Strategic Change

WILEY

REVIEW ARTICLE OPEN ACCESS

At the Cybersecurity Frontier: Key Strategies and Persistent Challenges for Business Leaders

Marco Balzano[1] | Giacomo Marzi[2]

[1]Department of Economics, Management, Mathematics and Statistics, University of Trieste, Trieste (TS), Italy | [2]IMT School for Advanced Studies Lucca, Lucca, Italy

Correspondence: Marco Balzano (marco.balzano@units.it)

Received: 5 June 2024 | **Revised:** 23 October 2024 | **Accepted:** 23 October 2024

Funding: This work was supported by the Italian Ministry of University and Research (MUR), D67G23000060001.

Keywords: business strategy | cyber attacks | cyber risks | cyber threats | cybersecurity | digital risks

ABSTRACT

This study disentangles the cybersecurity landscape, highlighting its strategic role in contemporary digital environments. Aligned with modern holistic management approaches, it uncovers key insights and strategic imperatives by distilling core lessons and identifying ongoing challenges in the field. We emphasize significant contributions to understanding enduring lessons and addressing unresolved challenges in cybersecurity literature. The findings underscore the relevance of adopting a strategic approach to cybersecurity, one that balances technological solutions with human behavior, training, and awareness. Additionally, the study examines the evolving nature of cyber threats, the impact of legal and regulatory frameworks, and ethical dilemmas, emphasizing the need for continuous adaptation and proactive management in the face of increasingly sophisticated digital risks.

JEL Classification: M10

1 | Introduction

The ubiquity of digital technologies has catalyzed unprecedented opportunities for growth, innovation, and efficiency (Carmel and Roche 2023). At the same time, the digital revolution has also significantly expanded the attack surface for potential cyber threats (Al-Emran et al. 2024; Corallo et al. 2021; Krutilla et al. 2021). Cybersecurity entails safeguarding critical digital assets against a variety of threats, including data breaches, cyber-attacks, and other malicious activities that can disrupt business operations, compromise customer trust, and result in significant financial and reputational damage (Alshabib and Martins 2021; Hoeltgebaum, Adams, and Fernandes 2021). From this angle, cybersecurity intertwines issues regarding aspects like human and social factors (e.g., Proctor and Chen 2015), technological issues (e.g., Santoso and Finn 2022), strategy (e.g., Allodi and Massacci 2017), ethics (e.g., Chen, Henry, and Jiang 2023), and policy dimensions (e.g., Turel, He, and Wen 2021), necessitating a holistic management approach to enhancing the value of cybersecurity while mitigating cyber risks (Corallo et al. 2021). Thus, cybersecurity-related issues cannot be overstated in a world where digital interactions and transactions form the backbone of social, economic, and political structures (Daniel, Mullarkey, and Agrawal 2023; Dinkova, El-Dardiry, and Overvest 2023; Hanelt et al. 2021).

In the digital economy where data are intrinsic elements of strategy (DalleMule and Davenport 2017), cybersecurity breaches can lead to shocking economic repercussions, including direct financial losses, regulatory fines, litigation costs, and the intangible costs of damaged reputations and lost trust (e.g., Żebrowski, Couce-Vieira, and Mancuso 2022). Therefore, enhancing cybersecurity is necessary for businesses seeking to

Summary

- Business leaders should embed cybersecurity into core business strategies, blending advanced technology with rigorous human training.
- To "stay ahead" of evolving cyber threats, organizations should maintain a proactive and adaptable approach to regulatory and ethical challenges.
- Address cybersecurity also means adopting a holistic management approach, encompassing multiple dimensions such as tackling political, economic, social, technological, environmental, and legal issues.
- Organizations should implement ongoing internal training programs to mitigate human error and enhance cybersecurity resilience.

protect their assets and maintain continuity in an increasingly hostile digital environment (e.g., Qin et al. 2018).

Despite the well-recognized relevance of cybersecurity in the literature (Radanliev, Roure, Maple, Ani 2022; Radanliev, Roure, Maple, Santos 2022), studies on cybersecurity still exhibit some degree of fragmentation, and the multiple facets constituting the broad concept of cybersecurity are scattered across various research streams. For example, Hepfer and Powell (2020) illustrate that cybersecurity must be embedded within the wider framework of business strategy to protect organizational assets and maintain operational continuity in an increasingly hostile digital environment. Chen, Henry, and Jiang (2023) emphasize the ethical dimensions of cybersecurity, particularly in terms of corporate transparency and risk disclosure, which are becoming essential as organizations face growing scrutiny from regulators and stakeholders alike. Other studies focus on the rapid evolution of cyber threats, often outpacing current security measures, emphasizing the dynamic nature of advanced persistent threats (APTs) and the necessity for businesses to develop adaptable and proactive security strategies (e.g., Carayannis et al. 2019; Zhu et al. 2022). Additionally, the role of the human factor remains a central element in cybersecurity, with human error often being the weakest link in the security chain (Proctor and Chen 2015). These errors might include mishandling sensitive information, falling prey to phishing attacks, or failing to adhere to security protocols (Ganin et al. 2020).

Motivated by these premises, the present study addresses the multifaceted challenges identified in the literature, aiming to contribute to developing more suitable cybersecurity strategies that are not only technologically sound but also aligned with the ethical, legal, and organizational imperatives of modern business management. As a result, we propose the following research question:

> *What are the enduring lessons, open challenges, and research gaps on cybersecurity within the strategic business management literature*?

To address this research question, we adopt a narrative review methodology (Popay et al. 2006). Our findings are framed around the Political, Economic, Social, Technological, Environment, and Legal (PESTEL) framework to analyze cybersecurity's role in business management. The PESTEL framework is commonly used in business management studies to integrate insights on broad issues, such as the implications of Industry 4.0 for the construction industry (Oesterreich and Teuteberg 2016) or the use of supervised machine learning and artificial neural network techniques (Schlegelmilch, Sharma, and Garg 2022). In the context of our research, the PESTEL framework is functional in framing cybersecurity as integral to business strategy. The political dimension addresses the policy implications, focusing on the role of government in cybersecurity, regulatory frameworks, national security concerns, and international cooperation in cyber defense. The economic dimension explores the business strategy aspect, analyzing the economic impact of cyber threats and the cost-effectiveness of cybersecurity measures. The social dimension focuses on human errors, social networks, and user behavior. The technological dimension underscores the evolution of cyber threats, advancements in cybersecurity technologies, and the technical challenges in safeguarding digital assets. The environmental dimension includes the broader ethical implications of cybersecurity practices and the role of stakeholder engagement and continuous interaction. The legal dimension includes studies on cybersecurity laws and regulations, compliance requirements, the legal consequences of cyber-attacks, and the evolving legal landscape concerning data protection, privacy laws, and intellectual property rights.

Thus, the present study offers several insights. First, it is critical to integrate cybersecurity strategies as a core component of the overall business strategy (e.g., Hepfer and Powell 2020). Also, studies show that human error or negligence often leads to breaches, underscoring the need for continuous education and training in cyber hygiene and awareness (e.g., Proctor and Chen 2015; Kortschot et al. 2018). Furthermore, the dynamic nature of cyber threats necessitates organizations remain agile and adaptable, investing in preventive and responsive measures to cope with the evolving landscape (e.g., Santoso and Finn 2022).

