations will substantially improve the understanding of cybersecurity adoption and how it affects overall organizational performance.

Conclusion

Organizations must be prepared to respond as cyberattacks increase in frequency. This study has proposed a comprehensive framework that incorporates the TOE framework, TAM, DOI, and the balanced scorecard to identify the factors that

impact cybersecurity technologies adoption by SMEs in the UK and their impact on organizational performance. This study's results showed that the factor with the highest impact on cybersecurity technologies adoption was organizational flexibility, followed by collaborative board oversight and vendor support.

In terms of theoretical contributions, the TOE framework, DOI theory, TAM, and the balanced scorecard elements have been integrated to extend a comprehensive framework to identify the variables and factors that influence cybersecurity technologies adoption in SMEs. While the TEO framework is widely used in the technology adoption surveys, employing it along with the balanced scorecard to frame cybersecurity technology adoption in SMEs was never attempted. This study presents empirical proof of the positive impact of cybersecurity technologies adoption on organizational performance, in addition to improving the current understanding of the critical variables that must be handled to guarantee cybersecurity adoption in SMEs.

In terms of practical contributions, compelling empirical evidence was presented to measure the factors that impact UK SMEs' adoption of cybersecurity technologies and the factors that affect organizational performance. This information is essential for cybersecurity technology vendors and SMEs seeking to adopt cybersecurity technologies. Cybersecurity technology vendors should emphasize improving their support services (vendor support), the usefulness of their products, and the ease of use of their technologies. SMEs adopting cybersecurity technologies should strive to increase organizational flexibility and train company board members on cybersecurity technologies in order to diminish resistance and recognize the real potential of cybersecurity.

Acknowledgements This project has been partially funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the author(s) and do not necessarily reflect those of the OPC.

Author contributions TH: the corresponding author conceived of the presented idea, performed the computations, wrote the first draft of the manuscript and verified the analytical methods. NO: conceptualization, supervision, validation, and editing. AD: writing- reviewing, and editing. DR: supervision, reviewing, visualizing and validating this study. NL: supervision, reviewing and editing.

Funding Partially funded by the Office of the Privacy Commissioner of Canada (OPC).

Data availability The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

Conflict of interest The authors have no conflicts of interest to declare.

Ethical approval This article does not contain any studies with human participants performed by any of the authors. Ethical committee approval: This study was approved by Research Ethics Board (REB). Survey participants agreed to participate in this research under the condition of anonymity of the respondents to the questionnaire used in this study.

Consent for publication All authors give consent to publish this manuscript.

