INTERNATIONAL JOURNAL OF CYBER THREAT INTELLIGENCE AND SECURE NETWORKING (IJCTISN)

eISSN: 3087-4297

Volume. 03, Issue. 04, pp. 10-21, April 2026

Cybersecurity Governance and Resilience in Small and Medium-Sized Enterprises: A Socio-Technical, Resource-Based, and Regulatory Framework for Sustainable Digital Competitiveness

Dr. Elena Marovic
Department of Information Systems, University of Ljubljana, Slovenia

Dr. Sofia Markovic
Faculty of Organizational Sciences, University of Belgrade, Serbia

Article received: 14/02/2026, Article Accepted: 10/03/2026, Article Published: 06/04/2026

© 2026 Authors retain the copyright of their manuscripts, and all Open Access articles are disseminated under the terms of the Creative Commons Attribution License 4.0 (CC-BY), which licenses unrestricted use, distribution, and reproduction in any medium, provided that the original work is appropriately cited.

ABSTRACT

Background: Small and medium-sized enterprises (SMEs) occupy a central role in employment generation, innovation, and economic dynamism, yet they remain disproportionately exposed to cyber risk because of constrained resources, limited formal governance, fragmented technical infrastructures, and rapidly evolving regulatory demands (World Bank, 2015; Gherghina et al., 2020; Heidt et al., 2019). The digitalization of SME operations, supply chain connectivity, cloud dependence, and growing exposure to disclosure and compliance pressures have transformed cybersecurity from a purely technical issue into a strategic, organizational, and relational concern (Proudfoot et al., 2024; Wallis & Dorey, 2024).

Objective: This article develops an integrated conceptual framework explaining how SMEs can build cybersecurity resilience through the interaction of internal capabilities, socio-technical alignment, relational governance, institutional legitimacy, and adaptive compliance under emerging regulatory regimes.
Methodology: A qualitative theory-building design was employed using integrative literature synthesis and conceptual analysis grounded in design-oriented reasoning. The study draws on the resource-based view, dynamic capabilities, socio-technical systems theory, relational governance, signaling theory, and institutional theory to interpret the cybersecurity challenges and strategic options facing SMEs (Barney, 1991; Teece et al., 1997; Bostrom & Heinen, 1977; Poppo & Zenger, 2002; Connelly et al., 2011; DiMaggio & Powell, 1983). The research logic follows a problem-centered, framework-development approach informed by action-oriented and design science perspectives (Castro et al., 2025).

Results: The analysis shows that SME cybersecurity resilience depends not merely on technology adoption but on the orchestration of managerial cognition, governance formalization, trust-based collaboration, risk disclosure, regulatory interpretation, secure data management, and continuous learning. The study identifies six interdependent pillars of resilience: strategic capability formation, socio-technical integration, adaptive governance, ecosystem trust, regulatory readiness, and intelligent security augmentation. It further demonstrates that compliance-driven security is insufficient unless translated into operational routines, organizational culture, and partner-level coordination.

Conclusion: Cybersecurity in SMEs should be understood as a dynamic organizational capability and a source of competitive legitimacy rather than as a narrow cost center. The article contributes a multi-theoretical framework and offers implications for SME leaders, policymakers, technology providers, and researchers concerned with digital resilience, responsible innovation, and long-term competitiveness.

Keywords: SMEs, cybersecurity resilience, socio-technical systems, dynamic capabilities, regulatory compliance, relational governance, digital competitiveness.

INTRODUCTION

Small and medium-sized enterprises occupy a decisive position in national and global economies because they generate employment, stimulate entrepreneurial dynamism, support regional development, and frequently serve as innovation intermediaries within larger production and service ecosystems (World Bank, 2015; Gherghina et al., 2020). Their significance, however, contrasts sharply with their persistent structural vulnerability. In the contemporary digital economy, SMEs are expected to participate in data-driven commerce, platform-mediated exchange, cloud-enabled coordination, digitally connected supply chains, and increasingly automated operational environments. This transformation expands opportunity, but it also widens the attack surface through which cyber threats can compromise continuity, trust, and strategic viability (Heidt et al., 2019; Hoong et al., 2024; Papathanasiou et al., 2025).

Cybersecurity has therefore emerged as an existential issue for SMEs, not merely because attacks are increasing in volume and sophistication, but because the consequences of disruption are proportionally more severe for firms with limited financial slack, less specialized staff, weaker redundancy, and fewer recovery pathways (Awan et al., 2025; Clark & Mujeye, 2025). The problem is not simply that SMEs lack advanced tools. More fundamentally, they often operate in environments characterized by fragmented decision-making, underdeveloped governance, incomplete risk visibility, inadequate vendor oversight, informal work practices, and ambiguous regulatory interpretation (Khan et al., 2025; El-Hajj & Mirza, 2024). The cybersecurity challenge in SMEs is therefore multidimensional: it is technical, organizational, institutional, relational, and strategic all at once.

This complexity requires moving beyond narrow depictions of cybersecurity as a matter of antivirus software, access controls, or incident response checklists. The literature increasingly indicates that cybersecurity performance depends on the alignment of human behavior, organizational routines, governance structures, external relationships, and technological resources (Bostrom & Heinen, 1977; Trist, 1981; Yeoh & Popovič, 2022). SMEs often struggle precisely because these elements evolve unevenly. A company may adopt cloud tools without revising internal controls; it may purchase security products without cultivating employee awareness; it may respond to customer security demands without embedding strategic risk management. Such misalignments help explain why technical investments often fail to translate into resilience.

At the same time, broader institutional and regulatory changes are intensifying the cybersecurity burden placed on smaller firms. New compliance expectations, including information security management standards and evolving legislative frameworks such as the NIS2 Directive and the Cyber Resilience Act, create pressure for more formalized governance, traceable accountability, and documented control practices (ISO/IEC, 2022; Shaffique, 2024; Joswig & Kurz, 2025; Kianpour et al., 2025). While such developments can strengthen the overall security ecosystem, they also risk widening the divide between firms capable of absorbing compliance complexity and those that remain under-resourced. The security divide between SMEs and larger firms has already been documented as a persistent pattern, reflecting differences in budget, expertise, strategic prioritization, and access to advanced solutions (Heidt et al., 2019). Regulatory expansion can mitigate insecurity, but it can also deepen asymmetry if not accompanied by supportive governance models and scalable implementation pathways.

