

When protection enables innovation: cybersecurity and digitalization in SMEs through the lens of protection motivation theory

Carlos F.A. Arranz¹, Marta F. Arroyabe^{2,*}, Ignacio Fernandez de Arroyabe³

¹School of Business, Operations, and Strategy (BOS), Greenwich Business School, University of Greenwich, London, SE10 9LS, United Kingdom

²Essex Business School, University of Essex, Colchester, CO4 3SQ, United Kingdom

³Chief Controls Office, Lloyds Bank Commercial Banking, London, EC2N 1HZ, United Kingdom

*Corresponding author. Essex Business School, University of Essex, Colchester, CO4 3SQ, United Kingdom. E-mail: mf17255@essex.ac.uk

Abstract

This study examines the relationship between cybersecurity and the digitalization of small and medium-sized enterprises (SMEs). Digitalization is conceptualized as a gradual, path-dependent process in which firms adopt digital technologies over time, increasing both connectivity and exposure to cyber threats. Drawing on protection motivation theory (PMT), we interpret digitalization as a form of motivated protective behavior shaped by two cognitive mechanisms: threat appraisal and coping appraisal. To investigate this relationship, we conducted a survey of 239 UK-based SMEs in 2022 and analyzed the data using regression models and artificial neural networks (ANN). The findings show that cybersecurity practices are significantly and positively associated with digitalization, but their association varies depending on SMEs' digital maturity. At early stages, digitalization is driven primarily by perceived cyber risk, whereas at more advanced stages, established cybersecurity routines and standards act as enablers of further digital adoption. This study contributes to the literature by extending PMT to the organizational level and demonstrating that cybersecurity is not merely a constraint or protective add-on, but a central mechanism shaping digital transformation in SMEs.

Keywords digitalization, cybersecurity, protection motivation theory, SMEs, machine learning

Introduction

The digitalization of companies increasingly relies on the adoption of emerging technologies such as cloud computing, big data, artificial intelligence (AI), machine learning (ML), robotics, smart devices, and blockchain [1,2]. These technologies enable firms to enhance productivity, efficiency, and innovation by automating processes, generating insights from data, and connecting with partners, customers, and infrastructures in real time [3–5]. In particular, the Internet of Things (IoT) and smart systems frameworks expand digitalization beyond internal systems, embedding computational power and connectivity in physical assets. Through sensors, distributed networks, and cloud infrastructures, companies become part of a broader digital ecosystem, facilitating access to information and new markets [6,7].

However, this growing interconnectivity introduces new vulnerabilities. As digital infrastructures expand, so too does the exposure of firms to cybersecurity incidents, including malware, phishing, denial-of-service attacks, ransomware, and tampering, particularly through poorly secured devices, platforms, or interfaces [8,9]. The increasing reliance on external networks, remote systems, and data sharing makes digitalized firms attractive and vulnerable targets [10]. As such, cybersecurity has emerged not only as a technical safeguard but as a strategic capability that is founda-

tional to business continuity, resilience, and digital transformation [11–13].

Despite the increasing relevance of cybersecurity in digital environments, its role in shaping the adoption of digital technologies remains contested. On one hand, several studies frame cybersecurity as a barrier to digitalization, citing concerns about cost, complexity, regulatory compliance, and potential operational disruptions [10,11]. From this perspective, technologies such as big data analytics, cloud platforms, robotics, or smart devices raise the stakes for companies by increasing the surface area for attacks. As firms weigh the costs of implementing adequate protective systems, particularly under regulatory constraints such as the GDPR, digitalization may be delayed or avoided altogether [14,15].

Conversely, a growing body of work suggests that cybersecurity can act as an enabler of digitalization, particularly when it is institutionalized through formal standards and integrated into organizational processes. Firms that implement cybersecurity routines (e.g. ISO 27001, Cyber Essentials, or internal governance mechanisms) may be more confident in adopting new digital technologies, knowing they have systems in place to mitigate associated risks [12,16,17]. In this view, cybersecurity enhances managerial control and trust, allowing firms to use technologies such as blockchain and secure cloud storage not only for efficiency but also as protection mechanisms against cyber threats [18,19].

Received: 11 November 2025. Revised: 6 July 2026. Accepted: 24 August 2026

© The Author(s) 2026. Published by Oxford University Press. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted reuse, distribution, and reproduction in any medium, provided the original work is properly cited.

This debate reveals a critical gap in literature: while digitalization and cybersecurity are increasingly intertwined, few studies have examined their relationship as a function of firm-level decision-making and perception. This is particularly true for small and medium-sized enterprises (SMEs), which face distinct challenges. SMEs often lack dedicated IT departments, operate with constrained resources, and rely heavily on the judgment of owner-managers, making them especially sensitive to both the perceived risks and benefits of digitalization [2,20]. At the same time, SMEs represent the backbone of many economies and are increasingly being targeted by cybercriminals due to their perceived vulnerabilities and lower levels of preparedness [10].

To address this gap, this study draws on protection motivation theory (PMT) to investigate the relationship between cybersecurity perceptions and practices and digital technology adoption in SMEs. PMT, originally developed to explain health behavior [21], has since been widely applied to cybersecurity at the individual level [22–24]. It posits that protective behaviors are driven by two sets of cognitive appraisals: threat appraisal, which considers the severity and vulnerability of a threat, and coping appraisal, which reflects the perceived efficacy of the response, the firm's ability to carry it out, and the associated costs. While PMT has been used extensively to understand user adoption of security behaviors, its application to organizational technology adoption remains limited [25,26]. For our study, PMT is the most appropriate theoretical lens for this context because it uniquely captures the cognitive risk perceptions and behavioral coping mechanisms that drive decision-making under uncertainty.

This study extends PMT to the organizational level, interpreting digitalization as a motivated protective behavior undertaken in response to cybersecurity threats. Firms may adopt digital technologies both as a means of protection and as an enabler of operational performance, but only if they believe they have the capabilities to manage cyber risks. The study also recognizes that digitalization is not binary, but a cumulative, dynamic process in which firms progressively integrate more complex technologies as they build competence and resilience. In doing so, the relationship between cybersecurity and digitalization may vary depending on the firm's stage of digital maturity. Operationally, this study defines a firm's digital maturity by the breadth of its digital integration, measured as the cumulative number of digital technologies the firm has adopted [2].

To explore these dynamics, we focus on two key research questions: are SMEs' perceptions of cybersecurity threat and coping capacity associated with their level of digitalization, and do these relationships vary across SMEs at different stages of digital maturity? To address these questions, we conducted a national survey of 239 SMEs in the UK in 2022 and analyzed the data using both regression models and artificial neural networks (ANN).

This paper makes several contributions. Theoretically, it extends PMT to the domain of SME digital transformation, showing how both perceived risk and organizational preparedness shape digitalization behavior. Empirically, it distinguishes between multiple dimensions of coping appraisal (technical controls, managerial practices, and formal standards) and demonstrates how these influence digitalization in different ways. It also shows that this influence is not uniform: the impact of cybersecurity varies significantly across firms with different digital maturity profiles, revealing heterogeneous patterns of motivation and response. Methodologically, the study combines causal and predictive techniques

to capture both linear and nonlinear dynamics in cybersecurity decision-making. In doing so, it contributes to a better understanding of how cybersecurity concerns shape the digital futures of SMEs.

Conceptual framework

This section outlines the theoretical foundation of the study, which is anchored in PMT [21]. We select PMT as our primary theoretical lens because it uniquely centers on the cognitive and behavioral mechanisms of decision-making under uncertainty, interpreting digitalization not merely as an operational upgrade, but as a motivated protective response to cybersecurity threats. While alternative frameworks offer valuable insights into organizational change and technology adoption, they do not fully capture these specific risk-driven mechanisms. For instance, the Technology–Organization–Environment (TOE) framework primarily explains how structural, environmental, and technological contexts influence an organization's adoption decisions [27]. Similarly, the dynamic capabilities perspective emphasizes a firm's overarching capacity to sense opportunities, seize them, and reconfigure internal competencies to adapt to rapidly changing environments [28]. Although these perspectives are highly relevant, they largely treat factors like cybersecurity as a contextual constraint or an operational requirement. In contrast, PMT allows us to map exactly how perceived risk (threat appraisal) and organizational preparedness (coping appraisal) directly motivate or stall technological integration. Thus, PMT provides a more precise framework for understanding the interdependent evolution of digitalization and cybersecurity in SMEs.

PMT and digital technology adoption

PMT was originally developed by Rogers (1975) [21] to explain how individuals engage in protective behaviors in response to perceived health threats. It has since been adapted to various domains, particularly in the field of cybersecurity, where it helps explain the cognitive mechanisms behind security-related decision-making [22,24]. PMT proposes that protective behaviors are the result of two parallel cognitive evaluations: threat appraisal and coping appraisal [29,30].

Threat appraisal refers to the individual or organization's evaluation of the risk posed by a particular threat. It comprises two components: perceived severity, or the extent to which the consequences of a threat are judged to be serious, and perceived vulnerability, which is the perceived likelihood that the threat will affect them [23,31]. In cybersecurity contexts, this might relate to the perceived business impact of a data breach or the likelihood of being targeted by phishing, malware, or ransomware attacks [32,33]. Previous research has shown that perceived threat alone does not always lead to protective behavior, but rather it must be accompanied by the belief that effective countermeasures are available and achievable [34].

In this context, the coping appraisal mechanisms are critical. Coping appraisal comprises three elements: response efficacy, or the perceived effectiveness of a recommended security measure; self-efficacy, or the belief in one's ability to successfully implement that measure; and response cost, or the perceived barriers such as time, effort, or financial resources required to act [22,30]. In

organizational settings, these elements manifest as managerial confidence in cybersecurity tools, the presence of internal capabilities to implement and maintain protective systems, and the perceived burden of adopting and integrating such measures into business operations [29].

Although PMT has primarily been used to study individual user behavior (e.g. password hygiene and secure browsing), recent scholarship has emphasized its potential for explaining organizational-level decision-making, particularly in the context of digital transformation and cybersecurity [25,26]. From this perspective, digitalization itself can be conceptualized as a form of motivated protective behavior. That is, firms may choose to adopt digital technologies not only for efficiency or productivity gains but also as a way to build resilience, maintain operational continuity, and safeguard assets in increasingly hostile cyber environments.