References

- Ahmadi H, Nilashi M, Shahmoradi L, Ibrahim O (2017) Hospital information system adoption: expert perspectives on an adoption framework for Malaysian public hospitals. *Comput Hum Behav* 67:161–189
- Ainin S, Parveen F, Moghavvemi S, Jaafar NI, Mohd Shuib NL (2015) Factors influencing the use of social media by SMEs and its performance outcomes. *Ind Manag Data Syst* 115(3):570–588
- Ajzen I (1991) The theory of planned behavior. *Organ Behav Hum Decis Process* 50(2):179–211
- Alshamailla Y, Papagiannidis S, Li F (2013) Cloud computing adoption by SMEs in the northeast of England: a multi-perspective framework. *J Enterp Inf Manag* 26(3):250–275
- Angst CM, Block ES, D'arcy J, Kelley K (2017) When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Q* 41(3):893–916
- Ashraf AR, Thongpapanl (Tek) N, Spyropoulou S (2016) The connection and disconnection between e-commerce businesses and their customers: exploring the role of engagement, perceived usefulness, and perceived ease-of-use. *Electron Commer Res Appl* 20:69–86
- Au Y, Zafar H (2008) A multi-country assessment of mobile payment adoption. No. Wp# 00551S-296-2008, Texas. Available at: <https://api.semanticscholar.org/CorpusID:35575634>.
- Autry C, Grawe S, Daugherty P, Richey R (2010) The effects of technological turbulence and breadth on supply chain technology acceptance and adoption. *J Oper Manag* 28(6):522–536
- Awa H, Ojiabo U, Emecheta BC (2015) Integrating TAM, TPB, and TOE frameworks and expanding their characteristic constructs for e-commerce adoption by SMEs. *J Sci Technol Policy Manag* 6(1):76–94
- Awa H, Ojiabo U, Orokor L (2017) Integrated technology (T-O-E) taxonomies for technology adoption. *J Enterp Inf Manag* 30(6):893–921
- Benz M, Chatterjee D (2020) Calculated risk? A cybersecurity evaluation tool for SMEs. *Bus Horiz* 63(4):531–540
- Boateng R, Mbokoh A, Boateng L, Senyo P, Ansong E (2016) Determinants of E-learning adoption among students of developing countries. *Int J Inf Learn Technol* 33(4):248–262
- Bujang MA, Omar ED, Baharum NA (2018) A review on sample size determination for Cronbach's alpha test: a simple guide for researchers. *Malays J Med Sci* 25(6):85–99
- Caffaro F, Micheletti Cremasco M, Roccatto M, Cavallo E (2020) Drivers of farmers' intention to adopt technological innovations in Italy: the role of information sources, perceived usefulness, and perceived ease of use. *J Rural Stud* 76:264–271
- Cao Y, Ajjan H, Hong P, Le T (2018) Using social media for competitive business outcomes: an empirical study of companies in China. *J Adv Manag Res* 15(2):211–235
- Cavelty DM (2014) Breaking the cyber-security dilemma: aligning security needs and removing vulnerabilities. *Sci Eng Ethics* 20(3):701–715
- Cegielski CG, Bourrie MD, Hazen BT (2013) Evaluating adoption of emerging IT for corporate IT strategy: developing a model using a qualitative method. *Inf Syst Manag* 30(3):235–249
- Chandra S, Kumar K (2018) Exploring factors influencing organizational adoption of augmented reality in e-commerce: empirical analysis using technology–organization–environment model. *J Electron Commer Res* 19(3):237–265
- Chang YW, Chang PY, Xu Q, Ho KH, Halim WL (2016) An empirical investigation of switching intention to private cloud computing in large enterprises. 22nd Asia-Pacific Conference on Communications (APCC), Yogyakarta, Indonesia, 323–329, IEEE. <https://doi.org/10.1109/APCC.2016.7581451>
- Charlton AB, Cornwell TB (2019) Authenticity in horizontal marketing partnerships: a better measure of brand compatibility. *J Bus Res* 100:279–298
- Chatzoglou P, Chatzoudes D, Frigidis L, Symeonidis S (2017) Examining the critical success factors for ERP implementation: an explanatory study conducted in SMEs. In: Ziemba E (ed) *Information technology for management: new ideas and real solutions. ISM AITM 2016 2016*. Lecture notes in business information processing, 277. Springer, Cham
- Cheng T-H (2021) The empirical study of usability and credibility on intention usage of government-to-citizen services. *J Appl Data Sci* 2(2):36–44
- Chiu C, Chen S, Chen C (2017) An integrated perspective of TOE framework and innovation diffusion in broadband mobile applications adoption by enterprises. *J Manag Econ Soc Sci* 6(1):14–39