Another important development is the growing visibility of cybersecurity as a signaling mechanism in markets and stakeholder relationships. Research on cybersecurity disclosure suggests that visible commitments to security affect stakeholder intentions and organizational outcomes, especially in environments where trust, legitimacy, and perceived preparedness shape economic exchange (Bansal & Axelton, 2024; Elsayed et al., 2024). For SMEs, this insight is profound. A mature cybersecurity posture can function not only as an internal defense system but also as an external signal of reliability, contractual competence, and ecosystem fitness. In digitally interconnected markets, suppliers, customers, regulators, financiers, and partners increasingly infer organizational quality from security practices. Cybersecurity thus moves from the margins of IT management into the domain of reputation, legitimacy, and competitive advantage.

Theoretical perspectives from strategic management and information systems research provide valuable foundations for understanding this shift. The resource-based view argues that firm performance depends on valuable, rare, inimitable, and organizationally embedded resources (Barney, 1991; Wade & Hulland, 2004). In the context of cybersecurity, this implies that resilience is not reducible to commodity technology; it depends on firm-specific capability combinations such as managerial awareness, process discipline, data governance, partner coordination, and secure operational routines (Bharadwaj, 2000; Melville et al., 2004). Dynamic capabilities extend this insight by emphasizing the firm's ability to sense threats and opportunities, seize appropriate responses, and reconfigure resources in volatile environments (Teece et al., 1997; Pavlou & El Sawy, 2011). Since cyber risk changes rapidly, SMEs require precisely this adaptive capacity rather than static compliance alone.

Yet strategic capability alone cannot fully explain SME cybersecurity outcomes. Socio-technical systems theory is equally essential because cyber incidents often arise from misfit among technologies, workflows, and human practices (Bostrom & Heinen, 1977; Trist, 1981). SMEs commonly depend on informal communication, generalized employee roles, flexible task boundaries, and improvised technology adoption. These characteristics may enhance agility, but they can also produce insecure practices when security responsibilities are unclear or when digital tools are layered onto unstructured routines. Cybersecurity failure in this sense is not merely a technical failure. It is often a systems design failure in which organizational structure and technical infrastructure evolve without mutual adjustment.

External relationships also matter significantly. SMEs rarely operate as isolated entities. They are embedded in supply chains, vendor ecosystems, outsourcing arrangements, collaborative partnerships, and sectoral networks. Relational governance research demonstrates that trust, contractual design, and partner coordination influence performance and risk management outcomes (Zaheer & Venkatraman, 1995; Zaheer et al., 1998; Poppo & Zenger, 2002; Claro et al., 2003; Kumar, 2022). In cybersecurity terms, this means that a firm's risk exposure is partly constituted by the governance quality of its interorganizational relationships. Service level agreements, vendor transparency, data handling terms, incident notification obligations, and collaborative security expectations are not peripheral legal details; they are core determinants of resilience (Nugraha & Martin, 2022; Wallis & Dorey, 2024).

Institutional and legitimacy perspectives add another layer. Organizations respond not only to direct technical threats but also to normative, coercive, and mimetic pressures arising from regulators, industry expectations, peer behavior, and public scrutiny (DiMaggio & Powell, 1983; Suchman, 1995). SMEs may adopt cybersecurity practices because customers demand certification, because insurers require controls, because regulators impose accountability, or because peer firms set new norms. These pressures influence both the pace and form of security adoption. However, not all adoption is substantive. Some organizations may pursue symbolic compliance, producing documentation without operational integration. The distinction between legitimacy-seeking behavior and capability-building behavior is therefore central to cybersecurity analysis.

Recent technological developments further complicate the SME security landscape. Artificial intelligence, machine learning, blockchain-based identity management, secure data risk management systems, quantum-safe technologies, tactical communication innovations, and software-defined networking architectures are reshaping the possibilities of digital security governance (Alanzi & Alkhatib, 2025; Fernandez de Arroyabe et al., 2024; Garcia Cid et al., 2022; He et al., 2025; Monzon Baeza et al., 2025; Hepworth et al., 2025). While many of these technologies appear promising, their relevance for SMEs depends on accessibility, explainability, governance compatibility, and the capacity of firms to translate advanced tools into usable practices. For smaller firms, the challenge is rarely technological possibility alone. The challenge is whether emerging solutions can be operationalized without generating excessive complexity, dependency, or false confidence.

The literature contains valuable insights into individual dimensions of this problem, including barriers to adoption, manager perceptions, disclosure effects, resilience frameworks, and regulatory trends (Hoong et al., 2024; Khan et al., 2025; Proudfoot et al., 2024; Wilson, 2025). However, a major gap remains. Existing studies often treat SME cybersecurity through fragmented lenses: technical controls, behavioral awareness, regulatory compliance, or strategic value. Fewer studies integrate these dimensions into a single explanatory framework that captures how internal capabilities, socio-technical alignment, partner governance, legitimacy pressures, and adaptive regulation interact. As a result, scholars and practitioners are left with piecemeal prescriptions rather than a coherent model of sustainable cybersecurity resilience.

This article addresses that gap by developing a multi-theoretical framework for understanding and strengthening cybersecurity governance in SMEs. Drawing on the resource-based view, dynamic capabilities, socio-technical systems theory, relational governance, signaling theory, and institutional theory, it explains why some SMEs remain trapped in reactive and fragile security postures while others progressively transform cybersecurity into a strategic and legitimizing capability. The article argues that resilience emerges from the coordinated development of six interdependent pillars: strategic capability formation, socio-technical integration, adaptive governance, ecosystem trust, regulatory readiness, and intelligent security augmentation. These pillars do not represent sequential stages in a simple maturity model; rather, they constitute a mutually reinforcing architecture through which cybersecurity becomes sustainable.

The significance of this argument is both theoretical and practical. Theoretically, it expands the study of SME cybersecurity beyond compliance or technical defense by positioning security as a dynamic organizational capability embedded in broader institutional and relational contexts. Practically, it helps SME leaders and policymakers understand why isolated investments often underperform and why resilience requires deeper alignment among people, processes, technology, and external expectations. In a business environment marked by digital dependence, regulatory intensification, and

ecosystem interconnectivity, SMEs can no longer treat cybersecurity as secondary infrastructure. It is increasingly a condition of survival, trustworthiness, and competitive participation.

Methodology

This study employs a qualitative, theory-building methodology designed to produce an integrative and publication-ready conceptual article grounded strictly in the provided scholarly references. The objective is not to test a single hypothesis through statistical estimation, nor to report primary fieldwork, but to synthesize the literature in a way that explains the mechanisms through which SMEs build or fail to build cybersecurity resilience. This methodological choice is appropriate because the reference base spans multiple theoretical traditions and applied domains, including information systems, strategic management, organizational theory, regulation, cybersecurity governance, supply chain relations, secure architectures, and digital innovation. A purely descriptive review would not sufficiently capture the interdependencies among these literatures. Instead, a conceptual synthesis approach is required to develop explanatory integration.