Although progress has been made, numerous challenges persist. For example, the rapid evolution of cyber threats often outpaces existing security measures. As technology advances, so do the methods employed by cybercriminals, creating a constant need for updated defenses and strategies (Baksi and Upadhyaya 2021; Zhu et al. 2022). Integrating cybersecurity into corporate culture and business processes is not always straightforward (Krishna, Krishnan, and Sebastian 2023). Furthermore, today's interconnected business landscape presents a challenge in managing cybersecurity across different jurisdictions with varying legal and regulatory frameworks (Lee et al. 2020; Pandey, Singh, and Gunasekaran 2023).

From the theoretical side, this study enriches our understanding of cybersecurity in business management. The proposed view underscores the significance of viewing cybersecurity through the lens of organizational behavior and culture, considering how attitudes, beliefs, and practices shape cybersecurity outcomes. Practically, this study offers implications for managers and entrepreneurs. It emphasizes the importance of incorporating cybersecurity into the core business strategy, not just as a peripheral IT issue. This involves allocating appropriate resources, fostering a culture of security awareness, and

integrating cybersecurity considerations into decision-making processes. It also highlights the need for continuous training and development programs to enhance the cybersecurity skills of employees. For policymakers, the study suggests developing holistic and coherent regulations that balance security requirements with privacy and ethical considerations.

2 | Method

In addressing our research question, we employed a narrative review methodology (Popay et al. 2006). Similarly to previous research, the presentation of the findings is framed around the PESTEL framework (e.g., Oesterreich and Teuteberg 2016; Schlegelmilch, Sharma, and Garg 2022), examining the multifaceted nature of cybersecurity in business management. Specifically, we considered cybersecurity as a core element of business strategy, unveiling in political, economic, social, technological, environmental, and legal dimensions. In this perspective, we argue that the PESTEL framework is a suitable lens for analyzing the strategic role of cybersecurity as it offers a multifaceted approach that aligns with the interconnected nature of cybersecurity challenges. Unlike narrower analytical tools, PESTEL captures the broad external forces that influence cybersecurity, making it particularly effective for a strategic analysis that requires a deep understanding of the external environment.

Our search strategy began with developing a detailed query in Scopus, focusing on top-tier management journals. This initial search was subsequently cross-validated in complementary databases such as Web of Science, ABI/INFORM, and Google Scholar to ensure a wide coverage of the relevant literature. Keywords and phrases selected for the search process were carefully chosen to reflect the various dimensions of our multifaceted lens. These included, but were not limited to, combinations of terms like "cybersecurity," "cyber risk," "hacker," "cyberattack," "cyber threat." Accordingly, we extracted a preliminary set of articles and subjected them to a critical appraisal. This appraisal focused on assessing each article's document information elements (DIEs), including criteria such as its contribution to the broader understanding of cybersecurity in the business management discipline, availability, quality, completeness, authority, currency, convenience, usability and standardization (Zhang et al. 2021).

Regarding our inclusion/exclusion criteria, to ensure a targeted and relevant analysis, we established specific boundary conditions that guided our selection of studies (Marzi et al. 2024). First, the research we included focuses on cybersecurity from a business management perspective, particularly those that explore the integration of cybersecurity into business strategies, decision-making processes, and organizational behavior to capture how cybersecurity functions as a strategic asset within organizations. Second, we emphasized recent studies that are relevant to contemporary challenges, ensuring that the insights apply to today's dynamic business environment. Third, we excluded studies that do not align with this strategic focus. Specifically, we included research that considered the firm the locus of attention. Thus, we excluded, for instance, studies lacking direct implications for business strategy. Similarly, we excluded studies with a purely technical focus, such as those that deal with encryption methods or software development, unless they are explicitly connected to broader business strategies. Fourth, research centered on non-business contexts, such as governmental or military cybersecurity strategies, was deemed outside the scope, as these do not directly contribute to our understanding of cybersecurity within the business management framework.

To further triangulate our methodology and ensure the reliability of our analysis, we confronted one additional management scholar, one IT scholar, and one practitioner. These raters, with backgrounds in business management, information technology, cybersecurity policy, and ethics, were essential in providing a multidisciplinary perspective to our study. The coding scheme comprised five categories, each aligned with a distinct framework aspect. It included a defined set of attributes to ensure a thorough and consistent literature analysis. To inspect the reliability of our coding process, we employed Krippendorff's Alpha, a robust statistical measure for assessing interrater reliability in studies with multiple raters and various levels of measurement. The analysis, conducted using the K-Alpha Calculator (Marzi, Balzano, and Marchiori 2024), yielded a Krippendorff's Alpha coefficient beyond the threshold for satisfactory reliability, indicating a high level of agreement among the raters.

Overall, the theoretical lenses adopted by authors in cybersecurity intersect with numerous domains, including technology, human behavior, economics, and policy, necessitating an interdisciplinary approach to understanding and mitigating risks. For instance, some studies leverage economic theories to assess cyber risks and the implications of public policies (e.g., Andrijcic and Horowitz 2006; Öğüt, Raghunathan, and Menon 2011). Other studies utilize cognitive models to understand decision-making processes in cybersecurity contexts, reflecting the field's reliance on theoretical constructs to explain and predict behaviors and outcomes (e.g., Aggarwal et al. 2022). Once obtaining the extracted pool of articles, we carried out a narrative synthesis of the findings. The outcome of this synthesis aimed at mapping knowledge in the field and illuminating open challenges and research avenues for practitioners and scholars.

3 | Cybersecurity: Enduring Lessons in Business Management

In this section, we present lessons and key inroads into cybersecurity research. Figure 1 proposes a schematic representation of the emerging cybersecurity literature.

3.1 | The Political Dimension of Cybersecurity

A focus on policy-related aspects of cybersecurity has yielded key lessons and insights. Recent academic works in this field underscore the complexity and necessity of sound policies in navigating the cybersecurity landscape. These studies highlight the role of policy in shaping cybersecurity strategies and responses, offering a multifaceted view of the interplay