- Church L (2008) End user security: the democratisation of security usability. *Security and Human Behaviour*. www.academia.edu/1124860/End_User_Security_The_democratisation_of_security_usability
- CISOMAG (2020) Cybersecurity investment to increase by 6% in 2020: Canals. <https://cisomag.eccouncil.org/cybersecurity-spending-to-grow/>
- COSO (2012) Enterprise risk management for cloud computing. Committee of Sponsoring Organizations of the Trade way Commission (COSO), UK, 1–24.
- Daud M, Rasiah R, George M, Asirvatham D, Thangiah G (2018) Bridging the gap between organizational practices and cyber security compliance: can cooperation promote compliance in organizations? *Int J Bus Soc* 19(1):161–180
- Davis FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q: Manag Inf Syst* 13(3):319–339
- Davis FD, Bagozzi RP, Warshaw PR (1989) User acceptance of computer technology: a comparison of two theoretical models on JSTOR. *Manage Sci* 35(8):982–1003
- De Man AP, Luvison D (2019) Collaborative business models: aligning and operationalizing alliances. *Bus Horiz* 62(4):473–482
- DePietro R, Wiarda E, Fleischer M (1990) The context of change: organization, technology, and environment. *Process Technol Innov* 199:151–175
- Donthu N, Gustafsson A (2020) Effects of COVID-19 on business and research. *J Bus Res* 117:284–289
- Elia S, Massini S, Narula R (2019) Disintegration, modularity and entry mode choice: mirroring technical and organizational architectures in business functions offshoring. *J Bus Res* 103:417–431
- Eriksson PE, Larsson J, Pesamaa O (2017) Managing complex projects in the infrastructure sector—a structural equation model for flexibility-focused project management. *Int J Project Manag* 35(8):1512–1523
- FBI (2017) Ransomware Prevention and Response for CISOs. Retrieved from Federal Bureau of Investigation 2017. <https://www.fbi.gov>
- Furnell S, Clarke N (2012) Power to the people? The evolving recognition of human aspects of security. *Comput Secur*. <https://doi.org/10.1016/j.cose.2012.08.004>
- Gangwar H, Date H, Raoot A (2014) Review on IT adoption: insights from recent technologies. *J Enterp Inf Manag* 27(4):488–502
- Gangwar H, Date H, Ramaswamy R (2015) Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *J Enterp Inf Manag* 28(1):107–130
- Gao X, Zhong W (2016) A differential game approach to security investment and information sharing in a competitive environment. *IIE Trans* 48(6):511–526
- Gavrea C, Iliș L, Stegerea R (2011) Determinants of organizational performance: the case of Romania. *Manag Mark* 6(2):285–300
- Ghobakhloo M, Sabouri M, Hong T, Zulkifli N (2012) Information technology adoption in small and medium-sized enterprises; an appraisal of two decades literature. *Interdiscip J Res Bus* 1(7):53e80
- Gounaris S, Koritos C (2008) Investigating the drivers of internet banking adoption decision: a comparison of three alternative frameworks. *Int J Bank Mark* 26(5):282–304
- Grover P, Kar AK, Janssen M, Ilavarasan PV (2019) Perceived usefulness, ease of use and user acceptance of blockchain technology for digital transactions—insights from user-generated content on Twitter. *Enterp Inf Syst* 13(6):771–800
- Guadagnoli E, Velicer W (1988) Relation of sample size to the stability of component patterns. *Psychol Bull* 103(2):165–175
- Gutierrez A, Boukrami E, Lumsden R (2015) Technological, organizational and environmental factors influencing managers' decision to adopt cloud computing in the UK. *J Enterp Inf Manag* 28(6):788–807
- Gyde M (2017) Organizations must disrupt cyber attacks before. *bahrain this week*. Retrieved from, <https://www.bahrainthisweek.com>.
- Hair J, Black W, Babin B, Anderson R (2010) *Multivariate data analysis* (7th edition). Prentice Hall
- Hasan S, Ali M, KurniaThurasamy SR (2021) Evaluating the cyber security readiness of organizations and its influence on performance. *J Inf Secur Appl* 58:102726
- Hasani T, O'Reilly N (2021) Analyzing antecedents affecting the organizational performance of start-up businesses. *J Enterp Emerg Econ* 13(1):107–130
- Hasani T, Dehghantanha A, Bojei J (2017) Investigating the antecedents to the adoption of SCRM technologies by start-up companies. *Telematics Inform* 34(5):655–675
- Hathaway M (2013) *Cyber readiness index 1.0*. Hathaway Global Strategies LLC, Great Falls, VA

