Journal of Computer Information Systems

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/ucis20

Navigating Cybersecurity: Environment's Impact on Standards Adoption and Board Involvement

Marta F. Arroyabe, Carlos F. A. Arranz, Ignacio Fernandez De Arroyabe & Juan Carlos Fernandez de Arroyabe

To cite this article: Marta F. Arroyabe, Carlos F. A. Arranz, Ignacio Fernandez De Arroyabe & Juan Carlos Fernandez de Arroyabe (27 Aug 2024): Navigating Cybersecurity: Environment's Impact on Standards Adoption and Board Involvement, Journal of Computer Information Systems, DOI: 10.1080/08874417.2024.2394440

To link to this article: https://doi.org/10.1080/08874417.2024.2394440

Published online: 27 Aug 2024.

JOURNAL OF COMPUTER INFORMATION SYSTEMS
https://doi.org/10.1080/08874417.2024.2394440

Taylor & Francis
Taylor & Francis Group

OPEN ACCESS Check for updates

Navigating Cybersecurity: Environment's Impact on Standards Adoption and Board Involvement

Marta F. Arroyabe[a], Carlos F. A. Arranz[b], Ignacio Fernandez De Arroyabe[c,d], and Juan Carlos Fernandez de Arroyabe[a]

[a]University of Essex, Colchester, UK; [b]University of Greenwich, London, UK; [c]Loughborough University, Loughborough, UK; [d]Lloyds Banking Group, London, UK

ABSTRACT
This study investigates cybersecurity governance dynamics within organizations, investigating the influence of supply chains, environmental factors, and stakeholder engagement. Utilizing the UK's Cyber Security Longitudinal Survey and employing artificial neural networks and k-means cluster analysis, we explore how organizational practices and external pressures shape cybersecurity strategies. Our findings show the managerial and political dimensions of improving organizational cybersecurity, highlighting the critical role of environmental influences alongside incident perception and self-efficacy. The research shows the necessity for organizations to remain receptive to external influences and identifies supply chains as critical factor in shaping cybersecurity practices, advocating for comprehensive security protocols. We demonstrate that guidance from governing bodies is essential for aligning with industry standards. The findings suggest a range of strategies, from implementing standards to encouraging board-level integration of cybersecurity, facilitated by a combination of coercive, normative, and mimetic pressures exerted by various agents, including governments, stakeholders, and the supply chain.

KEYWORDS
Cybersecurity; environment; implementation; standards; board

Introduction

In today's interconnected digital landscape, cybersecurity has emerged as a critical concern for organizations across industries.[1–3] The increasing frequency and sophistication of cyber threats pose significant challenges, requiring companies to adopt robust cybersecurity measures to safeguard their sensitive information, maintain operational resilience, and protect the interests of stakeholders.[4,5] However, implementing effective cybersecurity practices is not solely an internal endeavor; it is profoundly influenced by the broader environment in which companies operate.[6–9] This paper seeks to explore the intricate relationship between environment and cybersecurity in organizations, focusing on two key dimensions: the adoption of cybersecurity standards and the involvement of corporate boards in cybersecurity governance.

Firstly, the adoption of cybersecurity standards, such as ISO 27000 or Cyber Essentials, serves as a fundamental pillar in organizations' cybersecurity strategies.[7,10,11] These standards provide comprehensive frameworks and guidelines for identifying, assessing, and mitigating cyber risks, helping companies enhance their security posture and demonstrate their commitment to best practices. Furthermore, the involvement of corporate boards in cybersecurity governance plays a pivotal role in shaping organizations' cybersecurity attitudes.[12] Boards are tasked with managing strategic decisions, including those related to cybersecurity, and ensuring that adequate measures are in place to mitigate cyber risks.

Second, the literature has highlighted that the environment plays a significant role in shaping the implementation of cybersecurity within organizations.[3,13,14] Factors such as the regulatory landscape, including laws and regulations related to data protection and cybersecurity, can significantly impact how organizations implement cybersecurity measures. Compliance requirements imposed by regulatory bodies often mandate specific standards and practices that organizations must adhere to, influencing their cybersecurity strategies. For example, standards such as ISO 27001 and Cyber Essentials provide comprehensive guidelines for establishing robust cybersecurity programs.[11,15] Moreover, the rapidly evolving technological landscape presents opportunities and challenges for cybersecurity implementation.[16] Emerging technologies such as cloud computing, Internet of Things (IoT), and Artificial

CONTACT Juan Carlos Fernandez de Arroyabe jcfern@essex.ac.uk Essex Business School, University of Essex, Wivenhoe Park, Colchester CO4 3SQ, UK

Intelligence (AI) introduce new security risks that organizations must address. Organizations are increasingly interconnected through supply chains, making supply chain security a critical consideration in cybersecurity implementation.[17] This is because suppliers and partners may require organizations to have solid risk management practices and security controls to mitigate supply chain risks.

However, there is a significant research gap stemming from the limited understanding of how the environment influences cybersecurity practices, particularly concerning the adoption of cybersecurity standards and the involvement of corporate boards in cybersecurity governance.[7,12] Previous studies often focus on cybersecurity standards adoption or board involvement in cybersecurity governance separately, without providing a holistic perspective on how these dimensions interact and are influenced by the broader organizational context. Moreover, the multitude of agents influencing organizations and the various levels of influence make understanding the business environment a complex task.[18,19] Despite significant research efforts, the literature has resulted in a diversity of research approaches, which fail to provide a comprehensive understanding of how the environment impacts cybersecurity adoption. While existing literature acknowledges the importance of the organizational context in shaping cybersecurity decision-making, there is a lack of comprehensive research systematically examining the specific factors within the organizational environment that drive or hinder the implementation of cybersecurity measures.

To understand the relationship between the environment and cybersecurity, this paper adopts a theoretical framework rooted in institutional theory and stakeholder theory. Institutional theory offers insights into how institutional pressures, such as regulatory mandates and industry standards, influence organizational behaviors,[20,21] while stakeholder theory investigates the dynamic interactions between organizations and their stakeholders, encompassing governments, consumers, regulators, and the supply chain.[22,23] To develop this research, we conducted an empirical study based on the Cyber Security Longitudinal Survey database,[24] which was conducted by Ipsos Mori within the geographical context of the UK, yielding a sample of 3,000 companies and organizations. From an analytical perspective, we employed machine learning tools in this investigation. Specifically, Artificial Neural Networks (ANNs) were utilized to highlight the interaction between variables, addressing potential issues of collinearity and an unbalanced database.[25,26]

By examining the influence of the environment on cybersecurity standards adoption and board involvement in cybersecurity governance, this paper aims to contribute to a deeper understanding of the complexities inherent in cybersecurity management. Finally, by identifying the key factors driving cybersecurity decision-making within organizations, this research seeks to inform policymakers, practitioners, and scholars alike in their efforts to enhance cybersecurity resilience in an ever-evolving threat landscape.

Theoretical framework and research model

Cybersecurity and implementation

Cybersecurity is vital for organizations to safeguard their sensitive data, maintain operational continuity, and protect their reputation.[5,10,11,27] In today's interconnected digital landscape, where cyber threats are constantly evolving, organizations face significant risks such as data breaches, ransomware attacks, and financial fraud.[28] A robust cybersecurity framework not only shields against these threats but also ensures compliance with regulatory standards, encourages trust among customers and partners, and supports competitive advantage.[16,29] By investing in cybersecurity measures like encryption, access controls, and employee training, organizations can mitigate risks, reduce vulnerability, and uphold the integrity and confidentiality of their data and systems, thereby safeguarding their overall viability and success in the digital age.[3,16,30,31]

This study explores two primary aspects of cybersecurity implementation in companies. Firstly, we investigate the adoption of recognized cybersecurity standards, which provide structured frameworks for enhancing an organization's security posture. Secondly, we examine the integration of cybersecurity into the strategic decisions of the company's board of directors.

Regarding the first aspect, we focus on two prominent cybersecurity standards: ISO 27000 series and Cyber Essentials. These standards, while differing in scope and focus, both aim to enhance an organization's cybersecurity posture. The ISO 27000 series, particularly ISO 27001, provides a comprehensive framework for establishing, implementing, maintaining, and continually improving cybersecurity in organizations.[10,11] This standard covers various aspects of information security, including risk management, access control, cryptography, and incident response. By adhering to ISO 27001, organizations can demonstrate their commitment to information security best practices, gain a competitive edge, and ensure compliance with legal and regulatory requirements. Conversely, Cyber Essentials is a more focused and entry-level cybersecurity certification designed at helping organizations implement basic security measures to protect against common cyber threats[15,32] It focuses on five key areas: boundary firewalls and internet gateways, secure configuration, access control, malware protection, and patch management. Cyber Essentials certification provides a reference level of assurance regarding an organization's cybersecurity stance, making it particularly suitable for small and medium-sized enterprises (SMEs) and those seeking to enhance their cybersecurity resilience. Both ISO 27000 and Cyber Essentials play crucial roles in improving cybersecurity resilience within organizations. While ISO 27001 offers a comprehensive approach suitable for organizations of all sizes and sectors,[7] Cyber Essentials provides a practical starting point, especially for SMEs looking to establish foundational cybersecurity measures.[15] Ultimately, organizations can benefit from implementing both standards, tailoring their cybersecurity approach to their specific needs, risk profile, and regulatory requirements.

Regarding the second aspect, we focus on the integration of cybersecurity into the strategic decisions of company boards. The involvement of boards of directors in cybersecurity governance should be crucial for companies and organizations,[12] as senior managers play a fundamental role in shaping organizational strategy. Thus, providing updates to the boards of directors and keeping them informed about organizational performance, enables them to fulfill their oversight responsibilities, allowing senior managers to make informed strategic decisions.[12,33] However, current literature indicates that the degree of involvement of senior managers in cybersecurity is limited. For example, the UK's Cyber Security Breaches survey shows that while senior managers acknowledge the importance of cybersecurity, their level of engagement remain insufficient.[34] Notably, 60% of managers do not receive frequent cybersecurity updates, and a significant proportion lack cybersecurity training. Consequently, this gap in engagement often results in cybersecurity being treated as an operational issue rather than a strategic priority, frequently confined to IT departments.[25] The situation is particularly concerning in SMEs, where managers often underestimate their vulnerability to cyberattacks, despite evidence indicating that 40% of SMEs experience such incidents,[25,35] leading to inadequate investment in cybersecurity.