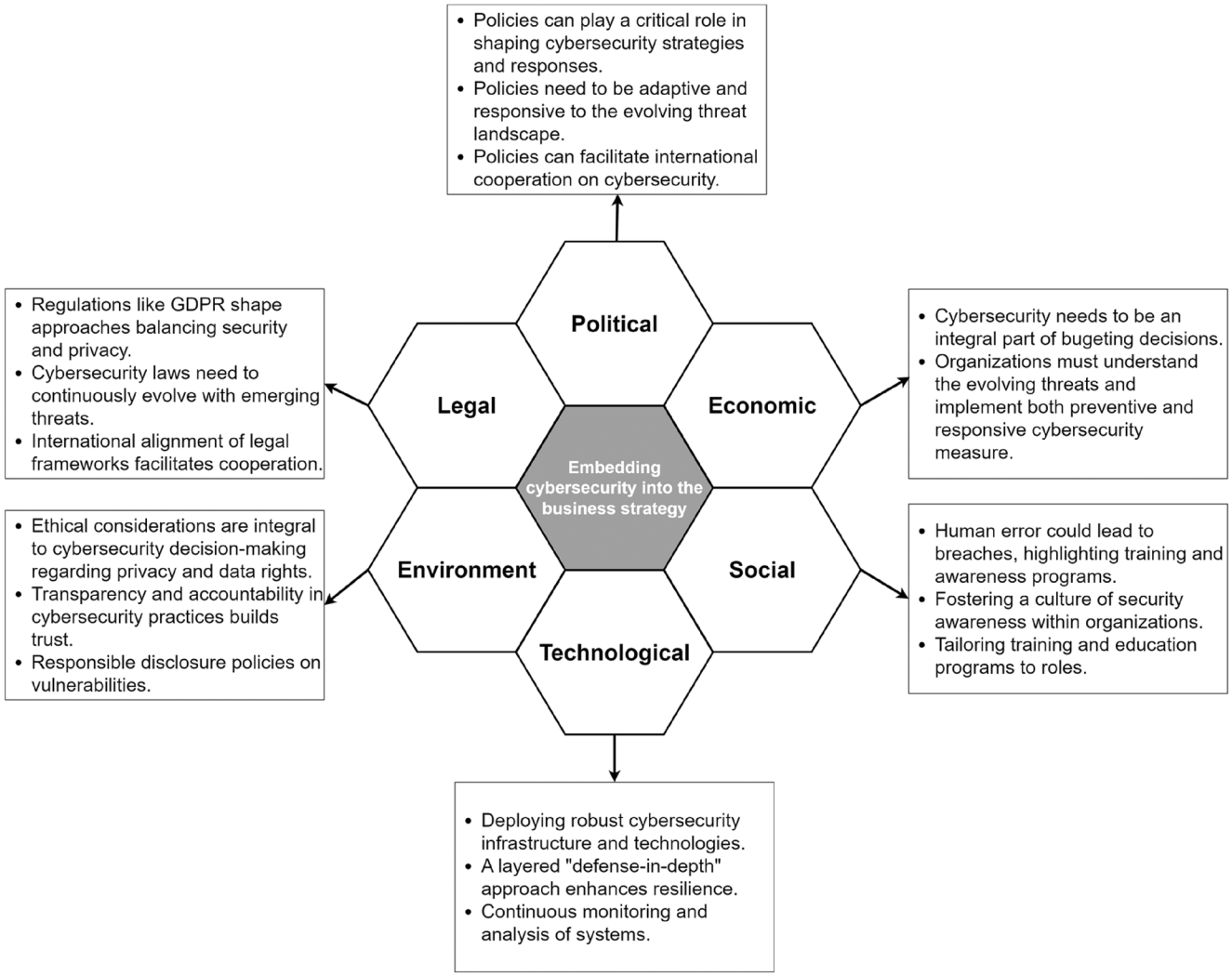

FIGURE 1 | Cybersecurity in business management: enduring lessons and key inroads.

between cybersecurity challenges and policy frameworks. For example, Alshabib and Martins (2021) dive into the regional differences in cybersecurity policy. Their research focuses on the Gulf Cooperation Council, exploring how perceived threats shape policy responses, highlighting the importance of understanding regional and political contexts in formulating effective cybersecurity policies. Relatedly, White et al. (2020) explore the factors that drive the implementation of cybersecurity measures within organizations. Their research offers insights into how policy can act as a catalyst for cybersecurity strategies, emphasizing the need for well-crafted policies responsive to the evolving nature of cyber threats. Li and Chen (2022) examine the role of policy in identifying and responding to emerging threats in the cyber landscape. Their research points to the role of adaptive and proactive policy frameworks that can keep pace with cyber attackers' rapidly evolving tactics and strategies. Plachkinova and Menard (2019) address the policy implications for Internet of Things (IoT) security. Their study explores how different messaging strategies influence user behavior in the context of IoT devices, pointing to the need for policy interventions that effectively communicate security risks and practices to users.

3.2 | The Economic Dimension of Cybersecurity

The economics of cybersecurity has evolved from focusing on single-firm investment models to more complex frameworks that account for interdependent security across organizations (Fedele and Roner 2022; Gordon and Loeb 2002). Early models, which centered on individual firms, often overlooked the interconnected nature of businesses, particularly the shared risks present in common networks or competitive market dynamics. Over time, research expanded to examine cybersecurity decisions in multifirm environments, especially for organizations operating on shared networks without direct competition (Kunreuther and Heal 2003; Varian 2004). This shift is particularly relevant in sectors such as banking, where firms are also deeply interconnected through shared vulnerabilities. More recently, scholars have integrated a temporal dimension, showing how cybersecurity investments are influenced by irreversibility and uncertainty, as well as by factors like depreciation and discount rates over long-term horizons (Krutilla et al. 2021).

Relatedly, Alshabib and Martins (2021) underscore the criticality of cybersecurity in economic collaborations, highlighting

the necessity for strong and harmonized economic policies to address emerging cyber threats. Building on this, Bamiatzi et al. (2023) investigate the intersection of corporate social responsibility (CSR) and cybersecurity, revealing that CSR compliance does not exempt companies from cyber threats. This underscores the imperative of investing in cybersecurity (Shaikh and Siponen 2024), and embedding it in budgeting decisions. Accordingly, Ebrahimi et al. (2022) explored the use of cross-lingual analytics on international dark web platforms, highlighting the strategic role of advanced analytics in identifying and mitigating cyber threats. Li, Guo, and He (2020) provide insights into the Chinese government's economic policies on cybersecurity. Their findings are essential for businesses seeking to understand governmental strategies, enabling them to align their economic policies with national and international regulatory frameworks.

3.3 | The Social Dimension of Cybersecurity

The social dimension of cybersecurity involves understanding and addressing the behaviors, practices, and culture of individuals within the organization as they interact with information technology systems (Yoo, Goo, and Rao 2020). In exploring the domain of cybersecurity with a focus on social factors, scholars provide deep insights into how human behavior, awareness, and culture intersect with cybersecurity. Drawing on these studies, we better understand the enduring lessons and insights in this area. Ahangama (2023) offers insight into the role of virtual social networks as a catalyst for cybersecurity awareness. This study underscores the influence of education level on individuals' cybersecurity awareness, emphasizing the critical role of targeted educational programs and information dissemination strategies in enhancing cybersecurity postures. Akter et al. (2022) propose a new concept of cybersecurity awareness capability, focusing on the human elements in cybersecurity. Their research advocates for an all-encompassing cybersecurity culture within organizations, going beyond technical solutions to include awareness and behavioral change in economic strategy planning. Such an approach is necessary for mitigating cyber risks and fostering a resilient economic environment in the face of evolving cyber threats. Chen et al. (2022) focus on the relationship between expressed risk concerns and actual online security behaviors in their work. Their study sheds light on the often complex and contradictory nature of human behavior in cybersecurity, revealing a gap between what individuals express about security concerns and their actual online practices. Tang et al. (2021) analyze social network structures and their cybersecurity implications. Their research contributes significantly to understanding social networks' complex structures, offering insights into the challenges of protecting personal data and privacy in digital ecosystems. Sarno and Black (2023) investigate the psychological factors influencing individuals' susceptibility to phishing attacks. Their research highlights the importance of understanding the psychological dimensions of cybersecurity, particularly in crafting strategies to enhance individuals' ability to detect and avoid such attacks. These studies collectively emphasize the critical role of human factors in cybersecurity. They highlight the necessity of understanding and addressing the complex interplay between human behavior, psychology, and cybersecurity practices. From enhancing awareness through targeted education to understanding the psychological underpinnings of susceptibility to cyber attacks, these insights are functional for developing more effective and human-centric cybersecurity strategies.

