Business Process Management Journal

The centrality of cybersecurity: business models, competitive strategies and sustainability practices

Patrizia Gazzola, Stefano Amelio, Enrica Pavione and Filippo Marubini

Department of Economics, University of Insubria, Varese, Italy

Received 11 July 2025
Revised 10 October 2025
30 December 2025
2 February 2026
11 February 2026
Accepted 11 February 2026

Abstract

Purpose – Cybersecurity has evolved from a technical function to a critical factor for business success. This paper provides a focused analysis of how emerging technologies—artificial intelligence (artificial intelligence), blockchain, and cloud-based Business Process Management tools—impact internal business processes.

Design/methodology/approach – This study explores the strategies adopted by ten leading global cybersecurity companies through a multiple case study design based on Gioia-inspired document analysis (2018–1024). The methods of collecting data related to the companies considered are multiple and include annual reports, sustainability reports, and online databases.

Findings – These technologies are shown to enhance threat detection, compliance, workflow automation, and decision-making efficiency, thus transforming cybersecurity capabilities into a strategic asset. The research highlights how business process innovation, driven by digital technologies, contributes to long-term differentiation and resilience in an increasingly complex and competitive environment. The analysis, which focuses only on companies with the largest market capitalizations, highlights a transformative approach that marks a shift towards a future in which cybersecurity is and will increasingly be a priority.

Originality/value – This study provides a novel contribution by integrating a comparative analysis of the business models, competitive strategies, and sustainability practices of ten leading cybersecurity firms, an approach not yet systematically explored in existing literature. By examining how emerging technologies are reshaping internal processes, the paper bridges gaps between strategic management, digital transformation, and sustainability. It offers new theoretical and managerial insights into how these technologies can be leveraged as key drivers of competitive advantage in a rapidly evolving cybersecurity landscape.

Keywords Cybersecurity, Strategy, AI, Blockchain, BPM, Sustainability

Paper type Research article

Introduction

The global competitive environment is significantly affected by the ongoing digital transformation, which involves several changes (Xia *et al.*, 2024; Chwiłkowska-Kubala *et al.*, 2023; Dąbrowska *et al.*, 2022). The digitalization landscape is growing rapidly across various industries, leading businesses of all sizes to invest in essential technologies such as blockchain (Sharma *et al.*, 2023; Gazzola *et al.*, 2023; Albayati *et al.*, 2020), cloud services, artificial intelligence (AI) (Moderno *et al.*, 2024), and machine learning (Onyshchenko *et al.*, 2020), not only to remain competitive but also to manage the growing number of cybersecurity threats (Al-Emran and Deveci, 2024; Li *et al.*, 2020). As cybersecurity spending is projected to increase globally by 2030 (Hoong *et al.*, 2024), it is evident that digital protection is no longer a purely technical issue but a strategic one, shaping business performance, reputation, and

Funding details: This publication is part of the project NODES which has received funding from the MUR – M4C2 1.5 of PNRR funded by the European Union NextGenerationEU (Grant agreement no. ECS00000036) – CUP J83B22000050001.

Business Process Management Journal
Emerald Publishing Limited
e-ISSN: 1758-4116
p-ISSN: 1463-7154
DOI 10.1108/BPMJ-07-2025-1110

long-term sustainability. In addition to rapid technological advances, digital transformation involves the widespread adoption of new business models (Gazzola *et al.*, 2024a, b) and profound changes in collective behaviors (Vătămănescu *et al.*, 2023; George and Schillebeeckx, 2022). In addition, cybersecurity is increasingly the focus of attention, not only from companies but also from academics (Singh *et al.*, 2023; Walton *et al.*, 2021).

While these innovations offer the potential for competitiveness, they also present a growing number of cybersecurity challenges (Al-Emran and Deveci, 2024; Guerreiro, 2021) that need to be addressed. As the business landscape continues to evolve, bridging the gap between technology and cybersecurity becomes critical to thriving in an ever-changing market environment (Knell, 2021; Khalatur *et al.*, 2022). As a result, organizations are dedicating significant financial and human resources to safeguard their digital operations and assets. The central role of cybersecurity (Hoong *et al.*, 2024) in the digital economy is evidenced by global spending on cybersecurity which, according to Global X, could reach and exceed $450 billion by 2030.

Although prior studies have highlighted the role of cybersecurity in enabling a competitive advantage (Yousaf *et al.*, 2021; Oluokun *et al.*, 2024) and examined business model innovation in digital contexts (Tohănean *et al.*, 2020; Van Looy, 2021), the existing literature remains fragmented. Most research focuses on one dimension at a time—technical aspects of cybersecurity, strategic models of competition, or sustainability practices—without systematically exploring their intersection. Moreover, while scholars have discussed the drivers of platform business model innovation and individual data control (Kemppainen *et al.*, 2022), there is still little understanding of how leading cybersecurity firms simultaneously integrate business models, competitive strategies, and sustainability practices into coherent strategic approaches. This represents a critical gap, given the dual pressures of digital security risks and environmental responsibility. To address this gap, this study seeks to answer the following research question: How do leading global cybersecurity firms integrate business models, competitive strategies, and sustainability practices to transform cybersecurity from a technical necessity into a source of competitive advantage?

Building on these premises, this research aims to explore the strategic approaches adopted by the ten largest global players in the cybersecurity sector. These companies are recognized as market leaders; therefore, they are considered examples of excellence. This study aims to analyze the business models implemented by these organizations, highlighting how they have succeeded in repositioning cybersecurity from a mere operational requirement to a true source of competitive advantage. It also seeks to examine how these organizations have embraced innovation in order to differentiate themselves in an increasingly crowded market, offering advanced solutions to protect their clients' digital infrastructures. Finally, the analysis also aims to explore sustainability-related initiatives, shedding light on how companies are responding to the growing expectations of consumers and regulatory bodies regarding environmental and social responsibility. A thorough understanding of these business models and their interaction with sustainable development goals can reveal valuable synergies and common ground between profitability and environmental stewardship. This integrated perspective stems from forward-looking strategies that reduce the ecological impact of the digital sector while simultaneously enhancing cybersecurity resilience (Alam, 2022).

This article contributes to the literature in three ways. First, it offers a theoretical contribution by advancing the understanding of cybersecurity not merely as an operational function but as a strategic driver, integrating insights from strategic management, digital transformation, and sustainability studies. Second, it makes an empirical contribution through a multiple case study approach using a Gioia-inspired qualitative analysis (Gioia *et al.*, 2013) of ten leading cybersecurity firms to provide systematic evidence of how industry leaders design their business models and sustainability practices, an approach not yet explored in the existing literature. Finally, the findings offer a managerial and policy contribution by providing practical guidance for managers seeking to align cybersecurity with competitive

differentiation and ESG goals and for policymakers designing regulatory frameworks that encourage both innovation and environmental responsibility.

By explicitly addressing the gap and highlighting the contributions, this study clarifies the centrality of cybersecurity in today's competitive context and provides a foundation for future research on the convergence of security, strategy, and sustainability.

Theoretical background and literature review

Investments in cybersecurity have become a top priority for organizations around the world. According to Li and Liu's (2021) comprehensive study, the aim of investment is to strengthen defences, prevent costly security breaches, and deter targeted cyber attacks. The literature on the topic is quite extensive and mainly aimed at analyzing companies' benefits that result from investments in cybersecurity (Kosutic and Pigni, 2022). Incentives to invest in security technologies often emerge when companies can expand their potential consumer base and gain a larger market share. Investing in cybersecurity not only attracts more customers but also acts as a barrier to entry for competitors, thus increasing market share (Yousaf *et al*., 2021; Tohãnean *et al*., 2020). According to Zhang *et al*. (2024), enterprises mitigate the risks of cyberattacks by investing in digital security and digital services, following the three core cybersecurity strategies of risk acceptance, risk balance, and risk reduction.

Most studies emphasize technical defenses or ROI of cybersecurity investments (Moore *et al*., 2016; Haber, 2025), but they underexplor how these measures integrate into broader business strategies (Mızrak, 2023). This can lead to missing important opportunities to leverage security as a source of competitive advantage. Market recognition and rewards for companies demonstrating a consistent commitment to improving their security underscore the critical importance of proactively addressing security issues before they manifest as potential vulnerabilities. To truly harness the transformative power of cybersecurity as a competitive advantage, organizations must actively and seamlessly integrate security into the very fabric of their organizations. This involves integrating security into the design and architecture of systems and networks, as well as adopting secure software development practices (Alawida *et al*., 2022).

Cybersecurity is not only important for protecting products and services from hackers (Oluokun *et al*., 2024), but also plays a crucial role in distinguishing companies from their competitors, as evidenced by the continuous advancements in software updates. This strategic focus on security offers companies in saturated markets a unique opportunity for differentiation (Al-Hawamleh, 2024). By prioritizing cybersecurity measures, a company can establish itself as more distinctive and attractive than its competitors (Rasel and Peter, 2025). The cybersecurity software market, characterized by fierce competition and rapid evolution, compels companies to constantly innovate and adapt to ever-changing threat scenarios. With the increasing frequency and sophistication of cyberattacks, companies must go beyond technical solutions, focusing instead on customer satisfaction, trust-building, and strategic alignment with sustainable business practices.

The increasing significance of protecting digital infrastructure and the investments in digital protection have led to an increase in companies that provide cybersecurity services in order to manage risks associated with digital operations (Van Looy, 2021). These businesses are mainly focused on the creation, transmission, storage, processing, and analysis of information or data (Almor and Berliner, 2024). Cybersecurity companies operate over various segments of the cybersecurity value chain, generally including activities such as risk assessment, threat detection, incident response, and recovery. Each segment of the value chain is interconnected and requires effective collaboration and information sharing to secure that cyber threats are addressed efficiently (Keenan, 2022). In order to effectively combat cybercrime activities and safeguard the digital ecosystem, companies operating in the cybersecurity sector must continuously update and adapt competitive strategies and business models and build robust standards (Kala, 2023).