The methodological logic of this article is informed by theory elaboration and framework construction. Theory elaboration extends prior theoretical insights to a new or under-integrated domain by clarifying mechanisms, resolving tensions, and specifying how multiple constructs interact. In this article, theories such as the resource-based view, dynamic capabilities, socio-technical systems, signaling theory, relational governance, and institutional theory are not treated as isolated explanatory silos. They are used as complementary lenses that illuminate different dimensions of SME cybersecurity. The research process therefore involved identifying the analytical strengths of each theoretical tradition and then mapping them onto recurrent themes in the cybersecurity literature related to SMEs.

The design is also aligned with design-oriented and action-sensitive scholarship. Castro et al. (2025) demonstrate the value of combining action research and design science for complex organizational problems, particularly when knowledge development is meant to generate practical and theoretically informed interventions. Although the present article does not report an empirical design science artifact, it adopts a similar intellectual orientation: the aim is to produce a framework that is both analytically rigorous and practically actionable. Cybersecurity challenges in SMEs are not only matters to be interpreted; they are matters to be addressed through better governance, capability development, and implementation logic. The article therefore follows a constructive conceptual method in which literature is used not merely to summarize current knowledge but to build a structured model capable of guiding future research and managerial reasoning.

The source base consists exclusively of the references provided in the prompt. These references were analyzed through iterative thematic clustering. In the first stage, the studies were grouped into major domains: SME economic significance and structural constraints; cybersecurity barriers and maturity; socio-technical and organizational capability perspectives; governance and interorganizational trust; regulation and legitimacy; disclosure and signaling; and emerging technologies such as blockchain, machine learning, quantum-safe approaches, and software-defined architectures. This clustering allowed the literature to be read not as a flat list of independent studies but as a set of interacting conversations.

In the second stage, cross-cutting constructs were identified. These constructs included capability, resilience, trust, legitimacy, governance, adaptation, disclosure, compliance, explainability, and digital sovereignty. The purpose of this step was to distinguish between surface-level topics and deeper explanatory elements. For example, a study on cybersecurity disclosure and a study on regulatory adaptation may initially appear separate, yet both can be connected through signaling and legitimacy dynamics. Likewise, a study on machine learning for resilience and one on security maturity assessment can both be linked through adaptive capability formation. This stage enabled conceptual integration across heterogeneous source types.

In the third stage, the article employed abductive reasoning to develop a higher-order framework. Abduction, in this context, refers to the process of moving iteratively between theory and observed patterns in the literature to generate the most plausible explanatory structure. The central question guiding this process was: what combination of organizational, relational, institutional, and technological conditions best explains durable cybersecurity resilience in SMEs? The result was the identification of six interdependent pillars that recur implicitly or explicitly across the source literature: strategic capability formation, socio-technical integration, adaptive governance, ecosystem trust, regulatory readiness, and intelligent security augmentation.

The first pillar, strategic capability formation, emerged from resource-based and dynamic capability studies showing that organizational performance depends on configured and adaptive resources rather than isolated assets (Barney, 1991; Bharadwaj, 2000; Wade & Hulland, 2004; Teece et al., 1997; Pavlou & El Sawy, 2011). The second pillar, socio-technical integration, was derived from classic and contemporary work emphasizing that system outcomes depend on the

alignment of human and technical subsystems (Bostrom & Heinen, 1977; Trist, 1981). The third pillar, adaptive governance, was grounded in literature on contracts, maturity frameworks, service level agreements, and organizational responses to security demands (Poppo & Zenger, 2002; Nugraha & Martin, 2022; Ozkan & Spruit, 2022). The fourth pillar, ecosystem trust, arose from work on relational governance, buyer-supplier performance, third-party coordination, and supply chain cybersecurity (Zaheer & Venkatraman, 1995; Zaheer et al., 1998; Claro et al., 2003; Bai et al., 2020; Wallis & Dorey, 2024). The fifth pillar, regulatory readiness, was informed by standardization, cybersecurity regulation, NIS2, digital sovereignty, and the Cyber Resilience Act (ISO/IEC, 2022; Proudfoot et al., 2024; Shaffique, 2024; Joswig & Kurz, 2025; Kianpour et al., 2025). The sixth pillar, intelligent security augmentation, emerged from research on explainable AI, machine learning resilience, blockchain identity management, secure data risk management, and quantum-safe technology (Zacharias et al., 2022; Fernandez de Arroyabe et al., 2024; Alanzi & Alkhatib, 2025; He et al., 2025; Garcia Cid et al., 2022).

The methodology is interpretive in that it treats the literature as a source of meaning, mechanism, and conceptual relationship rather than as a pool of effect sizes to be aggregated. This is important because the phenomenon under examination is not reducible to one measurable variable. Cybersecurity resilience in SMEs depends on formal structures and informal practices, regulatory texts and managerial cognition, contracts and trust, technical tools and workforce routines. Such multidimensionality makes interpretive conceptual analysis especially appropriate.

At the same time, the methodology is disciplined by explicit theoretical anchoring. Each major interpretive claim in the article is grounded in cited literature. The intent is not to speculate beyond the references, but to build a logically coherent synthesis from them. Major claims are therefore supported through consistent author-year citation, especially when discussing organizational vulnerabilities, governance forms, institutional pressures, and technology adoption patterns. This citation discipline also serves an important quality function: it prevents conceptual inflation by ensuring that every theoretical extension remains linked to the source base.

The results and discussion sections that follow should therefore be read as the output of a structured conceptual inquiry rather than as a narrative literature review in the conventional sense. The framework developed here is not a neutral summary of prior studies. It is an analytical model derived from them. Its value lies in its ability to explain why SMEs often experience cybersecurity as a recurring struggle despite awareness of risk, and what conditions allow that struggle to be transformed into sustained resilience and strategic advantage.

A limitation of this methodology must be acknowledged. Because the article is conceptual and based exclusively on the supplied references, it does not provide new empirical measurements or sector-specific case evidence. It therefore cannot claim direct causal verification in the statistical sense. However, conceptual integration is not a weaker form of scholarship when the field itself is fragmented. On the contrary, where knowledge is dispersed across technical, managerial, and regulatory subfields, rigorous synthesis is a necessary precondition for future empirical testing. The framework proposed here is thus intended to generate research propositions, implementation principles, and policy insights that can be examined in later studies.