3.4 | The Technological Dimension of Cybersecurity

Shukla, Sarmah, and Tiwari (2023) highlight the relevance of prioritizing digital assets in cybersecurity. The authors emphasize the importance of a strategic, targeted approach in risk management, illustrating the need for frameworks that effectively identify and prioritize critical digital assets, thus enhancing the efficacy of cybersecurity measures. Consistently, Saura, Palacios-Marqués, and Ribeiro-Soriano (2023) explore the technological adaptation in SMEs during the COVID-19 pandemic. Their study reveals SMEs' accelerated adoption of technology and the consequent cybersecurity challenges. Hoeltgebaum, Adams, and Fernandes (2021) apply statistical methods to network security data. Their findings underscore the importance of sophisticated technical strategies in detecting network anomalies, highlighting the growing role of advanced statistical and analytical methods in enhancing network security. Hong and Hofmann's (2021) critically examine the interdependence of digital communications and power systems in developed and developing nations, highlighting the cybersecurity risks inherent in the modern electric grid. Their study proposes a novel research agenda focusing on data integrity attacks against Outage Management Systems (OMS), a component for outage restoration and reliability planning. Integrating recent advancements in state estimation, load forecasting, and outage prediction, their work underscores the challenges and future research directions in safeguarding critical energy infrastructure from cyber threats. Santoso and Finn (2022) explore the use of deep-learning convolutional neural networks to bolster the cybersecurity of Robot Operating System (ROS) middleware, extensively used in civilian and military robotics. Cui et al. (2023) undertake an in-depth analysis of the challenges in maintaining the security of heterogeneous multiagent systems against a spectrum of cyber threats, including Denial-of-Service (DoS), false-data injection, camouflage, and actuation attacks. This advances the field by introducing distributed observers and estimators to address DoS and actuation attacks in cyber-physical layers, demonstrating through simulations and experiments the efficacy of their control schemes in ensuring uniformly ultimately bounded convergence of system responses to attacks.

3.5 | The Environmental Dimension of Cybersecurity

Understanding the interplay between ethical considerations and their consequential impact on the environmental landscape has become increasingly crucial in cybersecurity. Recent academic works in this field have provided enduring lessons, focusing on how ethical dimensions in cybersecurity echo through environmental contexts. These studies underscore the complex balance between technological advancement, ethical responsibility, and environmental stewardship, offering an insightful view of the challenges and integrated solutions in this critical area. Chen

et al. (2022) unfold the ethical implications of online behavior. This underscores the ethical responsibility of individuals in maintaining their cybersecurity and the cascading effects these decisions have on the environmental aspects of digital ecosystems. Ahangama (2023) further explores how social media platforms, often vectors of cyber threats, can also be instrumental in spreading cybersecurity awareness. Wright, Johnson, and Kitchens (2023) address the ethical challenges surrounding phishing attacks, emphasizing the importance of ethical considerations in designing and implementing cybersecurity measures against such threats. Their research highlights the necessity for a multilevel approach to cybersecurity that encompasses both technological aspects and the ethical dimensions of user behavior, organizational policies, and their environmental repercussions.

Furthermore, Chen, Henry, and Jiang (2023) explore the ethical aspects of cybersecurity in the context of corporate transparency and risk disclosure. Their research emphasizes the ethical obligation of corporations to disclose cybersecurity risks to stakeholders, illuminating the broader environmental and ethical implications of transparency in the digital age. Similarly, Tsang et al. (2023) investigate the ethical considerations in developing and deploying collaborative intrusion detection systems. This underscores the ethical challenges in balancing data sharing for security purposes with the protection of individual privacy, data rights and its subsequent impact on the environmental integrity of digital spaces.

3.6 | The Legal Dimension of Cybersecurity

The intersection of cybersecurity and legal frameworks, particularly concerning privacy, represents a dynamic area of study and application (Lee et al. 2020; Sukumar, Mahdiraji, and Jafari-Sadeghi 2023). In this context, preventive cybersecurity measures must balance implementing robust security protocols and protecting individual privacy rights. The European General Data Protection Regulation (GDPR) supports this balancing act. It offers a set of guidelines that ensure personal data protection while facilitating the development and implementation of effective cyber defense strategies. This legislative framework necessitates a nuanced understanding of legal requirements and technological capabilities, fostering an environment where security measures are technologically sound, legally compliant, and ethically justified. GDPR and similar privacy laws globally serve as regulatory mechanisms and catalysts for innovation in cybersecurity practices. By requiring stringent data protection requirements, these laws challenge organizations to develop advanced cybersecurity solutions to effectively prevent data breaches while ensuring user privacy. This has led to sophisticated technologies like encryption, anonymization, and secure data storage methods that align with legal standards.

Furthermore, the challenge lies in developing cybersecurity strategies that are proactive in preventing cyber threats and respecting privacy and individual rights. This requires a forward-thinking approach, where cybersecurity measures are designed with an inherent understanding of potential legal and ethical implications. The evolving nature of cyber threats, coupled with the rapid advancement of technology, demands continuous adaptation and revision of both legal frameworks and cybersecurity practices.

It is also worth mentioning the role of international cooperation in harmonizing cybersecurity and privacy laws (Didenko 2020). In this regard, cyber threats often transcend national boundaries, making international collaboration essential. This involves aligning disparate legal frameworks across different jurisdictions, facilitating cross-border data flow while ensuring compliance with various national and international privacy regulations.

4 | Discussion

The present study integrated insights pertaining to various subdimensions entailing cybersecurity in business management. The study corroborates strategic approaches to cybersecurity (e.g., AlDaajeh and Alrabaee 2024), thus framing cybersecurity as a core strategy element, reflecting an array of aspects of the organization. As a result, below, we attempt to highlight some of the open challenges and research gaps of cybersecurity in business management, and then discuss the key implications of the study. Table 1 outlines the key open challenges and research questions per each PESTEL dimension within cybersecurity research.

4.1 | Cybersecurity: Open Challenges in Business Management

Cybersecurity within organizations is marked by pressing open challenges for practice. For example, regarding policies, a prominent challenge in cybersecurity policy is the dynamic nature of cyber threats and the need for policies to be equally adaptable and responsive (Alshabib and Martins 2021). The challenge lies in crafting policy frameworks that are robust and flexible enough to respond to the evolving landscape of cyber threats. Another significant challenge presented by White et al. (2020) underscores the difficulty in ensuring the effective implementation of cybersecurity policies within organizations. The challenge here is multifaceted, involving the alignment of policy with organizational practices, the engagement of stakeholders, and the continuous updating of policies to reflect new threats and technologies.

Addressing such challenges, for example, in policy alignment, CSR integration, advanced analytics implementation, and the inclusion of human factors is key for advancing the strategic discourse in cybersecurity. Moreover, it is still difficult to align business strategies with evolving cybersecurity threats (Alshabib and Martins 2021; Li and Chen 2022). Businesses face the ongoing challenge of adapting their strategies to align with national and international cybersecurity policies, a complex task given these policies' varying and dynamic nature. Additionally, there is the challenge of integrating cybersecurity into the broader ethos of CSR (Bamiatzi et al. 2023). Firms must navigate how to embed cybersecurity within their CSR initiatives effectively, balancing ethical considerations with practical cybersecurity needs. Also, cybersecurity is affected by the proper management of complex digital ecosystems.

TABLE 1 | Open challenges and research questions about cybersecurity in business management.