As the rise of data-driven technologies and the increasing value and quantity of information have driven rapid growth in the cybersecurity industry in recent years, this demand has increased revenue and expanded the IT workforce, creating new job opportunities. The need for stronger security solutions has encouraged constant innovation in the field. In 2018, top vendors included Symantec, Kaspersky, McAfee, Trend Micro, and IBM, all of which were focused on steady security solutions. Technology giants such as Microsoft and Cisco have become key players in the sector, leveraging their strengths in software and networking. Newer companies such as Palo Alto Networks and Proofpoint have benefited from rapid growth thanks also to increasingly advanced technologies. Conversely, established providers such as Check Point, F5 Networks, Fortinet, and Sophos offer more comprehensive and tailored solutions for various sectors (Aslan *et al.*, 2023).

However, even though the more established giants have been able to maintain their dominant market position, new competitors such as CrowdStrike, FireEye, and Carbon Black have begun to challenge their leadership. These dynamic companies have revolutionized the security market by introducing innovative approaches and strategies, pushing the boundaries of cybersecurity to new levels. Their rapid rise has further emphasized the competitiveness and attractiveness of the software market (Uchendu *et al.*, 2021) and highlighted how the critical success factors are multiple and linked to investments in research, development, sales, and marketing (Butt *et al.*, 2020; Alam, 2022).

In addition to technical challenges, organizations operating in the cybersecurity sector often face bureaucratic constraints. These frequently stem from regulatory barriers and procedural inefficiencies, which can delay or disrupt the delivery of cybersecurity products and services. Studying and addressing such barriers in the most efficient way possible is essential for the sector's long-term development and operational resilience, as it enables better resource allocation and greater responsiveness to emerging digital threats (McLennan, 2022). The growing interdependence between organizational success and the demand for reliable cybersecurity frameworks underscores the need to adopt forward-looking, adaptable, and scalable strategies over time. Furthermore, the increasing emphasis on sustainability is driving many companies to incorporate environmentally responsible policies into their core operations (Jarvis, 2022; Li *et al.*, 2020).

The preceding considerations highlight how the literature on cybersecurity companies has focused primarily on analyzing their value chains and business models (Corallo *et al.*, 2020). This study aims to provide a new contribution by integrating a comparative analysis of the business models, competitive strategies, and sustainability practices of ten leading global cybersecurity companies, an approach not yet systematically explored in the existing literature. The attempt to bring together aspects related to corporate strategy, business models, innovation policies, and sustainability practices is intended to be the novelty of this article compared to the literature on the topic, which tends to focus on a single aspect of corporate strategy.

Cybersecurity, strategic asset, and sustainability

The literature increasingly recognizes that cybersecurity is not only a technical safeguard but also a source of strategic differentiation. Investments in digital protection enhance resilience, reduce risks of breaches, and strengthen customer trust (Zhang *et al.*, 2024; Zhuo and Chen, 2023). Research shows that strong security practices can expand market share, act as barriers to entry, and build competitive advantage (Yousaf *et al.*, 2021; Tohănean *et al.*, 2020). In saturated markets, cybersecurity can distinguish firms by embedding security into system design, software development, and service delivery (Alawida *et al.*, 2022; Oluokun *et al.*, 2024). However, most studies emphasize technical defenses or ROI of cybersecurity investments while underexploring how these measures integrate into broader business strategies.

Another stream of literature highlights how digital transformation reshapes business models. Cybersecurity providers operate across value chains involving risk assessment, detection, incident response, and recovery, requiring constant adaptation to evolving threats (Keenan, 2022; Kala, 2023). Traditional giants such as IBM and Cisco leverage their legacy in IT and networking, while younger firms like Palo Alto Networks and CrowdStrike have grown rapidly through innovation (Aslan *et al*., 2023; Uchendu *et al*., 2021). Subscription-based and service-oriented revenue models are becoming dominant, reflecting a shift toward recurring income and continuous updates (Butt *et al*., 2020; Alam, 2022). Beyond profitability, platform business models are increasingly influenced by individuals' control over their data, creating new drivers of innovation and regulation. Despite these insights, the literature often examines competitive strategies in isolation, rather than connecting them to sustainability and long-term resilience (Kosutic and Pigni, 2022; Direction, 2021).

A third body of work stresses the growing importance of sustainability in the digital sector. Companies are under pressure to reduce the environmental footprint of data centers, adopt energy-efficient technologies, and comply with global sustainability standards (Jarvis, 2022; Love *et al*., 2023). Examples include Microsoft's pledge to achieve carbon negativity by 2030 and the wider adoption of green data center practices (Lim and Pope, 2020). Scholars emphasize that sustainability is no longer a peripheral issue but a driver of corporate legitimacy and long-term competitiveness (Alam, 2022). Nevertheless, research on the intersection of cybersecurity strategy and environmental sustainability remains scarce. Most contributions treat ESG commitments separately from cybersecurity, leaving a gap in understanding how leading firms integrate the two in practice (Bruno *et al*., 2025).

Taken together, these three streams of literature underline the importance of cybersecurity as a competitive factor, the role of business model innovation, and the growing relevance of sustainability. However, there is still limited understanding of how these dimensions intersect within the strategic approaches of leading cybersecurity firms. Prior research has either focused on technical solutions, organizational strategies, or sustainability, but rarely on their integration (Ige *et al*., 2024). This study addresses this gap by conducting a comparative analysis of ten global leaders in cybersecurity, systematically examining how their business models, competitive strategies, and sustainability practices interact. By bridging these fragmented literatures, the paper advances both theoretical and practical debates on the centrality of cybersecurity in the contemporary competitive context.

Materials and methods

Research design

This study adopts a multiple case study design, drawing on the classical methodological frameworks proposed by Eisenhardt (1989) and Yin (2013), with the aim of building theoretical insights from the systematic comparison of several leading firms in the global cybersecurity industry. The choice of a multi-case study, rather than a single case, is consistent with the objective of examining how different companies integrate business models, competitive strategies, and sustainability practices while operating in a similar competitive and technological context. In line with Eisenhardt (1989), the research process followed an iterative path that included case selection, data collection from multiple sources, within-case analysis, cross-case comparison, and progressive refinement of emerging constructs.

The analysis is qualitative in nature and is based on document analysis and comparative content analysis of secondary sources relating to ten leading global cybersecurity companies (Palo Alto Networks, IBM, Cisco Systems, Microsoft, Fortinet, Proofpoint, Kaspersky, McAfee, Symantec, Trend Micro), which together account for more than 35% of the global cybersecurity market. Therefore, the study is positioned within qualitative, document-based research, rather than as a narrative review, and aims to inductively derive patterns and categories from corporate documents and reports.

Case and data selection

The ten companies were selected through theoretical sampling, following Yin's (2013) logic of choosing "information-rich" cases that are particularly suitable for illuminating the phenomenon under investigation. The inclusion criteria were as follows: (1) being recognized as a global leader in cybersecurity in terms of market capitalization and market share; (2) being included in international rankings such as Cybersecurity Ventures' lists of top cyber firms; and (3) availability of detailed and recent public documentation (financial reports, sustainability reports, ESG disclosures, cybersecurity and technology reports).

Data collection focused on the period 2018–2024, in order to capture both recent strategic developments and the evolution of sustainability initiatives in the cybersecurity sector. The main documentary sources considered were:

(1) Annual reports and Form 10-K (where applicable) for the years 2018–2023

(2) Sustainability reports, ESG or CSR reports for the years 2019–2023

(3) Integrated reports and climate-related disclosures (e.g. TCFD reports), when available

(4) Official company presentations and investor materials focused on cybersecurity strategy and business model innovation

(5) Corporate policies or reports relating to environmental sustainability, data center efficiency, and ethical use of AI

(6) Selected industry rankings and sectoral reports that profile leading cybersecurity firms (e.g. Cybersecurity Ventures, analyst reports)

In line with Bowen (2009), a document sampling matrix was developed to transparently show the types of documents analyzed for each company, the year of publication, and the main content focus. This matrix is presented in the manuscript as a table (Table 1), structured as follows:

(1) Company

(2) Document type (annual report, sustainability report, integrated report, policy document, sector report, etc.)

(3) Year(s) considered

(4) Main thematic relevance (business model, competitive strategy, sustainability practices, technological innovation)

Only documents that (a) contained explicit information on business models, strategic initiatives, and/or sustainability practices and (b) referred to the core cybersecurity activities of the company were included in the final sample. Documents that were purely promotional, repetitive, or lacking in substantive strategic content were excluded.