Gale et al. emphasize the necessity of involving company boards in cybersecurity, citing various factors such as the escalation of destructive cyberattacks, rising cybersecurity expenditures, and growing regulatory pressures.[12] According to Fox, the annual global cost of cybercrime is projected to soar to $9.5 trillion in 2024, with expectations that it will further rise to $10.5 trillion in 2025.[36] For instance, ransomware attacks affected 72.7% of all organizations in 2023. Consequently, ransomware-related costs are expected to surge to approximately USD 265 billion annually by 2031, a significant increase from $20 billion in 2021. The escalating cybersecurity expenditure by companies necessitates board-level approval for increasingly larger cybersecurity budgets. Furthermore, the literature emphasizes that cyber incidents not only generate economic, operational, and reputational issues for companies,[35,37–39] but can also impact the company's environment. Pal and Alam highlight how these impacts ripple through the value chain, necessitating the implementation of robust cybersecurity management standards across interconnected organizations.[17] The potential for cyberattacks to compromise data protection and confidentiality further underscores the need for strategic cybersecurity investment.[25] In light of these challenges, the significance of cybersecurity transcends individual companies and affects society as a whole, prompting regulatory efforts to mitigate potential vulnerabilities within companies.[12]

Institutional theory

Institutional theory has significantly influenced organization and management studies, providing insights into organizational behavior and change.[40] Previous research indicates that actors operate within an institutional environment that shapes their perceptions and actions, highlighting the importance of legitimacy—adapting to this environment—for organizational survival.[41] Scott's seminal work introduced a typology of institutions, categorizing them as regulative (e.g., laws, regulations), normative (e.g., standards, values), or mimetic constructs.[42]

Furthermore, the notion of institutional infrastructure, proposed as a means to define and categorize the conditions of a geographic area or region,[43] is particularly relevant. From both operational and organizational standpoints,[44,45] institutional infrastructure encompasses the formal and informal mechanisms within a region that either uphold or modify existing rules. Hinings et al. conceptualized institutional infrastructure as comprising cultural, structural, and relational elements that generate normative, cognitive, and regulatory forces.[43] These forces strengthen field governance, rendering field logic tangible and field governance achievable.

Despite its historical application in other domains, institutional theory has recently been extended to the realm of cybersecurity, as evidenced by several scholarly works (see, for example, Jeyaraj and Zadeh, Ogbanufe et al., Gale et al.).[12,46,47] The objective of these studies has been to elucidate how the intersection of institutional theory and cybersecurity offers various advantages in cybersecurity management. Specifically, this involves the creation of regulatory frameworks that provide organizations with a structured framework to adhere to, such as legal frameworks like General Data Protection Regulation (GDPR), aiding in avoiding penalties and maintaining legitimacy within industry norms. Additionally, adherence to industry standards signals organizational competence and commitment to effectively managing cyber risks, thereby enhancing competitive advantage. Moreover, collaborative efforts among organizations, as highlighted in Inter-organizational Dynamics, serve to address shared threats, aligning with industry norms and fortifying cybersecurity resilience amidst institutional pressures.

From an operational standpoint, institutional pressures manifest in three distinct forms, each exhibiting unique characteristics and levels of influence. Firstly, coercive pressures encompass regulatory mandates such as the GDPR, which impose legal obligations on organizations concerning data protection and breach notification. Additionally, industry standards like the Payment Card Industry Data Security Standards (PCI DSS), established by major credit card companies such as Visa, Mastercard, and American Express, exert coercive pressure by setting guidelines and requirements for handling payment card data to prevent fraud and enhance security.[48] These standards address various aspects of data security, including network security, data encryption, access control, regular monitoring and testing, and the maintenance of information security policies. Secondly, normative pressures stem from professionalization, dictating specific work methods and practices associated with a particular profession.[21,42] As highlighted by Gale et al. and Slapničar et al.,[12,49] these pressures may arise from formal education, training, professional certifications, and adherence to professional standards and networks, aiming to standardize practices in the sector through professional certifications, such as ISO or Cyber Essentials. Through these certifications, professionals advocate for structures, processes, and behaviors recognized as best practices in cybersecurity. Lastly, mimetic pressures emerge when organizations imitate practices perceived as legitimate by others, thereby legitimizing their practices.[21,42] Information exchange about practices, actions, and behaviors becomes crucial in this context. Following Gale et al. in the cybersecurity domain, mimetic forces include professionals moving between organizations, engaging the same external consultants, procuring technology from the same suppliers, and referring to the same publications.[12]

Stakeholder theory

Stakeholder theory is an organizational and management theory that emphasizes the importance of considering the interests and concerns of various stakeholders in decision-making and organizational actions[22,23,50] In traditional business thinking, the primary focus was often on maximizing value for shareholders; however, stakeholder theory suggests that companies should take into account the needs and perspectives of all individuals or groups with interests in the organization.

Stakeholder theory has been applied in the field of cybersecurity, examining their impact on cybersecurity management (for example, see Bauer and Van Eeten, Fischer-Hübner et al., Bansal and Axelton).[51–53] Specifically, stakeholder theory holds importance across various dimensions. Firstly, concerning the protection of customer data, as companies routinely collect and maintain customer data as part of their operations. Stakeholder theory emphasizes the importance of safeguarding this data, not only for the benefit of shareholders to avoid legal repercussions and reputational harm but also for the well-being and confidence of customers themselves.[51,52] Secondly, the welfare and security of employees, who serve as pivotal stakeholders in any organizational setup, are at risk. Following Kemper,[54] cybersecurity measures are indispensable for safeguarding their personal information, ensuring the security of their work environment, and screening against potential cyber threats that could disrupt their workflow or compromise confidential company data. Thirdly, concerning supplier relations, companies frequently depend on suppliers for diverse goods and services, with these suppliers potentially accessing sensitive information or systems.[55–57] By implementing cybersecurity measures, companies not only protect their data but also that of their suppliers, thereby raising trust and fostering continuing relationships. Moreover, the impact on the community holds significant weight, as cybersecurity incidents can resound more broadly within the community, particularly if they culminate in data breaches, financial losses, or disruptions to vital services. Stakeholder theory advocates for companies to contemplate the potential harm to the community while evaluating and mitigating cybersecurity risks. Lastly, regulatory compliance assumes principal importance, as governments and regulatory bodies routinely establish cybersecurity standards to safeguard the interests of various stakeholders, including consumers, businesses, and the general public.[52] The concept of self-efficacy strongly influences how effectively an organization can implement these stakeholder-driven cybersecurity measures.[58] High self-efficacy within an organization enhances its ability to adopt and adapt cybersecurity practices that not only meet regulatory standards but also align with the broader expectations of all stakeholders, ensuring comprehensive security measures are in place. In this context, conforming to these regulations is not merely a legal requisite but also aligns with stakeholder theory by showcasing a commitment to the broader social welfare. In essence, the nexus between stakeholder theory and cybersecurity underscores the necessity of considering the interests and welfare of all affected parties by a company's cybersecurity practices, transcending beyond just shareholders. By prioritizing the protection of customer data, ensuring employee safety, cultivating trust with suppliers, minimizing community impact, and complying with regulations, companies can uphold ethical principles while bolstering their cybersecurity posture.

Research model

Our research model delineates the influence of the business environment on cybersecurity implementation. We identify two key dependent variables for this investigation. Firstly, we examine the attainment of standards, such as ISO 27000 or Cyber Essentials. Secondly, we assess the integration of cybersecurity within the decision-making structures of the organization, notably within the board of directors.

To comprehend the environmental impact, we adopt two theoretical frameworks: institutional theory and stakeholder theory. Institutional theory underscores the role of institutional pressures as a catalyst for organizational behaviors, encompassing varying levels of pressures—coercive, normative, and mimetic. Conversely, stakeholder theory posits a reciprocal relationship, where organizations are influenced by their environment while also exerting influence, acknowledging diverse stakeholder typologies. Thus, our analysis incorporates two variables to estimate environmental impact: stakeholder typology and pressure intensity. In our investigation, we explore a spectrum of stakeholders, including governmental bodies, consumers, regulatory agencies, and the supply chain, among others. Additionally, we examine different degrees of pressure, ranging from coercive to mimetic. Consequently, our study poses two central research questions:

Research question 1 (RQ1): How does the business environment impact the adoption of cybersecurity standards within organizations?

Research question 2 (RQ2): How does the business environment influence the engagement of company boards in cybersecurity governance?

Furthermore, in our research, we acknowledge the heterogeneity of company behaviors regarding the implementation of standards and the integration of cybersecurity into company boards. In this context, we explore how the environment influences companies' cybersecurity practices, taking into account this diversity. Therefore, we pose the following research question:

Research question 3 (RQ3): How does the business environment influence companies, considering the heterogeneity in the implementation of standards and the integration of cybersecurity into company boards?

Methodology

Sample

To develop the research, we conducted an empirical study based on the Cyber Security Longitudinal Survey, administered by Ipsos Mori for the geographic area of the UK.[24] The survey utilized the government's Inter-Departmental Business Register (IDBR) as the sample frame, encompassing businesses across all sectors in the UK at the enterprise level. The IDBR is a primary sample frame for government business surveys and official statistics compilation.

The objective of the database is to enhance understanding of cybersecurity policies and processes within companies and organizations, as well as the linkages between these policies and processes and the likelihood and impact of a cyber-incident. It aims to quantify specific actions that result in improved cyber incident outcomes.

Data were collected through a multimode probability random survey (telephone and online). The first wave was conducted between March 9th and July 15th, 2021, gathering data from over 1,700 businesses and organizations in the UK. The second wave, the primary focus of our study, was conducted between April 8th and June 28th, 2022, gathering data from over 1,200 businesses and organizations. In Table 1, we observe the distribution of the sample by size, both for the years 2021 and 2022. In Table 2, we present the distribution of companies by sector according to the NACE classification.

Table 1. Distribution by sample size.

	2021		2022	
SIZE	Frequency	Per cent	Frequency	Per cent
Under 50	–	–	11	1.0
50–249	835	48.0	408	38.5
250–499	173	9.9	108	10.2
500–999	108	6.2	77	7.3
1,000 or more	89	5.1	83	7.8
Missing	536	30.8	373	35.2
Total	1741	100.0	1061	100.0

Table 2. Distribution by sample sector.

	2021		2022	
Sector	Frequency	Per cent	Frequency	Per cent
Utilities or production	13	.7	4	.4
Manufacturing	194	11.1	119	11.2
Construction	63	3.6	43	4.1
Retail or wholesale (including vehicle sales and repairs)	174	10.0	101	9.5
Transport or storage	64	3.7	35	3.3
Food or hospitality	116	6.7	63	5.9
Information or communication	107	6.1	53	5.0
Finance or insurance	50	2.9	28	2.6
Real estate	11	.6	6	.6
Professional, scientific, or technical	92	5.3	45	4.2
Administration	144	8.3	94	8.9
Education (excluding public sector schools, colleges, and universities)	36	2.1	17	1.6
Health, social care, or social work (excluding NHS)	105	6.0	61	5.7
Arts or recreation	26	1.5	14	1.3
Service or membership organisations	10	.6	5	.5
Charity	536	30.8	688	64.8
Total	**1741**	**100.0**	**1061**	**100.0**

Measures

The first dependent variable refers to the implementation of cybersecurity standards. The questionnaire inquires: Which of the following standards or accreditations, if any, does your organization adhere to? The questionnaire presents a multi-item response as follows: i) ISO 27001; ii) Cyber Essentials; iii) Cyber Essential Plus; and iv) Any other standards or accreditations. We coded this question, creating a variable (*standards*), as a binary variable, where it is assigned a value of zero if the company does not have any standards implemented and 1 if it has any of the aforementioned standards.

