Cybersecurity Assurance for SMEs: A Conceptual Framework Integrating Organizational Culture, Fraud Risk Management and Forensic Accounting

AWOLOWO, Francis <http://orcid.org/0000-0003-0172-0846>, ODE, Egena, ABIDOYE, Adenike, AJAO, Oluwaseun and JOGUNOLA, Olamide

RESEARCH ARTICLE OPEN ACCESS

Cybersecurity Assurance for SMEs: A Conceptual Framework Integrating Organizational Culture, Fraud Risk Management and Forensic Accounting

Ifedapo Francis Awolowo[1] | Egena Ode[2] | Adenike Abidoye[1] | Oluwaseun Ajao[2] | Olamide Jogunola[2]

[1]Sheffield Hallam University, Sheffield, UK | [2]Manchester Metropolitan University, Manchester, UK

Correspondence: Ifedapo Francis Awolowo (i.f.awolowo@shu.ac.uk)

Received: 24 December 2024 | **Revised:** 22 January 2026 | **Accepted:** 11 February 2026

Keywords: cybersecurity assurance | forensic accounting | fraud risk management | organisational culture | SMEs

ABSTRACT

As digitalization accelerates across the global economy, small and medium enterprises (SMEs) face increasing exposure to cybersecurity threats, not due to flaws in external platforms, but because of internal organizational vulnerabilities. This paper presents a conceptual framework that integrates the resource-based view (RBV) and dynamic capabilities theory (DCT) to explore how SMEs can strategically enhance their cyber resilience. We reconceptualize fraud risk management (FRM), forensic accounting (FA) and cyber-aware organizational culture as strategic resources that, when systematically integrated, enable dynamic capabilities for cyber resilience. These resources support organizational processes to sense emerging threats, seize response opportunities and reconfigure defencive capabilities in resource-constrained environments. By shifting the focus from technology-centric models to capability-driven strategies, this framework positions cybersecurity as a strategic asset, essential for sustaining operational continuity, safeguarding reputation and enhancing competitive advantage. The framework offers theoretical insights and practical guidance for SME leaders, policymakers and practitioners navigating cybersecurity challenges in resource-constrained environments.

1 | Introduction

Small and medium enterprises (SMEs) are central to economic prosperity worldwide, serving as critical drivers of employment, innovation and regional development. Globally, SMEs account for over 90% of all businesses and provide more than half of the employment opportunities, playing a particularly crucial role in both emerging and advanced economies (Petzold et al. 2019; Ribau et al. 2018). In the United Kingdom and the United States, SMEs account for 99.9% of the business population, contributing 63% of private-sector employment and 97.3% of total exports, respectively (Office of National statistics 2023; US Chamber of Commerce, 2024). Their vital contributions extend to other countries such as Germany, Canada and Nigeria, where SMEs anchor innovation ecosystems, drive inclusive growth and support socio-economic advancement (Deutschland 2023; Obi et al. 2018).

Despite their size and agility, SMEs face distinctive operational challenges, particularly in the digital era (N. Khan et al. 2025; Verma and Shri 2025). Digitalization has enabled SMEs to enhance market access, streamline operations and embrace remote business models, yet it has also significantly increased their exposure to cyber threats (Rachinger et al. 2019; Perano et al. 2023; Gašpar et al. 2025). Although many SMEs rely on secure third-party cloud platforms with robust security architecture, the primary source of their vulnerability is not flaws in these external platforms but rather internal organizational weaknesses (Al-Mutawa and Saeed Al Mubarak 2024; Innomesanghan et al. 2025). The contemporary threat landscape, characterized by advanced persistent threats, AI-driven phishing schemes and sophisticated ransomware attacks, continues to evolve rapidly (Le et al. 2024; Falch et al. 2023; Wilson and McDonald 2025).