Data analysis: coding and Gioia-inspired structure

The analytical process followed a Gioia-inspired approach (Gioia *et al*., 2013), adapting the first-order/second-order/aggregate dimensions logic to the context of document analysis on cybersecurity firms. The analysis unfolded according to the following three main steps:

(1) First-order coding (informant-centric concepts). Each document was read in full, and passages relating to business models, competitive strategies, sustainability initiatives, technological innovation (AI, blockchain, Business Process Management (BPM)), and cybersecurity positioning were coded line-by-line. At this stage, codes remained close to the original wording (e.g. "subscription-based revenue", "green data centers",

Table 1. Documents and data analysed for each company

Company	Document type	Years covered	Main thematic focus
Palo Alto Networks	Annual report/Form 10-K	2019–2023	Financial performance, market positioning, business model, R&D
Palo Alto Networks	Sustainability/ESG report	2019–2024	Environmental footprint, data center efficiency, ESG commitments
Palo Alto Networks	Cybersecurity product white papers	2020–2023	Next-generation firewalls, platform strategy, AI-driven security
IBM	Annual report/Form 10-K	2018–2023	Cloud and security revenues, strategic initiatives, acquisitions
IBM	ESG/sustainability report	2019–2023	Climate targets, green data centers, responsible innovation
IBM	Security division reports/ briefings	2019–2024	Threat intelligence, security services portfolio
Cisco Systems	Annual report/Form 10-K	2018–2023	Networking and security portfolio, recurring revenues, M&A
Cisco Systems	Sustainability/CSR report	2019–2024	Energy efficiency, circular economy, social responsibility
Cisco Systems	Security architecture white papers	2020–2024	Zero-trust, secure networking, cloud security
Microsoft	Annual report/Form 10-K	2018–2023	Cloud security revenues, strategic positioning, investments
Microsoft	Sustainability report/Climate report	2019–2023	Carbon negative pledge, data center decarbonisation, ESG strategy
Microsoft	Security/AI security reports	2020–2024	AI-driven threat detection, security operations, compliance
Fortinet	Annual report	2019–2023	Platform strategy, revenue mix, global expansion
Fortinet	ESG/sustainability report	2020–2023	Environmental performance, governance, social initiatives
Fortinet	Technical/product documentation	2019–2024	Integrated security fabric, AI and automation
Proofpoint	Annual report	2018–2023	Email security positioning, subscription model, customer segments
Proofpoint	ESG/sustainability disclosures	2020–2023	ESG policies, social and governance aspects
Proofpoint	Product and threat reports	2019–2024	Email risk, threat landscape, managed services
Kaspersky	Annual report/company overview	2018–2023	Endpoint security, geographic reach, partnerships
Kaspersky	Sustainability/CSR documents	2019–2023	Social responsibility, education projects, environmental initiatives
McAfee	Annual report/investor materials	2019–2023	Consumer and enterprise security, business model
McAfee	ESG/CSR report	2020–2023	ESG strategy, diversity, environmental policies
Symantec	Annual/financial reports	2018–2022	Enterprise security, portfolio evolution
Symantec	Sustainability/CSR disclosures	2019–2023	Environmental and social commitments
Trend Micro	Annual report	2019–2023	Security portfolio, geographic expansion, subscription revenues
Trend Micro	Sustainability report	2019–2023	Green IT initiatives, social impact, governance
All companies	Sector reports/rankings (e.g. Cybersecurity Ventures)	2019–2024	Market share, industry benchmarks, competitive landscape

Note(s): Document sampling matrix adapted from Bowen (2009). Shows types, years, and thematic focus of documents analyzed for each of the 10 cybersecurity firms (2018–2024)

Source(s): Our own elaboration

"AI-driven threat detection", "transparency reports", "strategic acquisitions in cloud security") in order to preserve the diversity of company-specific expressions.

(2) Second-order themes (researcher-centric themes). In a second step, first-order codes were compared across companies to identify more abstract themes, grouping similar practices and strategic patterns into broader categories. For example, codes related to various recurring revenue schemes (SaaS, managed services, security-as-a-service) converged into the theme "subscription-based and service-oriented business models"; codes referring to energy-efficient data centers, carbon neutrality commitments, and eco-efficient infrastructure were grouped under "environmental sustainability initiatives in cybersecurity infrastructure".

(3) Aggregate dimensions. Finally, second-order themes were clustered into aggregate dimensions that reflect the main domains investigated by the study: (1) cybersecurity as a strategic asset; (2) business model and competitive positioning; (3) sustainability and ESG integration; (4) technology-driven process optimization (AI, blockchain, BPM). These aggregate dimensions underpin the structure of the Results and Discussion sections and allow for a systematic comparison between firms.

To enhance transparency, the manuscript includes a data structure table inspired by Gioia *et al*. (2013) (Figure 1), where selected first-order concepts are visually connected to second-order themes and aggregate dimensions. This table clarifies the inductive logic by which the findings were derived from the underlying documentary evidence.

In addition, a SWOT analysis was developed for each company as a synthesis of the qualitative coding results. Rather than being a purely descriptive exercise, the SWOT tables draw directly from the coded material and the Gioia-inspired dimensions, summarizing how strengths, weaknesses, opportunities, and threats emerge from the combination of strategic choices, business models, and sustainability practices.

Analytical techniques

The overall analytical strategy combines the following:

(1) Qualitative document analysis, in line with Bowen (2009), used to systematically review and interpret corporate documents as "texts" that reflect organizational strategies and priorities;

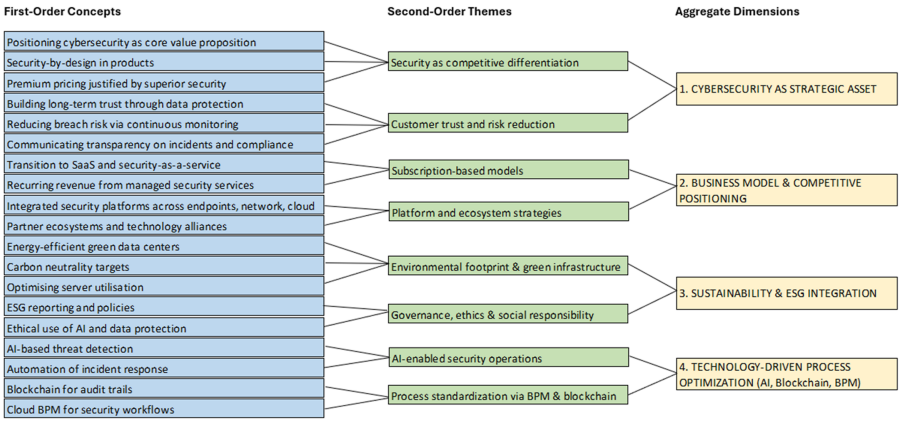

Figure 1. Data structure (Gioia-inspired). Data structure adapted from Gioia *et al*. (2013). Illustrates the inductive coding process from first-order concepts to aggregate dimensions. Source: Our own elaboration

(2) Thematic content analysis, applied to identify recurring patterns and themes across companies and to group similar practices into coherent categories;

(3) Cross-case comparison, in the tradition of multi-case studies (Eisenhardt, 1989; Yin, 2013), used to contrast how different firms configure their business models, competitive strategies, and sustainability initiatives.

This combination of techniques supports an inductive approach in which the findings are derived from the coded data and only subsequently linked back to the existing literature on cybersecurity, strategy, and sustainability.

Trustworthiness of the study

The quality of the qualitative research was addressed using the four main trustworthiness criteria (credibility, transferability, dependability, and confirmability) discussed by Duarte Alonso *et al*. (2024).

(1) Credibility. Credibility was enhanced through data triangulation across multiple document types (annual reports, sustainability reports, policy documents, sectoral analyses) and ten different companies. Two authors independently coded a subset of documents and then compared and discussed their coding schemes to align interpretations and resolve discrepancies. Iterative returns to the data were used to verify the coherence of emerging themes with the underlying texts.

(2) Transferability. To support transferability, the study provides thick descriptions of the sectoral context (global cybersecurity market), the competitive environment, and the regulatory and sustainability pressures affecting leading firms. The selection criteria for the ten companies and the time frame (2018–2024) are explicitly stated, enabling readers to assess the relevance of the findings for other contexts and for firms of different sizes or in other industries.

(3) Dependability. Dependability was pursued by clearly documenting the research process, from case selection to data collection and coding. The development of the document sampling matrix and the description of the Gioia-inspired analysis steps provide a procedural "audit trail" that would allow other researchers to replicate or extend the study with similar data sources.

(4) Confirmability. Confirmability was strengthened by (a) relying exclusively on publicly available documents, which can be independently accessed and verified; (b) maintaining a clear distinction between empirical evidence (first-order codes) and interpretive levels (second-order themes and aggregate dimensions); and (c) using joint coding sessions and cross-checks among authors to reduce individual bias in the interpretation of the data. Reflexive discussions among the research team were conducted to challenge initial assumptions and to ensure that the reported findings are grounded in the documentary evidence rather than in prior theoretical expectations.

Results

Tables 2 and 3 offer a detailed comparison of the top cybersecurity companies based on the different variables considered: year of foundation, headquarters, key products, market position and business model, financial performance, strategic initiatives, swot analysis, and sustainability. From the analysis it is possible to draw some initial conclusions.