Results

The analysis of the literature reveals that cybersecurity resilience in SMEs cannot be adequately explained by technical preparedness alone. Instead, resilience emerges as a compound organizational outcome shaped by strategic resources, managerial interpretation, socio-technical alignment, partner relationships, regulatory positioning, and the selective adoption of advanced security technologies. The results of this conceptual investigation are organized around six interdependent pillars that together explain how SMEs can move from fragile security postures toward durable cyber resilience.

The first result is that cybersecurity in SMEs is fundamentally a capability problem rather than a narrow procurement problem. The resource-based view suggests that firms derive sustained advantage from resources and capabilities that are valuable, difficult to imitate, and effectively organized (Barney, 1991). Information systems research extends this principle by showing that IT-related performance depends not simply on the possession of technology but on embedded capabilities such as managerial know-how, process integration, and organizational deployment (Bharadwaj, 2000; Melville et al., 2004; Wade & Hulland, 2004). Applied to cybersecurity, the implication is clear: buying tools does not automatically produce resilience. SMEs frequently adopt software, outsourced services, or compliance templates, yet remain vulnerable because the resources they acquire are not translated into firm-specific routines. Security capability exists when firms can interpret threats, prioritize actions, allocate responsibilities, and continuously adapt controls to changing conditions. This is consistent with the dynamic capability literature, which emphasizes the ability to sense environmental shifts, seize relevant opportunities or defensive actions, and reconfigure internal arrangements as conditions evolve (Teece et al., 1997; Pavlou & El Sawy, 2011).

A second result is that the internal weakness of many SMEs stems from socio-technical fragmentation. Classic socio-technical theory argues that organizational effectiveness depends on the joint optimization of social

and technical systems rather than the dominance of one over the other (Bostrom & Heinen, 1977; Trist, 1981). The cybersecurity literature on SMEs strongly reflects this logic even when not explicitly framed in those terms. Managerial awareness gaps, informal password practices, limited role segregation, insufficient training, and weak process documentation all reveal misalignment between technological systems and human work practices (Hoong et al., 2024; Wilson, 2025; Papathanasiou et al., 2025). Security breakdowns often occur not because SMEs completely ignore risk, but because the technical controls they adopt do not match the realities of everyday work. Employees may use unauthorized applications to maintain speed, managers may override controls to preserve client responsiveness, and shared devices or accounts may persist because staffing structures are lean. The result is a persistent gap between formal security intention and operational behavior. The literature therefore supports the conclusion that socio-technical integration is an independent pillar of resilience. Without it, even technically adequate controls remain brittle.

A third result concerns the significance of adaptive governance. Governance in this context refers to the set of rules, responsibilities, monitoring arrangements, escalation pathways, and decision structures through which cybersecurity is managed. Governance is often weak in SMEs because hierarchy is compressed, roles overlap, and formal policy development is deprioritized in favor of immediate business demands (Clark & Mujeye, 2025; Khan et al., 2025). Yet the literature shows that adaptable governance mechanisms are essential. Security maturity assessment models highlight the value of staged, context-sensitive progress rather than unrealistic one-size-fits-all controls (Ozkan & Spruit, 2022). Cybersecurity frameworks tailored for SMEs emphasize practical governance routines such as asset identification, incident planning, prioritization logic, and accountability allocation (Le et al., 2025; El-Hajj & Mirza, 2024). Service level agreement research similarly indicates that governance arrangements with providers materially influence protection quality, incident response, and accountability clarity (Nugraha & Martin, 2022). These findings suggest that cybersecurity governance must be adaptable, scalable, and embedded in business routines. The most resilient SMEs are not those with the thickest policy manuals, but those with governance arrangements proportionate to their structure and capable of iterative improvement.

A fourth result is that ecosystem trust and relational governance significantly shape SME security outcomes. Interorganizational research demonstrates that performance and coordination are shaped by the interplay of contracts, trust, and partner relationships (Zaheer & Venkatraman, 1995; Zaheer et al., 1998; Poppo & Zenger, 2002; Claro et al., 2003). In cybersecurity, this becomes especially salient because SMEs are often dependent on managed service providers, cloud vendors, logistics platforms, payment gateways, and digitally integrated suppliers or buyers. The supply chain cybersecurity literature emphasizes that cyber risk is relationally distributed; vulnerabilities travel across organizational boundaries (Wallis & Dorey, 2024). Research on buyer-supplier sustainability and collaborative innovation further reinforces the importance of governance quality in interfirm coordination (Kumar, 2022; Bai et al., 2020). The result emerging from the literature is that SMEs cannot secure themselves in isolation. Trust matters, but trust without contractual clarity is insufficient. Conversely, contracts without relational commitment may produce minimal compliance without real transparency. Effective cybersecurity in SME ecosystems requires balanced relational governance combining trust, monitoring, service expectations, and information-sharing norms.

A fifth result is that institutional and regulatory pressure has become a defining driver of SME cybersecurity transformation. Institutional theory explains that organizations adopt structures and practices under coercive, normative, and mimetic pressures (DiMaggio & Powell, 1983). Cybersecurity regulations, industry standards, insurer expectations, and customer demands increasingly constitute these pressures. ISO/IEC 27001 provides a recognized model for information security management systems, and its significance extends beyond compliance by shaping organizational language, role definition, auditability, and control standardization (ISO/IEC, 2022). New regulatory developments such as the NIS2 Directive and the Cyber Resilience Act intensify the expectation that firms, including smaller firms embedded in critical or digitally connected sectors, will adopt more systematic risk management and accountability practices (Shaffique, 2024; Joswig & Kurz, 2025; Kianpour et al., 2025). Research on cybersecurity regulations and organizational response indicates that formal rules do not operate in a vacuum; they reshape governance priorities, disclosure behavior, and managerial attention (Proudfoot et al., 2024; Kianpour & Raza, 2024). The result here is that regulatory readiness has become inseparable from cybersecurity resilience. SMEs that treat regulation as a one-time burden are likely to lag behind those that interpret compliance as a catalyst for capability development.