The second dependent variable concerns the integration of cybersecurity into the company's board. The questionnaire presents the question as a multi-item query: Does your organization have. . .?: i) One or more board members whose roles include oversight of cyber security risks; and ii) A designated staff member responsible for cybersecurity, who reports directly to the board. We created a new cumulative variable (*board*), reflecting potential board activities in terms of cybersecurity.

As independent variables, we considered the influence of the supply chain, sector, government actions, and stakeholder influences. The first independent variable assesses the influence of the supply chain on the management of companies and organizations. The questionnaire asks the following question: In the last 12 months, has your organization carried out any work to formally assess/manage potential cybersecurity risks presented by any suppliers/partners? The question has a multi-item response, including normative and coercive actions: i) Carried out a formal assessment of their cybersecurity, e.g., an audit; ii) Set minimum cybersecurity standards in supplier contracts; iii) Requested cybersecurity information on their supply chains; iv) Given them information or guidance on cybersecurity; and v) Stopped working with a supplier following a cyber-incident. In line with the previous variables, we created a new variable (*supplyrisk*) as a cumulative index of the five items.

The second set of independent variables captures the influence of the sector through mimetic actions, in terms of adopting cybersecurity practices that other companies within the sector have taken. The questionnaire poses a first question: In the last 12 months, have you reviewed or changed any cybersecurity policies or processes as a result of another organization in your sector experiencing a cybersecurity incident? (*peerincident*). The second question is: In the last 12 months, have you reviewed or changed any cybersecurity policies or processes as a result of another organization in your sector implementing similar measures? (*peermimetic*).

The next independent variable refers to the government's influence on cybersecurity management through normative actions. The questionnaire asks: In the last 12 months, has your organization used any information or guidance from the National Cyber Security Centre (NCSC) to inform your approach to cybersecurity? The response is multi-item: i) NCSC weekly threat reports; ii) The 10 Steps to Cyber Security; iii) The Cyber Security Board Toolkit; iv) NCSC guidance on secure home working or video conferencing; v) NCSC guidance for moving your business online; and vi) NCSC's Cyber Assessment Framework. The new variable (*NCSC*) captures the utilization of any of these normative mechanisms.

Lastly, the influence variable measures stakeholder influence on cybersecurity management, using coercive, normative, and mimetic influence mechanisms. The question posed is: Over the last 12 months, how much have your actions on cybersecurity been influenced by feedback from: i) External IT or cybersecurity consultants; ii) Any investors or shareholders; iii) Your customers; iv) Regulators for your sector; v) Your insurers; and vi) Whoever audits your accounts. In line with previous variables, we coded the variable (*influence*) as a cumulative index of the six items.

To control the results, we have included two control variables: the company's ability to improve in terms of cybersecurity and the incidents experienced in the last 12 months. Existing literature has already noted the positive impact of these variables on increasing cybersecurity measures within companies.[59–61] Specifically, the first variable is measured using a multi-item question. The question posed is: In this time, has your organization taken any steps to expand or improve any of the following aspects of your cybersecurity?: i) processes for updating and patching systems and software; ii) monitoring of users; iii) processes for managing cybersecurity incidents; iv) malware defenses; v) processes for user authentication and access control; vi) monitoring of systems or network traffic; and vii) network security. Consistent with previous variables, we recoded this variable (*improve*) as a cumulative index.

The second control variable measures the incidents experienced by organizations. The questionnaire presents the following question: Have any of the following happened to your organization in the last 12 months?: i) devices becoming infected with ransomware; ii) devices becoming infected with other malware (e.g., viruses, Trojans, or spyware); iii) unauthorized accessing of files, devices, networks, or servers by staff, even if accidental; iv) unauthorized accessing of files, devices, networks, or servers by people outside the organization; v) attacks attempting to slow down or take down websites, applications, or online services, i.e., denial of service attacks; vi) attempted hacking of online bank accounts; vii) attempted hacking of websites, social media, or user accounts; viii) people impersonating the organization in e-mails or online; ix) staff receiving fraudulent e-mails or attachments, or arriving at fraudulent websites, i.e., phishing attacks; x) unauthorized listening into video conferences or instant messaging; and xi) any other types of cybersecurity incidents. The *incidents* variable is created as a cumulative index of these 11 items.

Econometric method

To investigate our research questions through simulation, we employ ANNs, specifically a multilayer perceptron (MLP) architecture, as illustrated in Figure 1. This architecture functions as a supervised network, allowing for comparisons between predicted outcomes and known values of the independent variables. The MLP architecture consists of an input layer, hidden layers, and an output layer, with interconnected neurons and associated weights facilitating the analysis of interactions among input variables. In addition to traditional regression analysis, employing the ANN approach, as indicated by Paliwal and Kumar and Smith and Gupta,[26,62] helps address collinearity issues and unbalanced databases. This is particularly advantageous in cybersecurity research, where there are often varying responses to cybersecurity-related inquiries, leading to unbalanced datasets.[25]

The ANN-MLP architecture design was guided by the methodologies proposed by Wang and Arranz et al.[41,63] This design process involves two key considerations: determining the optimal number and size of hidden layers and selecting an appropriate learning

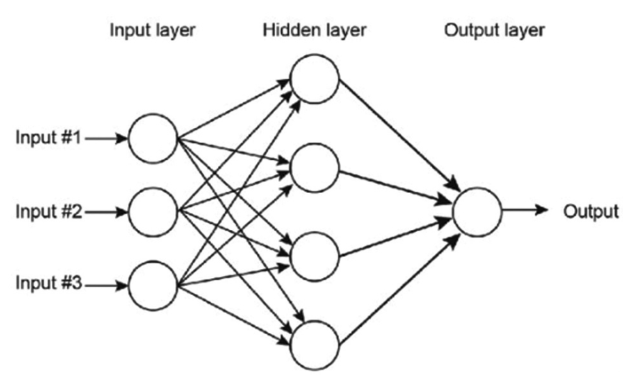

Figure 1. ANN Multilayer Perceptron (MLP) architecture. *Source*: Fernandez de Arroyabe et al. (2023b).

algorithm. Firstly, we explored various combinations of hidden layers and neurons through iterative testing, employing a trial-and-error approach to minimize error.[41,64] Different activation functions were tested to identify the architecture that best minimizes error. Secondly, we employed a backpropagation algorithm for the learning process, which iteratively adjusts the connection weights of each neuron to minimize error. The analytical equation representing our simulation with the ANN-MLP architecture is as follows

$$Digitalisation = h\left[\sum_{k=1}^{6} \alpha_k \cdot g\left(\sum_{j=1}^{6} \beta_{jk} \cdot X_j\right)\right]$$

with X_j being the input variable;

j the number of input variables;

h(.) and *g(.)* the activation functions;

α_k and β_{jk} the input and hidden network weights, respectively;

and *k* the number of hidden layers.

In Table 3, we show the ANN-MLP architectures for each simulation, containing both its structure and activation function.

Analysis and results

To ensure the robustness of our findings, we assessed the reliability and validity of our survey instrument and the resulting data. Firstly, in terms of the reliability of our survey, we compared the responses collected during the two survey waves and found no significant disparities between them. Secondly, following Podsakoff et al.[65] we conducted some checks to validate the reliability of both the questionnaires and responses, addressing both the common method variance (CMV) and common method bias (CMB). Through this analysis, we identified eight distinct constructs that collectively explained 63.20% (2021) and 59.89% (2022) of the variance. In each year, the primary factor explained approximately 20% of the variance, meeting the recommended threshold of 50%. Therefore, we conclude that CMV and CMB are not significant concerns in our research findings.

Prior to analyzing the research questions, we conducted a descriptive analysis of the variables utilized in the investigation. Table 4 presents the findings of the analysis of the dependent variables. Initially, this table provides insights into the cybersecurity certification status of the sample of companies for the years 2021 and 2022. In 2021, out of a total of 1,741 surveyed companies, 256 companies (14.7% of the sample) were certified with ISO 27001, 350 companies (20.1% of the sample) held the Cyber Essentials certification, 153 companies (8.8% of the sample) possessed the Cyber Essentials Plus certification, and 712 companies (41.1% of the sample) did not hold any of these certifications. Similarly, for the year 2022, out of a total of 1,061 companies surveyed, we observed a slight increase in the percentages. To examine if there were any

Table 3. ANN-MLP architecture for RQ1 and RQ2.

Research Question	Year	Output variable	ANN architecture	Activation Functions	Error Function	Input variables
First	2021	• Standard	6-3-1	• Hyperbolic tangent • Identity (SoftMax)	Cross-entropy	• NCSC • Supplyrisk • Peermimetic • Peerincident • Influence • Improve • Incidents
	2022	• Standard	6-4-1	• Hyperbolic tangent • Identity (SoftMax)	Cross-entropy	• NCSC • Supplyrisk • Peermimetic • Peerincident • Influence • Improve • Incidents
Second	2021	• Board	6-4-1	• Hyperbolic tangent • Identity (SoftMax)	Cross-entropy	• NCSC • Supplyrisk • Peermimetic • Peerincident • Influence • Improve • Incidents
	2022	• Board	6-3-1	• Hyperbolic tangent • Identity (SoftMax)	Cross-entropy	• NCSC • Supplyrisk • Peermimetic • Peerincident • Influence • Improve • Incidents

Table 4. Descriptive statistics of the dependent variables.

Dependent Variables	2021		2022	
Standards	Frequency	Per cent	Frequency	Per cent
ISO 27001	256	14.7	163	15.4
Cyber essentials	350	20.1	292	27.5
Cyber essentials plus	153	8.8	120	11.3
None of these	712	41.1	404	38.1
BOARD				
Board members whose roles of cyber security risks	840	48.2	532	50.1
A designated staff member responsible for cyber security in the board	1014	58.2	648	61.1
Total	**1,741**	**100%**	**1061**	**100**

significant differences, we conducted an ANOVA analysis, and the results did not reveal any significant differences. For the SME population (i.e. companies with less than 250 employees) 34% of the companies had either the ISO 27001, the Cyber Essentials or the Cyber Essentials Plus accreditation, being the Cyber Essentials the most common across SMEs. Regarding the integration of cybersecurity into company boards, we observe from the table that approximately 50% of the companies have already integrated one or more individuals into the board, with cybersecurity being a topic of discussion. We also note an insignificant increase in the year 2022 compared to the previous year. Similarly, we did not find any significant differences. This distribution is similar for SMEs.