In practice, the digitalization of companies is carried out through the incorporation of digital technologies such as big data, cloud computing, AI, ML, smart devices, robotics, data analytics, and blockchain. These technologies involve the integration of intelligent machines, storage systems, and smart production infrastructures, which are often enabled through wireless sensor networks, communication protocols, and distributed control systems [2]. Digital technologies, when combined with production and management systems, serve as the backbone of digital transformation, increasing efficiency, traceability, and responsiveness across supply chains and operational processes [3,6,35,36]. However, the adoption of these technologies also introduces new vulnerabilities. The deployment of IoT devices, for example, expands the attack surface and raises the likelihood of data breaches, while the integration of cloud platforms raises concerns about privacy, access control, and regulatory compliance [12]. As a result, decisions about whether and how to adopt digital technologies are increasingly conditioned by cybersecurity risk perceptions and organizational capacity to manage those risks.

This theoretical lens positions PMT as particularly useful in explaining heterogeneous digital adoption patterns among SMEs, who often lack formal IT departments and face acute resource constraints. In these firms, decision-makers are typically owners or senior managers whose perceptions of cyber threat severity, their confidence in available protections, and their willingness to absorb associated costs strongly shape the trajectory of digitalization. PMT provides a structured framework for evaluating how these perceptions translate into action, revealing the cognitive drivers of both adoption and avoidance in cybersecurity-intensive environments.

Cybersecurity in the firms

As explained above, the adoption of digital technologies involves the interconnection of organizations, leading to an increase in network-based activities. They are also increasingly exposed to cybersecurity incidents [15,37]. Companies are exposed to cybersecurity attacks, which are constantly growing, becoming more sophisticated, and diversifying in nature [10,14,38]. The literature identifies different types of cybersecurity attacks that use various techniques, including phishing, malware or web attacks, and the exploitation of vulnerabilities arising from the incorrect use of IT systems within organizations. The European Union Agency for Cybersecurity (ENISA) has classified various types of attacks in cy-

berspace [39], including malware, which accounts for 30% of all cyberattacks. Other attacks include website and domain attacks to steal personal information and bank details, as well as phishing attempts that seek to impersonate identities and deploy malware. Apart from external attacks, internal staff can also cause security breaches, either intentionally or unintentionally. ENISA [39] highlights the importance of this type of threat, noting that 77% of data leaks in firms result from internal sources. These cybersecurity incidents have an impact on SMEs in the form of disruptions, which can affect business operations and hinder staff from carrying out their daily work [10]. The cybersecurity impact not only results in economic losses for SMEs but can also have repercussions on their reputation and legal liabilities. For example, data breaches and noncompliance with the General Data Protection Regulation (GDPR) can lead to legal consequences and financial penalties for SMEs.

Against this backdrop, cybersecurity in organizations intends to protect IT systems, consisting of a set of measures, strategies and procedures aimed at alleviating the risks and vulnerabilities of information systems [17]. These actions can be of an operative nature, or even of a strategic and organizational nature [40]. First, there are cybersecurity control mechanisms, where the firm develops cybersecurity routines and procedures, developing activities such as software updates, the use of firewalls and identification routines, as well as network security measures, which can be combined with secure communication methods such as VPN and data encryption [10]. Second, companies introduce measures of an organizational and strategic nature concerning their cybersecurity (cybersecurity management), such as the assignment of teams for the management of information security, development of policies and cybersecurity risk assessment systems (for example, ISO 27000s, Cyber essentials), or the inclusion of cybersecurity issues in the meetings of the senior managers of the companies [40]. In this regard, companies find cybersecurity standards to be a mechanism that facilitates the establishment of procedures, processes, and routines within organizations to ensure the proper protection of the firms. This is the case with international standards such as ISO 27000 [17] and UK Cyber Essentials [41]. These standards provide guidelines and best practices for companies to enhance their cybersecurity measures and ensure the security of their systems, data, and networks. Implementing these standards can help SMEs establish a strong cybersecurity framework and demonstrate their commitment to protecting sensitive information and mitigating cyber risks.

Research questions

Drawing on PMT, we conceptualize the digitalization of SMEs as a motivated protective behavior, undertaken in response to perceived cybersecurity threats and the organization's perceived ability to manage those threats [21,22,24]. PMT posits that protective actions emerge through two cognitive evaluations: threat appraisal and coping appraisal. Threat appraisal refers to perceived severity and vulnerability to cyber incidents, while coping appraisal reflects beliefs about the effectiveness of protective actions (response efficacy), the firm's capability to carry them out (self-efficacy), and the costs associated with such actions (response cost) [23,26,29].

To operationalize PMT in the context of SME digitalization, we examine four interrelated dimensions of cybersecurity capac-

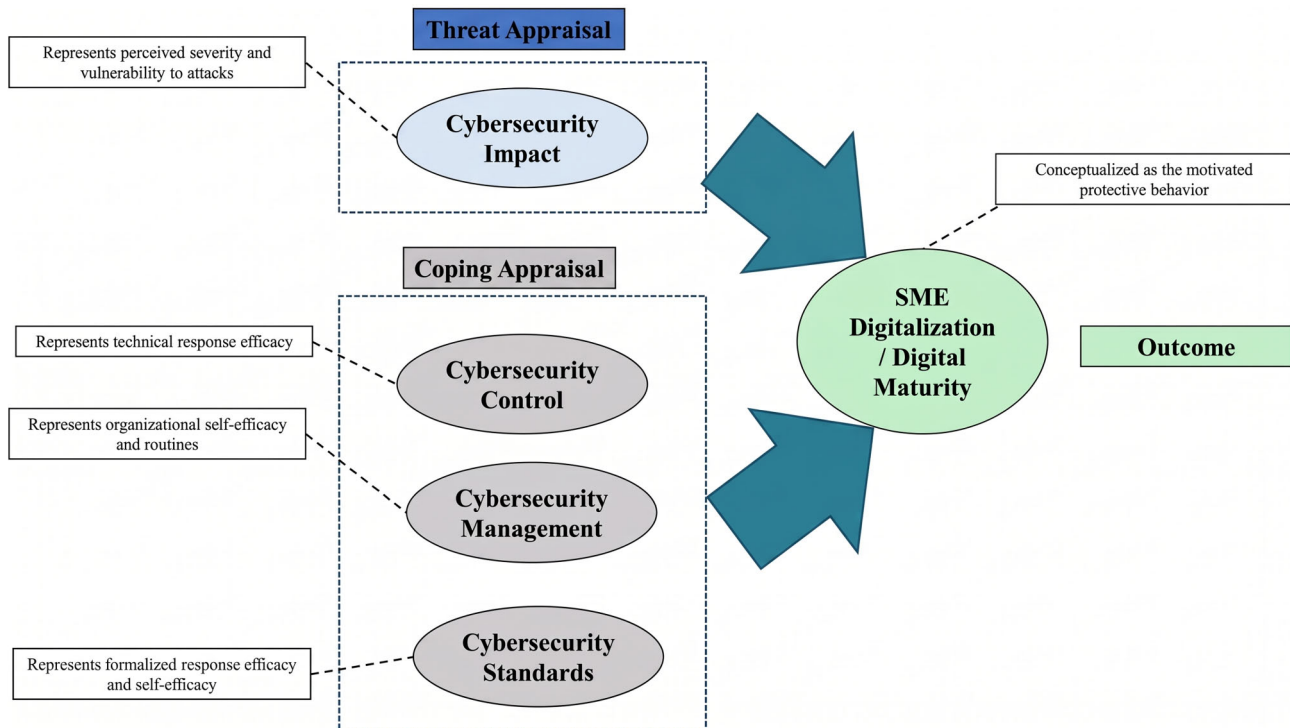


Figure 1 Conceptual framework.

ity: *cybersecurity control*, *cybersecurity management*, *cybersecurity impact*, and *cybersecurity standards*.

Cybersecurity control refers to the deployment of technical safeguards, including firewalls, malware detection systems, intrusion monitoring tools, and encryption protocols. These controls enhance response efficacy by reducing the likelihood and impact of cyber incidents [11,13]. However, maintaining and updating such systems may also introduce response costs, particularly in SMEs that lack specialized IT personnel [20,42]. Thus, depending on perceived capabilities, cybersecurity controls may either enable or inhibit further digitalization.

Cybersecurity management reflects the organizational routines, such as role assignments, security awareness training, monitoring practices, incident response planning, and internal accountability structures. These managerial practices contribute to self-efficacy, as they help SMEs internalize procedures for preventing, detecting, and responding to cyber threats [10,15]. Yet, building such routines requires time, learning, and investment that may be perceived as effort costs, especially in smaller firms with stretched managerial capacity [43].

Cybersecurity impact captures managers' perceptions of the severity and probability of cyberattacks and their economic, operational, reputational, and legal ramifications. SMEs often underestimate their own vulnerability, assuming they are "too small" to be targeted, which reduces perceived threat and thus weakens protective motivation [16,20,44]. However, as cyberattacks increasingly propagate opportunistically through supply chains, breaches involving SMEs have become more common, heightening awareness of potential harm [19,45]. When perceived threat severity outweighs perceived coping capability, SMEs may avoid digitalization due to fear of exposure [8]. Conversely, when coping capacity is perceived as high, threat awareness may motivate investment in secure digital infrastructures [24,33].

Cybersecurity standards, such as ISO/IEC 27002, NIST CSF, and GDPR-aligned data practices, provide codified protective procedures that formalize cybersecurity governance. Implementing such standards strengthens both response efficacy (confidence that controls are effective) and self-efficacy (confidence in the organization's ability to manage cyber risks) [15,17]. However, certification processes and compliance audits require financial resources, skilled personnel, and time, which create response cost barriers that are amplified in SMEs [46].

Importantly, digitalization in SMEs is not a singular adoption event but a cumulative, path-dependent transformation, where firms gradually incorporate increasingly complex digital tools, such as cloud computing, data analytics, AI-enabled decision support, IoT devices, and blockchain-based applications, as capabilities and routines develop [2,35]. Therefore, SMEs at different digital maturity levels will differ in their perceived threat severity, coping capacity, and response costs. Digitally nascent firms may view cybersecurity as a constraint, while digitally mature firms may leverage cybersecurity practices to enable further digitalization [3,18].

Hence, we propose the following research questions (see Fig. 1):

- Research Question 1a (RQ1a): Do SMEs' perceptions of cybersecurity threat and coping capacity associated with their level of digitalization?
- Research Question 1b (RQ1b): Do these associations vary across SMEs at different stages of digital maturity?

Methodology and data

Data

To address our research questions, we administered a survey targeting SMEs in the UK. The sample was drawn from the Govern-

Table 1 Distribution by Standard Industrial Classification (SIC) codes.