A sixth result is that cybersecurity disclosure functions as a strategic signal. Signaling theory holds that in contexts of information asymmetry, organizations send observable cues that stakeholders use to infer quality, reliability, and trustworthiness (Spence, 1973; Connelly et al., 2011). Studies on cybersecurity disclosure show that communicated security commitments affect stakeholder intentions and organizational performance perceptions (Bansal & Axelton, 2024; Elsayed et al., 2024). For SMEs, this means that cybersecurity can no longer remain entirely invisible. Clients, investors,

supply chain partners, and regulators increasingly evaluate whether a firm is security-conscious, not just whether it has avoided a breach. Cybersecurity disclosures, certifications, policy statements, incident communication practices, and visible governance structures all contribute to legitimacy formation (Suchman, 1995). The result is that cybersecurity operates simultaneously as defense and as signal. This dual role is particularly important for SMEs seeking to overcome liability of smallness in markets where trust deficits and perceived fragility can otherwise limit opportunity.

A seventh result concerns the importance of managerial cognition and organizational interpretation. Multiple studies emphasize that SME managers face cybersecurity not simply as a technical topic but as a practical leadership challenge constrained by uncertainty, competing priorities, and limited expertise (Hoong et al., 2024; Wilson, 2025). Barriers to adoption are therefore not reducible to financial shortage, although resource scarcity is significant (Khan et al., 2025). Equally important are managerial frames regarding what cybersecurity means, how urgent it is, whether it is strategic or merely technical, and who should own it. If managers interpret security only as an IT maintenance issue, it will rarely receive cross-functional attention. If they interpret it as a business continuity, trust, and competitiveness issue, then governance and investment decisions are more likely to reflect strategic seriousness. The literature thus indicates that resilience begins with interpretive capacity at the leadership level.

An eighth result is that advanced technologies can strengthen SME cybersecurity, but only when governance and explainability conditions are met. Machine learning-based approaches can improve resilience by helping firms assess risk patterns, identify anomalies, and prioritize interventions (Fernandez de Arroyabe et al., 2024). Explainable AI research is particularly relevant because SMEs often lack the institutional capacity to rely on opaque systems without interpretive support (Zacharias et al., 2022). Similarly, blockchain-based identity systems and secure data risk management methods offer promising mechanisms for privacy protection, integrity assurance, and distributed trust (Alanzi & Alkhatib, 2025; He et al., 2025). Quantum-safe technologies highlight the future-facing dimension of security strategy, especially for firms that manage sensitive or long-lived data assets (Garcia Cid et al., 2022). However, the literature does not support simplistic technological solutionism. Advanced tools generate value only when they are understandable, governable, proportionate, and integrated into broader routines. Intelligent augmentation strengthens resilience when it complements managerial judgment and organizational process rather than displacing them.

A ninth result is that digital sovereignty and autonomy are becoming increasingly relevant for SMEs. Research on digital sovereignty and NIS2 suggests that control over digital infrastructure, data flows, dependencies, and compliance obligations has strategic implications for organizations embedded in broader digital ecosystems (Kianpour et al., 2025). Tactical communication research, software-defined networking, and AI integration studies further underscore the trend toward more configurable, distributed, and intelligent digital environments (Baeza & Salor, 2024; Hepworth et al., 2025; Monzon Baeza et al., 2025). For SMEs, sovereignty should not be understood in a geopolitical sense alone. At the firm level, it refers to the extent to which organizations understand and govern their dependencies. A firm that relies heavily on opaque vendors, poorly negotiated service arrangements, or uncontrolled data architectures lacks practical sovereignty and is therefore more fragile. The literature suggests that resilience increasingly requires not just protection from attack, but informed control over technological dependence.

A tenth result is that the cybersecurity maturity gap between SMEs and larger enterprises is not merely quantitative but structural. Large firms possess more capital, specialized teams, audit infrastructures, and bargaining power with vendors. SMEs face not only fewer resources, but also different organizational conditions, including informality, role overlap, and narrower recovery margins (Heidt et al., 2019; Awan et al., 2025). Therefore, resilience strategies copied from large enterprises may fail when transplanted directly into smaller contexts. The literature strongly implies that SME security must be designed around proportionality, prioritization, and usability. What matters is not perfect symmetry with large-enterprise practice, but the development of fit-for-purpose resilience architectures aligned with SME realities.

Taken together, these results support the overarching conclusion that SME cybersecurity resilience depends on the orchestration of six pillars: strategic capability formation, socio-technical integration, adaptive governance, ecosystem trust, regulatory readiness, and intelligent security augmentation. These pillars interact dynamically. Strong governance without socio-technical integration becomes formalistic. Advanced technologies without managerial interpretation become opaque. Compliance without trust and partner coordination becomes brittle. Disclosure without substantive capability becomes symbolic. Resilience emerges only when these elements reinforce one another.

Discussion

The findings of this article suggest that the dominant ways in which cybersecurity is framed in many SME contexts are too narrow to produce sustainable resilience. A recurring misconception is that cybersecurity is

primarily a matter of defensive technology deployment. This framing is attractive because it simplifies a complex problem into a purchasable solution. Yet the literature synthesized here consistently indicates that SMEs experience cyber vulnerability because their risk exposure is organizationally and relationally constituted. In other words, cybersecurity failures are often rooted in the ways firms govern, coordinate, interpret, and embed digital practices rather than in the absence of any single tool. This section interprets the results through deeper theoretical reflection and explores their broader implications.

A central interpretive insight is that cybersecurity should be conceptualized as a dynamic organizational capability. The resource-based view and dynamic capability traditions together imply that what matters is not simply the stock of technological assets but the capacity to mobilize them under changing conditions (Barney, 1991; Teece et al., 1997; Pavlou & El Sawy, 2011). SMEs often struggle because they acquire fragmented resources without developing the routines required to convert those resources into resilience. A security awareness subscription, a cloud backup service, or an outsourced monitoring package can all be useful. However, none of these will protect the firm if leadership attention is inconsistent, if responsibilities are undefined, if third-party risks are not governed, or if employees routinely work around controls. The discussion therefore points toward a shift in managerial mindset: cybersecurity is not a one-time acquisition but a capability that must be learned, rehearsed, and adapted.

This insight also helps resolve an apparent tension in the literature between resource scarcity and strategic agency. It is certainly true that SMEs face resource constraints and are disadvantaged relative to larger firms (Heidt et al., 2019). However, the presence of constraints does not mean that SMEs are passive victims of structural disadvantage. Dynamic capability theory suggests that firms can compensate partially for resource scarcity through superior sensing, prioritization, and reconfiguration (Teece et al., 1997). In cybersecurity terms, this means that SMEs need not attempt to imitate the breadth of large-enterprise control systems. Instead, they can pursue strategic concentration: identify core assets, critical dependencies, plausible threat scenarios, and essential governance routines. Such prioritization aligns with context-sensitive maturity models and proportional frameworks that are more suitable for SMEs than maximalist compliance approaches (Ozkan & Spruit, 2022; Le et al., 2025).