PESTEL dimension	Open challenges	Research questions	Key references
Political	Crafting adaptable cybersecurity policies; international cooperation.	How can policy frameworks be more predictive and proactive against novel cyber threats?	Alshabib and Martins (2021), White et al. (2020)
Economic	Aligning cybersecurity with business strategy and CSR; managing complex digital ecosystems.	What are effective strategies for integrating cybersecurity within regional economic frameworks?	Bamiatzi et al. (2023), Ebrahimi et al. (2022)
Social	Bridging the gap between cybersecurity awareness and behavior; managing social network structures.	How can educational programs effectively influence online behaviors and practices?	Ahangama (2023), Akter et al. (2022)
Technological	Balancing technological advancement with security; developing advanced analytical methods for network security.	How can organizations incorporate advanced analytical techniques into their overall cybersecurity posture?	Shukla, Sarmah, and Tiwari (2023), Hoeltgebaum, Adams, and Fernandes (2021)
Environmental	Balancing ethical considerations with cybersecurity measures; ensuring corporate transparency in cybersecurity.	What are the ethical implications of different cybersecurity measures on stakeholders?	Chen, Henry, and Jiang (2023), Wright, Johnson, and Kitchens (2023)
Legal	Harmonizing cybersecurity and privacy laws; developing proactive cybersecurity strategies respectful of privacy.	How can legal frameworks be aligned across jurisdictions while protecting privacy?	Lee et al. (2020), Didenko (2020)

Translating awareness into secure practices and balancing technological advancement with security becomes central. Indeed, a primary challenge lies in managing the complexity of social network structures for cybersecurity (Tang et al. 2021). Protecting personal data and privacy within these intricate digital ecosystems remains a significant and ongoing challenge, especially with social networks' evolving nature and user behaviors. Another challenge is effectively translating cybersecurity awareness into practical and secure behaviors (Ahangama 2023). Despite increased awareness through education and social media, converting this awareness into tangible cybersecurity practices at both individual and organizational levels presents a substantial challenge. Additionally, SMEs' accelerated adoption of technology poses a challenge in balancing rapid technological advancement with robust cybersecurity measures (Saura, Palacios-Marqués, and Ribeiro-Soriano 2023). This is particularly pertinent in resource-constrained environments where the pace of technological change may outstrip the development of adequate security protocols.

Regarding the human factor, a challenge highlighted in these studies is translating cybersecurity awareness into actual behavioral change. Ahangama (2023) showcases the role of social media and education in enhancing cybersecurity awareness. However, converting this increased awareness into effective and secure online behaviors remains a significant challenge. The complexity lies in bridging the gap between what people know and how they act, especially in social media's dynamic and often informal context. Another key challenge is addressed by Chen et al. (2022) in their study point to the often-contradictory nature of human behavior in cybersecurity, where expressed concerns about online risks do not always translate into cautious behavior.

Regarding ethics, an open challenge is aligning individual ethical responsibility with actual cybersecurity behaviors (Chen et al. 2022). In particular, the challenge lies in bridging the gap between individuals' expressed concerns about online risks and their actual online practices. This gap poses ethical questions about personal accountability and the role of education in shaping responsible cybersecurity behaviors. Additionally, it is key to create and enforce ethical standards for information dissemination and data protection on these platforms, balancing the freedom of information with the need for security and privacy (Ahangama 2023).

4.2 | Cybersecurity: Avenues in Business Management

Following the proposed challenges, a number of research gaps become apparent. Li and Chen (2022) call for research on developing policies that proactively identify and mitigate emerging cyber threats. There is a gap in understanding how policy frameworks can be designed to be more predictive and preemptive in the face of novel threats, particularly those emanating from sophisticated hacker communities. Plachkinova and Menard (2019) highlight a gap in research on the efficacy of different policy communication strategies in influencing user

behavior and awareness of IoT security. More in-depth studies are needed to explore the most effective ways to communicate policy-related information to the public, ensuring that users are well-informed and motivated to adhere to cybersecurity best practices.

Notably, the strategic implementation of advanced analytics in cybersecurity (Ebrahimi et al. 2022) reveals a gap in understanding how such technologies can be integrated into global business strategies. Additional research is needed to explore how multinational corporations can strategically employ advanced analytics to enhance their cybersecurity measures while maintaining their competitive edge in the market. Similarly, while the importance of cybersecurity in regional cooperative frameworks is acknowledged by scholars (e.g., Alshabib and Martins 2021), there is a shortage of knowledge on the detailed strategic frameworks and models for effectively integrating cybersecurity policies within these specific regional contexts. This calls for research into developing and assessing strategic models that facilitate the integration of cybersecurity within regional cooperative strategies. Moreover, Akter et al. (2022) bring attention to the human factors in cybersecurity, yet there is a scarcity of research on strategic frameworks that incorporate these human aspects into organizational cybersecurity culture and planning. This presents an opportunity for future studies to develop strategies that integrate human factors into the broader cybersecurity strategy of organizations. Shukla, Sarmah, and Tiwari (2023), while emphasizing the importance of prioritizing digital assets, show a gap in the applicability and adaptability of such frameworks across different industries. Research is needed on how these models can be tailored to various sectors and how they can evolve in response to emerging cyber threats.

Moreover, integrating advanced statistical methods in network security indicates a gap in integrating these technical methods into broader organizational cybersecurity strategies (Hoeltgebaum et al. 2022). Future research could focus on how organizations can effectively incorporate these advanced analytical techniques into their overall cybersecurity posture, ensuring that technical detection methods align with strategic security objectives.

Interestingly, there are research opportunities for analyzing the psychological factors that influence cybersecurity behavior. Sarno and Black (2023) explored the psychological aspects of phishing susceptibility. However, there are still open questions about the psychological factors affecting various cybersecurity behaviors. For example, future research could delve into the human biases and cognitive aspects that increase or reduce the risks connected to cyberspace. Moreover, while the importance of education in enhancing cybersecurity awareness is recognized, there is a lack of detailed research on effective educational and training methodologies that can lead to actual behavioral change. Studies need to focus on developing and evaluating educational programs that increase awareness and effectively influence online behaviors and practices.

Regarding ethics, Wright, Johnson, and Kitchens (2023) discuss the ethical considerations in defending against phishing attacks. However, there is a lack of comprehensive research on the ethical implications of different cybersecurity measures and how they impact various stakeholders. Further research is needed to explore the ethical dimensions of cybersecurity strategies, particularly those that affect user privacy and data rights. Similarly, Chen, Henry, and Jiang (2023) identify a gap in the detailed understanding of the ethical implications of corporate transparency in cybersecurity. There is a need for more in-depth research on the ethical responsibilities of corporations in disclosing cybersecurity risks, balancing the need for transparency with the potential impacts on stakeholder trust and corporate reputation.

Also, Tsang et al. (2023) raise questions about the ethical balance between collaborative security efforts and individual privacy rights. This area requires further exploration, particularly in developing ethical frameworks that guide data sharing for security purposes while protecting individual privacy. Concurrently, there are significant research gaps in exploring the ethical dimensions of cybersecurity measures, the responsibilities of corporate transparency, and the balance between collaborative security and privacy. Addressing these challenges and gaps is crucial for developing a more ethical and responsible approach to cybersecurity.

4.3 | Theoretical Implications

The present study offers a number of theoretical implications. Indeed, positioning cybersecurity as a strategic concern within the contemporary business management landscape, this study calls for a paradigm shift in how organizations conceptualize, implement, and integrate cybersecurity within their strategic frameworks. This perspective pushes the boundaries of traditional business management theories and offers novel insights into cybersecurity's strategic management in an interconnected digital era. One of the primary theoretical implications of this study is the reconceptualization of cybersecurity as an integral part of business strategy (Hepfer and Powell 2020) rather than a peripheral aspect. This shift in perspective challenges traditional views and situates cybersecurity at the core of strategic decision-making, highlighting its role in safeguarding organizational assets, reputation, and operations.