- Hazen BT, Byrd TA (2011) Logistics information technology adoption: the effect of a positive buyer-supplier relationship on performance outcomes. *PACIS*, p 76
- He W, Wang FK, Chen Y, Zha S (2017) An exploratory investigation of social media adoption by small businesses. *Inf Technol Manag* 18:149–160
- Hermanson DR, Tompkins JG, Veliyath R, Ye Z (2020) Strategic planning committees on U.S. public company boards: axiomatic or paradoxical? *Long Range Plan* 53(5):101967
- Hopkins M, Dehghantanha A (2016) Exploit kits: the production line of the cybercrime economy? In: 2015 2nd international conference on information security and cyber forensics, *InfoSec 2015*. <https://doi.org/10.1109/InfoSec.2015.7435501>
- Hsu C, Lee JN, Straub DW (2012) Institutional influences on information systems security innovations. *Inf Syst Res* 23(3):918–939
- Hsu P, Ray S, Li Y (2014) Examining cloud computing adoption intention, pricing mechanism, and deployment model. *Int J Inf Manag* 34(4):474–488
- Hussein RMS, Mourad M (2014) The adoption of technological innovations in a B2B context: an empirical study on the higher education industry in Egypt. *J Bus Ind Mark* 29(6):525–545
- Hwang K, Choi M (2017) Effects of innovation-supportive culture and organizational citizenship behavior on e-government information system security stemming from mimetic isomorphism. *Gov Inf Q* 34(2):183–198
- Izuagbe R, Ibrahim NA, Ogiemien LO, Olawoyin OR, Nwokeoma NM, Ilo PI, Osayande O (2019) Effect of perceived ease of use on librarians' e-skills: basis for library technology acceptance intention. *Libr Inf Sci Res* 41(3):100969
- James L (2018) Making cybersecurity a strategic business priority. *Netw Secur* 2018(5):6–8
- Ji H, Liang Y (2016) Exploring the determinants affecting e-government cloud adoption in China. *Int J Bus Manag* 11(4):81
- Johansson B, Ruivo P (2013) Exploring factors for adopting ERP as SaaS. *Proc Technol* 9(1):94–99
- Johnson RD, Diman K (2017) An investigation of the factors driving the adoption of cloud-based human resource information systems by small- and medium-sized businesses. *Electronic HRM in the smart era*. Emerald Publishing Limited, pp 1–31
- Joshi A, Gimenez E (2014) Decision-driven marketing. *Harv Bus Rev* 92(7):64–71
- Kaplan RS, Norton DP (1992) The balanced scorecard—measures that drive performance. *Harv Bus Rev* 70(1):71–79
- KasperskyLab (2018) KSN report: ransomware and malicious cryptominers 2016–2018. Retrieved from Kaspersky Business Hub, <https://cloud.kaspersky.com>.
- Kim D, Solomon M (2016) *Fundamentals of information systems security*. Jones and Bartlett Learning, Burlington, MA
- Kong HK, Kim TS, Kim J (2012) An analysis on effects of information security investments: a BSC perspective. *J Intell Manuf* 23(4):941–953
- Kraemer S, Carayon P, Clem J (2009) Human and organizational factors in computer and information security: pathways to vulnerabilities. *Comput Secur* 28(7):509–520
- Kurnia S, Karnali RJ, Rahim MM (2015) A qualitative study of business-to-business electronic commerce adoption within the Indonesian grocery industry: a multitheory perspective. *Inf Manag* 52(4):518–536
- Lai Y, Sun H, Ren J (2018) Understanding the determinants of big data analytics (BDA) adoption in logistics and supply chain management: an empirical investigation. *Int J Logist Manag* 29(2):676–703
- Laurell C, Sandström C, Berthold A, Larsson D (2019) Exploring barriers to adoption of virtual reality through social media analytics and machine learning – an assessment of technology, network, price and trialability. *J Bus Res* 100:469–474
- Li Y, Liu Q (2021) A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Rep* 7:8176–8186
- Li H, No WG, Wang T (2018) SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *Int J Account Inf Syst* 30:40–55
- Li L, He W, Xu L, Ash I, Anwar M, Yuan X (2019) Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *Int J Inf Manag* 45:13–24
- Lim BT, Ling FY, Ibbs CW, Raphael B, Ofori G (2011) Empirical analysis of the determinants of organizational flexibility in the construction business. *J Constr Eng Manag* 137(3):225–237
- Lin A, Chen NC (2012) Cloud computing as an innovation: perception, attitude, and adoption. *Int J Inf Manag* 32(6):533–540