SIC section	Sector (simplified)	Percentage (%)
A	Agriculture	1
C	Manufacturing	8
E	Utilities and waste	0
F	Construction	6
G	Wholesale and retail	9
H	Transport and storage	3
I	Accommodation and food	3
J	Information and communication	17
K	Financial services	3
L	Real estate	1
M	Professional, scientific, and technical	20
N	Administrative and support	8
O	Public administration	0
P	Education	3
Q	Health and social work	4
R	Arts and recreation	6
S	Other services	5
T	Households	0
U	Extraterritorial	2
Total		100

ment's Inter-Departmental Business Register, which includes organizations from all sectors of the UK economy. A random probability sampling approach was used to reduce selection bias, with an initial target population of 1000 SMEs. Data collection took place between February and May 2022, covering the period from 2019 to 2022. The survey was conducted online in two waves. After reviewing the returned questionnaires and excluding nonresponses and incomplete entries, the final dataset used for analysis comprised 239 SMEs. The distribution of the sample is made up of a high percentage (77.8%) of microenterprises (1–9 employees), with less representation (16.4%) of small companies (10–49 employees), and lastly, medium-sized companies (50–249 employees), with 5.8%. Regarding the sectoral distribution, following SIC classification, we find 19 sectors represented, finding a very balanced sample (see Table 1). Thus, the most represented sectors are *professional, scientific, and technical activities* (SIC: 74 909), *agents involved in the sale of a variety of goods* (SIC: 46 190), *manufacture of loaded electronic boards activities* (SIC: 26 120), *business support service activities* (SIC: 82 990), *human health activities* (SIC: 86 900), *amusement and recreation activities* (SIC: 93 290), and *repair of computers and peripheral equipment* (95 110). Finally, we have found a homogeneous geographical distribution of the sample across the UK.

Measures

The first variable of our research captures digital technologies. In this study, a firm's digital maturity is operationalized as its *degree of digitalization*, which is considered the degree of penetration of digital technologies in SMEs. A higher cumulative number of digital technologies used by SMEs corresponds to a greater degree of

digital maturity. Following previous studies, we employ a multi-item question asking which of the following *digital technologies* has your enterprise adopted?, containing multi-item options: (i) AI; (ii) Cloud computing; (iii) Robotics; (iv) Smart devices; (v) Big data analytics; (vi) High-speed infrastructure; and (vii) Blockchain [2,5].

The second group of variables refers to the management of cybersecurity in SMEs. Previous works [10] classify cybersecurity actions in two variables. The first variable refers to the cybersecurity processes and routines used in the period 2019–2022 (*cybercontrols*), using a multi-item question. The items chosen in this question are: (i) Regular software updates (including patching); (ii) Encrypting or securing data; (iii) Malware protection; (iv) Use of VPN; (v) Firewalls and network security; (vi) Identity and Access Management; (vii) Physical security controls on firm-owned devices; (viii) Only allowing access via firm-owned devices; (ix) A segregated guest wireless network; and (x) Regular backing up data securely. The second variable refers to the strategic and organizational measures in the implementation of cybersecurity in SMEs (*cybermanagement*), during the period 2019–2022. The question is multi-item: (i) An outsourced provider that manages your cybersecurity; (ii) Staff members with information security or governance responsibilities; (iii) A formal policy or policies in place covering cybersecurity risks; (iv) Invested in threat intelligence; (v) An independent cybersecurity assessment; (vi) Any business-as-usual health checks that are undertaken regularly; and (vii) Formal cybersecurity discussions with the CEO, board or equivalent. Both *cybercontrols* and *cybermanagement* were constructed as cumulative indices based on the total number of measures each SME adopted.

The next variable refers to the cybersecurity impacts in economic and management terms in SMEs (*cyberimpacts*). In line with the literature by Fernandez de Arroyabe and Fernandez de Arroyabe [10] and drawing on the taxonomy proposed by Agrafiotis *et al.* [47], we consider the following incidents generated: (i) Stopped the business-as-usual activities; (ii) Negative impact on the revenue or share value; (iii) Repair or recovery costs; (iv) Fines from regulators or authorities, or associated legal costs; and (v) Reputational damage and loss of customer trust. Consistent with the previous variables, *cyberimpacts* was constructed as a cumulative index representing the breadth of incidents experienced.

The last variable is the possession of the cybersecurity standards (*cyberstandards*). The question posed was: Has your organization adopted the International Standard for Information Security Management (ISO 27001) or Cyber Essential (note, the ISO 27001 is an international standard to manage information security from the International Organization for Standardization (ISO), while Cyber Essentials is a UK Government backed scheme to certify firms have a minimum level of cyber security.)? The variable is measured by a Likert scale from 1 to 4, being 1 (No, I am not aware of these certifications); 2 (No, and do not intend to do so); 3 (No, but is intending to do so); and 4 (Yes).

Methods

To test our research questions, we employed a two-stage analytical strategy combining regression analysis and ANN. This approach balances the interpretability and inferential power of regression with the exploratory and pattern-recognition capabilities of ANN, especially for identifying nonlinear relationships

and interactions between cybersecurity and digitalization factors [48,49].

Regression models were used to estimate the effects of cybersecurity factors on digitalization levels and to test the significance of each dimension. However, due to potential issues of collinearity and unbalanced response rates, particularly regarding incident-related questions, we complemented this with a multilayer perceptron (MLP)-based ANN model [46,50].

For the simulation with ANN, we use the typology of ANN as a MLP. In the context of neural networks, the architecture is referred to as that of a supervised network, which is so named because the predicted results can be compared to known values of the output variables. Specifically, the architecture of a MLP consists of an input layer, one or more hidden layers, and an output layer. By connecting the neurons in the hidden and output layers with their respective weights, it becomes possible to analyze the interaction between the input variables. This ANN approach is particularly useful in the cybersecurity context, where data sparsity, nonlinear effects, and managerial decision complexity often limit the explanatory power of traditional linear models.

To develop the ANN-MLP architecture, we adopted the methodology of Wang [51], Ciurana *et al.* [52], Arranz *et al.* [46], and Arroyabe *et al.* [46]. The design process entails two critical factors: determining the number and size of hidden layers and selecting the appropriate learning algorithm. The number of inputs and outputs of the network is determined by the number of input and output variables, whereas the number and size of hidden layers are determined through a *trial-and-error approach* involving several combinations of the number of hidden layers and neurons [46,52] (To accurately model function approximation, Ciurana *et al.* (2008) [52] suggest that a two-layer neural network is adequate.), with various activation functions tested to identify the optimal architecture that minimizes the error. Our optimal architectures converged on a single hidden layer configuration, with the specific number of hidden units dynamically varying between 1 and 12 neurons depending on the simulation. Specifically, the hyperbolic tangent function was utilized as the activation function for the hidden layers, while the SoftMax function was employed for the output layer. Additionally, we employ the *backpropagation algorithm* for learning, which adjusts the connection weights of each neuron, reducing the error. The network was trained using a minibatch method with a gradient descent optimization algorithm, configured with an initial learning rate of 0.4, a lower boundary of 0.001, 10 learning epochs, and a momentum of 0.9. To evaluate classification performance and guide the learning process, we used cross-entropy error, establishing a stopping rule of one consecutive step with no decrease in error. To ensure model validation and reproducibility, the dataset was randomly partitioned into a training set (70%) to estimate the network parameters and train the model, and a testing set (30%) to evaluate the model's predictive accuracy and prevent overfitting. The resulting models demonstrated strong predictive capability, achieving overall classification accuracies on the testing subsets that ranged from 50.0% to 100% across the different cluster models.

Analysis and results

We first checked the robustness of the survey and the results. Firstly, we analyzed the responses obtained in the two waves,

and we did not find significant discrepancies between the two waves. Second, we performed checks of the survey to verify the robustness of the questionnaires and answers, testing the common method variance and common method bias, following the method of Podsakoff *et al.* [53]. The analysis has identified eight distinct constructs that collectively account for 60.03% of the variance. The first factor accounts for 19.19% of the variance, which is in line with the recommended threshold of 50%. Consequently, we can infer that common method variance and common method bias are not a significant concern in our findings. Furthermore, an initial assessment of the control variables indicates a weak positive covariance between firm size and the degree of digitalization (covariance = 0.090, $r = 0.116$, $P = .112$). Because this relationship is not statistically significant, it suggests that firm size alone does not definitively drive digital maturity within our specific sample of SMEs.

Regarding the level of adoption of digital technologies by SMEs, our results show that the most frequently adopted digital technology is cloud computing, accounting for 49.8% of cases. AI, big data, smart devices, and high-speed infrastructure are adopted to a lesser degree, with a prevalence of 10% among SMEs. The adoption of robotics and blockchain is relatively infrequent. The results indicate that the degree of penetration of digital technologies adopted by SMEs is low. Only 13.8% of companies adopt two or more digital technologies, while 7.9% adopt three or more technologies (While these descriptive statistics provide a baseline for the degree of digitalization, it is important to acknowledge the possibility that participants may be underreporting their actual technological footprint. Because the data relies on self-reported measures from single respondents, adoption rates may appear artificially low due to a lack of visibility across all organizational departments or the presence of decentralized, informal technology use (often referred to as “shadow IT”) within the SMEs.).

Regarding cybersecurity control systems, we observe that 50% of the SMEs adopted software updates, firewalls, and backing up, as cybersecurity control systems; however, the least incorporated are VPN, access management, and network segregation, which are adopted in <20% of companies. In line with the previous variable, we have analyzed the degree of penetration of control systems (*cybercontrol*), measured as a cumulative index of the ten cybersecurity control systems. The results show that SMEs combine various cybersecurity control mechanisms (between 4 and 7 different control mechanisms), being the most frequently used software updates, firewall and malware protection, combined with access management measures, physical controls or VPN. Regarding cybersecurity management systems, in general, only 10% of companies use some cybersecurity management procedures, such as outsourcing management, the assignment of personnel to assume these responsibilities, or the setting of policies for cybersecurity. Additionally, our results show there is very little use of several systems simultaneously (*cybermanagement*), such as the existence of personnel and discussions on the board of companies, or the establishment of cybersecurity policies. Regarding the cybersecurity impact (*cyberimpact*), the most frequent impact is the stoppage of activities and costs derived from the damages of the incidents. Very infrequent, they damage the firm's reputation or problems with the authorities. Regarding the use of cybersecurity standards (*cyberstandards*), either in the case of Cyber Essentials or ISO 27000s, ~20% of SMEs are either in the process of implementation or have implemented one of these standards.