The socio-technical dimension of the findings is equally consequential. One reason cybersecurity programs underperform is that organizations often assume that secure behavior will naturally follow from policy or software implementation. Socio-technical theory challenges this assumption by emphasizing that technical systems interact with human roles, norms, and incentives (Bostrom & Heinen, 1977; Trist, 1981). In SMEs, work is often characterized by flexibility, informality, and speed. These qualities are not inherently negative; in fact, they may underpin entrepreneurial responsiveness. The problem arises when security design ignores them. For instance, if a security control materially slows client service and no alternative process is designed, employees may bypass it. If incident reporting is framed as blame rather than learning, emerging issues may be concealed. If authentication rules are imposed without regard to mobile or remote work patterns, shadow practices may proliferate. The broader implication is that resilience requires human-centered security design. SMEs should build controls that employees can realistically follow, understand, and internalize.

This perspective challenges conventional compliance thinking. Formal regulations and standards are important, but they do not guarantee effective practice. Institutional theory helps explain why. Organizations often adopt structures in response to coercive or normative pressure, but such adoption can be ceremonial if not tied to substantive operational change (DiMaggio & Powell, 1983; Suchman, 1995). The contemporary expansion of cybersecurity regulation creates both opportunity and risk for SMEs. On the positive side, regulation can elevate attention, clarify expectations, and reduce ambiguity. It can also create a common language that helps smaller firms negotiate with partners and service providers. On the negative side, regulation can encourage symbolic conformity, especially when firms lack the capacity to translate formal requirements into operational discipline. This suggests that policymakers and auditors should be cautious about equating documented compliance with actual resilience. For SMEs, the most effective regulatory support is likely to involve scalable guidance, implementation pathways, and sector-sensitive benchmarks rather than uniform burden transfer.

The discussion also reveals a critical distinction between compliance orientation and resilience orientation. Compliance orientation is externally anchored: the firm asks what controls must be documented, what obligations must be met, and what evidence must be produced. Resilience orientation is internally and relationally anchored: the firm asks what must function under stress, which relationships matter most, where dependencies are concentrated, and how adaptation will occur when a threat materializes. The two orientations are not mutually exclusive, but they are not identical. The literature reviewed here implies that SMEs that pursue resilience only through compliance are likely to remain vulnerable because compliance tends to privilege minimum thresholds and static representations. By contrast, resilience requires anticipation, learning, and cross-boundary coordination.

Relational governance emerges from the findings as one

of the most underappreciated dimensions of SME cybersecurity. Smaller firms are often advised to strengthen internal controls, yet many of their most significant exposures originate externally through vendors, customers, software providers, and integrated platforms (Wallis & Dorey, 2024). Trust research shows that trust can reduce coordination costs and enable collaboration, but trust must be complemented by reliable governance mechanisms (Zaheer et al., 1998; Poppo & Zenger, 2002). In cybersecurity, this means that SMEs should avoid both extremes: naïve trust in vendors and purely transactional relationships with no information-sharing culture. Effective relational governance includes clear service expectations, incident notification clauses, data handling provisions, role clarity, escalation routes, and a willingness among partners to communicate emerging issues. This is especially important because SMEs often have lower bargaining power and may accept opaque vendor arrangements that leave them exposed. Building resilience therefore involves not only securing systems but also negotiating and managing dependencies more intelligently.

Signaling theory adds another layer to this interpretation. In digitally mediated markets, stakeholders frequently cannot directly observe the true quality of a firm's internal cybersecurity capability. They instead rely on signals such as certifications, disclosures, governance structures, breach communication quality, and evidence of disciplined risk management (Spence, 1973; Connelly et al., 2011). This has two major implications for SMEs. First, cybersecurity investments can generate external value by enhancing perceived reliability, especially in business-to-business relationships where supplier trust is critical. Second, signals must be credible. If disclosure outpaces substance, then reputational risk may increase rather than decrease. The growing research on cybersecurity disclosure suggests that stakeholders do respond to visible security commitments (Bansal & Axelton, 2024; Elsayed et al., 2024). However, the durability of those responses depends on underlying capability. Thus, the optimal strategy for SMEs is not performative signaling, but credible signaling grounded in real governance.

The role of advanced technologies requires careful and balanced interpretation. There is understandable enthusiasm around machine learning, blockchain-based identity management, explainable AI, secure data risk management, and quantum-safe technologies (Alanzi & Alkhatib, 2025; Fernandez de Arroyabe et al., 2024; Garcia Cid et al., 2022; He et al., 2025; Zacharias et al., 2022). These tools can enhance detection, prediction, data integrity, and future-proofing. Yet the SME context calls for prudence. Sophisticated technologies can introduce new dependencies, costs, interpretive burdens, and governance challenges. Explainability is especially important because smaller firms may not have internal specialists capable of validating complex outputs. A machine learning system that identifies risk but cannot explain why may be underused or misused. A blockchain identity system may improve integrity but be operationally excessive if the surrounding governance is weak. The lesson is not that SMEs should avoid advanced technologies, but that technological sophistication should follow governance readiness rather than substitute for it.

The concept of digital sovereignty deepens this conversation. Increasingly, resilience depends on whether firms understand where their data resides, who controls critical services, how contractual obligations are distributed, and what happens when external providers fail or become compromised (Kianpour et al., 2025). SMEs are often digitally dependent but strategically underinformed. They may rely on cloud ecosystems, software-as-a-service platforms, integrated payment tools, or outsourced IT providers without full visibility into risk transfer, jurisdictional exposure, or exit constraints. This condition creates a sovereignty deficit at the firm level. Digital sovereignty for SMEs should therefore be interpreted as informed dependence rather than total independence. Smaller firms cannot internalize every capability, but they can seek greater transparency, contractual clarity, and fallback readiness. In this sense, sovereignty is a resilience principle, not a political slogan.

The article's integrated framework also has implications for future research. First, scholars should move beyond binary distinctions such as compliant versus non-compliant, or protected versus unprotected. Cybersecurity resilience in SMEs is better understood as a configuration problem. Different combinations of managerial attention, governance structures, partner trust, and technological augmentation may produce different resilience pathways. Second, empirical research should investigate how the six proposed pillars interact over time. Longitudinal and comparative studies would be especially valuable in determining whether certain pillars serve as prerequisites for others or whether multiple sequences are viable. Third, sectoral variation deserves attention. SMEs in finance-adjacent services, manufacturing supply chains, health-related services, or digitally intensive retail may experience distinct combinations of regulatory pressure and ecosystem risk. Fourth, future work should examine the micro-foundations of leadership interpretation. The way SME owners and managers understand cybersecurity may be decisive in shaping investment and governance trajectories.