- Liu N, Nikitas A, Parkinson S (2020) Exploring expert perceptions about the cyber security and privacy of connected and autonomous vehicles: a thematic analysis approach. *Transp Res part F: Traffic Psychol Behav* 75:66–86
- Lloyd G (2020) The business benefits of cyber security for SMEs. *Comput Fraud Secur* 2020(2):14–17
- Loi R, Lin X, Tan AJM (2019) Powered to craft? The roles of flexibility and perceived organizational support. *J Bus Res* 104:61–68
- Lu H, Pishdad-Bozorgi P, Wang G, Xue Y, Tan D (2019) ICT implementation of small- and medium-sized construction enterprises: organizational characteristics, driving forces, and value perceptions. *Sustainability* 11(12):3441
- Maduku DK, Mpinganjira M, Duh H (2016) Understanding mobile marketing adoption intention by South African SMEs: a multi-perspective framework. *Int J Inf Manag* 36(5):711–723
- Martin-Rojas R, Garcia-Morales VJ, Gonzalez-Alvarez N (2019) Technological antecedents of entrepreneurship and its consequences for organizational performance. *Technol Forecast Soc Chang* 147:22–35
- McManus S, Seville E, Vargo J, Brunson D (2008) Facilitated process for improving organizational resilience. *Nat Hazard Rev* 9(2):81–90
- Mican D, Sitar-Tăut DA, Moisescu OI (2020) Perceived usefulness: a silver bullet to assure user data availability for online recommendation systems. *Decis Support Syst* 9:113420
- Mohd Amir RI, Mohd IH, Saad S, Abu Seman SA, Tuan Besar TBH (2020) Perceived ease of use, perceived usefulness, and behavioral intention: the acceptance of crowdsourcing platform by using technology acceptance model (TAM). Charting a sustainable future of ASEAN in business and social sciences. Springer, pp 403–410
- Molinillo S, Japutra A (2017) Organizational adoption of digital information and technology: a theoretical review. *Bottom Line* 30(1):33–46
- Morgan S (2021) Top 5 cybersecurity facts, figures, predictions, and statistics for 2020 To 2021. <https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021/>.
- Nicholson S (2019) How ethical hacking can protect organizations from a greater threat. *Comput Fraud Secur* 2019(5):15–19
- Njenga K, Jordaan P (2016) We want to do it our way: the neutralization approach to managing information systems security by small businesses. *Afr J Inf Syst* 8(1):41–63
- Oh K, Cruickshank D, Anderson A (2009) The adoption of e-trade innovations by Korean small and medium sized firms. *Technovation* 29(2):110–121
- Oliveira T, Martins MF (2011) Literature review of information technology adoption models at firm level. *Electron J Inf Syst Eval* 14(1):110–121
- Oorschot J, Hofman E, Halman J (2018) A bibliometric review of the innovation adoption literature. *Technol Forecast Soc Chang* 134:1–21
- Ouiridi ME, Ouiridi AE, Segers J, Pais I (2016) Technology adoption in employee recruitment: the case of social media in Central and Eastern Europe. *Comput Hum Behav* 57:240–249
- Owusu A (2017) Business intelligence systems and bank performance in Ghana: the balanced scorecard approach. *Cogent Bus Manag*. <https://doi.org/10.1080/23311975.2017.1364056>
- Pala A, Zhuang J (2019) Information sharing in cybersecurity: a review. *Decis Anal* 16(3):172–196
- Pan MJ, Jang WY (2008) Determinants of the adoption of enterprise resource planning within the technology-organization-environment framework: Taiwan's communications industry. *J Comput Inf Syst* 48(3):94–102
- Park Y, El Sawy OA, Fiss PC (2017) The role of business intelligence and communication technologies in organizational agility: a configurational approach. *J Assoc Inf Syst* 18(9):648–686
- Pearson N (2014) A larger problem: financial and reputational risks. *Comput Fraud Secur* 2014(4):11–13
- Pejic M, Celjo A, Zoroja J (2016) Technology acceptance model for business intelligence systems: preliminary research. *Proc Comput Sci* 100:995–1001
- Plewa C, Troshani I, Francis A, Rampersad G (2012) Technology adoption and performance impact in innovation domains. *Ind Manag Data Syst* 112(5):748–765
- Prasad A, Green P (2015) Governing cloud computing services: reconsideration of IT governance structures. *Int J Account Inf Syst* 19:45–58
- Qin X, Shi Y, Lyu K, Mo Y (2020) Using a Tam-Toe model to explore factors of building information modelling (BIM) adoption in the construction industry. *J Civ Eng Manag* 26(3):259–277