https://doi.org/10.1002/cjas.70051

A recent UK report from a BT study shows that SMEs face a rise in cyberattacks, with an average cost of £7960 to recover from a breach, indicating a 67% increase (Williams 2025). The report also highlights that about 39% of SMEs in the UK have not provided cybersecurity training to staff, despite the growing frequency and severity of cyberattacks. Rawindaran et al. (2023) argue that SMEs often lack the resources and expertise to protect themselves, their systems adequately and their data, thereby making them more vulnerable to attacks. This means that SME owners and employees are heavily focused on day-to-day operations, making cybersecurity one of the least prioritized items on their list (Rawindaran et al. 2023; Reed 2024). According to the DSIT - Department for Science and Innovation and Technology (2025) report, one in four businesses (approximately 612,000), accounting for 43% of UK businesses, reported a cybersecurity breach or attack in the past 12 months. Recent studies have identified phishing and ransomware as the most prevalent and disruptive attack types (Ali et al. 2025; Awan and Alam 2025). Further research highlighted that these attacks are time-consuming due to their volume, with the report emphasizing the need for additional staff training (Le et al. 2025; Ungureanu et al. 2024). Wilson and McDonald (2025) emphasized that SMEs have erroneously favoured technical and third-party solutions over training and internal policies. Thus, taking a singular view, focusing mostly on technical aspects and ignoring contextual factors, may not reveal the true picture (Arroyabe et al. 2024).

These attack vectors specifically exploit SME vulnerabilities, such as misconfigured security settings, human error and insufficient employee awareness. Could computing and remote work have heightened the risks SMEs face (Reed 2024; Türen et al. 2025)? In addition, although SMEs increasingly engage in secure API-based data exchanges, reducing some direct risks, they remain vulnerable due to their integration within broader digital supply chains (Türen et al. 2025). A breach in one partner can propagate through interconnected systems (Wilson et al. 2023; Renaud and Ophoff 2021). This can expose even well-defended organizations to collateral risk (Le et al. 2025; Ungureanu et al. 2024; Wilson and McDonald 2025). This underscores the critical need for SMEs to build internal capabilities that go beyond perimeter security to include behavioural, cultural and financial resilience, essential for navigating this complex environment. This paper builds on the thesis that the risk lies not in platform architecture but in SME-specific practices.

Cybersecurity has traditionally been conceptualized as a technical problem solved through firewalls, antivirus software and intrusion detection systems (Ali et al. 2025; Algamdi et al. 2025). Although essential, these measures often fail to address the organizational, behavioural and financial dimensions of cyber resilience. SMEs require an integrative perspective that embeds cybersecurity into the core of their strategic and operational fabric. This paper reframes cybersecurity assurance for SMEs through the dual theoretical lenses of the resource-based view (RBV) and dynamic capability (DC) theory.

RBV posits that firms gain a competitive advantage by effectively deploying internal resources that are valuable, rare, inimitable and nonsubstitutable (VRIN) (Barney 2001). These resources may include organizational knowledge, culture, processes and technical competencies. In parallel, DC theory explains how firms survive and thrive in volatile environments by developing capabilities that enable them to sense threats and opportunities, seize them effectively and reconfigure internal assets accordingly (Teece 2009; Teece 2018a, 2018b). By integrating these perspectives, SMEs can move beyond static, compliance-based cybersecurity to adopt adaptive, resource-anchored strategies that support long-term resilience.

In this conceptual framework, this research argues that SMEs can build cyber resilience by developing and strategically integrating three interrelated strategic resources: fraud risk management systems, forensic accounting expertise and a cyber-aware organizational culture. When coordinated through higher-order organizational routines, these resources collectively enable dynamic capabilities (i.e., the capacity to sense emerging threats, seize opportunities to mitigate risks and continuously reconfigure internal controls) (Teece 2007; Teece 2018a, 2018b). Together, these elements equip SMEs to not only defend against cyber threats but also to adapt and evolve in response to an increasingly hostile digital environment. Previous findings suggest that internal factors related to human behaviour and financial controls are repeatedly highlighted as critical vulnerabilities. For instance, many SME breaches involve elements of fraud or misuse (internal or external) and failures in internal controls (Abdul Mumin et al. 2024; Wilson and McDonald 2025; Zainal et al. 2022); thus, fraud risk management becomes a natural cornerstone of cyber resilience. Moreover, human factor addressed through organizational culture and awareness has been widely documented as a leading cause of security failures (lack of awareness has been linked to phishing successes) (Ghaderi et al. 2024; Wilson and McDonald 2025), including SME leaders underestimating cyber risks (Zwilling et al. 2022). This paper further argues that a cyber-aware culture can foster employee awareness, which can, in turn, reduce human errors. Furthermore, forensic accounting, as a specialized investigative function, has increasingly been identified as a tool for uncovering cyber-fraud (Awolowo 2019).