Table 5 presents the descriptive results of the independent variables. The first variable (*supplyrisk*) provides insights into the influence of the supply chain on cybersecurity management within companies for the years 2021 and 2022. In 2021, among the 1,741 surveyed companies, 248 (14.2% of the sample) conducted a formal assessment of their cybersecurity through an audit. Additionally, 153 companies (8.8% of the sample) established minimum cybersecurity standards in supplier contracts, while 178 companies (10.2% of the sample) requested cybersecurity information from their supply chains. Furthermore, 229 companies (13.2% of the sample) offered cybersecurity information or guidance to their suppliers, and 48 companies (2.8% of the sample) terminated relationships with suppliers following a cyber-incident. Similarly, in 2022, among the 1,061 surveyed companies, we obtained comparable results without significant differences between the two years. For the SMEs, only 20% of the companies carried out any work to formally assess/manage potential cybersecurity risks presented by any suppliers/partners. The second variable (*peer*) examines the influence of the environment on cybersecurity, considering responses to mimetic pressures such as incidents within the sector or changes in sector strategies. In 2021, out of the total of 1,741 organizations surveyed, 304 (17.5% of the sample) were aware of another organization within their sector experiencing a cybersecurity incident. Additionally, 219 organizations (12.6% of the sample)

Table 5. Descriptive statistics of the independent variables.

Independent Variables	2021		2022	
Supplyrisk	Frequency	Per cent	Frequency	Per cent
Carried out a formal assessment of their cyber security, e.g. an audit	248	14.2%	118	11.1
Set minimum cyber security standards in supplier contracts	153	8.8	171	16.1
Requested cyber security information on their supply chains	178	10.2	168	15.8
Given them information or guidance on cyber security	229	13.2	144	13.6
Stopped working with a supplier following a cyber- incident	48	2.8	28	2.6
PEER				
Another organization in your sector experiencing a cyber-incident	304	17.5	200	18.9
Another organization in your sector implementing similar measures	219	12.6	124	11.7
NCSC				
NCSC weekly threat reports	160	9.2	162	15.3
The 10 Steps to Cyber Security	265	15.2	233	22
The Cyber Security Board Toolkit	113	6.5	135	12.7
NCSC guidance on secure home working or video conferencing	168	9.6	151	14.2
NCSC guidance for moving your business online	51	2.9	48	4.5
NCSC's Cyber Assessment Framework	204	11.7	199	18.8
INFLUENCE				
External IT or cyber security consultants	492	28.3	570	53.7
Any investors or shareholders	161	13.4	191	17.0
Your customers	266	15.3	279	26.3
Whoever audits your accounts	357	20.5	314	39.1
Your insurers	491	28.2	396	37.3
Regulators for your sector	420	24.1	269	25.4
Total	**1,741**	**100%**	**1061**	**100**

Table 6. Descriptive statistics of the control variables.

Control variables	2021		2022	
Improve	Frequency	Per cent	Frequency	Per cent
Your processes for updating and patching systems and software	857	49,2	537	50.6
The way you monitor your users	651	37.4	383	36.1
Your processes for managing cyber security incidents	769	44.2	511	48.2
Your malware defences	977	56.1	637	60.0
Your processes for user authentication and access control	1070	61.5	704	66.4
The way you monitor systems or network traffic	808	46,4	522	49.2
Your network security	1129	64.8	711	67.0
INCIDENTS				
Devices becoming infected with ransomware	51	2.9	40	3.8
Devices becoming infected with other malware (e.g. viruses, Trojans or spyware)	184	10.6	125	11.8
Unauthorized accessing of files, devices, networks or servers by staff, even if accidental	91	5.2	76	7.2
Unauthorized accessing of files, devices, networks or servers by people outside your organization	86	4.9	48	4.5
Attacks that try to slow or take down your website, applications or online services, i.e. denial of service attacks	103	5.9	70	6.6
Attempted hacking of online bank accounts	57	3.3	45	4.2
Attempted hacking of your website, social media or user accounts	198	11.4	137	12.9
People impersonating your organization in e-mails or online	665	38.2	448	42.2
Staff receiving fraudulent e-mails or attachments, or arriving at fraudulent websites i.e. phishing attacks	1187	68.2	783	73.8
Unauthorized listening into video conferences or instant messaging	22	1.3	5	.5
Any other types of cyber security incidents	102	5.9	80	7.5
Total	**1,741**	**100%**	**1061**	**100**

reported that another organization in their sector had adopted similar cybersecurity measures. Similarly, in 2022, 200 organizations (18.9% of the sample) reported awareness of another organization within their sector encountering a cybersecurity incident, while 124 organizations (11.7% of the sample) indicated awareness of another organization in their sector implementing similar cybersecurity measures. These percentages are very similar for the SME population, where 13.2% and 9.7% of the companies reviewed or changed any cybersecurity policies or processes as a result of other organizations in the sector experiencing a cybersecurity incident and implementing similar measures, respectively. The third variable (*NCSC*) in our analysis pertains to normative actions undertaken by organizations based on the resources provided by the NCSC. Within the scope of our study conducted in 2021, encompassing a total of 1,741 surveyed organizations, the utilization and perceived value of various NCSC resources were examined. Notably, findings revealed that a proportion of respondents acknowledged the significance of specific resources. For instance, 160 organizations (9.2% of respondents) reported deriving value from NCSC weekly threat reports. Similarly, 265 organizations (15.2% of respondents) found utility in implementing *The 10 Steps to Cyber Security*. Additionally, 113 organizations (6.5% of respondents) disclosed their utilization of the *Cyber Security Board Toolkit. Moreover*, NCSC guidance on secure home working or video conferencing was deemed helpful by 168 organizations (9.6% of respondents), while 51 organizations (2.9% of respondents) availed themselves of NCSC guidance for transitioning their business operations online. Furthermore, 204 organizations (11.7% of respondents) reported employing *NCSC's Cyber Assessment Framework*. Similarly, for the year 2022, minor variations were observed compared to the previous year, with an increase in the percentage of organizations utilizing NCSC-driven mechanisms. Around 20% of SMEs declared to find useful or valuable any of the NCSC resources. Finally, the table presents data on the influence of various stakeholders on cybersecurity practices (*influence*) (coercive, normative and mimetic), within organizations. The categories include external IT or cybersecurity consultants, investors or shareholders, customers, auditors of organizational accounts, insurers, and regulators specific to the organization's sector. For example, in the year 2021, 492 organizations (28.3% of the sample) reported being influenced by external IT or cybersecurity consultants, while in 2022, this number increased to 570 organizations (53.7% of the sample). Similar trends are observed across other stakeholder categories, indicating varying degrees of influence exerted by different external entities on cybersecurity practices within organizations over the two years under study. Majority of SMEs (57.10%) did not report influence from stakeholders on their cybersecurity practices, however, the most significant one is IT or cybersecurity consultants across both years.

Table 6 presents data about the augmentation of cybersecurity measures and encountered incidents within organizations, serving as control variables in our research. Within the *improve* variable, diverse aspects of cybersecurity enhancement are delineated alongside the number of respondents who reported enhancements in each domain. The percentages provided reflect the proportion of organizations indicating improvement within each category. Notably, the highest reported enhancement was observed in improving the processes for user authentication and access control, with 1,070 organizations (61.5%) reporting improvements. Specifically, 857 organizations have prioritized improving the processes for updating and patching systems and software, involving the regular updating of systems and software to address vulnerabilities. Additionally, 651 organizations are focusing on refining the way they monitor their users, potentially through the implementation of tools to track user activities. Furthermore, 769 organizations are concentrating on refining the processes for managing cybersecurity incidents, aiming to develop effective protocols for incident response and mitigation. Moreover, 977 organizations are placing emphasis on enhancing malware defenses, which may involve deploying updated antivirus software and conducting regular malware scans. Similarly, 808 organizations are directing efforts toward improving the monitor systems or network traffic, likely through the deployment of intrusion detection systems. Lastly, 1129 organizations are concentrating on enhancing network security, which could encompass implementing firewalls and conducting regular security assessments to fortify network defenses against potential breaches. As with the main sample, the most common improvement for SMEs is network improvement followed by user authentication and access control. In the *incidents* variable, different types of cybersecurity incidents are listed along with the number of occurrences reported by respondents. Similarly, percentages indicate the proportion of respondents who reported experiencing each type of incident. For example, the most commonly reported incident was *Staff receiving fraudulent e-mails or attachments, or arriving at fraudulent websites (i.e., phishing attacks)*, with 1,187 organizations (68.2%) reporting this type of incident, while the least reported incident was *Unauthorized listening into video conferences or instant messaging*, with only 22 organizations (1.3%) reporting such incidents. In this line, over 40% of SMEs reported phishing attacks and over 23% reported incidents related to people impersonating your organization in e-mails or online.

Regarding the first research question (RQ1), which investigates how the business environment impacts the adoption of cybersecurity standards within organizations, the results of the simulation using ANN-MLP are presented in Figures 2 and Table 7. We assessed the suitability of the ANN-MLP design by employing cross-entropy error in both the training and testing phases, along with evaluating the predictive capability

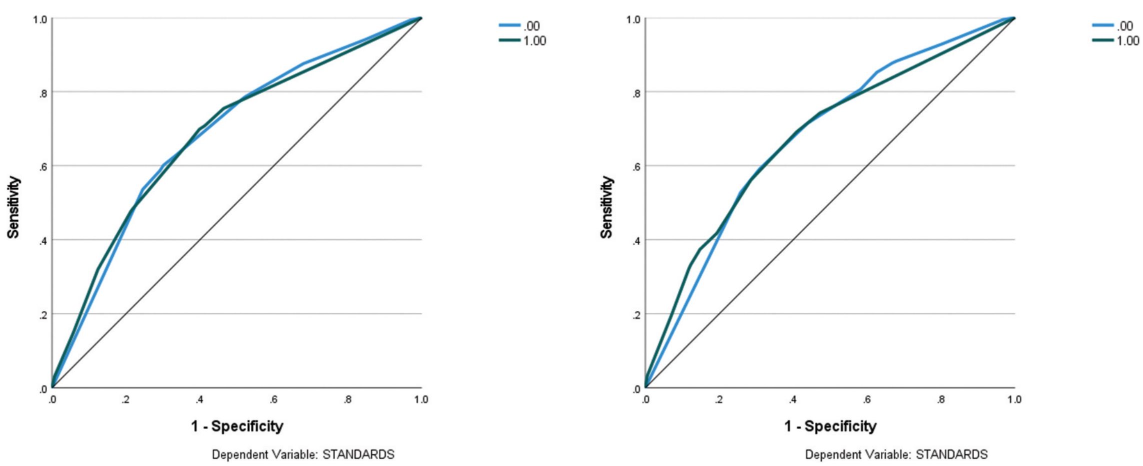

Figure 2. ROC curves in ANN-MLP simulation for RQ1.

Table 7. RQ1 simulation outcomes.

Dependent Variable *Standard*	2021 Importance	2021 Normalized Importance	2022 Importance	2022 Normalized Importance
NCSC	.185	90.6%	.247	100.0%
SUPPLYRISK	.151	73.8%	.140	56.8%
PEERINCIDENT	.058	28.5%	.019	7.9%
PEERMIMETIC	.146	71.4%	.099	40.3%
INFLUENCE	.132	64.8%	.109	44.1%
IMPROVE	.204	100.0%	.209	84.4%
INCIDENTS	.123	60.4%	.176	71.3%

of our models using the ROC (Receiver Operating Characteristic) curve. The ROC curve is a graphical representation of sensitivity versus specificity and serves as an indicator of classification performance.[26] The accuracy of the model for both years is higher when the curve deviates from the 45-degree line. Specifically, both ROC curves demonstrated that the chosen architectures could predict over 60% of the output variable values (Figure 2).