- Quigley K, Burns C, Stallard K (2015) Cyber Gurus': a rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Gov Inf Q* 32(2):108–117
- Raguseo E, Vitari C (2018) Investments in big data analytics and firm performance: an empirical investigation of direct and mediating effects. *Int J Prod Res* 56(15):5206–5221
- Rahayu R, Day J (2015) Determinant factors of e-commerce adoption by SMEs in developing country: evidence from Indonesia. *Proc Soc Behav Sci* 195:142–150
- Rai A, Patnayakuni R, Seth N (2006) Firm performance impacts of digitally-enabled supply chain integration capabilities. *MIS Q* 30(2):225–246
- Ramayah T, Ling NS, Taghizadeh SK, Rahman SA (2016) Factors influencing SMEs website continuance intention in Malaysia. *Telemat Inf* 33(1):150164
- Ramdani B, Chevers D, Williams DA (2013) SMEs' adoption of enterprise applications: a technology-organization-environment model. *J Small Bus Enterp Dev* 20(4):735–753
- Reuver M, Sørensen C, Basole RC (2018) The digital platform: a research agenda. *J Inf Technol* 33(2):124–135
- Rindasu SM (2017) Emerging information technologies in accounting and related security risks—what is the impact on the Romanian accounting profession. *J Account Manag Inf Syst* 16(4):581–609
- Rioli L, Savicki V (2003) Information system organizational resilience. *Omega* 31(3):227–233
- Rodriguez M, Trainor K (2016) A conceptual model of the drivers and outcomes of mobile CRM application adoption. *J Res Interact Mark* 10(1):67–84
- Rogers EM (2003) *Diffusion of innovations*, 5th edn. Simon and Schuster, New York, NY, USA
- Rosenberg N (1983) *Inside the black box: technology and economics*. Cambridge University Press, London
- Sallehudin H, Razak RC, Ismail M (2015) Factors influencing cloud computing adoption in the public sector: an empirical analysis. *J Entrep Bus* 3(1):30–45
- San-Martina S, Jiménez NH, López-Catalán B (2016) The firms benefits of mobile CRM from the relationship marketing approach and the TOE model. *Span J Mark-ESIC* 20(1):18–29
- Senyo PK, Effah J, Addae E (2016) Preliminary insight into cloud computing adoption in a developing country. *J Enterp Inf Manag* 29(4):505–524
- Shee H, Miah SJ, Fairfield L, Pujawan N (2018) The impact of cloud-enabled process integration on supply chain performance and firm sustainability: the moderating role of top management. *Supply Chain Manag* 23(6):500–517
- Shen H, Lan F, Xiong H, Lv J, Jian J (2020) Does top management team's academic experience promote corporate innovation? Evidence from China. *Econ Model* 89:464–475
- Sila I (2013) Factors affecting the adoption of B2B e-commerce. *Electron Commer Res* 13(2):199–236
- Simola J (2019) Comparative research of cybersecurity information sharing models. *Inf Secur: Int J* 43(2):175–195
- Singh SK, Gupta S, Busso D, Kamboj S (2019) Top management knowledge value, knowledge sharing practices, open innovation and organizational performance. *J Bus Res* 128:788–798
- Smith GE, Watson KJ, Baker WH, Pokorski IJJA (2007) A critical balance: collaboration and security in the IT-enabled supply chain. *Int J Prod Res* 45(11):2595–2613
- Smith S, Winchester D, Bunker D, Jamieson R (2010) Circuits of power: a study of mandated compliance to an information systems security" De Jure" standard in a government organization. *MIS Q* 34(3):463–486
- Sophonthummapharn K (2009) The adoption of techno-relationship innovations: a framework for electronic customer relationship management. *Mark Intell Plan* 27(3):380–412
- Su W-J (2021) The effects of safety management systems, attitude and commitment on safety behaviors and performance. *Int J Appl Inf Manag* 1(4):187–199
- Suroso JS, Hwa TH, Syafaat R, Pasaribu FA, Mujiatun S (2019) Assessing an information security governance using IPPF in multi-finance company. *Int Conf Inf Manag Technol (ICIMTech)* 9:596–601
- Tiwana A, Konsynski B (2010) Complementarities between organizational IT architecture and governance structure. *Inf Syst Res* 21(2):288–304
- Tsai M, Lee W, Wu H (2010) Determinants of RFID adoption intention: evidence from Taiwanese retail chains. *Inf Manag* 47(5–6):255–261
- Tsou HT, Hsu SHY (2015) Performance effects of technology–organization–environment openness, service co-production, and digital-resource readiness: the case of the IT industry. *Int J Inf Manage* 35(1):1–14