Fraud risk management (FRM) refers to the systems, protocols and practices an organization uses to identify, assess and mitigate the risks of financial fraud. Positioned as a structural resource, FRM is crucial for SMEs navigating cybersecurity threats, which often overlap with or lead to financial misreporting, unauthorized transactions or internal collusion (Bozkus Kahyaoglu and Caliyurt 2018; Abdul Mumin et al. 2024). The ability to design and sustain fraud risk controls, such as internal audits, access restrictions and incident monitoring, forms the foundation of SME cybersecurity assurance. Unlike passive risk assessments, FRM mechanisms foster a culture of accountability, procedural rigour and early warning, all of which are vital in detecting and responding to cyber-fraud incidents before they escalate.

Forensic accounting (FA) is the second pillar of our framework. This specialized discipline applies accounting, investigative and legal expertise to identify financial irregularities and support litigation or internal investigations. Although forensic accounting may traditionally be viewed as an operational capability, in this context, it transcends routine activities and instead exemplifies a dynamic capability. Dynamic capabilities enable firms to adapt to environmental uncertainty by developing higher-order competencies that sense, seize and reconfigure internal processes in response to emerging challenges (Teece 2018a, 2018b). FA embodies these principles by detecting latent financial threats (sensing), initiating investigative responses (seizing) and redesigning internal control structures post-incident (reconfiguring).

Moreover, integrating forensic accounting into cybersecurity responses goes beyond predefined procedures or static rule-following. It involves judgment, real-time investigation and cross-functional collaboration that adapts to the complexity and novelty of each incident. In SMEs, where resource constraints heighten the stakes of cyber incidents, the ability to dynamically deploy forensic skills becomes an organizational differentiator (Arroyabe et al. 2024; Rawindaran et al. 2023). This agility and capacity for organizational learning are the hallmarks of dynamic, rather than ordinary capabilities (S. Ahmad et al. 2025). Thus, forensic accounting functions not merely as a support activity but as a strategic enabler of adaptive cyber resilience (Awolowo 2019; Daraojimba et al. 2023). As a specialized investigative function, forensic accounting can help SMEs to better detect and respond to breaches that evade automated tools.

The third element, cyber-aware organizational culture, functions as a valuable and inimitable resource (Algamdi et al. 2025; Zwilling et al. 2022). Culture shapes how individuals within the organization perceive, prioritize and act upon cybersecurity threats. In SMEs, where leadership is often centralized and informal communication channels dominate, culture is both a risk and an opportunity. A cyber-aware culture ensures that employees are trained to recognize phishing attempts, report anomalies, comply with security protocols and champion a proactive cyber mindset (Wilson and McDonald 2023; Akter et al. 2022). According to COSO (2019), governance and culture form the bedrock of effective enterprise risk management. In practice, this means that leadership must consistently reinforce the importance of cybersecurity, embed it into performance evaluations and allocate resources that enable awareness-building and behavioural change.

Together, these three elements form a synergistic internal architecture that aligns with both the resource-based view (RBV) and dynamic capabilities (DC) principles. Fraud risk management contributes structure and compliance mechanisms; forensic accounting introduces responsiveness, expertise and investigative agility; and cyber-aware culture fosters shared responsibility and vigilance. Importantly, these internal factors are not externally imposed but emerge from within the SME's resource environment, making them more sustainable and contextually relevant. This integration represents a shift from technology-centric cybersecurity approaches to people- and capability-driven strategies.