Accordingly, this redefinition of cybersecurity as a core strategic imperative within business management corroborates that a narrow perspective is no longer tenable in the face of increasingly sophisticated and pervasive cyber threats. The integration of cybersecurity into the core of business strategy necessitates a broader theoretical understanding that incorporates elements of organizational behavior, decision-making, and leadership (Santoso and Finn 2022). This prompts a reevaluation of how business strategies are formulated, suggesting that cybersecurity considerations must be embedded in the earliest stages of strategic planning rather than being an afterthought (Hanelt et al. 2021). In this perspective, this shift challenges existing models of strategic management that prioritize traditional market-based factors while often neglecting the role of digital security in sustaining competitive advantage (Rothrock, Kaplan, and Van Der Oord 2018). The study thus calls for developing new strategic management theories explicitly designed to account for cybersecurity as a fundamental component of business resilience and success.

Moreover, this study sheds light on the relationship between human factors and cybersecurity, particularly within organizational behavior. The study underscores the critical role that human element—such as employee behavior, awareness, and organizational culture—play in shaping cybersecurity outcomes (Proctor and Chen 2015). This focus enhances the academic debate on the partly-overlooked social and psychological dimensions of cybersecurity, which have profound implications for theories of organizational behavior. By highlighting how human errors and behavioral biases can compromise even the most advanced technological defenses, the study suggests cybersecurity should be approached as a socio-technical issue (Kortschot et al. 2018). This perspective challenges the prevailing view that cybersecurity can be adequately addressed through technical solutions alone, proposing that organizational behavior theories need to incorporate a more nuanced understanding of how human factors interact with technology in complex organizational settings (Ahangama 2023). This insight opens up new avenues for theoretical development, particularly in leadership, employee training, and organizational culture, where the focus should shift towards fostering a security-aware organizational environment that can proactively manage and mitigate cyber risks (Akter et al. 2022).

The study also points out the centrality of cybersecurity's ethical and legal dimensions, arguing that these aspects extend far beyond compliance. In business management, cybersecurity has traditionally been framed in terms of regulatory requirements and legal obligations (Lee et al. 2020). Besides, this study also highlights the ethical dilemmas and broader social responsibilities that organizations face in the digital age (Chen et al. 2022). The study suggests that the ethical management of cybersecurity involves complex decisions about transparency, privacy, and corporate accountability, which have significant implications for how businesses engage with their stakeholders and the wider society (Chen, Henry, and Jiang 2023). This perspective might encourage future researchers to dig deeper into ethical frameworks that go beyond compliance and are rooted in the principles of CSR and ethical leadership (Wright, Johnson, and Kitchens 2023). The focus on the ethical implications of cybersecurity practices prompts a rethinking of ethical considerations' role in strategic decision-making, particularly in how organizations balance the need for robust cybersecurity measures with the rights and privacy of individuals (Tsang et al. 2023). This insight is functional for expanding the discourse on business ethics to include the digital realm, where the stakes are increasingly high, and the consequences of ethical lapses can be far-reaching and severe.

4.4 | Implications for Practice

Following the findings from the present studies, businesses should approach cybersecurity as a core component of their overall strategy, deeply integrated into every aspect of their operations. To this end, the integration of cybersecurity, the implementation of continuous employee training, the adoption of a multidimensional approach, and the enhancement of transparency and ethical standards are all vital steps that business leaders must take to manage the complex challenges of cybersecurity effectively. These practices, derived from the study's findings, provide a proactive roadmap for organizations seeking to secure their digital landscapes while maintaining the trust and confidence of their stakeholders.

Specifically, treating cybersecurity as an integral part of the business strategy allows organizations to identify and mitigate risks proactively, enhancing their resilience against increasingly sophisticated cyber threats. For instance, incorporating cybersecurity into supply chain protocols ensures that potential vulnerabilities are addressed before they can be exploited, thereby safeguarding the organization's operations and reputation. Moreover, this approach aligns with international standards and regulatory requirements, strengthening the organization's market position and building trust among stakeholders.

Equally important is the need for continuous and adaptive training programs tailored to employees' specific roles and responsibilities. Since human error is often the weakest link in cybersecurity, organizations should invest in ongoing education and training to cover technical aspects and emphasize behavioral awareness. By doing so, employees become well-equipped to recognize and respond to cyber threats, reducing the likelihood of breaches caused by simple mistakes. Continuous training fosters a security culture within the organization, where employees actively contribute to the company's defense strategy. This proactive stance mitigates risks and enhances the organization's overall resilience in the face of evolving threats.

Moreover, to effectively manage cybersecurity, organizations should adopt a multidimensional framework that considers cybersecurity's political, economic, social, technological, environmental, and legal aspects. This approach ensures that all external and internal factors influencing cybersecurity are considered, allowing organizations to develop robust and adaptable strategies to changing conditions. For example, the political dimension would involve staying ahead of regulatory changes, ensuring compliance and readiness in a landscape where laws and standards continually evolve. Similarly, the economic dimension focuses on aligning cybersecurity initiatives with the organization's business goals, ensuring that investments in cybersecurity yield tangible benefits while protecting critical assets. This holistic framework enables organizations to anticipate and respond to a wide range of cyber threats, securing their operations and safeguarding their reputation.

Furthermore, enhancing transparency and ethical standards in cybersecurity practices is essential for building and maintaining stakeholder trust. Organizations must be transparent about their cybersecurity policies, potential risks, and actions to mitigate them. This transparency is increasingly central in today's digital economy, where trust and security are key drivers of customer and partner relationships. Upholding high ethical standards in data protection and incident response shields the organization from legal and reputational risks and aligns with broader CSR initiatives. By openly communicating their cybersecurity efforts and being forthcoming about incidents, organizations

demonstrate their commitment to protecting the interests of all stakeholders, which can serve as a significant competitive advantage in markets where trust is a critical asset.

5 | Conclusion

This study has provided key insights and strategic imperatives on the multifaceted dimensions of cybersecurity within business management literature. Adopting the PESTEL framework, our analysis has highlighted enduring lessons and open challenges across cybersecurity's political, economic, social, technological, environmental, and legal aspects.

Several key lessons emerge from this analysis. First, cybersecurity should be an integral part of business strategy rather than a peripheral IT function. Second, human behavior and organizational culture significantly shape cybersecurity outcomes. Training, education and promoting secure practices are as vital as deploying technological controls. Third, the evolving nature of cyber threats necessitates agile security strategies focused on prediction, prevention, detection, and response. However, significant challenges persist. The rapid pace of technological change poses an ongoing test for security measures. Integrating cybersecurity considerations across business functions remains difficult. Complex digital ecosystems strain existing security protocols. Ensuring legal and ethical balance amid new threats persists as an open debate. This study offers multiple theoretical and practical implications. It emphasizes the value of a holistic management approach toward cybersecurity. For scholars, it highlights rich avenues for future research at the intersection of technology, ethics, behavioral science, and management strategy. For practitioners, it underscores the need for an holistic cyber risk management encompassing detection, mitigation and continuity planning. As digitalization accelerates across industries, the strategic importance of cybersecurity will continue to grow. This study has brought together the scattered insights across business management literature, possibly paving the way for an integrated discipline of cybersecurity management. It has elucidated the main inroads made as well as areas for further research. Ultimately, advancing our understanding of cybersecurity requires interdisciplinary efforts in technology, business, law, and sociology. An integrated, proactive, and ethical approach is indispensable for safeguarding interconnected digital landscapes.