Regarding the *first research question* (RQ1a) on how cybersecurity is associated with the level of adoption of digital technologies in SMEs, Table 2 presents the regression results. Cybersecurity has a positive association with the digitalization of SMEs, and allocation as a driver for the adoption of digital technologies. More in detail, we find that *cybercontrol* ($\beta = -0.176$; $P < .001$), *cybermanagement* ($\beta = -0.392$; $P < .001$), *cyberimpact* ($\beta = -0.586$; $P < .01$), and *cyberstandards* ($\beta = -0.521$; $P < .001$) have a positive and significant effect on the dependent variable.

Additionally, in complement to the regression analysis for RQ1, we conducted an analysis using ANN-MLP. The results have revealed that the optimal architecture for predicting cybersecurity impact is 4-5-1. This architecture consists of four neurons in the input layer, five neurons in the hidden layer, and one neuron in the output layer. The hyperbolic tangent function was used as the activation function for the hidden layer, while the SoftMax function was used for the output layer. We evaluated the fitting of the ANN-MLP design by applying cross-entropy error in both the training and testing phases, also, we assessed the predictability of our models using the Receiver Operating Characteristic (ROC) curve. The ROC curve is a graph of sensitivity versus specificity that indicates the classification performance [50]. The accuracy of the model is higher when the curve moves away from the 45-degree line. Our ROC curve revealed that the selected architecture can predict >70% of the output variable values (see Fig. 2).

Additionally, from the simulation with ANN-MLP, Fig. 3 shows the normalized importance of each input variable on the output variable. The normalized importance is estimated with Garson's algorithm, where the relative importance of each input variable arises as the absolute sum of the weights of each variable in each neuron and layer. Cybersecurity control has the highest importance (*cybercontrol*: 0.339; 100% normalized value), followed by cybersecurity impact (*cyberimpact*: 0.249; 73.3% normalized value), standards (*cyberstandards*: 0.209; 61.5% normalized value), and finally, the cybersecurity management, has the least importance (*cybermanagement*: 0.204; 60.0% normalized value).

Regarding the *second research question* (RQ1b), which examines how the level of digitalization acquired by SMEs affects the relationship between cybersecurity and the degree of digitalization in SMEs, we conducted an exploratory analysis to classify the SMEs into different groups based on their degree of digitalization. Then, we analyzed if the effect of cybersecurity and the degree of penetration of digital technologies is homogenous across different levels of digitalization. Using the K-mean Cluster as a statistical model [54,55], we have proceeded in two stages. First, the K-mean input variables are the seven digitalization technologies. Second, we proceed to the choice of the most robust solution using Silhouette analysis [54,55]. This analysis allows us to determine the robustness of the cluster solution, the cohesion of each cluster and the separation of the groups. Silhouette index takes values in the interval $[-1, 1]$, with values closer to 1 being the most robust solution. After proceeding to obtain the Silhouette index, the three clusters solution has a higher value of Silhouette (0.75). Furthermore, we performed a complementary analysis, using the Schwarz' Bayesian Criterion [56,57], and the results confirm that the solution three clusters are the most robust in terms of cohesion and separation.

The results of the K-mean cluster analysis show that SMEs are grouped into three clusters. Additionally, we have performed a ro-

bustness check of the analysis, using ANOVA, and the results show a significant difference in the degree of digitalization as a function of the cluster variable. In Table 3, we present the mean values of each variable used in the analysis for each cluster. Overall, we observe that Cluster 1 (Digitally Mature) has a higher level of digitalization compared to Clusters 2 (Non-Adopters), and 3 (Developing Adopters), which aligns with a higher level of cybersecurity in the companies within Cluster 1 (Digitally Mature).

Cluster 1 (Digital Mature), composed of 25 companies, has an average level of digitalization of 3.4, indicating that each SME, on average, adopts between three and four digital technologies (out of the maximum range of six). In this cluster, 96% of them adopt cloud computing, to a lesser extent big data (64%), and high-speed infrastructure (40%). The adoption of smart devices, robotics, AI, or blockchain is less frequent. As for protection methods, we observe that cybercontrols have an average score of 5.4, while cybermanagement has a score of 2.1. This is, in 76% of the cases, SMEs in this cluster maintain software updates, and use encryption software (68%), firewalls (68%), malware protection (52%), or backup solutions (52%). To a lesser extent, they employ network segregation and access control, for example. Regarding cybersecurity management in terms of procedures and routines, it decreases in comparison to control systems (average: 2.1). The most frequently used practices include staff allocation (40%), periodic checks (32%), board discussions (32%), and the use of cybersecurity policies (32%). Regarding the implementation of cybersecurity standards, ~50% of them have implemented or are in the process of implementing cyber essentials standards, and to a lesser extent, the implementation of ISO 27000 (38.1%). However, there is a lack of awareness regarding the cybersecurity impact that incidents have on the SMEs in this cluster, although this is common across all the clusters.

As for Cluster 2 (Non-Adopters), containing 119 SMEs, we see that the level of digitalization is almost non-existent, with an average score of 0.1 on a scale of 0–6. Thus, when SMEs have adopted any digital technology, it is primarily robotics (2.5%), big data (1.7%), and blockchain (1.7%). Further analyzing these results, we find that the adoption of these digital technologies is concentrated in only 7% of the SMEs. In terms of the implementation of cybersecurity mechanisms, it is very limited, primarily based on software updates (28%), firewalls (25%), and backup solutions (24.4%). Regarding organizational procedures and routines, the allocation of specific personnel (5.9%) and outsourcing (5.0%) are the most common practices. As for the implementation of cybersecurity standards, it only applies to <5% of SMEs, both in ISO and Cyber Essentials. Similarly, there is almost no knowledge of cybersecurity incidents.

Cluster 3 (Developing Adopters), involving 95 companies, is positioned in an intermediate position compared to the previous clusters. In terms of the level of digitalization, it is limited, with an average adoption score of 1.2 for digital techniques. The most adopted digital technologies are high-speed infrastructure (12.6%), smart devices (9.5%), and big data (8.4%). Regarding cybersecurity management, the frequent use of control mechanisms such as firewalls (58.9%), backup solutions (57.9%), malware protection (56.8%), and software updates (66.3%) can be observed. To a lesser extent, organizational procedures and routines are implemented, such as periodic checks (20.0%) and policies (22.1%). Approximately 25% of the companies have implemented cybersecurity standards. Lastly, in line with the previous clusters, there is

Table 2 Regression analysis.

Variables	Model 1	Model 2	Model 3	Model 4	Model 5
Size	0.176* (0.044)	0.029 (0.264)	−0.229 (0.280)	0.156 (0.266)	0.258 (0.281)
Growth	0.319*** (0.129)	0.244** (0.143)	0.244** (0.144)	0.270** (0.143)	0.282** (0.151)
Competencies	−0.320*** (0.114)	−0.218*** (0.133)	−0.167*** (0.070)	−0.447*** (0.168)	−0.212** (0.175)
CYBERCONTROL		0.176*** (0.060)			
CYBERMANAGEMENT			0.392*** (0.092)		
CYBERIMPACT				0.586** (0.229)	
CYBERSTANDARDS					0.521*** (0.157)
-2 Log Likelihood	340.512	368.859	356.357	340.512	340.512
Chi-Square	21.7434	16.752	27.867	21.743	21.743
Sig.	0.000	0.002	0.000	0.001	0.001
Cox and Snell	0.156	0.116	0.185	0.102	0.156
Nagelkerke	0.144	0.115	0.197	0.108	0.166
McFadden	0.047	0.090	0.072	0.038	0.060

Notes: Dependent variable: Degree of digitalization. Number of observations: 239. * $P < .05$; ** $P < .01$; and *** $P < .001$.

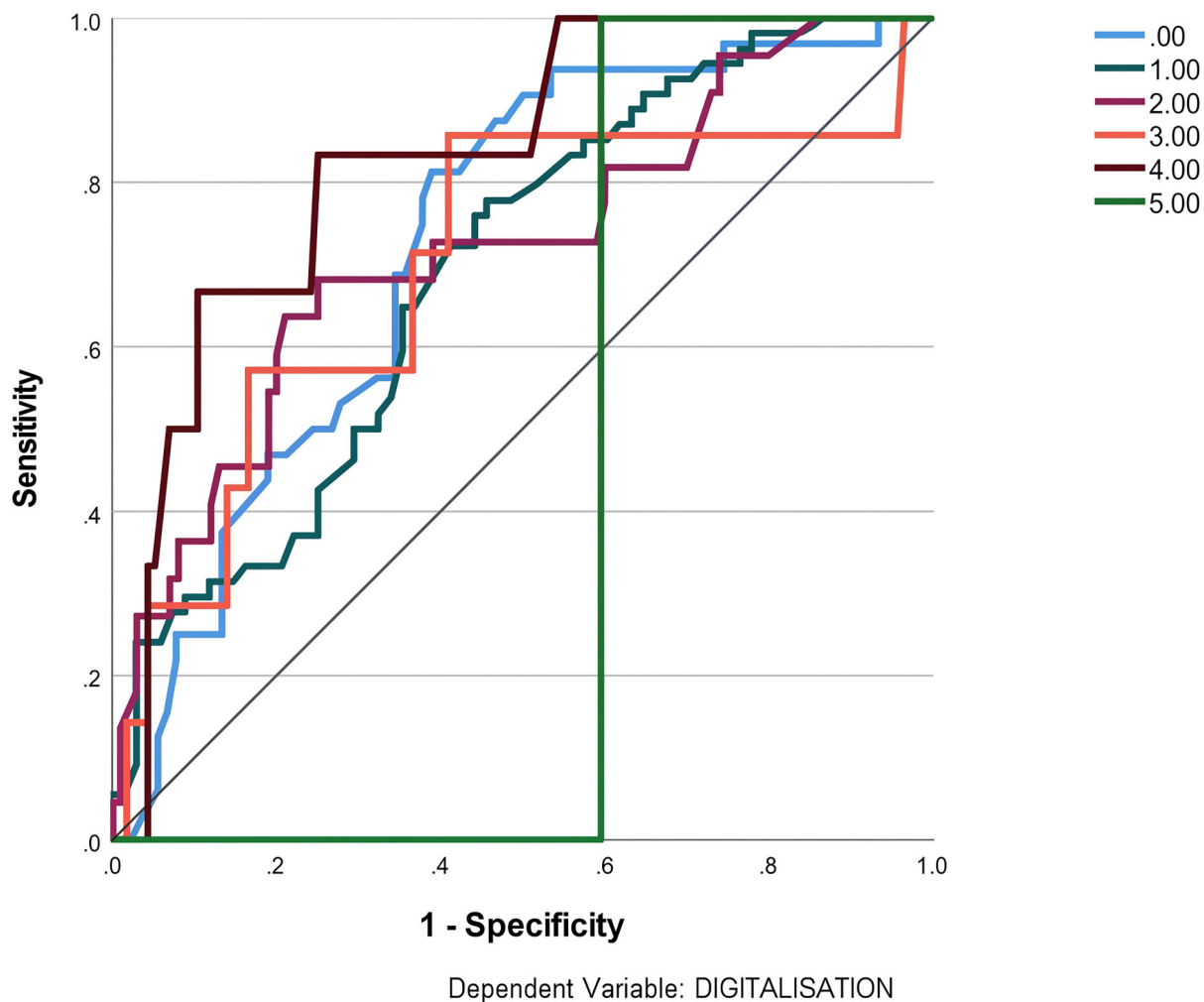


Figure 2 ROC curve in ANN-MLP simulation. Note: The legend values (0–5) represent the categorical levels of the dependent variable, DIGITALIZATION, operationalized as the cumulative number of digital technologies adopted by an SME.