Table 2. Comparison of the top 10 cybersecurity companies (part 1)

Aspect	Palo Alto Networks	IBM	Cisco systems	Microsoft	Fortinet
Founded	2005	1911	1984	1975	2000
Headquarters	Santa Clara, CA	Armonk, NY	San Jose, CA	Redmond, WA	Sunnyvale, CA
Key Products	NGFWs, Cortex XDR, Prisma Cloud	QRadar, Guardium	Secure Firewall, Umbrella	Microsoft Defender, Azure Security	FortiGate, FortiGuard Labs
Market Position	Leader in NGFW, strong in enterprise security	Leader in enterprise IT	Dominant in networking, strong in security	Leader in cloud and enterprise security	Strong in integrated security platforms
Business Model	Product sales, subscriptions, professional services	Product sales, services, subscriptions	Hardware, software, subscriptions	Software sales, cloud services, subscriptions	Hardware sales, subscriptions
Financial Performance	Over $8 B revenue (2024)	$60 B revenue, strong in R&D	Strong growth in cybersecurity	Strong growth in cloud and security	Strong growth in services and subscriptions
Strategic Initiatives	Acquisitions in SOAR, SD-WAN	Acquisitions in AI, cloud security	Acquisitions in MFA, network intelligence	Acquisitions in AI, IoT security	Expansion in AI, SASE, cloud security

(*continued*)

Table 2. Continued

Aspect	Palo Alto Networks	IBM	Cisco systems	Microsoft	Fortinet
SWOT Analysis	• Strengths: Innovative Technology Leadership, Comprehensive Product Suite, Strong Market Position, Robust Financial Performance • Weaknesses: High Cost of Solutions, Complexity of Products • Opportunities: Growing Demand for Cybersecurity, Expansion into Emerging Markets • Threats: Intense Competition, Rapid Technological Changes, Regulatory Challenges	• Strengths: Strong Brand and Market Leadership, Diverse Product and Service Portfolio, Strong R&D, Global Presence • Weaknesses: High Operating Costs, Legacy Systems, Slow Growth in Key Segments • Opportunities: Expansion in Cloud Computing, Growth in AI and Quantum Computing, Cybersecurity Demand • Threats: Intense Competition, Rapid Technological Changes, Economic Uncertainty	• Strengths: Market Leadership, Diverse Portfolio, Innovation and R&D, Global Reach, Strong Financial Performance • Weaknesses: Reliance on Hardware, Complex Product Portfolio, Slow Adaptation to Emerging Trends • Opportunities: Growth in Cloud Computing and IoT, 5G Networks • Threats: Intense Competition, Market Saturation, Technological Disruption, Regulatory Challenges	• Strengths: Brand Reputation, Financial Strength, Diverse Product Portfolio, Strong Integration and Ecosystem • Weaknesses: Dependence on Core Products, Complexity of Offerings • Opportunities: Cloud Computing and AI Growth, Emerging Markets Expansion • Threats: Intense Competition, Cybersecurity Risks	• Strengths: Comprehensive Product Portfolio, Strong Brand and Reputation, Advanced Threat Intelligence, Global Reach • Weaknesses: Dependence on Hardware Sales, Complex Product Integration • Opportunities: Growth in Cloud and IoT Security, Expansion into Emerging Markets • Threats: Evolving Cyber Threats, Regulatory Changes, Economic Uncertainty
Sustainability	Focus on energy-efficient data centers. Supporting initiatives that increase access to education and technology	Net-zero by 2030. Focus on energy efficiency, renewable energy use, and sustainable practices throughout its global operations	Net-zero by 2040. Focus on social impact through initiatives like the Cisco Networking Academy	Carbon negative by 2030. Investments in renewable energy and energy-efficient data centers	Energy-efficient design. Education initiatives

Source(s): Our own elaboration

Table 3. Comparison of the top 10 cybersecurity companies (part 2)

Aspect	Proofpoint	Kaspersky	McAfee	Symantec	Trend micro
Founded	2002	1997	1987	1982	1988
Headquarters	Sunnyvale, CA	Moscow, Russia	San Jose, CA	Mountain View, CA	Tokyo, Japan
Key Products	Email Security, Data Protection	Kaspersky Endpoint Security	Total Protection, Cloud Security	Symantec Endpoint Protection	XDR, Cloud Security
Market Position	Leader in email security	Strong in EMEA, challenges in NA	Strong in consumer security	Strong in enterprise security	Strong in APAC, cloud security
Business Model	Subscription-based, managed services	Product sales, subscriptions	Subscription-based, consumer focus	Subscription-based, enterprise focus	Subscription-based, cloud security
Financial Performance	Stable, strong growth in cloud security	Stable, challenges due to geopolitical issues	Stable, driven by consumer sales	Stable under Broadcom, enterprise focus	Strong growth in cloud offerings
Strategic Initiatives	Focus on AI, threat detection	Focus on AI, industrial security	Expansion in AI, cloud security	Focus on AI, ransomware protection	Focus on cloud security, AI

(*continued*)

Table 3. Continued

Aspect	Proofpoint	Kaspersky	McAfee	Symantec	Trend micro
SWOT Analysis	• Strengths: Comprehensive Product Portfolio, Strong Customer-Centric Approach, Subscription-Based Revenue Model • Weaknesses: High Dependence on Email Security, Limited Global Reach • Opportunities: Growing Demand for Cloud Security, Expansion into Emerging Markets • Threats: Rapid Evolution of Cyber Threats, Regulatory Challenges, Competitive Pressure	• Strengths: High Detection Rate, Ease of Use, Global Recognition • Weaknesses: Dependence on Regular Updates, Geopolitical and Regulatory Challenges • Opportunities: Rising Demand for Cybersecurity Solutions, Expanding IoT and Cloud Security • Threats: Emerging Competitors, Evolving Cyber Threats, Political and Regulatory Risks	• Strengths: Comprehensive Product Portfolio, Brand Recognition, Competitive Pricing, Strategic Growth through M&A • Weaknesses: Dependence on Regular Updates, Limited Operating System Support • Opportunities: Rising Demand for Cybersecurity, Cloud and IoT Security Expansion • Threats: Intense Competition, Rapidly Evolving Cyber Threats, Regulatory and Political Risks	• Strengths: Market Leadership, Diverse Product Portfolio, Global Presence • Weaknesses: Limited Market Share Growth, Post-Merger Integration Challenges • Opportunities: Growing Cybersecurity Demand, Acquisitions and Partnerships • Threats: Intense Competition, Rapidly Evolving Threat Landscape	• Strengths: Market Leadership, Diverse Product Portfolio, Global Presence • Weaknesses: Limited Market Share Growth, Post-Merger Integration Challenges • Opportunities: Growing Cybersecurity Demand, Acquisitions and Partnerships • Threats: Intense Competition, Rapidly Evolving Threat Landscape
Sustainability	Focus on energy-efficient data centers. Training programs in the areas of cybersecurity awareness and education	Energy-efficient operations. Social initiatives aimed at improving cybersecurity education and awareness across different regions	Focus on energy-efficient operations. Diversity and inclusion within its workforce	Energy-efficient operations. Community outreach programs aimed at improving cybersecurity awareness and education, particularly in underrepresented regions	Focus on energy-efficient operations. Diversity and inclusion within its organization

Source(s): Our own elaboration

Different founding dates and longevity

The companies considered vary significantly in terms of age and market experience. IBM, founded in 1911, is by far the oldest company, with more than a century of history in enterprise IT. On the other hand, newer companies such as Palo Alto Networks (founded in 2005) and Fortinet (founded in 2000) have made rapid strides in cybersecurity despite their relatively recent founding. This shows that, if experience plays an important role, innovation and adaptability are the features that have allowed younger companies to emerge as key players in a highly competitive industry.

Concentration of headquarters in the United States

The majority of the companies evaluated in this study are headquartered in the United States, thus highlighting the country's leadership position in the cybersecurity sector. Organizations such as Palo Alto Networks, Cisco, McAfee, and Microsoft are located in major US technology hubs such as Silicon Valley. However, the presence of significant players outside the United States, including Kaspersky (Russia) and Trend Micro (Japan), underscores the decidedly international nature of this sector.

(1) Aggregate dimensions obtained from the Gioa Methodology

Starting from the Goia methodology, it is possible to formulate some summary considerations relating to the main aggregate dimensions: (1) cybersecurity as a strategic asset; (2) business model and competitive positioning; (3) integration of sustainability and ESG; and (4) technology-driven process optimization (AI, blockchain, BPM).

Cybersecurity as a strategic asset. Each company specializes in distinct areas of this market. For example, Palo Alto Networks and Fortinet focus primarily on network security, with their next-generation firewalls forming a core part of their offering. In line with its global cloud strategy, Microsoft emphasizes cloud and enterprise security with solutions such as Defender and Azure Security. Proofpoint focuses mainly on email protection, while Kaspersky is recognized for its expertise in endpoint protection. This variety of areas of specialization reveals how companies are able to carve out competitive niches even within the same sector.

The positioning of each company reflects both historical strengths and current strategic choices. IBM and Cisco are leaders in enterprise IT and networking, respectively, while Microsoft's dominance in cloud infrastructure reinforces its role in enterprise-level security. In contrast, Fortinet and Palo Alto Networks are known for their comprehensive security platforms and firewall capabilities. Proofpoint's leadership in email security represents an example of specialization, while McAfee and Symantec continue to operate in parallel across both the consumer and enterprise segments.

Business model and competitive positioning. Many companies today base their revenue models on subscriptions, especially in the areas of cloud security and software platforms. This trend reflects a broader shift in the industry toward predictable and recurring revenue streams that support continuous protection, updates, and services. McAfee, Symantec, and Proofpoint are strongly based on these subscription models, while Fortinet and Palo Alto Networks combine hardware sales with subscription services, particularly for their cloud-integrated offerings.

Several industry leaders have strategically invested in AI, machine learning, and cloud technologies. Palo Alto Networks and Microsoft have been particularly active in promoting AI-powered tools. Cisco has expanded its portfolio through targeted acquisitions, strengthening its presence in both networking and security. Fortinet's use of AI-driven solutions further demonstrates the growing importance of automation in defending against constantly evolving threats.

Integration of sustainability and ESG. The core business of the companies considered in this analysis involves the provision of highly specialized services that include areas such as technology, management, systems auditing, cyber law, and computer forensics

(Yigitbasioglu *et al.*, 2023; Chowdhury *et al.*, 2022). Within the broader field of cybersecurity, companies are striving to promote sustainable initiatives aimed at mitigating the negative environmental impact of the IT industry, which is known to be one of the most polluting and energy-intensive sectors. Examples of these green initiatives include the development of energy-efficient data centers, the adoption of green policies, the improvement of products' environmental footprint, and investments in cleaner and more sustainable technologies. When effectively implemented, these can lead to significant cost reductions, particularly by mitigating the growing energy demands of IT operations. In addition to financial benefits, such initiatives also enhance a company's environmental reputation and support a more responsible public image (Lim and Pope, 2020).