The article also points to several managerial implications. SME leaders should begin by reframing cybersecurity as a business resilience and trust issue rather than as a technical overhead. They should identify their most critical digital assets, business dependencies, and plausible disruption scenarios. Governance should be made explicit even when organizational size is small.

Someone must own risk review, someone must coordinate incidents, and partner contracts must specify security expectations. Employee practices should be analyzed not only for compliance but for usability and workflow fit. Where advanced technologies are adopted, explainability and accountability should guide selection. Finally, visible but credible signaling should be cultivated through meaningful disclosures, standard adoption where appropriate, and responsible communication.

Policy implications are equally important. Governments and regulators frequently recognize the importance of SMEs but underestimate the implementation challenge they face. If regulatory expansion is not accompanied by tailored support, toolkits, sector guidance, and proportionate assessment models, many SMEs may respond with superficial compliance or defensive disengagement. A more effective policy approach would treat SME cybersecurity as an ecosystem issue requiring cooperative capability building. Industry associations, insurers, standard bodies, service providers, and public agencies all have roles to play in translating abstract requirements into workable practices.

This study has limitations. It is conceptual and literature-based, which means that it does not empirically test the proposed framework across sectors or regions. It also relies exclusively on the provided references, which, while substantial and contemporary, cannot exhaust every strand of the cybersecurity and organizational resilience literature. Nonetheless, the contribution of the article lies in its integrative power. Fragmented problems require synthetic theory. By bringing together strategic management, information systems, organizational theory, governance research, and emerging technology scholarship, the article offers a coherent way to think about SME cybersecurity that is broader than most technical or regulatory treatments alone.

Ultimately, the discussion leads to a simple but consequential conclusion: SMEs do not become cyber resilient by accumulating controls. They become resilient by developing the organizational ability to align technology, people, governance, relationships, and external expectations under conditions of uncertainty. That ability can be cultivated. It requires strategic focus, relational intelligence, institutional awareness, and design discipline. Cybersecurity, in this sense, is no longer peripheral to SME competitiveness. It is one of its defining conditions.

Conclusion

This article developed an integrated conceptual framework for understanding cybersecurity resilience in SMEs by synthesizing insights from strategic management, information systems, socio-technical theory, relational governance, signaling theory, and institutional analysis. The central argument advanced throughout the article is that cybersecurity in SMEs must be understood as a dynamic, organizationally embedded, and externally conditioned capability rather than as a standalone technical function. Such a reframing is necessary because the challenges facing SMEs are not limited to the absence of tools. They arise from the intersection of limited resources, informal organizational structures, expanding digital dependence, regulatory intensification, partner-level exposure, and the uneven integration of technology into daily work.

The analysis identified six interdependent pillars of cybersecurity resilience: strategic capability formation, socio-technical integration, adaptive governance, ecosystem trust, regulatory readiness, and intelligent security augmentation. Together, these pillars explain why some SMEs remain in reactive, fragmented, and vulnerable security postures while others progressively construct more resilient and credible digital operating models. The article showed that strategic resources matter, but only when transformed into routines and managerial attention. Human and technical systems must be aligned to avoid the common pattern of control failure through workarounds and informal deviations. Governance must be practical, proportionate, and iterative. Trust in partners must be balanced with contractual clarity and accountability. Regulatory pressure must be translated into substantive capability rather than symbolic compliance. Advanced technologies such as machine learning, blockchain-based identity systems, and quantum-safe approaches can be beneficial, but their value depends on explainability, governance fit, and organizational readiness.

A major contribution of the article is its insistence that cybersecurity is also a matter of legitimacy and signaling. In increasingly digital markets, stakeholders interpret visible security practices as indicators of reliability, professionalism, and long-term viability. SMEs therefore have strong incentives to treat cybersecurity not merely as a defensive necessity but as a source of trust and competitive positioning. This insight is especially relevant in supply-chain-driven and digitally mediated environments where organizational reputation depends partly on perceived security maturity.

The article also clarifies that there is no universal blueprint for SME cybersecurity. Smaller firms should not attempt to replicate large-enterprise security architectures in a simplistic manner. Instead, they require proportionate, strategically prioritized, and context-sensitive resilience models. What matters is not maximal complexity, but coherent alignment among assets, workflows, responsibilities, dependencies, and regulatory demands. The most sustainable path forward lies in capability building, not control accumulation for its own sake.

For researchers, the article offers a framework that can guide future empirical inquiry into configurations of resilience, sectoral variation, leadership interpretation, and the practical impact of regulation on SME security trajectories. For practitioners, it provides a structured way to think about cybersecurity as an integrated business concern. For policymakers, it reinforces the need for scalable and implementation-sensitive approaches to supporting SMEs under new regulatory environments.

In conclusion, cybersecurity resilience in SMEs is best understood as a strategic and socio-technical achievement shaped by internal capability, external governance, and adaptive learning. SMEs that cultivate these qualities are more likely not only to defend against cyber threats but also to sustain trust, legitimacy, and competitiveness in an increasingly uncertain digital economy.

References

1. Ahmed, S. D., Al-Ismail, F. S. M., Shafiullah, M., AL-Sulaiman, F. A., & El-Amin, I. M. (2020). Grid integration challenges of wind energy: A review. IEEE Access, 8, 10857–10878. https://doi.org/10.1109/ACCESS.2020.2964896

2. Alanzi, H. M., & Alkhatib, M. (2025). Blockchain-based identity management system prototype for enhanced privacy and security. Electronics, 14, 2605. https://doi.org/10.3390/electronics142605

3. Annoni, P. G. J., & Seiler, P. (2016). Wind farm flow modeling using an input-output reduced-order model. In Proceedings of the American Control Conference (pp. 506–512).

4. Awan, M., Alam, A., & Kamran, M. (2025). Cybersecurity challenges in SMEs. Journal of Cybersecurity Risk Analysis, 3, 89–102.

5. Baeza, V. M., & Salor, L. C. (2024). New horizons in tactical communications: An overview of emerging technologies possibilities. IEEE Potentials, 43, 12–19.

6. Bai, C., Sheng, S., & Li, J. (2020). Third-party relational governance and collaborative innovation performance. International Journal of Innovation Studies, 4, 123–135.