Acknowledgments

This research was also supported by the "Resilienza Economica e Digitale" project (CUP D67G23000060001) funded by the Italian Ministry of University and Research (MUR) as "Department of Excellence" (Dipartimenti di Eccellenza 2023-2027, Ministerial Decree no. 230/2022). Open access publishing facilitated by University of Trieste as part of the Wiley - CRUI-CARE agreement.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

Aggarwal, P., F. Moisan, C. Gonzalez, and V. Dutt. 2022. "Learning About the Effects of Alert Uncertainty in Attack and Defend Decisions via Cognitive Modeling." *Human Factors* 64, no. 2: 343–358.

Ahangama, S. 2023. "Relating Social Media Diffusion, Education Level and Cybersecurity Protection Mechanisms to e-Participation Initiatives: Insights From a Cross-Country Analysis." *Information Systems Frontiers* 25: 1695–1711.

Akter, S., M. R. Uddin, S. Sajib, W. J. T. Lee, K. Michael, and M. A. Hossain. 2022. "Reconceptualizing Cybersecurity Awareness Capability in the Data-Driven Digital Economy." *Annals of Operations Research*: 1–26.

AlDaajeh, S., and S. Alrabaee. 2024. "Strategic Cybersecurity." *Computers & Security* 141: 103845.

Al-Emran, M., M. A. Al-Sharafi, B. Foroughi, et al. 2024. "Evaluating the Barriers Affecting Cybersecurity Behavior in the Metaverse Using PLS-SEM and Fuzzy Sets (fsQCA)." *Computers in Human Behavior* 159: 108315.

Allodi, L., and F. Massacci. 2017. "Security Events and Vulnerability Data for Cybersecurity Risk Estimation." *Risk Analysis* 37, no. 8: 1606–1627.

Alshabib, H. N., and J. T. Martins. 2021. "Cybersecurity: Perceived Threats and Policy Responses in the Gulf Cooperation Council." *IEEE Transactions on Engineering Management* 69, no. 6: 3664–3675.

Andrijcic, E., and B. Horowitz. 2006. "A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property." *Risk Analysis* 26, no. 4: 907–923.

Baksi, R. P., and S. J. Upadhyaya. 2021. "Decepticon: A Theoretical Framework to Counter Advanced Persistent Threats." *Information Systems Frontiers* 23: 897–913.

Bamiatzi, V., M. Dowling, F. Gogolin, F. Kearney, and S. Vigne. 2023. "Are the Good Spared? Corporate Social Responsibility as Insurance Against Cyber Security Incidents." *Risk Analysis* 43, no. 12: 2503–2518.

Carayannis, E. G., E. Grigoroudis, S. S. Rehman, and N. Samarakoon. 2019. "Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience." *IEEE Transactions on Engineering Management* 68, no. 1: 223–234.

Carmel, E., and E. M. Roche. 2023. "The Dominant Cybersecurity Industry Clusters: Evolution and Sustainment." *Industry and Innovation* 30, no. 3: 361–391.

Chen, J., H. Ge, N. Li, and R. W. Proctor. 2022. "What I Say Means What I Do: Risk Concerns and Mobile Application-Selection Behaviors." *Human Factors* 64, no. 8: 1331–1350.

Chen, J., E. Henry, and X. Jiang. 2023. "Is Cybersecurity Risk Factor Disclosure Informative? Evidence From Disclosures Following a Data Breach." *Journal of Business Ethics* 187, no. 1: 199–224.

Corallo, A., M. Lazoi, M. Lezzi, and P. Pontrandolfo. 2021. "Cybersecurity Challenges for Manufacturing Systems 4.0: Assessment of the Business Impact Level." *IEEE Transactions on Engineering Management* 70, no. 11: 3745–3765.

Cui, Y., L. Cao, X. Gong, M. V. Basin, J. Shen, and T. Huang. 2023. "Resilient Output Containment Control of Heterogeneous Multiagent Systems Against Composite Attacks: A Digital Twin Approach." *IEEE Transactions on Cybernetics* 54, no. 5: 3313–3326.

DalleMule, L., and T. H. Davenport. 2017. "What's Your Data Strategy." *Harvard Business Review* 95, no. 3: 112–121.

Daniel, C., M. Mullarkey, and M. Agrawal. 2023. "RQ Labs: A Cybersecurity Workforce Skills Development Framework." *Information Systems Frontiers* 25, no. 2: 431–450.

Didenko, A. N. 2020. "Cybersecurity Regulation in the Financial Sector: Prospects of Legal Harmonization in the European Union and Beyond." *Uniform Law Review* 25, no. 1: 125–167.

Dinkova, M., R. El-Dardiry, and B. Overvest. 2023. "Should Firms Invest More in Cybersecurity?" *Small Business Economics* 63: 21–50.

Ebrahimi, M., Y. Chai, S. Samtani, and H. Chen. 2022. "Cross-Lingual Cybersecurity Analytics in the International Dark Web With Adversarial Deep Representation Learning." *MIS Quarterly* 46, no. 2: 1209–1226.

Fedele, A., and C. Roner. 2022. "Dangerous Games: A Literature Review on Cybersecurity Investments." *Journal of Economic Surveys* 36, no. 1: 157–187.

Ganin, A. A., P. Quach, M. Panwar, et al. 2020. "Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management." *Risk Analysis* 40, no. 1: 183–199.

Gordon, L. A., and M. P. Loeb. 2002. "The Economics of Information Security Investment." *ACM (Association for Computing Machinery) Transactions on Information and System Security* 5, no. 4: 438–457.

Hanelt, A., R. Bohnsack, D. Marz, and C. Antunes Marante. 2021. "A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change." *Journal of Management Studies* 58, no. 5: 1159–1197.

Hepfer, M., and T. C. Powell. 2020. "Make Cybersecurity a Strategic Asset." *MIT Sloan Management Review* 62, no. 1: 40–45.

Hoeltgebaum, H., N. Adams, and C. Fernandes. 2021. "Estimation, Forecasting, and Anomaly Detection for Nonstationary Streams Using Adaptive Estimation." *IEEE Transactions on Cybernetics* 52, no. 8: 7956–7967.

Hong, T., and A. Hofmann. 2021. "Data Integrity Attacks Against Outage Management Systems." *IEEE Transactions on Engineering Management* 69, no. 3: 765–772.

Kortschot, S. W., D. Sovilj, G. A. Jamieson, S. Sanner, C. Carrasco, and H. Soh. 2018. "Measuring and Mitigating the Costs of Attentional Switches in Active Network Monitoring for Cybersecurity." *Human Factors* 60, no. 7: 962–977.

Krishna, B., S. Krishnan, and M. P. Sebastian. 2023. "Examining the Relationship Between National Cybersecurity Commitment, Culture, and Digital Payment Usage: An Institutional Trust Theory Perspective." *Information Systems Frontiers* 25, no. 5: 1713–1741.

Krutilla, K., A. Alexeev, E. Jardine, and D. Good. 2021. "The Benefits and Costs of Cybersecurity Risk Reduction: A Dynamic Extension of the Gordon and Loeb Model." *Risk Analysis* 41, no. 10: 1795–1808.

Kunreuther, H., and G. Heal. 2003. "Interdependent security." *Journal of Risk and Uncertainty* 26, no. 2–3: 231–249.

Lee, J. K., Y. Chang, H. Y. Kwon, and B. Kim. 2020. "Reconciliation of Privacy With Preventive Cybersecurity: The Bright Internet Approach." *Information Systems Frontiers* 22: 45–57.