To support improvements in sustainability, several international certification frameworks have been introduced to guide organizations toward environmentally sound and responsible practices. One such example is the Australian Standard for Environmental Claims (AS 4360), which defines criteria to ensure that sustainability claims are accurate and verifiable. On a broader scale, international standards such as ISO 14000 provide detailed frameworks for integrating sustainability into corporate strategy, operational processes, and business governance (Love *et al.*, 2023).

In the field of cybersecurity, sustainability also refers to how these companies approach the environmental impact of their data centers and operational practices. Microsoft's commitment to become carbon negative by 2030 is a strong example for other tech companies. Similarly, many companies are beginning to integrate energy-efficient practices and sustainable data center operations, recognizing the environmental impact of their operations in cybersecurity and IT infrastructure. Additionally, many companies are emphasizing the ethical use of AI in cybersecurity and ensuring that data privacy and security align with global standards.

Technology-driven process optimization. Alongside the traditional strategic, financial, and operational factors examined in this study, emerging technologies are increasingly shaping internal processes and value delivery mechanisms within cybersecurity firms. In particular, three technologies—artificial intelligence (AI), blockchain, and cloud-based BPM systems—are driving notable changes in how these companies function and adapt to evolving challenges.

AI is being leveraged for more sophisticated threat detection, predictive risk modeling, automated compliance tasks, and accelerated incident response. For instance, Microsoft and Palo Alto Networks have adopted AI tools to minimize alert fatigue and streamline security triage workflows (Jada and Mayayise, 2024; IBM Security, 2023).

Blockchain, with its characteristics rooted in transparency and immutability, is emerging as a solution for creating and maintaining secure audit trails and enabling secure decentralized structures. Companies such as Fortinet and IBM have begun integrating blockchain technologies into their security infrastructures to strengthen regulatory compliance and data integrity (Alevizos, 2025; Cyble Inc, 2025).

Cloud-based BPM platforms offer real-time visibility, standardized processes, and automation in risk assessment. Organizations like Cisco and McAfee use these platforms to coordinate internal procedures in areas such as policy governance, patch lifecycle management, and regulatory compliance (CMW Lab, 2023).

These technologies offer multiple strategic advantages, including faster incident response, reduced operational costs, greater scalability, and improved alignment between cybersecurity functions and business objectives. They also reflect a broader trend toward integrating cybersecurity into companies' digital transformation agendas (Lewis *et al.*, 2025).

(2) SWOT Analysis Highlights

Starting from the implications derived from the aggregate dimensions described, the SWOT analysis completes the qualitative analysis of the companies considered. From a SWOT analysis perspective, these companies exhibit significant strengths and specific vulnerabilities. Palo Alto Networks, for example, is a prominent player in the next-generation firewall and

enterprise security markets, but it must constantly contend with intense competition and rapidly evolving threats. Microsoft's strong cloud foundation grants it a significant advantage, although growth in saturated segments poses a challenge. Finally, Kaspersky's expertise in endpoint protection is well established; however, it faces geopolitical constraints that limit its access to certain markets, such as North America.

In conclusion, the comparative analysis of the leading cybersecurity companies highlights a sector characterized by intense competition and considerable diversity. These companies differ significantly in terms of year of foundation, geographical distribution, strategic focus, and market position. While some have established dominance in specific areas, others have chosen to concentrate on specialized and niche segments. Recently, models such as the widespread adoption of subscription-based revenue, the integration of AI, and the growing focus on sustainability reflect broader and more complex transformations within the sector.

Ultimately, a company's capacity to remain competitive appears closely tied to its ability to innovate, respond to evolving security threats, and strategically capitalize on its core capabilities in an increasingly dynamic digital environment.

Discussion and conclusion

Innovation is increasingly supporting the alignment between cybersecurity capabilities and internal process efficiency. The adoption of AI, blockchain, and BPM platforms marks a shift from traditional reactive models to more proactive, process-oriented approaches. These technologies are not merely incremental improvements but are reshaping the way cybersecurity companies design operations, manage data, and make strategic decisions.

The current cybersecurity landscape is shaped by the convergence of rapid technological development, geopolitical tensions, and shifting economic conditions. In this context, cybersecurity has evolved from a purely technical function into a strategic pillar for companies operating in complex and volatile environments. This study aimed to demonstrate how industry leaders have integrated cybersecurity into their core business, enabling them to remain competitive and future-oriented (Dunn Cavelty and Wenger, 2020).

Although these companies operate in global markets, they must contend with regulatory frameworks and customer expectations that vary widely. The lack of common guidelines means that commercial, national, and international dynamics often determine operational strategies (Pattison, 2020). Despite such differences, the companies analyzed exhibit a consistent pursuit of efficiency and competitive advantage through two main strategic levers: differentiation of security products (Rajan *et al.*, 2021) and continuous innovation.

Proprietary technologies, early market entry, and sustained R&D efforts are increasingly influencing success in this sector. By leveraging innovative features, companies position themselves at the forefront of the market, justify premium pricing, and reinforce their leadership. A key driver in shaping the evolution of the industry is the growing emphasis on high-performance, high-value-added services (Costa, 2021).

Effective differentiation requires a deep understanding of the target audience. Players in the cybersecurity field, whether hardware or software-based, tend to tailor their offerings to meet evolving security needs. This is made possible by ongoing innovation, which, combined with technological progress, enables market share expansion and, consequently, supports higher pricing. Among the most impactful strategies are the integration of proprietary systems, first-mover initiatives, and consistent investments in product development (Ryan, 2020).

Innovation, as a fundamental growth engine across the industry, drives companies to refine their technologies in response to ever-evolving threats (Rashid *et al.*, 2021; Benaroch, 2020). Financial reports and corporate communications provide clear evidence of the centrality of R&D in business strategies (Blum, 2020). These companies channel significant resources into security services, threat intelligence, and opportunities offered by emerging sectors such as cloud computing, IoT, mobile platforms, and endpoint protection (Hallman *et al.*, 2020).

Given their role in safeguarding systems and data, core security services continue to represent a primary area of investment. Threat intelligence, made possible by large-scale data analysis, allows companies to anticipate risks and develop preventive responses (Marotta and Madnick, 2021). These risks, together with the expansion into emerging technologies, introduce new challenges, pushing companies to design flexible solutions capable of adapting to the evolving threat landscape (Tagarev, 2020).

The growing demand for cybersecurity solutions reinforces the importance of ongoing investments in innovation. R&D has become both a differentiating factor and a necessity for companies seeking to meet specific industry needs and outperform the competition. At the same time, strategic partnerships are key to long-term success. Companies can enhance their capabilities, enter new markets, and expand the range of services offered (Ogbanufe *et al.*, 2021). These partnerships strengthen the ecosystem and foster cooperation within the sector.

Starting from these general considerations, this research presents original and innovative results both in jointly considering the aggregate dimensions derived from the Gioia methodology (1) cybersecurity as a strategic asset; (2) business model and competitive positioning; (3) integration of sustainability and ESG; and (4) technology-driven process optimization) and in integrating the aforementioned variables with a SWOT analysis. The competitive nature of the security software market requires continuous innovation and adaptation. As cyber threats become increasingly sophisticated and pervasive, leading security software vendors must remain vigilant in improving customer satisfaction, building customer loyalty, and aligning their business models with sustainable development principles. The interconnectedness of business success, environmental responsibility, and the growing demand for robust cybersecurity solutions underscores the need for comprehensive research into the strategies and practices employed by these industry leaders (Jarvis, 2022).

The research also highlights how the ten leading companies analyzed actively align their operating models with sustainability principles. The global emphasis on ESG (Environmental, Social, and Governance) factors has driven these companies to integrate ethical and environmental considerations into their digital strategies (Savaş and Karataş, 2022; Burton and Lain, 2020). The most common initiatives include awareness campaigns, the drafting of transparency reports, and the implementation of strict privacy compliance policies (Gale *et al.*, 2022).

Furthermore, to increase transparency and consumer trust, more and more companies are now publishing detailed user data statistics—especially in the wake of an attack or upon law enforcement request—clearly outlining the regulatory frameworks adopted and the number of users affected. These communications aim to address growing concerns over data governance, particularly in a context of increasing regulatory scrutiny across different jurisdictions (Bechara and Schuch, 2021). This responsiveness reflects broader political shifts and heightened cybersecurity directives, such as those issued by US executive authorities, which now position cybersecurity as a strategic—and even marketing—imperative (Karpiuk, 2021).

Understanding their business models and their implications for sustainable development can pave the way for a more secure and environmentally responsible future. By delving deeper into the strategies adopted by these security software vendors, researchers can uncover potential synergies between profitability and environmental sustainability. This holistic approach would enable the creation of innovative solutions that not only strengthen cybersecurity but also minimize the digital landscape's ecological footprint (Alam, 2022). Therefore, it is crucial that stakeholders, researchers, and industry practitioners collaborate and explore the intricate interplay between cybersecurity, sustainable development, and long-term business success. By collaborating and sharing insights, they can bridge the gap between the dynamic needs of the industry and the growing demand for environmentally friendly solutions. Already, several companies have adopted disruptive business models, integrating competition and cooperation to meet global cybersecurity demands (Langley *et al.*, 2021; Burström *et al.*, 2021). Only through collective effort and comprehensive research can we ensure a safer, greener, and more secure digital future for all. In this light, sustainability is not a

side concern but a foundational aspect of cybersecurity implementation. Financial performance, technical innovation, and brand leadership are all strengthened by ESG alignment (Safitra *et al.*, 2023).