Regarding the results, Table 7 displays the simulation outcomes. This table offers insights into the significance of various independent variables in forecasting cybersecurity impact using ANN-MLP analysis. The *Importance* column quantifies the importance score of each independent variable in predicting the cybersecurity impact. The *Normalized Importance* column illustrates the relative importance of each independent variable after normalization, facilitated by Garson's algorithm.[66–68] This algorithm calculates the absolute sum of the weights of each variable in every neuron and layer, assigning a percentage value relative to the most important variable. Notably, the normative measures of the *NCSC* rank as the most significant external predictor in both years, boasting an importance score of .185 and normalized importance of 90.6% in 2021. Following closely is the supply chain, exhibiting an importance score of .151 and a normalized importance of 73.8%. Moreover, *peermimetic* and *influence* emerge as the third and fourth most influential variables, with an importance score of .146 and a normalized importance of 73.7%, and .132 and a normalized importance of 64.8%, respectively. The variable *peerincident* demonstrates moderate importance in forecasting cybersecurity impact, with scores of .058 and a normalized importance value of 28.5%. Furthermore, the table presents results for the year 2022, where we can observe that with minor variations, the displayed results are similar. Additionally, we conducted an ANOVA analysis to determine the presence of significant differences between the two years, and the results do not show any disparities. The control variables *improve* and *incidents* demonstrate the effect of both variables on the implementation of standards. We observe that both values have high normalized importance (100.0% and 60.4%, respectively), comparatively equivalent to the effect of *NCSC* on the implementation of standards, and to a lesser extent, *supply chain*. For the SMEs, the most significant predictors are *NCSC* (100% of normalized importance), *supply risk* (92.2%), followed by *incidents* (72.1%) and *improve* (61.3%).

Regarding the second research question (RQ2), which investigates the influence of the business environment on board engagement in cybersecurity governance, we employed an ANN-MLP simulation. The results of this analysis are presented in Table 8. Similar to a previous analysis, the model's predictive power was evaluated using the ROC curve and accuracy metrics. For both years of study, the selected ANN-MLP architectures demonstrated robust predictive capabilities, accurately forecasting over 60% of the output variable values (see Figure 3). This level of predictive accuracy suggests that our model captures significant patterns in the relationship between business environment factors and board-level cybersecurity governance engagement.

Building upon the model's predictive capabilities, Table 8 provides an overview of the analysis of the relative importance of various independent variables in predicting board engagement in cybersecurity governance. The findings reveal a spectrum of influential factors. Notably, *NCSC* demonstrates a moderate level of importance, scoring .111 in importance and having normalized importance of 48.8%. Conversely, *influence* emerges as a crucial predictor, with an importance score of .140 and normalized importance of 61.6%, indicating its significant contribution to the predictive power of the model. Additionally, *supplyrisk* stands out with an importance score of .141 and a normalized importance of 61.8%, suggesting its substantial influence in the predictive process, surpassing NCSC in importance. While *peerincident* shows the highest normalized importance with a value of .169 and a normalized importance of 74.2%; *peermimetic* exhibits importance scores of .071, indicating a lower level of normalized importance (31.3%). Moreover, Table 8 illustrates the outcomes for the year 2022, where it is evident that despite minor fluctuations, the presented results remain consistent.

Table 8. RQ2 simulation outcomes.

Dependent Variable	2021		2022	
Board	Importance	Normalized Importance	Importance	Normalized Importance
NCSC	.111	48.8%	.065	23.1%
SUPPLYRISK	.141	61.8%	.073	26.1%
PEERINCIDENT	.169	74.2%	.144	51.3%
PEERMIMETIC	.071	31.1%	.113	40.1%
INFLUENCE	.140	61.6%	.240	85.4%
IMPROVE	.140	61.4%	.085	30.3%
INCIDENTS	.228	100.0%	.281	100.0%

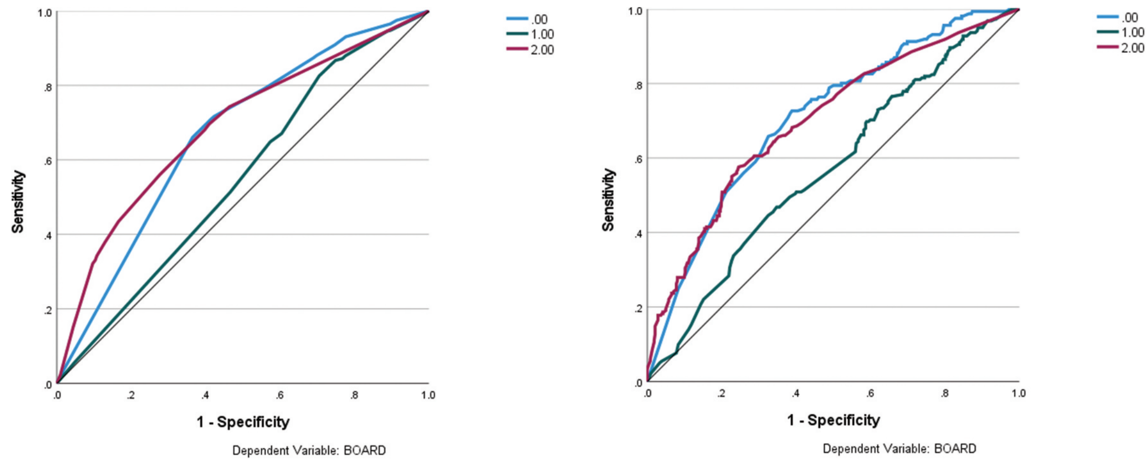

Figure 3. ROC curves in ANN-MLP simulation for RQ2.

Furthermore, we performed an ANOVA analysis to ascertain whether significant differences existed between the two years, and the findings indicate no discernible disparities. As in the previous analysis, the variables *improve* and *incidents* have a significant impact on the integration of cybersecurity into the boards of companies. As control variables, we observe that their normalized importance within firms is equivalent to external influence. For the SMEs, the most important factors are *improve* (100%) and *incident* (93.1%) followed by *supply risk* (85.4%), *NCSC* (70.3%) and *peermimetic* (62.9%).

Regarding the third research question (RQ3), which investigates the varied practices of companies concerning the adoption of standards and the incorporation of cybersecurity into their board activities, we undertook an exploratory study to categorize companies into clear groups based on their adherence to standards and the initiatives undertaken by their boards within the organization. We utilized a K-means clustering algorithm as our statistical approach,[69,70] and implemented a two-phase procedure. Initially, the inputs for the K-means algorithm included the standards adopted (*standards*) and the activities related to board governance within the company (*board activities*). Following this, we determined the most effective solution through Silhouette analysis.[69,70] This method allowed us to assess the robustness of our clustering solution, including the internal cohesion of each cluster and the distinction between different clusters. The silhouette score can vary from −1 to 1, with scores nearer to 1 indicating a stronger clustering solution. After calculating the Silhouette score, we found that a solution consisting of three clusters had a higher Silhouette score of 0.62. In addition to this, we performed an additional verification using the Bayesian Information Criterion (BIC),[71] which confirmed the solidity of our three-cluster solution in terms of both internal coherence and differentiation between clusters.

The outcome of the K-means cluster analysis led the categorization of SMEs into three distinct clusters. Furthermore, we conducted a robustness test of the analysis via ANOVA, revealing significant differences in the degree of adherence to standards and internet-related activities among SMEs belonging to each cluster. Tables 9 presents the results of the distribution of companies within each cluster, and the key characteristics of each cluster.

In Figure 4, we display the average values of the variables' *standard* and *board activities* based on companies' membership in each cluster. Specifically, Cluster 1 exhibits a higher level of board activities compared to all other clusters. Conversely, Cluster 3 demonstrates the highest level of standard implementation. These two clusters also show lower levels of board activities in the case of Cluster 3 and standard integration in the case of Cluster 1. However, Cluster 2 has minimal board activities in terms of cybersecurity and no implementation of standards. Based on these characteristics, we have categorized the clusters as follows: Proactive Governance Leaders (Cluster 1), characterized by high board engagement in cybersecurity matters but lower standard implementation; Reactive Compliance Adherents (Cluster 2), showing minimal board activities and standard

Table 9. Distribution of companies/cluster.

Cluster	Frequency	Per cent	Categorisation
1	620	35.6	Proactive Governance Leaders
2	697	40.0	Reactive Compliance Adherents
3	239	13.7	Strategic Standard Implementers
Total	1556	89.4	
Missing	185	10.6	
Total	**1741**	**100.0**	

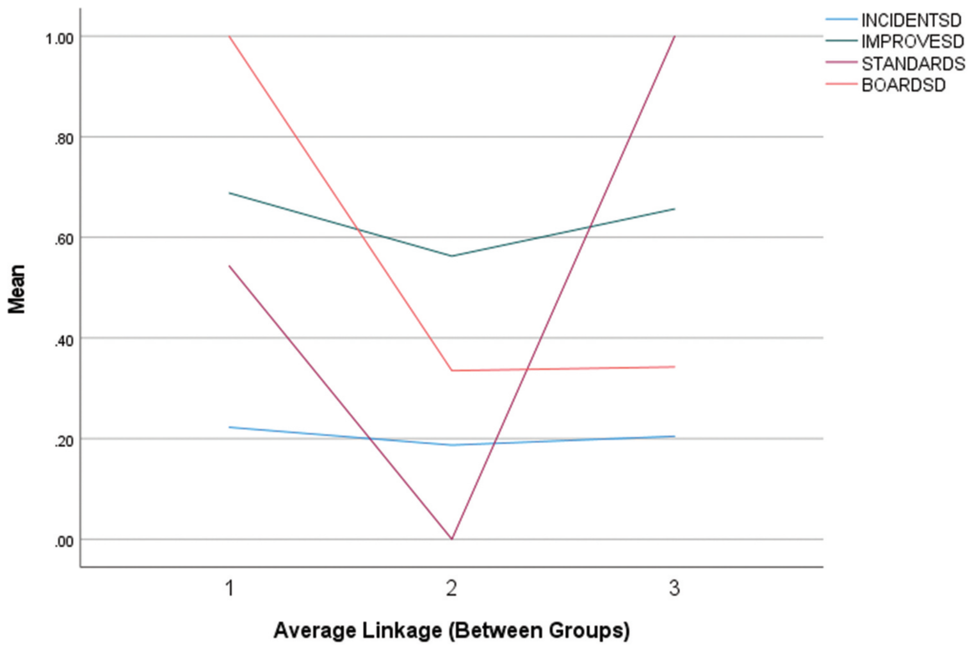

Figure 4. The average values of the variables' standard and board activities/cluster.

implementation, suggesting a reactive stance primarily driven by compliance requirements; and Strategic Standard Implementers (Cluster 3), exhibiting the highest level of standard implementation but lower board activities, indicating a strategic focus on cybersecurity through standardization rather than direct board involvement. These cluster categorizations provide valuable insights into the varied approaches SMEs adopt in addressing cybersecurity governance, reflecting different strategic priorities and resource allocations within the cybersecurity domain.