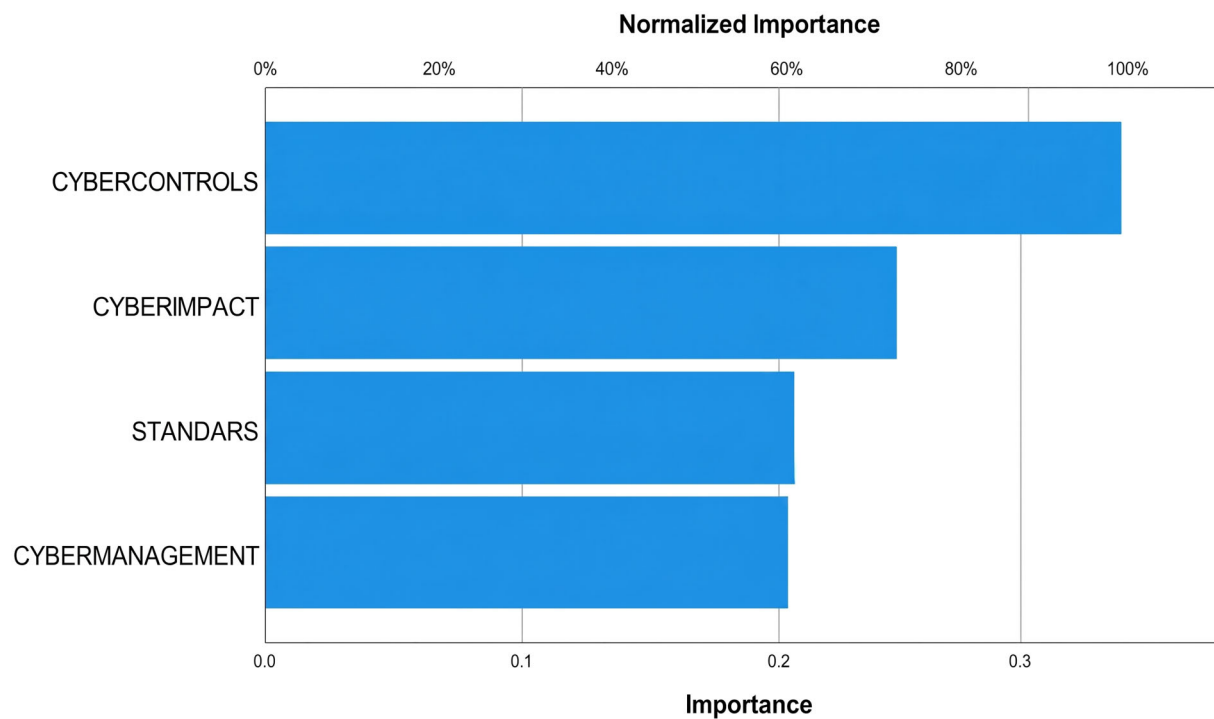


Figure 3 Normalized importance of ANN-MLP simulation.

Table 3 Mean values of clusters.

Variables	Range		Cluster 1 (digital mature)		Cluster 2 (nonadopters)		Cluster 3 (developing adopters)	
	Min.	Max.	Mean	Std. D.	Mean	Std. D.	Mean	Std. D.
DIGITALIZATION	0.00	6.00	3.440	1.260	0.100	0.399	1.242	0.430
CYBERCONTROLS	0.00	10.00	5.400	3.500	1.705	2.799	4.252	3.361
CYBERMANAGEMENT	0.00	7.00	2.120	2.697	0.235	0.788	1.084	1.843
CYBERIMPACT	0.00	5.00	0.320	1.029	0.092	0.318	0.147	0.618
ISO	1.00	4.00	2.285	1.270	1.619	0.961	1.930	1.025
CYBER ESSENTIALS	1.00	4.00	2.714	1.189	1.619	0.854	2.027	1.150
TOTAL SMES			25		119		95	

Note: For Cluster 1, 60% are microenterprises, 28% small companies, and 12% medium-sized companies. For Cluster 2, 71% are microenterprises, 20% small companies, and 9% medium-sized companies. For Cluster 3, 87% are microenterprises, 11% small companies, and 2% medium-sized companies.

a significant lack of awareness regarding the impact of cybersecurity incidents on the SMEs in this cluster.

To further explore RQ2 and identify the differences in perception among the three clusters regarding which cybersecurity variable has the most impact on the degree of digitalization of SMEs, we conducted an ANN-MLP analysis. Figure 4 displays the normalized importance of cybersecurity variables, illustrating the architecture of the ANN-MLP and the degree of robustness for each cluster. The results reveal significant differences among the three clusters. In Cluster 1 (Digitally Mature), which has a higher level of adoption of digital techniques and a greater degree of cybersecurity implementation, the findings indicate that cybersecurity management (cybermanagement) and cybersecurity standards (standards) are of greater importance in the adoption of digital technologies, while cybersecurity control mechanisms (cybercontrol) and cybersecurity impact (cyberimpact) are of lesser importance.

However, for the clusters with a lower level of digitalization, Cluster 2 (Non-Adopters) highlights the importance of cybersecurity impact (cyberimpact), while Cluster 3 (Developing Adopters) emphasizes the significance of cybersecurity control (cybercontrol) in the adoption of digital technologies.

Discussion

Baseline configurations: technology complexity and cybersecurity myopia

Our results have demonstrated the limited level of digitalization in SMEs, primarily based on the use of cloud computing, sometimes complemented by AI applications, smart devices, or high-speed infrastructure. The findings corroborate previous studies that have

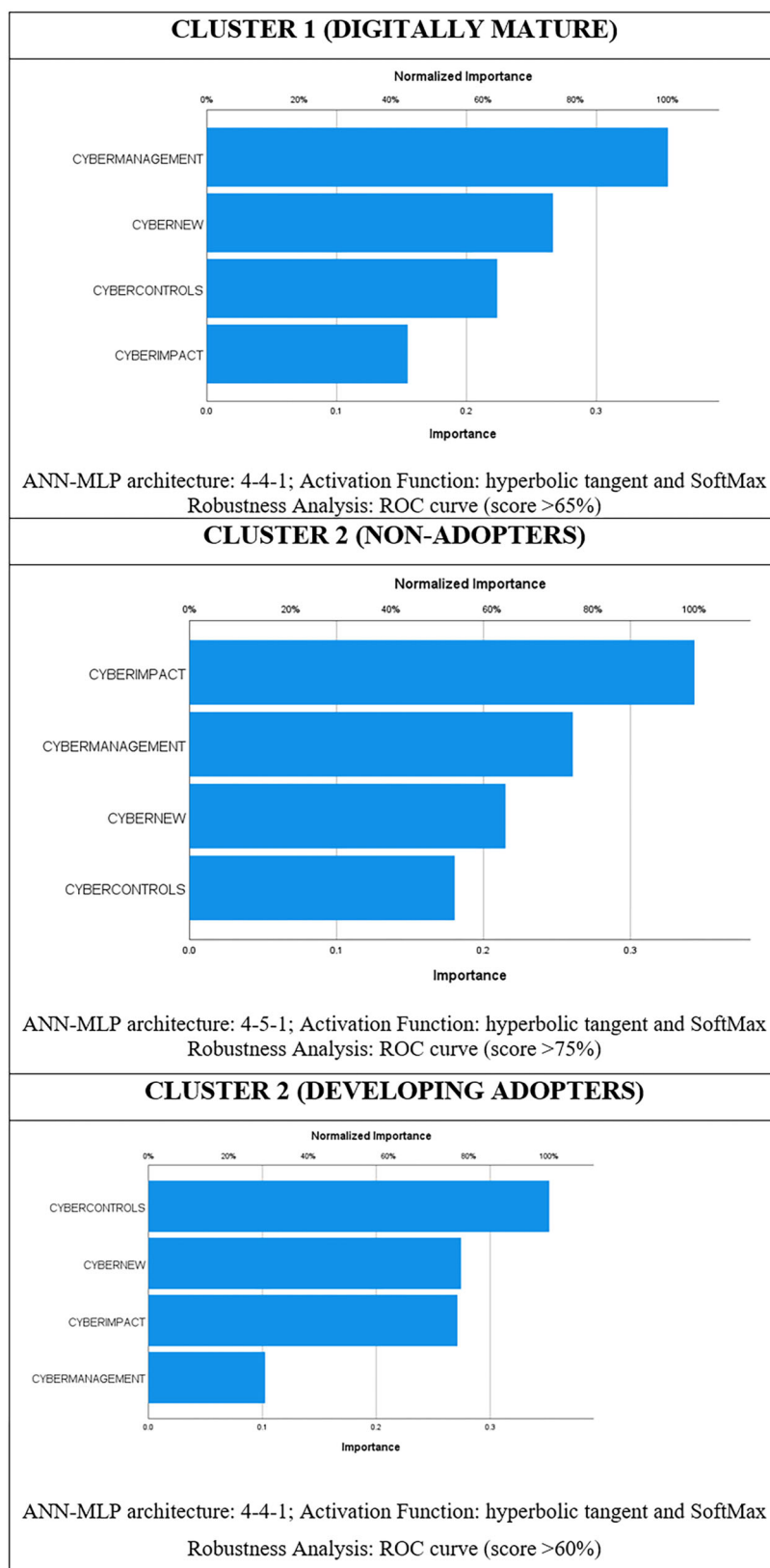


Figure 4 Normalized importance of ANN-MLP simulation Clusters.

argued the complexity of adopting digital technologies as the primary obstacle to achieving a higher level of digitalization [2]. We observe that cloud computing is characterized as having a lower level of complexity compared to, for example, the use of big data, which requires analytical capabilities, or AI applications and smart devices, which require knowledge of the wide variety of applications available in the market and their potential use. Therefore, in line with the literature, this complexity serves as a disincentive for SMEs to adopt these technologies [2,58]. Moreover, Kshetri, and Ballestar *et al.* [18,59] pointed out that blockchain and robotics have been characterized not only by their level of complexity but also by their specificity; for example, blockchain has seen extensive use in logistics, making it challenging for SMEs to adopt digitalization. From a PMT perspective, these findings reflect the role of response cost, one of PMT's core coping appraisal dimensions. When SMEs perceive the implementation of advanced digital technologies as costly or complex, their coping appraisal decreases, reducing motivation to adopt such technologies [34]. Moreover, limited internal expertise lowers self-efficacy, further constraining digitalization decisions [23].