In conclusion, this study shows that leading cybersecurity firms are not only reacting to technological changes; they are actively shaping the future of the sector. Technologies like IoT, AI, and blockchain will continue to drive transformation, offering opportunities but also presenting new vulnerabilities (Contieri *et al.*, 2022). Meeting these challenges requires proactive innovation and long-term commitment to adaptive security strategies (Khan and La Torre, 2021; Senol and Karacuha, 2020). As digitalization accelerates, the distinction between today's tech firms and tomorrow's AI- or IoT-driven companies is becoming increasingly fluid (Volberda *et al.*, 2021). This evolution calls for countries and businesses alike to invest in sophisticated cybersecurity infrastructures in order to gain competitive advantage at a global scale. The convergence of cybersecurity, business model innovation, and sustainability reflects a structural shift in the digital economy. Leading firms are no longer treating security as a defensive necessity but as a proactive strategy for differentiation, growth, and legitimacy. By integrating sustainability practices into their competitive approaches, these companies illustrate how the pursuit of digital security and environmental responsibility can reinforce one another.

Ultimately, this study highlights that the centrality of cybersecurity in today's competitive context rests not only on technological solutions but also on its integration into broader business strategies and sustainability commitments. This study demonstrates that cybersecurity has evolved beyond a defensive, technical function into a strategic pillar that shapes competitiveness, business resilience, and long-term sustainability. By examining ten leading firms, the analysis reveals how cybersecurity capabilities are embedded in business models, leveraged as sources of competitive differentiation, and increasingly aligned with sustainability principles. Recognizing and leveraging this convergence is essential for firms seeking to remain competitive, resilient, and responsible in the digital era.

The novelty of this research lies in its integrated perspective. Prior literature has treated cybersecurity, competitive strategy, and sustainability as largely separate domains. This study systematically shows how these dimensions converge within the practices of leading global firms. Specifically, the findings highlight three critical insights: (1) cybersecurity is a strategic asset (security investments do not merely protect digital infrastructures but actively create competitive advantage through differentiation, trust-building, and entry barriers); (2) business model transformation (the shift toward subscription-based and service-oriented models illustrates how cybersecurity firms adapt to recurring threats by embedding security into value creation and delivery processes); and (3) sustainability integration (ESG initiatives, such as carbon-neutral data centers, transparency reports, and ethical AI use, are no longer external add-ons but integrated into the core strategies of cybersecurity leaders). Together, these insights extend strategic management literature by framing cybersecurity as both a driver of innovation and a foundation of sustainable competitive advantage.

That said, the study has some limitations. First, it focused solely on companies with the largest market capitalizations, excluding smaller or unlisted firms and startups. Second, the data was sourced entirely from publicly available documents, without direct input from company executives. It should be emphasized, however, that this research is part of a broader project that, starting with an in-depth analysis of the main market players, aims, in a subsequent step, to broaden the scope of analysis to include small and medium-sized companies, especially innovative startups. Finally, although SWOT analysis allows for the rapid analysis of multiple domains and systems through modeling, multidimensional analysis, and data integration, in the current turbulent and unpredictable environment, it should be integrated with new functional analysis tools for building scenarios and supporting strategic decisions.

Implications and future developments

From a managerial standpoint, this study shows that cybersecurity strategy must be aligned with broader business goals, not treated as a siloed function. Managers can draw on these cases to understand how security can reinforce brand differentiation, support recurring revenue models, and enhance customer trust. At the same time, sustainability practices are becoming a competitive lever in their own right, particularly as clients and regulators demand accountability for the environmental impact of IT operations. For policymakers, the findings underline the importance of regulatory frameworks that simultaneously promote cybersecurity resilience and sustainability compliance. Transparent reporting standards and ESG disclosure requirements can encourage firms to adopt greener cybersecurity infrastructures without undermining security performance.

Future research should extend the analysis to smaller market players and explore how firms of varying sizes navigate regulatory pressures and technological shifts. The present study offers a foundation for broader sectoral analysis, with the goal of capturing the full complexity of a field that is rapidly becoming central to the functioning of modern economies. This study focused on leading firms with the largest market shares, offering insights into best practices but not capturing the full diversity of the sector. Future research should extend the analysis to small and medium-sized enterprises and innovative startups, which face different constraints but often pioneer agile and sustainable solutions. Further studies could also explore sectoral differences (e.g. finance, healthcare, critical infrastructure) to understand how cybersecurity strategies adapt to specific regulatory and environmental pressures. Another promising direction is to investigate the role of sustainability-oriented innovations, such as environmentally optimized data centers and green AI, in accelerating the diffusion of secure and sustainable business practices.

References

Al-Emran, M. and Deveci, M. (2024), "Unlocking the potential of cybersecurity behavior in the metaverse: overview, opportunities, challenges, and future research agendas", *Technology in Society*, Vol. 77, 102498, doi: 10.1016/j.techsoc.2024.102498.

Al-Hawamleh, A.M. (2024), "Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: eevidence from the KSA", *Digital Policy, Regulation and Governance*, Vol. 26 No. 3, pp. 317-336, doi: 10.1108/DPRG-11-2023-0168.

Alam, S. (2022), "Cybersecurity: past, present and future", arXiv preprint arXiv:2207.01227, doi: 10.48550/arXiv.2207.01227.

Alawida, M., Omolara, A.E., Abiodun, O.I. and Al-Rajab, M. (2022), "A deeper look into cybersecurity issues in the wake of Covid-19: a survey", *Journal of King Saud University-Computer and Information Sciences*, Vol. 34 No. 10, pp. 8176-8206, doi: 10.1016/j.jksuci.2022.08.003.

Albayati, H., Kim, S.K. and Rho, J.J. (2020), "Accepting financial transactions using blockchain technology and cryptocurrency: a customer perspective approach", *Technology in Society*, Vol. 62, 101320, doi: 10.1016/j.techsoc.2020.101320.

Alevizos, L. (2025), "Automated cybersecurity compliance and threat response using AI, blockchain and smart contracts", *International Journal of Information Technology*, Vol. 17 No. 2, pp. 767-781, doi: 10.1007/s41870-024-02324-9.

Almor, T. and Berliner, D. (2024), "From Orange to cyber: the role of international business policy in creating 'Startup Nation'", in *Handbook of International Business Policy*, Edward Elgar Publishing, pp.226-242, doi: 10.4337/9781035308682.00021.

Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A. and Akin, E. (2023), "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions", *Electronics*, Vol. 12 No. 6, 1333, doi: 10.3390/electronics12061333.

Bechara, F.R. and Schuch, S.B. (2021), "Cybersecurity and global regulatory challenges", *Journal of Financial Crime*, Vol. 28 No. 2, pp. 359-374, doi: 10.1108/JFC-07-2020-0149.

Benaroch, M. (2020), "Cybersecurity risk in IT outsourcing—challenges and emerging realities", in *Information Systems Outsourcing: the Era of Digital Transformation*, Springer International Publishing, Cham, pp. 313-334, doi: 10.1007/978-3-030-45819-5_13.

Blum, D. (2020), *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment*, Springer Nature, Silver Spring, MD, p. 333, doi: 10.1007/978-1-4842-5952-8.

Bowen, G.A. (2009), "Document analysis as a qualitative research method", *Qualitative Research Journal*, Vol. 9 No. 2, pp. 27-40, doi: 10.3316/QRJ0902027.

Bruno, E., Pistolesi, F. and Teti, E. (2025), "Cybersecurity policy, ESG and operational risk: a virtuous relationship to improve banks' performance", *International Review of Economics and Finance*, Vol. 99, 104053, doi: 10.1016/j.iref.2025.104053.

Burström, T., Parida, V., Lahti, T. and Wincent, J. (2021), "AI-enabled business-model innovation and transformation in industrial ecosystems: a framework, model and outline for further research", *Journal of Business Research*, Vol. 127, pp. 85-95, doi: 10.1016/j.jbusres.2021.01.016.

Burton, J. and Lain, C. (2020), "Desecuritising cybersecurity: towards a societal approach", *Journal of Cyber Policy*, Vol. 5 No. 3, pp. 449-470, doi: 10.1080/23738871.2020.1856903.

Butt, U.J., Abbod, M.F. and Kumar, A. (2020), "Cyber threat ransomware and marketing to networked consumers", in *Handbook of Research on Innovations in Technology and Marketing for the Connected Consumer*, IGI Global, pp. 155-185, doi: 10.4018/978-1-7998-0131-3.ch008.

Chowdhury, N., Nystad, E., Reegård, K. and Gkioulos, V. (2022), "Cybersecurity training in Norwegian critical infrastructure companies", *International Journal of Safety and Security Engineering (IJSSE)*, Vol. 12 No. 3, pp. 299-310, doi: 10.18280/ijsse.120304.

Chwiłkowska-Kubala, A., Cyfert, S., Malewska, K., Mierzejewska, K. and Szumowski, W. (2023), "The impact of resources on digital transformation in energy sector companies", *Technology in Society*, Vol. 74, 102315, doi: 10.1016/j.techsoc.2023.102315.

CMW Lab (2023), *BPM and Cybersecurity in 2025: How CMWLab Enhances Security and Automation*, CMW Lab Blog, Foxboro, MA.

Contieri, P.G.S., Anholon, R. and De Santa-Eulalia, L.A. (2022), "Industry 4.0 enabling technologies in manufacturing: implementation priorities and difficulties in an emerging country", *Technology Analysis and Strategic Management*, Vol. 34 No. 5, pp. 489-503, doi: 10.1080/09537325.2021.1908536.

Corallo, A., Lazoi, M. and Lezzi, M. (2020), "Cybersecurity in the context of industry 4.0: a structured classification of critical assets and business impacts", *Computers in Industry*, Vol. 114, 103165, doi: 10.1016/j.compind.2019.103165.