Figure 5 shows the influence of the environment on the sample companies based on their cluster membership. Overall, we observe that companies integrated into Cluster 1 are more influenced by various types of agents and levels of pressure. Secondly, Cluster 3 is influenced by the environment, with Cluster 2 being the least influenced by the environment in terms of impacting

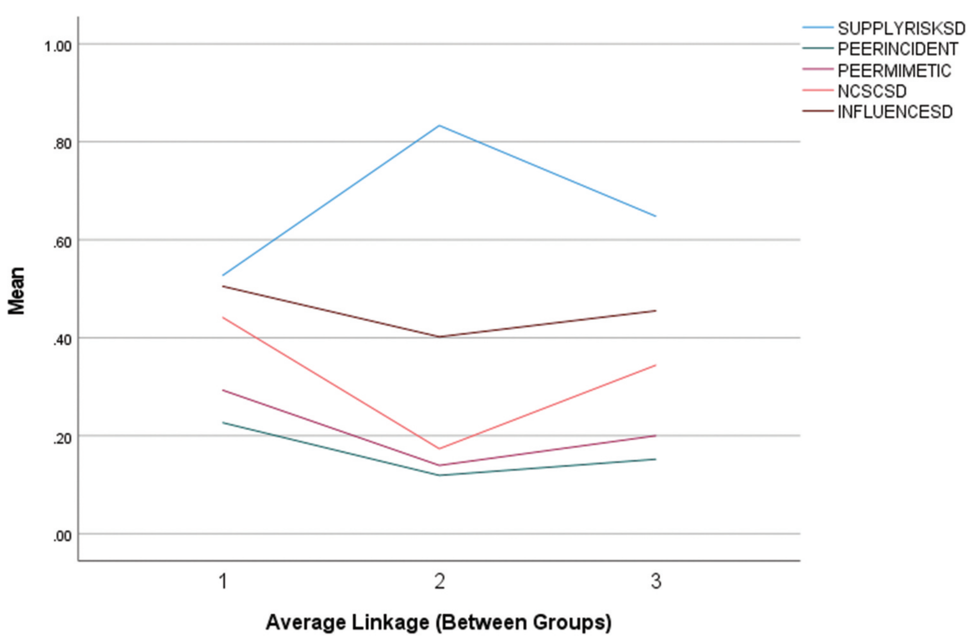

Figure 5. The average values of the independent variables/cluster.

cybersecurity activities. However, we note that the supply chain has the greatest impact on Cluster 2 compared to the other clusters.

Discussion

The findings of this study make a significant contribution to our understanding of the intricate relationship between the business environment and cybersecurity practices within organizations. By employing a multidimensional approach that incorporates both institutional and stakeholder theories, we have provided several insights into how the business environment impacts the adoption of cybersecurity standards and the integration of cybersecurity into organizational decision-making processes.

The descriptive analysis of the dataset provided an overview of the cybersecurity stance of UK companies during the years 2021 and 2022. Our examination focused on cybersecurity standards and the integration of cybersecurity into the boards of companies. Firstly, the data on standards showed a modest shift toward increased cybersecurity compliance among the surveyed companies. Specifically, the proportion of companies obtaining certifications such as ISO 27001 and Cyber Essentials exhibited incremental growth from 2021 to 2022. This trend suggests a growing recognition of the value of cybersecurity certifications in reinforcing organizational defenses against cyber threats. However, as noted by Mirtsch et al.,[7] the complexity, in terms of time and procedures, of implementing international standards acts as a barrier to higher degrees of implementation. Second, we also explored the extent to which cybersecurity is integrated into corporate governance structures, specifically within the boards of companies. Our findings indicate that approximately half of the surveyed companies have incorporated one or more individuals into their board of directors, with a specific focus on cybersecurity. This is noteworthy as it shows that cybersecurity is increasingly recognized as a critical discussion topic at the board level. These results align with existing literature, highlighting the growing trend toward integrating designated cybersecurity personnel within the corporate governance framework.[12,30] This shift not only facilitates a more agile approach to managing cybersecurity issues but also reflects a broader organizational transformation. Companies increasingly recognize the importance of transitioning the perception of cybersecurity from a purely operational concern to a strategic priority.[1,4] This evolution highlights the proactive measures companies are taking to enhance their cybersecurity attitude, recognizing the fundamental role of strategic governance in protecting against cyber threats.

From our findings, we observe that relationships with the supply chain significantly influence cybersecurity management in organizations. Pal and Alam and Melnyk et al. have previously noted that the implementation of basic cybersecurity criteria, such as coercive and normative measures, in agreements with the supply chain, coupled with an active exchange of cybersecurity practices and knowledge, reflects a shift toward more cooperative security efforts.[17,56] The application of these coercive measures in the supply chain may indicate that companies have taken firm actions, such as severing ties with suppliers after cybersecurity breaches, emphasizing the vital importance of cybersecurity in preserving supply chain integrity.[56,57] Moreover, our study highlights the impact of mimetic factors, such as industry-specific incidents or strategic changes, on organizations' cybersecurity policies. A significant portion of organizations acknowledged being aware of cybersecurity breaches within their industry and noted the implementation of similar security measures by their counterparts. This trend of mimetic behavior indicates that organizations are responding not only to immediate threats but also adapting to changes in the cybersecurity landscape, influenced by the experiences and actions of their peers. Thus, we extend previous literature on cybersecurity by highlighting how mimetic measures affect cybersecurity management in organizations.[46] Moreover, we observe that normative measures have an impact on cybersecurity management in organizations. This is evident in the reliance on guidance from authoritative sources such as the NCSC, which, suggests a strategic orientation toward informed decision-making regarding cybersecurity.[32] Therefore, from our results, we can confirm that the environment of companies and organizations affects cybersecurity management, with a diverse portfolio of measures including coercive, normative, and mimetic ones. Additionally, our findings shed light on the various impacts that external stakeholders have on corporate cybersecurity practices. The increasing reliance on external IT and cybersecurity advisors, along with the effects on investors, customers, auditors, insurers, and industry regulators, emphasizes the complex array of pressures and influences dictating corporate cybersecurity strategies. The trends we have observed confirm previous work demonstrating an expanded commitment to cybersecurity beyond individual organizational boundaries, incorporating a broad spectrum of perspectives and external pressures.

In our exploration of the first research question (RQ1), which investigates how the business environment affects the adoption of cybersecurity standards within organizations, the analysis identified the effectiveness of environmental influence on standard implementation. Our results demonstrate that normative institutional pressures from administrations such as the NCSC have a significant effect, normalizing procedures and practices. In this regard, Mirtsch et al. emphasize that standardization fundamentally involves creating routines and organizational procedures for cybersecurity management, thereby reducing potential vulnerabilities and hazards.[7] Similarly, we observe that interaction with suppliers and customers demands standardized practices to prevent potential incidents in the value chain, corroborating previous works highlighting the importance of standards in the supply chain.[13,57] Along the same lines, stakeholders interact with organizations and, in that interaction, apply pressure to establish standard cybersecurity processes to avoid potential incidents. In the context of SMEs, our results show that normative pressures, particularly those exerted by bodies like the NCSC, are markedly influencing these companies toward adopting standardized cybersecurity practices. This highlights the importance of such regulatory bodies in not only setting standards but also in fostering a cybersecurity culture that prioritizes resilience and proactive risk management within the SME sector.[12] The engagement with these standards reflects an increasing awareness among SMEs of the critical role that compliance plays in securing trust and competitiveness in digital markets.[7] Our findings reinforce previous studies highlighting organizations' susceptibility to stakeholder influence in improving cybersecurity practices.[51,52] Additionally, we observe that in quantitative terms, this effect is equivalent to that produced by internal drivers such as self-efficacy and incidents experienced by organizations. Previous literature highlighted how cybersecurity incidents impact organizations economically, operationally, and in terms of social responsibility, leading to a reactive effect on the likelihood of investing in cybersecurity protection.[59] Our results extend previous literature by highlighting how the environment has a similar quantitative effect on self-efficacy and incidents.

Regarding the second research question (RQ2), which investigates the influence of the business environment on company boards' engagement in cybersecurity governance, the findings demonstrate that the environment quantitatively influences similar internal drivers such as previous incidents and self-efficacy. More specifically, we observe differences in terms of the agents that affect and how they affect organizations' standardization. Our results show the mimetic influence on incidents in the sector. Jeyaraj and Zadeh have previously discussed sector incidents as a driver in organizations' protection.[46] We also observe, similar to the case of standardization, that interaction with the supply chain and stakeholders has a positive effect on integrating cybersecurity into the board. For SMEs, our analysis highlights the complex interplay of external and internal factors influencing the integration of cybersecurity within the strategic framework of company boards. The results show that while normative pressures from regulatory bodies such as the NCSC play a pivotal role, it is the direct interactions with suppliers and customers that exhibit a more pronounced influence on board-level cybersecurity engagement. Thus, the results show that active interaction with suppliers and consumers, combined with coercive and normative measures from regulators, insurers, etc., positively affects the strategic nature of cybersecurity in organizations. This is in line with Herr that have previously emphasized the role of insurers or regulators in cybersecurity management.[72] Furthermore, we also observe that regulatory measures from the NCSC have a positive effect on the integration of practices in the boards of companies, highlighting the importance of regulatory measures as a means to imbue cybersecurity with a strategic character.[25]

Finally, we can conclude from our results that the influence of the environment can have a specific character, aimed at achieving specific objectives such as standardization, as is the case with government normative measures, or mimetic pressures derived from sector incidents, which directly impact the active presence of cybersecurity in company boards. Moreover, our results allow us to identify environment pressures, such as relationships with the supply chain and the influence of stakeholders, which through coercive and normative pressures, generally influence cybersecurity management. Figure 6, we represent the effect of the environment, depending on the objective, standardization, and integration into the board, and its specificity.

These insights provide a detailed understanding of the various factors that drive both organizational and

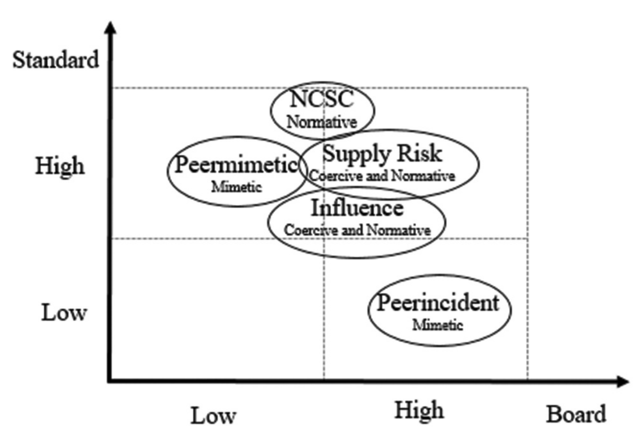

Figure 6. The matrix of performance/environment.

board-level engagement with cybersecurity, showcasing the complex interplay of external pressures and internal governance mechanisms.