Regarding cybersecurity in SMEs, our results reveal a limited implementation of control and management systems, as well as cybersecurity standards, confirming previous research that highlights SMEs' myopia toward cybersecurity [10]. The literature indicates that SMEs perceive themselves as less likely targets for cybersecurity attacks, leading to low involvement of senior managers in cybersecurity management and the use of limited cybersecurity systems [16,20]. Our results support previous works [10], concluding that cybersecurity management primarily relies on control systems such as firewalls, malware protection, and software updates. While the implementation of organizational security procedures and processes is almost nonexistent across the broader SME sample, where cybersecurity management mainly involves assigning responsibilities without defining policies or routines, our cluster analysis reveals that these organizational measures become a critically important, distinguishing capability for the specific subset of highly digitalized firms. Moreover, our results emphasize the low awareness SMEs have of potential attacks and their limited interest in implementing cybersecurity standards, corroborating previous literature [10,20]. This pattern aligns with low threat appraisal, where SMEs underestimate both attack likelihood (perceived vulnerability) and the severity of consequences [29]. PMT suggests that when threat appraisal is low, protective behavior is unlikely, even when coping strategies are available [24]. Thus, SMEs' limited cybersecurity investment emerges not simply from resource constraints, but from cognitive underestimation of cyber risk.

The interdependent nexus of cybersecurity capacity and digitalization (RQ1a)

Regarding the *first research question* (RQ1a), which investigates the relationship between cybersecurity and the degree of digitalization in SMEs, our results demonstrate a positive association. First, in line with previous literature, an increase in the cybersecurity management level will potentially lead to a higher level of digitalization [11,15,60]. Corallo *et al.* [15], and ISO/IEC 27002:2022 [17] have emphasized how cybersecurity protection facilitates on-

line activities, mitigates potential incidents, and establishes organizational procedures and processes for conducting online operations. Through the PMT lens, this reflects increased self-efficacy (belief that the organization can manage threats) and response efficacy (belief that security measures are effective), both of which increase motivation to adopt digital technologies [22,23].

In this regard, we highlight that the greater implementation of cybersecurity standards positively impacts online activities by defining organizational processes and procedures (e.g. [15,17]). Theoretical perspectives, such as the self-determination theory [61,62] suggest that managers make decisions based on factors including control over activities. Considering the significance of senior managers' decisions in SMEs, we can infer that greater control over online activities, enabled by routines, procedures, and organizational processes, will facilitate the decision to increase the level of digitalization.

Furthermore, the results show that a higher cybersecurity impact in SMEs is associated with a higher likelihood of increasing the level of digitalization. Existing cybersecurity literature has emphasized the role of cloud computing, blockchain, and smart devices as enablers of cybersecurity protection in organizations [18,63]. SMEs upload their data to the cloud, relying on IT service providers' secure servers to safeguard their data and avoid data breaches and potential issues with GDPR compliance. Similarly, Kshetri [18], and Dahiya *et al.* [19] have drawn parallels between encryption tools and blockchain, where the underlying principles of cryptography, decentralization, and consensus ensure trust in transactions. Finally, although more fragile from a cybersecurity perspective, the use of smart devices with their own protections and encryption systems allows SMEs to utilize digital platforms for conducting their activities [19]. This finding highlights a second PMT mechanism: when perceived threat severity increases but coping appraisal is strong, organizations are more likely to pursue protective actions; in this case, digitalization [26,29]. In other words, digital technologies could be being adopted not only for efficiency gains but as defensive infrastructure. However, while our PMT framework conceptualizes digitalization as a protective response enabled by cybersecurity preparedness, we must also acknowledge the reciprocal nature of this relationship. The adoption of new digital technologies inherently expands an organization's attack surface, which in turn compels them to implement stronger cybersecurity controls and management systems to protect these new assets. Therefore, rather than a strictly unidirectional causal pathway, our findings suggest that cybersecurity and digitalization coevolve in a mutually reinforcing cycle where technological adoption and protective capacity continuously drive one another.

Lastly, the results highlight the importance of cybersecurity factors in the level of digitalization of SMEs. We observe that cybersecurity control measures and cybersecurity impact have relatively greater importance compared to cybersecurity standards and cybersecurity management influencing the degree of digitalization in SMEs. As mentioned earlier, the literature has already underscored the limited importance of cybersecurity in SMEs compared to large companies, with SMEs primarily focusing on basic control systems while neglecting routines and organizational processes [10]. This reflects a reactive protection posture, where SMEs engage in protective behaviors only after perceiving immediate cyber threat [23], rather than proactively building organizational security capacity [24].

Overall, our findings emphasize the positive influence of cybersecurity measures on digitalization in SMEs, emphasizing the relative importance of different cybersecurity factors in this context.

Maturity-based heterogeneity in cognitive appraisals (RQ1b)

Regarding the *second research question* (RQ1b), which investigates whether the effect of cybersecurity on the penetration of digital technologies is homogenous across different levels of digitalization, our results have shown heterogeneity in this effect. First, the results reveal a group of SMEs (Cluster 1—Digitally Mature) that predominantly combine cloud computing with big data and high-speed infrastructure as their primary digital technologies. This sector comprises companies that manage and explore data, such as publishing activities or information services, as well as businesses that utilize networks to transmit significant informational packages, such as motion pictures, videos, and television. In line with previous studies, we observe that sector-specific technological needs, along with the prior level of digitalization, influence the level of digitalization (see for example, [64]). The literature has identified experience, competencies, and skills in handling digital technologies as motivating factors for digitalization [6,35]. Moreover, we find that the level of implementation of cybersecurity systems is the highest in this cluster, with a substantial number of SMEs having cybersecurity standards in place, along with corresponding cybersecurity procedures, routines, and organizational processes. This facilitation of new digital technology adoption is attributable to the presence of cybersecurity management practices. When considering the importance of cybersecurity at the level of digitalization, these SMEs prioritize cybersecurity management and cybersecurity standards as the factors with the most significant impact, compared to cybersecurity impact and cybersecurity control. These results confirm that the possession of organizational processes, routines, and cybersecurity measures resulting from the implementation of standards or cybersecurity management facilitates digitalization [17]. Possessing appropriate protection measures in the organization, coupled with an organizational structure and processes, enables managers to have greater control over the situation, making them more inclined to introduce new digital technologies by mitigating the uncertainty of potential cybersecurity incidents [62].

Secondly, Cluster 2 (Non-Adopters) comprises SMEs with an incipient adoption of digitalization and cybersecurity. Although these companies potentially belong to sectors that are susceptible to digitalization, such as consultancy, architecture or engineering activities, scientific research and development, or market research, they have not fully embraced digitalization. Furthermore, the level of cybersecurity in this cluster follows a parallel with the level of digitalization, being scarce and primarily based on minimal cybersecurity control tools. When considering the factor with the most significant impact, we find that cybersecurity impact takes precedence, followed by cybersecurity measures. Thus, the results align with previous studies indicating that the trigger for digitalization in these companies is their use as a cybersecurity protection system [19,59].

Lastly, the results demonstrate a third group with an intermediate level of digitalization and cybersecurity, belonging to sectors similar to those in Cluster 2 (Non-Adopters). These companies have achieved a certain level of digitalization, not only driven by

market needs but also consider an adequate system of protection based on cybersecurity control mechanisms as the catalyst for digitalization [19,59]. Interestingly, cybersecurity standards appear to have a secondary role in this cluster. This is in line with previous studies that consider that senior managers perceive the importance of controlling activities and mitigating uncertainties in the network as key factors in the decision to adopt digital technologies [61,62].

Overall, these differences reflect varying combinations of threat appraisal and coping appraisal across maturity stages, consistent with PMT [21,26]. For the majority of SMEs in our sample, risk appraisals remain low, a condition that inherently corresponds to the limited degree of overall digital adoption observed. According to PMT principles, without a significant perceived threat, there is little motivation to engage in complex protective behaviors, such as extensive technological integration. Because PMT captures fundamental cognitive mechanisms rather than fleeting technological trends, these underlying appraisal behaviors represent stable psychological processes [21,65]. However, as SMEs become more digitally advanced and their attack surface expands, their threat appraisal naturally increases. Within this specific subset of advanced firms, those with high threat appraisal and strong coping appraisal advance in digitalization, while those with high threat but low coping capacity remain stalled.

Furthermore, these empirical findings validate our theoretical choice of PMT over alternative organizational frameworks. If analyzed strictly through the TOE framework, cybersecurity might have been reduced to a static environmental constraint or technological barrier [27,66]. Instead, our data reveals it is a dynamic, cognitive driver that actively motivates adoption depending on the firm's maturity. Similarly, while the dynamic capabilities perspective elegantly describes how advanced SMEs (such as those in Cluster 1—Digitally Mature) “sense and seize” digital opportunities by reconfiguring their organizational routines and assets [28], it largely assumes the motivation to do so. By viewing this through the lens of PMT, our results clarify the psychological mechanics behind capability building: the development of advanced digital and cybersecurity capabilities is directly motivated by the cognitive need to align escalating threat appraisals with robust coping mechanisms.

Conclusion

The objective of this study was to examine how cybersecurity influences the digitalization of SMEs. We conceptualized digitalization as a dynamic, cumulative process in which firms progressively adopt digital technologies (from basic to more complex systems) as they acquire new capabilities. In parallel, this process increases organizational exposure to cyber threats, making cybersecurity not only a technical requirement but also a strategic variable that shapes the trajectory of digital adoption.