Costa, C.F.D.S. (2021), "Artificial intelligence & cybersecurity: European union panorama", available at: https://www.researchgate.net/profile/Carlos-Filipe-Da-Silva-Costa/publication/354343066_Artificial_Intelligence_Cybersecurity_European_Union_panorama/links/6132a21a0360302a007a6f50/Artificial-Intelligence-Cybersecurity-European-Union-panorama.pdf (accessed 21 May 2025).

Cyble Inc (2025), *The Role of Blockchain in Securing Incident Management Logs*, Cyble Knowledge Hub, available at: https://cyble.com/knowledge-hub/incident-management-with-blockchain/ (accessed 21 May 2025).

Dąbrowska, J., Almpanopoulou, A., Brem, A., Chesbrough, H., Cucino, V., Di Minin, A., Giones, F., Hakala, H., Marullo, C., Mention, A., Mortara, L., Nørskov, S., Nylund, P.A., Oddo, C.M., Radziwon, A. and Ritala, P. (2022), "Digital transformation, for better or worse: a critical multi-level research agenda", *R&D Management*, Vol. 52 No. 5, pp. 930-954, doi: 10.1111/radm.12531.

Direction, S. (2021), "Investing in cybersecurity: gaining a competitive advantage through cybersecurity", *J. bus. strat*, Vol. 37, pp. 19-21, doi: 10.1108/SD-11-2020-0205.

Duarte Alonso, A., Vu, O.T.K., Nguyen, T.Q., McClelland, R., Nguyen, N.M., Huynh, H.T.N. and Tran, T.D. (2024), "Industry 4.0 involvement and knowledge management across industries: a

qualitative investigation from an emerging economy", *Journal of Business Research*, Vol. 174, 114538, doi: 10.1016/j.jbusres.2024.114538.

Dunn Cavelty, M. and Wenger, A. (2020), "Cyber security meets security politics: complex technology, fragmented politics, and networked science", *Contemporary Security Policy*, Vol. 41 No. 1, pp. 5-32, doi: 10.1080/13523260.2019.1678855.

Eisenhardt, K.M. (1989), "Building theories from case study research", *Academy of Management Review*, Vol. 14 No. 4, pp. 532-550, doi: 10.5465/amr.1989.4308385.

Gale, M., Bongiovanni, I. and Slapnicar, S. (2022), "Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead", *Computers and Security*, Vol. 121, 102840, doi: 10.1016/j.cose.2022.102840.

Gazzola, P., Pavione, E., Barge, A. and Fassio, F. (2023), "Using blockchain to improve supply chain transparency", *Sustainability*, Vol. 15 No. 10, 7884, doi: 10.3390/su15107884.

Gazzola, P., Drago, C., Pavione, E. and Pignoni, N. (2024a), "Sustainable business models: an empirical analysis of environmental sustainability in leading manufacturing companies", *Sustainability*, Vol. 16 No. 19, 8282, doi: 10.3390/su16198282.

Gazzola, P., Pavione, E., Amelio, S. and Mauri, M. (2024b), "Sustainable strategies and value creation in the food and beverage sector", *Sustainability*, Vol. 16 No. 22, 9798, doi: 10.3390/su16229798.

George, G. and Schillebeeckx, S.J.D. (2022), "Digital transformation, sustainability, and purpose in the multinational enterprise", *Journal of World Business*, Vol. 57 No. 3, 101326, doi: 10.1016/j.jwb.2022.101326.

Gioia, D.A., Corley, K.G. and Hamilton, A.L. (2013), "Seeking qualitative rigor in inductive research: notes on the Gioia methodology", *Organizational Research Methods*, Vol. 16 No. 1, pp. 15-31, doi: 10.1177/1094428112452151.

Guerreiro, S. (2021), "Conceptualizing on dynamically stable business processes operation: a literature review on existing concepts", *Business Process Management Journal*, Vol. 27 No. 1, pp. 24-54, doi: 10.1108/BPMJ-02-2020-0072.

Haber, M. (2025), "Return on investment", in *Attack Vectors: the History of Cybersecurity*, Apress, Berkeley, CA, pp. 231-238, doi: 10.1007/979-8-8688-1709-0_14.

Hallman, R.A., Major, M., Romero-Mariona, J., Phipps, R., Romero, E., John, M. and Miguel, S. (2020), "Return on cybersecurity investment in operational technology systems", *COMPLEXIS*, pp. 43-52, doi: 10.5220/0009416200430052.

Hoong, Y., Rezania, D. and Baker, R. (2024), "When traditional SME managers encounter cybersecurity", *Technology in Society*, Vol. 78, 102650, doi: 10.1016/j.techsoc.2024.102650.

IBM Security (2023), "Artificial intelligence (AI) cybersecurity – optimize analysts' time with AI-powered solutions", available at: https://www.ibm.com/solutions/ai-cybersecurity (accessed 25 May 2025).

Ige, A.B., Kupa, E. and Ilori, O. (2024), "Aligning sustainable development goals with cybersecurity strategies: ensuring a secure and sustainable future", *GSC Advanced Research and Reviews*, Vol. 19 No. 3, pp. 344-360, doi: 10.30574/gscarr.2024.19.3.0236.

Jada, I. and Mayayise, T.O. (2024), "The impact of artificial intelligence on organisational cyber security", *Data and Information Management*, Vol. 8 No. 2, 100063, doi: 10.1016/j.dim.2023.100063.

Jarvis, C. (2022), "Enterprise threat intelligence", in *Next-Generation Enterprise Security and Governance*, CRC Press, pp. 1-46, doi: 10.1201/9781003121541.

Kala, E.S.M. (2023), "Critical role of cyber security in global economy", *Open Journal of Safety Science and Technology*, Vol. 13 No. 4, pp. 231-248, doi: 10.4236/ojsst.2023.134012.

Karpiuk, M. (2021), "Organisation of the national system of cybersecurity: selected issues", *Studia Iuridica Lublinensia*, Vol. 30 No. 2, pp. 233-244, doi: 10.17951/sil.2021.30.2.233-244, available at: https://www.ceeol.com/search/article-detail?id=983433 (accessed 30 May 2025).

Keenan, A. (2022), "Cybersecurity in the global economy", available at: https://static1.squarespace.com/static/612fdeb8ae0c5815484a61c9/t/61db89d68bc0bb15e77862c2/1641777623117/G20_1.pdf (accessed 28 May 2025).

Kemppainen, L., Pikkarainen, M., Koivumäki, T. and Xu, Y. (2022), "Drivers for platform business model innovation: individuals in control over their personal data", doi: 10.24840/2183-0606_010.003_00031.

Khalatur, S., Pavlova, H., Vasilieva, L., Karamushka, D. and Danileviča, A. (2022), "Innovation management and financial sector digitalization", *Entrepreneurship and Sustainability Issues*, Vol. 9 No. 4, pp. 56-76, doi: 10.9770/jesi.2022.9.4(3).

Khan, F.S. and La Torre, D. (2021), "Quantum information technology and innovation", *Technology Analysis and Strategic Management*, Vol. 33 No. 11, pp. 1281-1289, doi: 10.1080/09537325.2021.1991576.

Knell, M. (2021), "The digital revolution and digitalized network society", *Review of Evolutionary Political Economy*, Vol. 2 No. 1, pp. 9-25, doi: 10.1007/s43253-021-00037-4.

Kosutic, D. and Pigni, F. (2022), "Cybersecurity: investing for competitive outcomes", *Journal of Business Strategy*, Vol. 43 No. 1, pp. 28-36, doi: 10.1108/JBS-06-2020-0116.

Langley, D.J., van Doorn, J., Ng, I.C., Stieglitz, S., Lazovik, A. and Boonstra, A. (2021), "The internet of everything", *Journal of Business Research*, Vol. 122, pp. 853-863, doi: 10.1016/j.jbusres.2019.12.035.

Lewis, C., Kristensen, I. and Caso, J. (2025), *AI is the Greatest Threat—and Defense—in Cybersecurity Today*, McKinsey & Company, available at: https://www.mckinsey.com/about-us/new-at-mckinsey-blog/ai-is-the-greatest-threat-and-defense-in-cybersecurity-today (accessed 31 May 2025).

Li, Y. and Liu, Q. (2021), "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments", *Energy Reports*, Vol. 7, pp. 8176-8186, doi: 10.1016/j.egyr.2021.08.126.

Li, Z., Guo, X. and He, Q. (2020), "A study of Chinese policy attention on cybersecurity", *IEEE Transactions on Engineering Management*, Vol. 69 No. 6, pp. 3739-3756, doi: 10.1109/TEM.2020.3029019.

Lim, A. and Pope, S. (2020), "Organizational boundary spanning and CSR policy", *Business Ethics: A European Review*, Vol. 29 No. 3, pp. 451-470, doi: 10.1111/beer.12266.

Love, P.E., Matthews, J., Porter, S.R., Carey, B. and Fang, W. (2023), "Quality II: a new paradigm for construction", *Developments in the Built Environment*, Vol. 16, 100261, doi: 10.1016/j.dibe.2023.100261.

Marotta, A. and Madnick, S. (2021), "Convergence of regulatory compliance and cybersecurity", *Issues in Information Systems*, Vol. 22 No. 1, doi: 10.48009/1_iis_2021.

McLennan, M. (2022), *The Global Risks Report 2022*, 17th ed., World Economic Forum, Cologny, available at: https://tatsigroup.com/fa/wp-content/uploads/2022/02/the-global-risks-report-2022.pdf (accessed 1 June 2025).