Regarding the third research question (RQ3), which explores the heterogeneity of organizations' behaviors regarding the implementation of standards and the integration of cybersecurity in the board of the companies, we have developed a taxonomy for the three clusters by categorizing them based on their characteristic features, behaviors, and attributes as observed in the data. This taxonomy provides a structured framework for understanding the distinct characteristics, behaviors, and attributes of each cluster, facilitating deeper insights into their cybersecurity governance practices and strategic orientations.

Cluster 1: Proactive governance leaders

This cluster consists of companies exemplifying proactive involvement and leadership in cybersecurity governance. For instance, financial institutions such as banks and investment firms often fall into this category. These companies display extensive board activities, showcasing a robust dedication to supervision of cybersecurity matters and making strategic decisions. While they also implement cybersecurity standards, their focus might be somewhat less pronounced than in Cluster 3. However, they remain highly responsive to environmental stimuli, showing an inclination to adjust to emerging cybersecurity threats and changing industry dynamics.

Cluster 2: Reactive compliance adherents

This cluster represents organizations that demonstrate a reactive approach to cybersecurity governance and standardization. An example of a sector that could be included in this cluster is the retail industry. Retail companies often exhibit minimal board activities related to cybersecurity, indicating a lack of strategic oversight or prioritization of cybersecurity at the leadership level. Instead, their focus may be primarily on operational aspects of the business, such as sales and customer service. However, when stimulated by regulatory requirements or external pressures, such as supply chain regulations, these organizations adhere to cybersecurity practices to ensure compliance. While they may be less influenced by environmental factors compared to other clusters, retail companies show heightened sensitivity to supply chain dynamics, given their reliance on various suppliers and partners for inventory, distribution, and other aspects of their operations.

Cluster 3: Strategic standard implementers

This cluster comprises organizations that prioritize the rigorous implementation of cybersecurity standards and protocols, representing sectors such as finance and healthcare. These organizations demonstrate the highest level of standard implementation among the clusters, reflecting a constant commitment to cybersecurity best practices and regulatory compliance. While their board activities related to cybersecurity may be comparatively lower that Cluster 1, they compensate by focusing on robust cybersecurity standards and protocols to safeguard sensitive data and ensure regulatory compliance. Despite their careful approach to internal cybersecurity measures, they exhibit moderate sensitivity to environmental influences, demonstrating a balanced approach to cybersecurity management that integrates both internal standards and external contextual factors, such as emerging threats and industry regulations.

Conclusion

In this study, we have investigated the intricate dynamics of cybersecurity governance and standardization within organizations, investigating the impact of various factors such as supply chains, environmental influences, and stakeholder engagement, among others. Through the application of advanced analytical methods like ANN-MLP models and K-means cluster analysis, we have uncovered valuable insights into the complex interplay between organizational practices and external forces in shaping cybersecurity strategies.

Theoretical contributions

From a *theoretical standpoint*, our research makes significant contributions to the cybersecurity field. By uncovering how external pressures, including regulatory mandates and industry norms, shape organizational behavior in cybersecurity governance, we align with institutional theory. The identification of clusters based on cybersecurity practices further emphasizes the role of institutional isomorphism in fostering conformity among organizations operating within similar environments. Additionally, our study enriches stakeholder theory by clarifying the diverse influences applied by stakeholders on organizational cybersecurity practices. By recognizing the complex nature of stakeholder pressures, our research underscores the importance of effectively managing stakeholder relationships to strengthen cybersecurity resilience.

Managerial and policy implications

Our research also provides some interesting *managerial and policy implications* for enhancing cybersecurity within organizations. Firstly, similar to the significance of incident perception and self-efficacy, we highlight the importance of environmental influence effectiveness in cybersecurity practices. This emphasizes the need for organizational managers to foster permeability toward the environment. Secondly, our study reveals a diverse array of agents and levels of influence shaping a complex ecosystem impacting organizations. Notably, we identify supply chain dynamics as a significant influencer of cybersecurity practices, emphasizing the necessity of robust cybersecurity protocols throughout the supply chain. The proactive engagement of boards in cybersecurity governance is crucial in cultivating a culture of cybersecurity awareness and accountability at the highest organizational levels. Additionally, guidance from authoritative bodies like the NCSC can inform organizations' cybersecurity strategies, ensuring alignment with industry standards and best practices. Moreover, our findings delineate specific measures aimed at implementing standards or catalyzing companies toward integrating cybersecurity activities into their boards. These encompass a spectrum of coercive, normative, and mimetic mechanisms originating from entities such as governments, stakeholders, and the supply chain.

For SMEs, the strategic integration of cybersecurity within the corporate governance structure is not merely a regulatory requirement but a critical component of sustainable business practice. Our findings suggest that SMEs benefit significantly from engaging with external IT and cybersecurity consultants, underscoring the value of expert guidance in navigating the complex cybersecurity landscape. Managers and business leaders within SMEs should prioritize establishing long-term relationships with reputable cybersecurity firms that can provide tailored solutions and ongoing support. Additionally, given the substantial influence of supply chain interactions on cybersecurity practices, SME managers need to develop rigorous vetting processes for their suppliers, ensuring that their cybersecurity standards align with organizational needs and compliance requirements. Implementing regular security audits and requiring cybersecurity assurances in supplier contracts can mitigate potential vulnerabilities from third-party associations.

From a policymaker's standpoint, effective cybersecurity policy initiatives must recognize the varied effects of different agents and mechanisms. This is, we found more specific measures aimed at achieving the implementation of standards or revitalizing companies in terms of including cybersecurity activities in their boards. This ranges from broader measures with a less specific purpose, aimed at enhancing cybersecurity within the company. These latter measures combine a variety of coercive, normative, and mimetic mechanisms originating from entities such as government, stakeholders, or the supply chain. From the perspective of implications for policymakers, it is essential to consider that effective cybersecurity promotion policies should acknowledge that not all agents and mechanisms have the same effect. This involves aligning policy objectives with the most appropriate mechanisms while considering the diversity of actors involved.

Limitations and future research

Despite the insights this study provides there are few limitations that should be acknowledged. Firstly, the reliance on survey data may introduce response biases and limit the generalizability of findings. Future research endeavors could employ mixed-methods approaches to triangulate results and enhance their robustness. Secondly, our study focused on organizations within specific sectors, potentially constraining the transferability of findings to other industry contexts. Future investigations could explore cybersecurity governance across a broader array of industries to capture diverse perspectives and practices. Lastly, the dynamic nature of cybersecurity threats and regulations necessitates ongoing monitoring and adaptation of organizational strategies. Longitudinal studies could provide valuable insights into the evolution of cybersecurity governance practices over time.

Disclosure statement

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

ORCID

Marta F. Arroyabe http://orcid.org/0000-0003-3223-0268
Carlos F. A. Arranz http://orcid.org/0000-0002-6866-0684
Juan Carlos Fernandez de Arroyabe http://orcid.org/0000-0003-1451-3782

References

1. Uddin MH, Mollah S, Islam N, Ali MH. Does digital transformation matter for operational risk exposure? Technol Forecast Soc Change. 2023;197:122919. doi:10.1016/j.techfore.2023.122919.
2. Benz M, Chatterjee D. Calculated risk? A cybersecurity evaluation tool for SMEs. Bus Horiz. 2020;63 (4):531–540. doi:10.1016/j.bushor.2020.03.010.

3. 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. doi:10.1016/j.compind.2019.103165.
4. Fernandez de Arroyabe IF, Arranz CF, Arroyabe MF, de Arroyabe JCF. Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: a UK survey for 2018 and 2019. Comput Secur. 2023;124:102954. doi:10.1016/j.cose.2022.102954.
5. Morris D, Madzudzo G, Garcia-Perez A. Cybersecurity threats in the auto industry: tensions in the knowledge environment. Technol Forecast Soc Change. 2020;157:120102. doi:10.1016/j.techfore.2020.120102.
6. Lezzi M, Lazoi M, Corallo A. Cybersecurity for industry 4.0 in the current literature: a reference framework. Comput Ind. 2018;103:97–110. doi:10.1016/j.compind.2018.09.004.
7. 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 Manag. 2020;68(1):87–100. doi:10.1109/TEM.2020.2977815.
8. Georgiadou A, Mouzakitis S, Askounis D. Detecting insider threat via a cyber-security culture framework. J Comput Inf Syst. 2022;62(4):706–716. doi:10.1080/08874417.2021.1903367.
9. Bhandari P, Creighton D, Gong J, Boyle C, Law KM. Evolution of cyber-physical-human water systems: challenges and gaps. Technol Forecast Soc Change. 2023;191:122540. doi:10.1016/j.techfore.2023.122540.
10. ISO/IEC 15408-1:2009. Information technology—security techniques—evaluation criteria for it security—part 1: introduction and general model. Geneva (Switzerland): ISO/IEC; 2018. https://www.iso.org/standard/50341.html.
11. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection—information security controls. Geneva (Switzerland): ISO/IEC; 2022.
12. Gale M, Bongiovanni I, Slapnicar S. Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead. Comput Secur. 2022;121:102840. doi:10.1016/j.cose.2022.102840.
13. Krawczyk-Sokołowska I, Caputa W. Awareness of network security and customer value: the company and customer perspective. Technol Forecast Soc Change. 2023;190:122430. doi:10.1016/j.techfore.2023.122430.
14. Choo KR. The cyber threat landscape: challenges and future research directions. Comput Secur. 2011;30(8):719–731. doi:10.1016/j.cose.2011.08.004.
15. National Cyber Security Centre (NCSC). About Cyber Essentials. 2024 [accessed 2024 Aug 10]. https://www.ncsc.gov.uk/cyberessentials/overview.
16. Daim T, Lai KK, Yalcin H, Alsoubie F, Kumar V. Forecasting technological positioning through technology knowledge redundancy: patent citation analysis of IoT, cybersecurity, and Blockchain. Technol Forecast Soc Change. 2020;161:120329. doi:10.1016/j.techfore.2020.120329.
17. Pal O, Alam B. Cyber security risks and challenges in supply chain. Int J Adv Res Comput Sci. 2017;8(5):662–670.
18. Hasan S, Ali M, Kurnia S, Thurasamy R. Evaluating the cyber security readiness of organizations and its influence on performance. J Inf Secur Appl. 2021;58:102726. doi:10.1016/j.jisa.2020.102726.
19. Malatji M, Von Solms S, Marnewick A. Socio-technical systems cybersecurity framework. Inf Comput Secur. 2019;27(2):233–272. doi:10.1108/ICS-03-2018-0031.
20. Scott WR. Institutional theory: onward and upward. In: Greenwood R, Oliver C, Lawrence TB, Meyer RE, editors. The sage handb of organizational institutionalism. London (UK): SAGE Publications Ltd; 2017. p. 853–869.
21. DiMaggio PJ, Powell WW. The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. Am Sociol Rev. 1983;48(2):147–160. doi:10.2307/2095101.
22. Friedman AL, Miles S. Developing stakeholder theory. J Manage Stud. 2002;39(1):1–21. doi:10.1111/1467-6486.00280.
23. Freeman RE. The politics of stakeholder theory: some future directions. In: Freeman R. editor. R Edward freeman's selected works on stakeholder theory and business ethics. Cham (Switzerland): Springer International Publishing; 2023. p. 119–132.
24. GOV.UK. Cyber security longitudinal survey. London (UK): Department for Science, Innovation and Technology and Department for Digital, Culture, Media & Sport; 2024. https://www.gov.uk/government/collections/cyber-security-longitudinal-survey.
25. Fernandez de Arroyabe JCF, Arroyabe MF, Fernandez IF, Arranz CFA. Cybersecurity resilience in SMEs: a machine learning approach. J Comput Inf Syst. 2023; 1–17. doi:10.1080/08874417.2023.2248925.
26. Paliwal M, Kumar UA. Neural networks and statistical techniques: a review of applications. Expert Syst Appl. 2009;36(1):2–17. doi:10.1016/j.eswa.2007.10.005.
27. Georgiadou A, Mouzakitis S, Bounas K, Askounis D. A cyber-security culture framework for assessing organization readiness. J Comput Inf Syst. 2022;62(3):452–462. doi:10.1080/08874417.2020.1845583.
28. Babiceanu RF, Seker R. Cyber resilience protection for industrial internet of things: a software-defined networking approach. Comput Ind. 2019;104:47–58. doi:10.1016/j.compind.2018.10.004.
29. Bertino E, Choo KKR, Georgakopolous D, Nepal S. Internet of Things (IoT) smart and secure service delivery. ACM Trans Internet Technol. 2016;16(4):22–29. doi:10.1145/3013520.
30. Zwilling M, Klien G, Lesjak D, Wiechetek Ł, Cetin F, Basim HN. Cyber security awareness, knowledge and behavior: a comparative study. J Comput Inf Syst. 2022;62(1):82–97. doi:10.1080/08874417.2020.1712269.
31. Conteh NY, Schmick PJ. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. Int J Adv Comput Res. 2016;6(23):31–43. doi:10.19101/IJACR.2016.623006.
32. Calder A. Cyber essentials: a pocket guide. Ely (UK): IT Governance Ltd; 2014.
33. Landefeld S, Mejia L, Handy A, Hinnen T. Is that a target on your back?: board cybersecurity oversight duty after the target settlement. Corp Gov Advis. 2017;25(6):1–9.