Li, Z., X. Guo, and Q. He. 2020. "A Study of Chinese Policy Attention on Cybersecurity." *IEEE Transactions on Engineering Management* 69, no. 6: 3739–3756.

Li, W., and H. Chen. 2022. "Discovering Emerging Threats in the Hacker Community: A Nonparametric Emerging Topic Detection Framework." *MIS Quarterly* 46, no. 4: 2337–2350.

Marzi, G., M. Balzano, A. Caputo, and M. M. Pellegrini. 2024. "Guidelines for Bibliometric-Systematic Literature Reviews: 10 Steps to Combine Analysis, Synthesis and Theory Development." *International Journal of Management Reviews*.

Marzi, G., M. Balzano, and D. Marchiori. 2024. "K-Alpha Calculator—Krippendorff's Alpha Calculator: A User-Friendly Tool for Computing Krippendorff's Alpha Inter-Rater Reliability Coefficient." *MethodsX* 12: 102545.

Oesterreich, T. D., and F. Teuteberg. 2016. "Understanding the Implications of Digitization and Automation in the Context of Industry 4.0: A Triangulation Approach and Elements of a Research Agenda for the Construction Industry." *Computers in Industry* 83: 121–139.

Öğüt, H., S. Raghunathan, and N. Menon. 2011. "Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection." *Risk Analysis: An International Journal* 31, no. 3: 497–512.

Pandey, S., R. K. Singh, and A. Gunasekaran. 2023. "Supply Chain Risks in Industry 4.0 Environment: Review and Analysis Framework." *Production Planning & Control* 34, no. 13: 1275–1302.

Plachkinova, M., and P. Menard. 2019. "An Examination of Gain-and Loss-Framed Messaging on Smart Home Security Training Programs." *Information Systems Frontiers* 24, no. 6: 1395–1416.

Popay, J., H. Roberts, A. Sowden, et al. 2006. "Guidance on the Conduct of Narrative Synthesis in Systematic Reviews. 2006." *ESRC Methods Programme*. Lancaster: Lancaster University.

Proctor, R. W., and J. Chen. 2015. "The Role of Human Factors/Ergonomics in the Science of Security: Decision Making and Action Selection in Cyberspace." *Human Factors* 57, no. 5: 721–727.

Qin, Y., Q. Zhang, C. Zhou, and N. Xiong. 2018. "A Risk-Based Dynamic Decision-Making Approach for Cybersecurity Protection in Industrial Control Systems." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 50, no. 10: 3863–3870.

Radanliev, P., D. De Roure, C. Maple, and U. Ani. 2022. "Super-Forecasting the 'Technological Singularity' Risks From Artificial Intelligence." *Evolving Systems* 13, no. 5: 747–757.

Radanliev, P., D. De Roure, C. Maple, and O. Santos. 2022. "Forecasts on Future Evolution of Artificial Intelligence and Intelligent Systems." *IEEE Access* 10: 45280–45288.

Rothrock, R. A., J. Kaplan, and F. Van Der Oord. 2018. "The Board's Role in Managing Cybersecurity Risks." *MIT Sloan Management Review* 59, no. 2: 12–15.

Santoso, F., and A. Finn. 2022. "A Data-Driven Cyber–Physical System Using Deep-Learning Convolutional Neural Networks: Study on False-Data Injection Attacks in an Unmanned Ground Vehicle Under Fault-Tolerant Conditions." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 53, no. 1: 346–356.

Sarno, D. M., and J. Black. 2023. "Who Gets Caught in the Web of Lies?: Understanding Susceptibility to Phishing Emails, Fake News Headlines, and Scam Text Messages." *Human Factors* 66, no. 6: 1742–1753.

Saura, J. R., D. Palacios-Marqués, and D. Ribeiro-Soriano. 2023. "Leveraging SMEs Technologies Adoption in the Covid-19 Pandemic: A Case Study on Twitter-Based User-Generated Content." *Journal of Technology Transfer* 48, no. 5: 1696–1722.

Schlegelmilch, B. B., K. Sharma, and S. Garg. 2022. "Employing Machine Learning for Capturing COVID-19 Consumer Sentiments From Six Countries: A Methodological Illustration." *International Marketing Review* 40, no. 5: 869–893.

Shaikh, F. A., and M. Siponen. 2024. "Organizational Learning From Cybersecurity Performance: Effects on Cybersecurity Investment Decisions." *Information Systems Frontiers* 26, no. 3: 1109–1120.

Shukla, M., S. P. Sarmah, and M. K. Tiwari. 2023. "A Multi-Objective Framework for the Identification and Optimization of Factors Affecting Cybersecurity in the Industry 4.0 Supply Chain." *International Journal of Production Research* 61, no. 15: 5266–5281.

Sukumar, A., H. A. Mahdiraji, and V. Jafari-Sadeghi. 2023. "Cyber Risk Assessment in Small and Medium-Sized Enterprises: A Multilevel Decision-Making Approach for Small e-Tailors." *Risk Analysis* 34, no. 10: 2082–2098.

Tang, R., Z. Miao, S. Jiang, X. Chen, H. Wang, and W. Wang. 2021. "Interlayer Link Prediction in Multiplex Social Networks Based on Multiple Types of Consistency Between Embedding Vectors." *IEEE Transactions on Cybernetics* 53, no. 4: 2426–2439.

Tsang, R. C., A. A. Baldwin, J. F. Hair, E. Affuso, and K. D. Lahtinen. 2023. "The Informativeness of Sentiment Types in Risk Factor Disclosures: Evidence from Firms with Cybersecurity Breaches." *Journal of Information Systems* 37, no. 3: 157–190.

Turel, O., Q. He, and Y. Wen. 2021. "Examining the Neural Basis of Information Security Policy Violations: A Noninvasive Brain Stimulation Approach." *MIS Quarterly* 45, no. 4: 1715–1744.

Varian, H. R. 2004. "System Reliability and Free Riding." In *Economics of Information Security*, edited by J. J. Camp and S. Lewis, 1–16. Boston, MA: Springer.

White, G. R., R. A. Allen, A. Samuel, A. Abdullah, and R. J. Thomas. 2020. "Antecedents of Cybersecurity Implementation: A Study of the Cyber-Preparedness of UK Social Enterprises." *IEEE Transactions on Engineering Management* 69, no. 6: 3826–3837.

Wright, R. T., S. L. Johnson, and B. Kitchens. 2023. "Phishing Susceptibility in Context: A Multilevel Information Processing Perspective on Deception Detection." *MIS Quarterly* 47, no. 2: 803–832.

Yoo, C. W., J. Goo, and H. R. Rao. 2020. "Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness." *MIS Quarterly* 44, no. 2: 907–931.

Żebrowski, P., A. Couce-Vieira, and A. Mancuso. 2022. "A Bayesian Framework for the Analysis and Optimal Mitigation of Cyber Threats to Cyber-Physical Systems." *Risk Analysis* 42, no. 10: 2275–2290.

Zhang, G., J. Wang, J. Liu, and Y. Pan. 2021. "Relationship Between the Metadata and Relevance Criteria of Scientific Data." *Data Science Journal* 20, no. 1: 5.

Zhu, T., D. Ye, Z. Cheng, W. Zhou, and S. Y. Philip. 2022. "Learning Games for Defending Advanced Persistent Threats in Cyber Systems." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 53, no. 4: 2410–2422.