To understand this relationship, we drew on the PMT [21,22], which posits that individuals and organizations engage in protective behavior when they (1) appraise the severity and likelihood of a threat (threat appraisal), and (2) believe they have the capacity and tools to cope with it (coping appraisal). We operationalized four dimensions of cybersecurity (controls, management, impact, and standards) as indicators of these two cognitive processes. This framework enabled us to interpret digitalization as a motivated response to cybersecurity concerns, driven by

firms' perceptions of cyber risk and their confidence in mitigating it [23,26,29].

Our first contribution is theoretical. We extend PMT from its traditional focus on individual behavior to organizational decision-making in the context of digital transformation. While prior research has applied PMT to individual users' adoption of cybersecurity practices [24,34], few studies have examined how firms, and in particular SMEs, respond to cybersecurity threats when planning or implementing digital technologies [67]. Our findings show that SMEs' level of digitalization is significantly influenced by both threat appraisal (e.g. perceived cyber impact) and coping appraisal (e.g. existing controls, standards, and management practices). Firms with higher perceived risk and stronger internal capabilities are more likely to digitalize. This expands the theoretical scope of PMT and offers a more nuanced understanding of technology adoption under conditions of uncertainty. However, this contribution must be qualified by the size of the organizations that participated in our study. Because our sample consists predominantly of micro and small enterprises, these dynamics specifically reflect the unique, resource-constrained realities of this population and may not fully represent the digitalization and cybersecurity pathways of larger, well-resourced organizations.

A second contribution lies in our understanding of digitalization as an uneven and path-dependent process. Prior literature has often treated digitalization as a binary or linear transformation [3,68]. While the generally low levels of adoption in our sample might initially suggest a simple binary between adopters and nonadopters, our study challenges this view by revealing meaningful nuances in how cybersecurity factors influence adoption decisions across different stages. Through cluster analysis, we identified three distinct groups: digitally advanced SMEs with mature cybersecurity capabilities; digitally limited firms with minimal cyber awareness; and an intermediate group relying primarily on technical controls. These findings highlight that cybersecurity affects digitalization heterogeneously, depending on where firms are situated in their transformation journey.

At low levels of digitalization, cybersecurity may act as a basic protective tool. For example, firms may adopt cloud platforms to outsource data protection or use simple firewalls to guard against attacks. In this case, threat appraisal is often low, and coping capacity is rudimentary. As SMEs become more digitally advanced, they begin to integrate more sophisticated cybersecurity routines (e.g. ISO 27001, policy frameworks, and internal roles), which enhance self-efficacy and response efficacy. In such contexts, cybersecurity becomes a strategic enabler of digitalization rather than a barrier. This reflects the full activation of PMT: perceived threats motivate protective action when firms believe they have the capacity to respond effectively [22,29].

Our third contribution is practical. For SME managers, our findings highlight the importance of building cybersecurity capabilities not only to defend against threats but to unlock digital opportunities. Technical measures alone, such as firewalls or antivirus software, are insufficient for sustained transformation. Instead, firms should invest in organizational cybersecurity management practices, including staff training, executive oversight, and adoption of standards like Cyber Essentials or ISO/IEC 27002 (ISO/IEC 27002:2022). These routines increase managerial confidence and institutional readiness for adopting new technologies. This practical implication is directly supported by our cluster analysis results, which demonstrated that the most digitally advanced sub-

set of SMEs (Cluster 1—Digitally Mature) was uniquely characterized not just by technical controls, but by a significantly higher implementation of these strategic and organizational cybersecurity management measures.

For policymakers, our findings suggest that cybersecurity support schemes should be better aligned with digitalization policy. Rather than treating cybersecurity as an end in itself, governments should recognize its enabling role in SME transformation. Public programs that subsidize cybersecurity certification, offer training, or provide toolkits for developing internal processes can lower perceived response costs and raise coping appraisal, especially in smaller firms with limited resources [10,20].

Finally, we offer a methodological contribution by combining regression analysis with machine learning (ANN-MLP) to model complex, nonlinear relationships among variables. This dual approach addresses common empirical challenges in cybersecurity research, including collinearity, non-normality, and unbalanced response data [46]. Our ANN results confirm and extend the regression findings, revealing the relative importance of different cybersecurity dimensions depending on the digital maturity of firms. Our paper illustrates the value of hybrid analytic models for studying multifactor phenomena such as digitalization.

Finally, while this study offers valuable insights, certain limitations present avenues for future research. First, our findings are based on a sample of UK SMEs. While the UK provides a robust context due to its established regulatory frameworks (e.g. GDPR) and national cybersecurity initiatives (e.g. Cyber Essentials), future research should explore whether these dynamics generalize to SMEs operating in other institutional or regulatory environments with different compliance pressures. Second, our survey data was collected in 2022. Given the rapid evolution of both digital technologies and the cybersecurity threat landscape, specific technological adoption patterns may shift. However, because our conceptual framework relies on PMT, the underlying cognitive mechanisms we observe represent stable psychological processes [21]. Therefore, the fundamental relationships between perceived protection capacity and technology adoption are likely to persist over time. Nonetheless, future research using more recent data could examine how emerging challenges, such as AI-driven cyber threats, might alter these specific appraisal thresholds. Moreover, as the digital landscape continues to evolve rapidly, future studies should also broaden the scope of digital tools tracked to include emerging innovations such as Virtual Reality and Augmented Reality, which will inevitably introduce new, unique cybersecurity challenges for SMEs.

Conflicts of interest

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

Funding

Research funded by the Economic and Social Research Council (ESRC) Digital Security by Design Social Science Hub+. Grant number RC-MN1164X.

Author contributions

Marta F Arroyabe (Conceptualization [equal], Data curation [equal], Formal Analysis [equal], Funding acquisition [equal], Investigation [equal], Methodology [equal], Project administration [equal]), Carlos Arranz (Conceptualization [equal], Data curation [equal], Formal Analysis [equal], Investigation [equal], Methodology [equal]), Ignacio Fernandez de Arroyabe (Conceptualization [equal], Data curation [equal], Formal Analysis [equal], Funding acquisition [equal], Investigation [equal], Methodology [equal], Project administration [equal]).

References

1. He Q, Meadows M, Angwin D *et al.* Strategic alliance research in the era of digital transformation: perspectives on future research. *Brit J Manag* 2020;**31**:589–617. <https://doi.org/10.1111/1467-8551.12406>
2. Masood T, Sonntag P. Industry 4.0: adoption challenges and benefits for SMEs. *Comput Ind* 2020;**121**:103261. <https://doi.org/10.1016/j.compind.2020.103261>
3. Dalenogare LS, Benitez GB, Ayala NF *et al.* The expected contribution of Industry 4.0 technologies for industrial performance. *Int J Prod Econ* 2018;**204**:383–94. <https://doi.org/10.1016/j.ijspe.2018.08.019>
4. Sharma R, Jabbour CJC, Sousa Jabbour ABL. Sustainable manufacturing and industry 4.0: what we know and what we don't. *JEIM* 2020;**34**:230–66. <https://doi.org/10.1108/JEIM-01-2020-0024>
5. Nambisan S, Lyytinen K, Yoo Y, Eds, *Handbook of Digital Innovation*. Camberley: Edward Elgar Publishing, 2020. <https://doi.org/10.4337/9781788119986>
6. Bharadwaj AS, El Sawy OA, Pavlou PA *et al.* Digital business strategy: toward a next generation of insights. *MIS Quart* 2013;**37**:471–82. <https://doi.org/10.25300/MISQ/2013/37.2.3>
7. Vial G. Understanding digital transformation: a review and a research agenda. *Manag Digit Transf* 2021;**28**:13–66. https://doi.org/10.4324/9781003008637_10.4324/9781003008637-4
8. Choo KR. The cyber threat landscape: challenges and future research directions. *Comput Secur* 2011;**30**:719–31. <https://doi.org/10.1016/j.cose.2011.08.004>
9. Shin YY, Lee JK, Kim M. Preventing state-led cyberattacks using the bright internet and internet peace principles. *JAIS* 2018;**19**:152–81. <https://doi.org/10.17705/1jais.00488>
10. Fernandez de Arroyabe I, Fernandez de Arroyabe JC. The severity and effects of cyber-breaches in SMEs: a machine learning approach. *Enterpr Inf Syst* 2021;**17**:1942997. <https://doi.org/10.1080/17517575.2021.1942997>
11. Bertino E, Choo KKR, Georgakopolous D *et al.* Internet of Things (IoT) smart and secure service delivery. *ACM Trans Internet Technol* 2016;**16**:22–9.
12. Lezzi M, Lazoi M, Corallo A. Cybersecurity for Industry 4.0 in the current literature: a reference framework. *Comput Ind* 2018;**103**:97–110. <https://doi.org/10.1016/j.compind.2018.09.004>
13. Babiceanu RF, Seker R. Cyber resilience protection for industrial Internet of Things: a software-defined networking approach. *Comput Ind* 2019;**104**:47–58. <https://doi.org/10.1016/j.compind.2018.10.004>
14. Conteh NY, Schmick PJ. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. *IJACR* 2016;**6**:31–8. <https://doi.org/10.19101/IJACR.2016.623006>
15. Corallo A, Lazoi M, Lezzi M. Cybersecurity in the context of industry 4.0: a structured classification of critical assets and business impacts. *Comput Ind* 2020;**114**:103165. <https://doi.org/10.1016/j.compind.2019.103165>
16. Benz M, Chatterjee D. Calculated risk? A cybersecurity evaluation tool for SMEs. *Bus Horiz* 2020;**63**:531–40. <https://doi.org/10.1016/j.bushor.2020.03.010>
17. ISO/IEC. Information security, cybersecurity and privacy protection—information security controls. ISO/IEC 27002:2022. Vernier, 2022.
18. Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommun Policy* 2017;**41**:1027–38. <https://doi.org/10.1016/j.telpol.2017.09.003>
19. Dahiya A, Gupta BB, Alhalabi W *et al.* A comprehensive analysis of Blockchain and its applications in intelligent systems based on IoT, cloud and social media. *Int J Intell Sys* 2022;**37**:11037–77. <https://doi.org/10.1002/int.23032>
20. Kabanda S, Tanner M, Kent C. Exploring SME cybersecurity practices in developing countries. *J Organ Comput Electron Comm* 2018;**28**:269–82. <https://doi.org/10.1080/10919392.2018.1484598>
21. Rogers RW. A protection motivation theory of fear appeals and attitude change. *J Psychol* 1975;**91**:93–114. <https://doi.org/10.1080/00223980.1975.9915803>
22. Floyd DL, Prentice-Dunn S, Rogers RW. A meta-analysis of research on protection motivation theory. *J Appl Soc Psychol* 2000;**30**:407–29. <https://doi.org/10.1111/j.1559-1816.2000.tb02323.x>
23. Liang H, Xue YL. Understanding security behaviors in personal computer usage: a threat avoidance perspective. *JAIS* 2010;**11**:394. <https://doi.org/10.17705/1jais.00232>
24. Johnston AC, Warkentin M. Fear appeals and information security behaviors: an empirical study. *MIS Quart* 2010;**34**:549–66. <https://doi.org/10.2307/25750691>
25. Posey C, Bennett B, Roberts T *et al.* When computer monitoring backfires: invasion of privacy and organizational injustice as precursors to computer abuse. *J Inf Syst Secur* 2011;**7**:24–47.
26. Marikeyan D, Papagiannidis S. Protection motivation theory: a review. In: S. Papagiannidis (ed.), *TheoryHub Book*. 2023. <http://open.ncl.ac.uk> (1 January 2024, date last accessed).
27. Tornatzky LG, Fleischer M, *The Processes of Technological Innovation*. Lexington: Lexington Books, 1990.
28. Teece DJ. Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance. *Strat Manag J* 2007;**28**:1319–50. <https://doi.org/10.1002/smj.640>
29. Boss SR, Galletta DF, Lowry PB *et al.* 'What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quart* 2015;**39**:837–64. <https://doi.org/10.25300/MISQ/2015/39.4.5>
30. Meso P, Ding Y, Xu S. Applying protection motivation theory to information security training for college students. *J Inf Priv Secur* 2013;**9**:47–67. <https://doi.org/10.1080/15536548.2013.10845672>
31. Goh ZH, Hou M, Cho H. The impact of a cause-effect elaboration procedure on information security risk perceptions: a