- Turel O, Bart C (2014) Board-level IT governance and organizational performance. *Eur J Inf Syst* 23(2):223–239
- Valkohammadi C, Ahmadi M (2015) The impact of knowledge management practices on organizational performance: a balanced scorecard approach. *J Enterp Inf Manag* 28(1):131–159
- Venkatesh V, Bala H (2012) Adoption and impacts of interorganizational business process standards: role of partnering synergy. *Inf Syst Res* 23(4):1131–1157
- Venkatesh V, Morris MG, Davis GB, Davis FD (2003) User acceptance of information technology: toward a unified view. *MIS Q: Manag Inf Syst* 27(3):425–478
- Wall JD, Lowry PB, Barlow JB (2016) Organizational violations of externally governed privacy and security rules: explaining and predicting selective violations under conditions of strain and excess. *J Assoc Inf Syst* 17(1):39–76
- Wallace S, Green KY, Johnson C, Cooper J, Gilstrap C (2020) An extended TOE framework for cybersecurity-adoption decisions. *Commun Assoc Inf Syst* 47:338–363
- Wang YS, Li HT, Li CR, Zhang DZ (2016) Factors affecting hotels' adoption of mobile reservation systems: a technology-organization-environment framework. *Tour Manag* 53:163–172
- Wu IL, Chen JL (2014) Knowledge management driven firm performance: the roles of business process capabilities and organizational learning. *J Knowl Manag* 18(6):1141–1164
- Wu MY, Wang Y (2014) The benefits of unified communications for small business. *Int J Electron Bus Manag* 12(4):236–246
- Yang Z, Sun J, Zhang Y, Wang Y (2015) Understanding SaaS adoption from the perspective of organizational users: a tripod readiness model. *Comput Hum Behav* 45:254–264
- Yenipazarli A (2019) Incentives for environmental research and development: consumer preferences, competitive pressure and emissions taxation. *Eur J Oper Res* 276(2):757–769
- Yi M, Jackson J, Park J, Probst J (2006) Understanding information technology acceptance by individual professionals: toward an integrative view. *Inf Manag* 43(3):350–363
- Yuan XW, Yi JB (2011) Environment characteristics, top management styles and organizational outcomes: a fit perspective. *Commun Comput Inf Sci* 233:54–63
- Yun C (2020) Early innovation adoption: effects of performance-based motivation and organizational characteristics. *Public Perform Manag Rev* 43(4):790–817
- Zhu K, Kraemer K (2005) Post-adoption variations in usage and value of e-business by organizations: cross-country evidence from the retail industry. *Inf Syst Res* 16(1):61–84
- Zimmermann V, Renaud K (2019) Moving from a 'human-as-problem' to a 'human-as-solution' cybersecuritymindset. *International Journal of Human-Computer Studies* 131: 169–187

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.