34. GOV.UK. Cyber security breaches survey 2023. London (UK): Department for Science, Innovation and Technology and Department for Digital, Culture, Media & Sport; 2023. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023.
35. European Union Agency for Cybersecurity (ENISA). Cybersecurity for SMEs. Challenges and recommendations. Athens (Greece): ENISA; 2021 [accessed 2024 Aug 10]. https://www.enisa.europa.eu/publications/cybersecurity-for-smes-challenges-and-recommendations.
36. Fox J. Top cybersecurity statistics for 2024. Cobalt. 2024 [accessed 2024 Aug 10]. https://www.cobalt.io/blog/cybersecurity-statistics-2024#:~:text=75%25%20of%20security%20professionals%20have,burden%20on%20organizations%20 .
37. Fernandez de Arroyabe IF, Fernandez de Arroyabe JCF. The severity and effects of cyber-breaches in SMEs: a machine learning approach. Enterp Inf Syst. 2021;17(3):1942997. doi:10.1080/17517575.2021.1942997.
38. Arranz CFA, Arroyabe MF, Arranz N, Fernandez de Arroyabe JC. Digitalisation dynamics in SMEs: an approach from systems dynamics and artificial intelligence. Technol Forecast Soc Change. 2023;196:122880. doi:10.1016/j.techfore.2023.122880.
39. Arroyabe MF, Arranz CF, de Arroyabe IF, de Arroyabe JCF. The effect of it security issues on the implementation of industry 4.0 in SMEs: barriers and challenges. Technol Forecast Soc Change. 2024;199:123051. doi:10.1016/j.techfore.2023.123051.
40. Greenwood R, Meyer RE, Lawrence TB, Oliver C. The sage handbook of organizational institutionalism. Thousand Oaks (CA): Sage Press; 2017.
41. Arranz CFA, Sena V, Kwong C. Institutional pressures as drivers of circular economy in firms: a machine learning approach. J Clean Prod. 2022;355:131738. doi:10.1016/j.jclepro.2022.131738.
42. Scott WR. Institutions and organizations. 2nd ed. Thousand Oaks (CA): Sage Press; 1995.
43. Hinings CR, Logue D, Zietsma C. Fields, institutional infrastructure and governance. In: Greenwood R, Meyer R, Lawrence T Oliver C. editors. The sage handbook of organizational institutionalism. Thousand Oaks (CA): Sage Press; 2017. p. 163–189.
44. Wooten M, Hoffman AJ. Organizational fields: past, present and future. In: Greenwood R, Meyer R, Lawrence T Oliver C. editors. The sage handbook of organizational institutionalism. Thousand Oaks (CA): Sage Press; 2017. p. 55–74.
45. Zietsma C, Groenewegen P, Logue DM, Hinings CR. Field or fields? Building the scaffolding for cumulation of research on institutional fields. Acad Manag Ann. 2017;11(1):391–450. doi:10.5465/annals.2014.0052.
46. Jeyaraj A, Zadeh A. Institutional isomorphism in organizational cybersecurity: a text analytics approach. J Organ Comput Electron Commer. 2020;30(4):361–380. doi:10.1080/10919392.2020.1776033.
47. Ogbanufe O, Kim DJ, Jones MC. Informing cybersecurity strategic commitment through top management perceptions: the role of institutional pressures. Inf Manag. 2021;58(7):103507. doi:10.1016/j.im.2021.103507.
48. Kalkan K, Kwansa F, Cobanoglu C. Payment card industry data security standards (PCI DSS) compliance in restaurants. J Hosp Financ Manag. 2010;16(2):3. doi:10.1080/10913211.2008.10653863.
49. Slapničar S, Axelsen M, Bongiovanni I, Stockdale D. A pathway model to five lines of accountability in cybersecurity governance. Int J Acc Inf Syst. 2023;51:100642. doi:10.1016/j.accinf.2023.100642.
50. Freeman RE, Harrison JS, Wicks AC, Parmar BL, De Colle S. Stakeholder theory: the state of the art. Cambridge (UK): Cambridge University Press; 2010.
51. Bauer JM, Van Eeten MJ. Cybersecurity: stakeholder incentives, externalities, and policy options. Telecomm Policy. 2009;33(10–11):706–719. doi:10.1016/j.telpol.2009.09.001.
52. Fischer-Hübner S, Alcaraz C, Ferreira A, Fernandez-Gago C, Lopez J, Markatos E, Akil M. Stakeholder perspectives and requirements on cybersecurity in Europe. J Inf Secur Appl. 2021;61:102916. doi:10.1016/j.jisa.2021.102916.
53. Bansal G, Axelton Z. Impact of cybersecurity disclosures on stakeholder intentions. J Comput Inf Syst. 2024;64(1):78–91. doi:10.1080/08874417.2023.2180785.
54. Kemper G. Improving employees' cyber security awareness. Comput Fraud Secur. 2019;2019(8):11–14. doi:10.1016/S1361-3723(19)30085-5.
55. Deane J, Baker W, Rees L. Cybersecurity in supply chains: quantifying risk. J Comput Inf Syst. 2023;63(3):507–521. doi:10.1080/08874417.2022.2081882.
56. Melnyk SA, Schoenherr T, Speier-Pero C, Peters CF, Chang JF, Friday D. New challenges in supply chain management: cybersecurity across the supply chain. Int J Prod Res. 2022;60(1):162–183. doi:10.1080/00207543.2021.1984606.
57. Cheung KF, Bell MG, Bhattacharjya J. Cybersecurity in logistics and supply chain management: an overview and future research directions. Transp Res E Logist Transp Rev. 2021;146:102217. doi:10.1016/j.tre.2020.102217.
58. Bandura A. Self-efficacy: toward a unifying theory of behavioral change. Psychol Rev. 1977;84(2):191. doi:10.1037/0033-295X.84.2.191.
59. Dodge CE, Fisk N, Burruss GW, Moule RK, Jr, Jaynes CM. What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. Criminol Public Policy. 2023;22(4):849–868. doi:10.1111/1745-9133.12641.
60. De Kimpe L, Walrave M, Verdegem P, Ponnet K. What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behav Inf Technol. 2022;41(8):1796–1808. doi:10.1080/0144929X.2021.1905066.
61. Meso P, Ding Y, Xu S. Applying protection motivation theory to information security training for college students. J Inf Priv Secur. 2013;9(1):47–67. doi:10.1080/15536548.2013.10845672.
62. Smith KA, Gupta JN. Neural networks in business: techniques and applications for the operations researcher.

Comput Oper Res. 2000;27(11–12):1023–1044. doi:10.1016/S0305-0548(99)00141-0.
63. Wang Q. Artificial neural networks as cost engineering methods in a collaborative manufacturing environment. Int J Prod Econ. 2007;109(1):53–64. doi:10.1016/j.ijpe.2006.11.006.
64. 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(1):171–178. doi:10.1016/j.ijpe.2008.05.009.
65. Podsakoff PM, MacKenzie SB, Podsakoff NP. Sources of method bias in social science research and recommendations on how to control it. Annu Rev Psychol. 2012;63(1):539–569. doi:10.1146/annurev-psych-120710-100452.
66. Garson GD. Interpreting neural-network connection weights. AI Expert. 1991;6(4):47–51.
67. Gorr WL, Nagin D. Neural network models for time series forecasts. Int J Forecast. 1999;15(3):369–385.
68. Nix D, Weigend A. Estimating the mean and variance of the target probability distribution. In: Leen TK, Tesauro G, Touretzky DS, editors. Advances in neural information processing systems. Cambridge (MA): MIT Press; 1994. p. 590–597.
69. Dudek A. Silhouette index as clustering evaluation tool. In: Jajuga K, Batóg J, Walesiak M, editors. Classification and data analysis: theory and applications. Cham (Switzerland): Springer International Publishing; 2020. p. 19–33.
70. Mamat AR, Mohamed FS, Mohamed MA, Rawi NM, Awang MI. Silhouette index for determining optimal k-means clustering on images in different color models. Int J Eng Technol. 2018;7(2):105–109. doi:10.14419/ijet.v7i2.14.11464.
71. Fraley C, Raftery AE. How many clusters? Which clustering method? Answers via model-based cluster analysis. Comput J. 1998;41(8):578–588. doi:10.1093/comjnl/41.8.578.
72. Herr T. Cyber insurance and private governance: the enforcement power of markets. Regul Gov. 2021;15(1):98–114. doi:10.1111/rego.12266.