Mızrak, F. (2023), "Integrating cybersecurity risk management into strategic management: a comprehensive literature review", *Research Journal of Business Management*, Vol. 10 No. 3, pp. 98-108, doi: 10.17261/Pressacademia.2023.1807.

Moderno, O.B.D.S., Braz, A.C. and Nascimento, P.T.D.S. (2024), "Robotic process automation and artificial intelligence capabilities driving digital strategy: a resource-based view", *Business Process Management Journal*, Vol. 30 No. 1, pp. 105-134, doi: 10.1108/BPMJ-08-2022-0409.

Moore, T., Dynes, S. and Chang, F.R. (2016), "Identifying how firms manage cybersecurity investment", in *Workshop on the Economics of Information Security (WEIS)*, Darwin Deason Institute for Cyber Security, Southern Methodist University, Dallas, TX, pp. 1-27, available at: https://tylermoore.ens.utulsa.edu/ciso15ibm.pdf

Ogbanufe, O., Kim, D.J. and Jones, M.C. (2021), "Informing cybersecurity strategic commitment", *Information and Management*, Vol. 58 No. 7, 103507, doi: 10.1016/j.im.2021.103507.

Oluokun, A., Ige, A.B. and Ameyaw, M.N. (2024), "Building cyber resilience in fintech through AI and GRC integration: an exploratory study", *GSC Advanced Research and Reviews*, Vol. 20 No. 1, pp. 228-237, doi: 10.30574/gscarr.2024.20.1.0245.

Onyshchenko, V., Yehorycheva, S., Maslii, O. and Yurkiv, N. (2020), "Innovation and digital tech in financial security", *International Conference Building Innovations*, pp. 749-759, doi: 10.1007/978-3-030-85043-2_69.

Pattison, J. (2020), "From defence to offence: ethics of private cybersecurity", *European Journal of International Security*, Vol. 5 No. 2, pp. 233-254, doi: 10.1017/eis.2020.6.

Rajan, R., Rana, N.P., Parameswar, N., Dhir, S. and Dwivedi, Y.K. (2021), "Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management", *Technological Forecasting and Social Change*, Vol. 170, 120872, doi: 10.1016/j.techfore.2021.120872.

Rasel, F.M. and Peter, B. (2025), "AI-driven frameworks for enhancing cybersecurity in multi-cloud environments", *International Journal of Advanced Engineering Technologies and Innovations*, Vol. 1 No. 1, pp. 24-32, available at: https://www.researchgate.net/profile/Furqan-Md-Rasel/publication/390757136_AI-Driven_Frameworks_for_Enhancing_Cybersecurity_in_Multi-_Cloud_Environments/links/67fcfa33d1054b0207d32ae9/AI-Driven-Frameworks-for-Enhancing-Cybersecurity-in-Multi-Cloud-Environments.pdf (accessed 31 May 2025).

Rashid, Z., Noor, U. and Altmann, J. (2021), "Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem", *Future Generation Computer Systems*, Vol. 124, pp. 436-466, doi: 10.1016/j.future.2021.05.033.

Ryan, M. (2020), "The ransomware revolution: how emerging encryption technologies created a prodigious cyber threat", PhD thesis, UNSW Sydney, doi: 10.26190/unsworks/22132.

Safitra, M.F., Lubis, M. and Fakhrurroja, H. (2023), "A framework for the future of cybersecurity", *Sustainability*, Vol. 15 No. 18, 13369, doi: 10.3390/su151813369.

Savaş, S. and Karataş, S. (2022), "Cybersecurity governance overview", *International Cybersecurity Law Review*, Vol. 3 No. 1, pp. 7-34, doi: 10.1365/s43439-021-00045-4.

Senol, M. and Karacuha, E. (2020), "Creating and implementing national cybersecurity strategy", *Journal of Engineering*, Vol. 2020, pp. 1-19, doi: 10.1155/2020/5267564.

Sharma, A., Sharma, A., Singh, R.K. and Bhatia, T. (2023), "Blockchain adoption in agri-food supply chain management: an empirical study of the main drivers using extended UTAUT", *Business Process Management Journal*, Vol. 29 No. 3, pp. 737-756, doi: 10.1108/BPMJ-10-2022-0543.

Singh, N., Krishnaswamy, V. and Zhang, J.Z. (2023), "Intellectual structure of cybersecurity research", *Enterprise Information Systems*, Vol. 17 No. 6, 2025545, doi: 10.1080/17517575.2022.2025545.

Tagarev, T. (2020), "Governance in collaborative cybersecurity networks", *Future Internet*, Vol. 12 No. 4, p. 62, doi: 10.3390/fi12040062.

Tohănean, D., Buzatu, A.I., Baba, C.A. and Georgescu, B. (2020), "Business model innovation through digital technologies", *Amfiteatru Economic*, Vol. 22 No. 55, pp. 758-774, available at: https://www.ceeol.com/search/article-detail?id=888540 (accessed 31 May 2025).

Uchendu, B., Nurse, J.R.C., Bada, M. and Furnell, S. (2021), "Developing a cybersecurity culture", *Computers and Security*, Vol. 109, 102387, doi: 10.1016/j.cose.2021.102387.

Van Looy, A. (2021), "Business process management and digital innovation", *Information and Management*, Vol. 58 No. 2, 103413, doi: 10.1016/j.im.2020.103413.

Vătămănescu, E.M., Nicolescu, L., Gazzola, P. and Amelio, S. (2023), "Integrating smart mobility and electric car sharing adoption in a common framework: antecedents and mediators", *Journal of Cleaner Production*, Vol. 418, 138254, doi: 10.1016/j.jclepro.2023.138254.

Volberda, H.W., Khanagha, S., Baden-Fuller, C., Mihalache, O.R. and Birkinshaw, J. (2021), "Strategizing in a digital world", *Long Range Planning*, Vol. 54 No. 5, 102110, doi: 10.1016/j.lrp.2021.102110.

Walton, S., Wheeler, P.R., Zhang, Y. and Zhao, X. (2021), "Cybersecurity research: current state and future directions", *Journal of Information Systems*, Vol. 35 No. 1, pp. 155-186, doi: 10.2308/ISYS-19-033.

Xia, H., Ye, P., Jasimuddin, S.M. and Zhang, J.Z. (2024), "Evolution of digital transformation in China", *Technology Analysis and Strategic Management*, Vol. 36 No. 9, pp. 2014-2034, doi: 10.1080/09537325.2022.2124909.

Yigitbasioglu, O., Green, P. and Cheung, M.Y.D. (2023), "Digital transformation and accountants", *Accounting, Auditing and Accountability Journal*, Vol. 36 No. 1, pp. 209-237, doi: 10.1108/AAAJ-02-2019-3894.

Yin, R.K. (2013), *Case Study Research: Design and Methods*, 5th ed., SAGE Publication, Thousand Oaks, CA.

Yousaf, Z., Radulescu, M., Sinisi, C.I., Serbanescu, L. and Păunescu, L.M. (2021), "Sustainable digital innovation in SMEs", *Sustainability*, Vol. 13 No. 10, 5715, doi: 10.3390/su13105715.

Zhang, J.Z., Goel, L. and Williamson, S. (2024), "Understanding enterprise cybersecurity information sharing", *Enterprise Information Systems*, Vol. 18 No. 3, 2310844, doi: 10.1080/17517575.2024.2310844.

Zhuo, C. and Chen, J. (2023), "Can digital transformation overcome the innovation dilemma?", *Technological Forecasting and Social Change*, Vol. 190, 122378, doi: 10.1016/j.techfore.2023.122378.

Further reading

Ayobami, A. (2024), *How Blockchain Technology is Revolutionizing Audit and Control in Information Systems*, ISACA Industry News, available at: https://www.isaca.org/resources/news-and-trends/industry-news/2024/how-blockchain-technology-isrevolutionizing-audit-and-control-in-information-systems (accessed 20 May 2025).

Bederna, Z. and Szádeczky, T. (2023), "Managing the financial impact of cybersecurity incidents", *Security Defence Quarterly*, Vol. 41 No. 1, available at: https://www.ceeol.com/search/article-detail?id=1120686 (accessed 31 May 2025).

De Marchi, V., Di Maria, E., Golini, R. and Perri, A. (2020), "Nurturing international business research through global value chains literature", *International Business Review*, Vol. 29 No. 5, 101708, doi: 10.1016/j.ibusrev.2020.101708.

Jardine, E. (2020), "Taking the growth of the internet seriously when measuring cybersecurity", in *Researching Internet Governance: Methods, Frameworks, Futures*, pp. 146-168, available at: https://www.researchgate.net/profile/Eric-Jardine/publication/345628238_Taking_the_Growth_of_the_Internet_Seriously_When_Measuring_Cybersecurity/links/5fa95192a6fdcc0624203696/Taking-the-Growth-of-the-Internet-Seriously-When-Measuring-Cybersecurity.pdf (accessed 1 June 2025).

Karmeni, K., Beldi, A. and Saadi, T. (2025), "Exploring the performance effects of digitalisation: a measurement tool based on the sustainability balanced scorecard framework", *Technology Analysis and Strategic Management*, Vol. 37 No. 11, pp. 2174-2188, doi: 10.1080/09537325.2024.2346156.

Kramer, F.D., Teplinsky, M.J. and Butler, R.J. (2022), *Cybersecurity for Innovative Small and Medium Enterprises and Academia*, Atlantic Council, Scowcroft Center for Strategy and Security, Washington, DC, 13: 978-1-61977-210-6.

Pinto, T. and Teixeira, A.A.C. (2020), "Research output and economic growth", *Scientometrics*, Vol. 123 No. 2, pp. 945-978, doi: 10.1007/s11192-020-03419-3.

Corresponding author
Stefano Amelio can be contacted at: stefano.amelio@uninsubria.it