7. Bansal, G., & Axelton, Z. (2024). Impact of cybersecurity disclosures on stakeholder intentions. Journal of Computer Information Systems, 64, 78–91.

8. Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17, 99–120.

9. Bharadwaj, A. (2000). A resource-based perspective on IT capability and firm performance. MIS Quarterly, 24, 169–196.

10. Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. MIS Quarterly, 1, 17–32.

11. Castro, V., Peña, M. L., Marcos, E., & Salgado, M. (2025). Combining action research with design science. International Journal of Qualitative Methods, 24, 1–15.

12. Clark, A., & Mujeye, S. (2025). A critical analysis of SME cybersecurity policies and practices. In Proceedings of the ACM International Conference on Information Security and Privacy (pp. 178–183).

13. Claro, D. P., Hagelaar, G., & Omta, O. (2003). The determinants of relational governance and performance. Industrial Marketing Management, 32, 703–716.

14. Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling theory: A review and assessment. Journal of Management, 37, 39–67.

15. DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited. American Sociological Review, 48, 147–160.

16. El-Hajj, M., & Mirza, Z. A. (2024). Protecting SMEs: A cybersecurity risk assessment framework. Electronics, 13, 3910.

17. Elsayed, A., Ismail, M., & Ahmed, S. (2024). The impact of cybersecurity disclosure on banks' performance. Future Business Journal, 10, 115.

18. Fernandez de Arroyabe, J. C., Arranz, N., & Li, J. (2024). Cybersecurity resilience in SMEs: A machine learning approach. Journal of Computer Information Systems, 64, 1–17.

19. Garcia Cid, M. I., González, J. Á., Martín, L. O., & Gómez, D. D. R. (2022). Disruptive quantum safe technologies. In Proceedings of the ARES Conference (pp. 1–8).

20. Gherghina, Ș. C., Botezatu, M. A., Hosszu, A., & Simionescu, L. N. (2020). SMEs as engines of economic growth. Sustainability, 12, 347.

21. He, C., Wang, Y., Zhang, T., Hao, F., & Ma, Y. (2025). Blockchain-based secure data risk management method. Electronics, 14, 3058.

22. Heidt, M., Gerlach, J., & Buxmann, P. (2019).

Security divide between SMEs and large companies. Information Systems Frontiers, 21, 1285–1305.

23. Hepworth, E., Salisbury, U., Li, M., Rodgers, E., & Force, N. Z. D. (2025). Software-defined networking architecture for coalition tactical networks.

24. Hoong, Y., Davis, P. A. E., & Windekilde, I. M. (2024). SME managers and cybersecurity challenges. Technology in Society, 78, 102650.

25. ISO/IEC. (2022). ISO/IEC 27001: Information security management systems. Geneva: ISO.

26. Joswig, T., & Kurz, W. (2025). NIS2 adoption in EU SMEs. Journal of Next-Generation Research, 5, 99.

27. Khan, N., Furnell, S., Bada, M., Nurse, J., & Rand, M. (2025). Barriers to cybersecurity adoption in SMEs. Information & Computer Security.

28. Kianpour, M., & Raza, S. (2024). Cybersecurity regulation risks. International Cybersecurity Law Review, 5, 169–212.

29. Kianpour, M., Davis, P. A. E., & Windekilde, I. M. (2025). Digital sovereignty and NIS2 directive. International Journal of Information Security, 24, 245–267.

30. Kumar, A. (2022). Buyer–supplier relationships and sustainability. Annals of Operations Research, 322, 157–181.

31. Le, T. D., Le Dinh, T., & Uwizeyemungu, S. (2025). Cybersecurity framework for SMEs. Enterprise Information Systems, 19, 10.

32. Luiz, J., Magada, T., & Mukumbuzi, R. (2021). Strategic responses to institutional voids. Management International Review, 61, 681–711.

33. Melville, N., Kraemer, K., & Gurbaxani, V. (2004). IT and organizational performance. MIS Quarterly, 28, 283–322.

34. Monzon Baeza, V., Parada, R., Concha Salor, L., & Monzo, C. (2025). AI integration in tactical communication systems. Systems, 13, 752.

35. Nugraha, Y., & Martin, A. (2022). Cybersecurity service level agreements. Journal of Cybersecurity, 8, 1.

36. Ozkan, B. Y., & Spruit, M. (2022). Adaptable security maturity assessment. Information Systems Management, 39, 325–342.

37. Papathanasiou, A., Liontos, G., Katsouras, A., Liagkou, V., & Glavas, E. (2025). Cybersecurity guide for SMEs. Journal of Information Security, 16, 1–43.

38. Pavlou, P. A., & El Sawy, O. A. (2011). Dynamic capabilities. Decision Sciences, 42, 239–273.

39. Poppo, L., & Zenger, T. (2002). Contracts and relational governance. Strategic Management Journal, 23, 707–725.

40. Proudfoot, J., Cram, W., & Madnick, S. (2024). Cybersecurity regulations and organizations. European Journal of Information Systems, 34, 1–24.

41. Shaffique, M. R. (2024). Cyber Resilience Act. Computer Law & Security Review, 54, 106009.

42. Spence, M. (1973). Job market signaling. Quarterly Journal of Economics, 87, 355–374.

43. Suchman, M. (1995). Managing legitimacy. Academy of Management Review, 20, 571–610.

44. Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities. Strategic Management Journal, 18, 509–533.

45. Trist, E. (1981). The evolution of socio-technical systems. Toronto: Ontario Quality of Working Life Centre.

46. Wade, M., & Hulland, J. (2004). Resource-based view and IS research. MIS Quarterly, 28, 107–142.

47. Wallis, T., & Dorey, P. (2024). Cybersecurity in supply chains. Applied Sciences, 14, 5805.

48. Wilson, M. (2025). Cybersecurity perspectives of UK SMEs. Information Security Journal, 34, 1–35.

49. World Bank. (2015). SMEs, age, and jobs: A review of the literature. Washington, DC: World Bank.

50. Yeoh, W., & Popovič, A. (2022). Cybersecurity critical success factors. Computers & Security, 118, 102724.

51. Zaheer, A., McEvily, B., & Perrone, V. (1998). Does trust matter? Organization Science, 9, 141–159.

52. Zaheer, A., & Venkatraman, N. (1995). Relational governance strategy. Strategic Management Journal, 16, 373–392.

53. Zacharias, J., von Zahn, M., Chen, J., & Hinz, O. (2022). Explainable AI feature selection. Electronic Markets, 32, 2159–2184.