- construal fit perspective. *J Cybersecur* 2022;**8**:026. <https://doi.org/10.1093/cybsec/tyab026>
32. Dodge CE, Fisk N, Burruss GW *et al.* What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminol Public Policy* 2023;**22**:849–68. <https://doi.org/10.1111/1745-9133.12641>
 33. Warkentin M, Johnston AC, Shropshire J *et al.* Continuance of protective security behavior: a longitudinal study. *Decis Supp Syst* 2016;**92**:25–35. <https://doi.org/10.1016/j.dss.2016.09.013>
 34. Sommestad T, Karlzén H, Hallberg J. A meta-analysis of studies on protection motivation theory and information security behaviour. *Int J Inf Secur Priv* 2015;**9**:26–46. <https://doi.org/10.4018/IJISP.2015010102>
 35. Ciarli T, Kenney M, Massini S *et al.* Digital technologies, innovation, and skills: emerging trajectories and challenges. *Res Policy* 2021;**50**:104289. <https://doi.org/10.1016/j.respol.2021.104289>
 36. Dabrowska J. Digital transformation, for better or worse: a critical multi-level research agenda. *R & D Manag* 2022;**52**:930–54. <https://doi.org/10.1111/radm.12531>
 37. Rajan R, Rana NP, Parameswar N *et al.* Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management. *Technol Forecast Social Change* 2021;**170**:120872. <https://doi.org/10.1016/j.techfore.2021.120872>
 38. Mirtsch M, Kinne J, Blind K. Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis. *IEEE Trans Eng Manage* 2020;**68**:87–100. <https://doi.org/10.1109/TEM.2020.2977815>
 39. ENISA, *ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected*. Malevizi: European Union Agency For Cybersecurity, 2020. <https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends> (1 January 2024, date last accessed).
 40. ISO/IEC. Information technology—security techniques—evaluation criteria for IT security—Part 1: introduction and general model. ISO/IEC 15408-1:2022. Vernier, 2018. <https://www.iso.org/standard/50341.html> (1 January 2024, date last accessed).
 41. Calder A, *Cyber essentials: a pocket guide*. Ely: IT Governance Ltd, 2014.
 42. Lee Y, Larsen KR. Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *Eur J Inf Syst* 2009;**18**:177–87. <https://doi.org/10.1057/ejis.2009.11>
 43. Albrechtsen E, Hovden J. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Comput Secur* 2010;**29**:432–45. <https://doi.org/10.1016/j.cose.2009.12.005>
 44. Williams EJ, Joinson AN. Developing a measure of information seeking about phishing. *J Cybersecur* 2020;**6**:001. <https://doi.org/10.1093/cybsec/tyaa001>
 45. Arroyabe MF, Arranz CF, Arroyabe IF *et al.* The effect of IT security issues on the implementation of industry 4.0 in SMEs: barriers and challenges. *Technol Forecast Social Change* 2024;**199**:123051. <https://doi.org/10.1016/j.techfore.2023.123051>
 46. Arranz CF, Arroyabe MF, Arranz N *et al.* Digitalization dynamics in SMEs: an approach from systems dynamics and artificial intelligence. *Technol Forecast Social Change* 2023;**196**:122880. <https://doi.org/10.1016/j.techfore.2023.122880>
 47. Agraftiotis I, Nurse JR, Goldsmith M *et al.* A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. *J Cybersecur* 2018;**4**:006. <https://doi.org/10.1093/cybsec/tyy006>
 48. Alpaydin E, *Machine Learning*. Cambridge: MIT Press, 2021. <https://doi.org/10.7551/mitpress/13811.001.0001>
 49. Smith KA, Gupta J. Neural network in business: techniques and applications for the operations researcher. *Comput Operat Res* 2000;**27**:1023–44. [https://doi.org/10.1016/S0305-0548\(99\)00141-0](https://doi.org/10.1016/S0305-0548(99)00141-0)
 50. Paliwal M, Kumar UA. Neural networks and statistical techniques: a review of applications. *Expert Syst Appl* 2009;**36**:2–17. <https://doi.org/10.1016/j.eswa.2007.10.005>
 51. Wang Q. Artificial neural networks as cost engineering methods in a collaborative manufacturing environment. *Int J Prod Econ* 2007;**109**:53–64. <https://doi.org/10.1016/j.iipe.2006.11.006>
 52. Ciurana J, Quintana G, Garcia-Romeu ML. Estimating the cost of vertical high-speed machining centres, a comparison between multiple regression analysis and the neural networks approach. *Int J Prod Econ* 2008;**115**:171–8. <https://doi.org/10.1016/j.iipe.2008.05.009>
 53. Podsakoff PM, MacKenzie SB, Lee JY *et al.* Common method biases in behavioral research: a critical review of the literature and recommended remedies. *J Appl Psychol* 2003;**88**:879–903. <https://doi.org/10.1037/0021-9010.88.5.879>
 54. Dudek A. Silhouette index as clustering evaluation tool. In: *Classification and Data Analysis: Theory and Applications* 28. Cham: Springer International Publishing, 2020:19–33. https://doi.org/10.1007/978-3-030-52348-0_10.1007/978-3-030-52348-0_2
 55. Mamat AR, Mohamed FS, Mohamed MA *et al.* Silhouette index for determining optimal k-means clustering on images in different color models. *Int J Eng Technol* 2018;**7**:105–9.
 56. Kass RE, Wasserman L. A reference Bayesian test for nested hypotheses and its relationship to the Schwarz criterion. *J Am Stat Assoc* 1995;**90**:928–34. <https://doi.org/10.1080/01621459.1995.10476592>
 57. Fraley C, Raftery AE. How many clusters? Which clustering method? Answers via model-based cluster analysis. *Comput J* 1998;**41**:578–88. <https://doi.org/10.1093/comjnl/41.8.578>
 58. Moeuf A, Lamouri S, Pellerin R *et al.* Identification of critical success factors, risks and opportunities of industry 4.0 in SMEs. *Int J Prod Res* 2019;**58**:1–17.
 59. Ballestar MT, Díaz-Chao Á, Sainz J *et al.* Knowledge, robots and productivity in SMEs: explaining the second digital wave. *J Bus Res* 2020;**108**:119–31. <https://doi.org/10.1016/j.jbusres.2019.11.017>
 60. Orzes G, Rauch E, Bednar S *et al.* Industry 4.0 implementation barriers in small and medium sized enterprises: a focus group study. In: *Proceedings of the 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*. Piscataway: IEEE, 2018. <https://doi.org/10.1109/IEEM.2018.8607477>

61. Deci EL, Olafsen AH, Ryan RM. Self-determination theory in work organizations: the state of a science. *Annu Rev Organ Psychol Organ Behav* 2017;**4**:19–43. <https://doi.org/10.1146/annurev-orgpsych-032516-113108>
62. Adams N, Little TD, Ryan RM. Self-determination theory. In: M. L. Wehmeyer, K. A. Shogren, T. D. Little, S. J. Lopez (eds), *Development of Self-Determination Through the Life-Course*. 2017, 47–54. New York: Springer., https://doi.org/10.1007/978-94-024-1042-6_10.1007/978-94-024-1042-6_4
63. Al Nafea R, Almaiah MA. Cyber security threats in cloud: literature review. In: *Proceedings of the 2021 International Conference on Information Technology (ICIT)*. Piscataway: IEEE, 2021, 779–86.
64. Fromhold-Eisebith M, Marschall P, Peters R *et al.* Torn between digitized future and context dependent past—how implementing ‘Industry 4.0’ production technologies could transform the German textile industry. *Technol Forecast Social Change* 2021;**166**:120620. <https://doi.org/10.1016/j.techfore.2021.120620>
65. Conner M, Norman P. Predicting and changing health behaviour: a social cognition approach. In: *Predicting and Changing Health Behaviour: Research and Practice with Social Cognition Models*. Vol. **3**. Columbus: McGraw-Hill Education, 2015, 1–29.
66. Baker J. The technology–organization–environment framework. In: *Information Systems Theory: Explaining and Predicting Our Digital Society*. Vol. **1**. New York: Springer, 2011, 231–45.
67. Peter MK, Zobair KM, Lindeque JP *et al.* How much more will it need? Determinants of risk-driven cybersecurity adoption in Swiss SMEs: a structural equation modelling approach. *J Cybersecur* 2025;**11**:027. <https://doi.org/10.1093/cybsec/tyaf027>
68. Horváth D, Szabó RZ. Driving forces and barriers of Industry 4.0: do multinational and small and medium-sized companies have equal opportunities?. *Technol Forecast Social Change* 2019;**146**:119–32. <https://doi.org/10.1016/j.techfore.2019.05.021>