Moreover, each of the three core elements presented in this paper aligns with one of the core dynamic capability processes: sensing, seizing and reconfiguring (Teece 2007), thereby covering a comprehensive adaptive cycle. In other words, these components collectively enable SMEs to sense threats (through forensic analysis of anomalies), seize opportunities to mitigate risk (through robust fraud risk management processes) and reconfigure/transform the organization (through cultivating cyber-aware cultures that learn and evolve) (Arndt et al. 2022; Bleady et al. 2018; Doherty and Terry 2013). This theoretical lens guided the inclusion of the three elements and, though important, the exclusion of others such as traditional security measures (firewalls, access controls), which are technical resources that SMEs can acquire off-the-shelf. This paper focuses on higher order internal factors that SMEs must develop and coordinate internally. Hence, this paper emphasizes an integrative fraud-control process, a culture of security and investigative capability. These components have been selected because first evidence shows they address the most prevalent internal weaknesses of SMEs (S. Ahmad et al. 2025; Arroyabe et al. 2024; Al-Mutawa and Saeed Al Mubarak 2024; Wilson and McDonald 2025) and secondly, together, they correspond to a holistic dynamic capability to sense, respond and adapt to cyber threats (Helfat and Peteraf 2015; Jin et al. 2024; Teece 2007; Wang and Ahmed 2007).

This paper positions cybersecurity assurance as a strategic imperative for SME resilience and competitiveness in the digital economy. It addresses the following research questions:

What strategic resources do SMEs need to develop, and how must these resources be integrated to enable dynamic capabilities for sensing, seizing and reconfiguring against cyber threats?

How do fraud risk management, forensic accounting and cyber-aware culture interact to enhance an SME's cybersecurity assurance, and how can these be integrated within a dynamic capabilities' framework?

What actionable strategies can SME managers implement to develop these capabilities (fraud risk management, forensic accounting, cyber-aware culture) under typical resource constraints, and what benefits can be expected?

The motivation for this study arises from the increasing vulnerability of SMEs to sophisticated cyberattacks and the limitations of conventional, purely technical cybersecurity models (Ali et al. 2025; Algamdi et al. 2025; N. Khan et al. 2025; Verma and Shri 2025). Despite their vital role in global economies, SMEs remain disproportionately under-resourced and underprepared for cyber incidents. Although much of the existing literature focuses on large enterprises and technical defences, this study explores a novel framework that conceptualizes cybersecurity assurance as a strategic function embedded in behavioural, financial and cultural capacities.

By identifying fraud risk management systems, forensic accounting expertise and cyber-aware culture as strategic resources and by explicating how their integration enables dynamic capabilities, this study reorients how SME cybersecurity is understood from a technology-centric to a capability-driven model. The framework emphasizes that sustainable cyber resilience emerges not from possessing individual resources but from developing organizational routines that orchestrate resources to adapt to evolving threats (Teece 2018a, 2018b) continuously.

The remainder of this paper is structured as follows: Section 2 examines the theoretical underpinnings of the resource-based view and dynamic capability perspectives; Section 3 presents the integrated conceptual framework; Section 4 outlines the paper's theoretical and practical contributions; and Section 5 concludes with implications for policy and future research directions.

2 | Theoretical Background and Context

2.1 | The Role of SMEs in the Global Economy

The economic significance of SMEs is multifaceted. They provide a substantial share of total employment in many countries, helping to absorb labour in regions where larger firms may have little to no presence. In Nigeria, for instance, SMEs account for approximately 96% of all businesses and contribute to 84% of the country's employment (Obi et al. 2018). This capacity to generate jobs is crucial, particularly in developing economies, where high levels of unemployment and underemployment pose significant social and economic challenges.

Moreover, SMEs are instrumental in driving innovation and competition. They are often more agile than larger corporations, enabling them to explore niche markets, experiment with new business models and adopt cutting-edge technologies. This capacity for innovation is particularly important in today's fast-paced economic landscape, where technological advancements can rapidly shift industry dynamics. SMEs are frequently at the forefront of innovation, introducing new products and services that challenge existing market norms and drive economic progress. In Germany, for instance, SMEs account for 99.3% of all firms and make significant contributions to innovation, with many serving as suppliers and partners to larger corporations across various sectors (Deutschland 2023).

In addition to their role in job creation and innovation, SMEs make significant contributions to local communities and the broader economy through their involvement in supply chains. They often provide goods and services that larger firms require, creating a ripple effect that stimulates economic activity and fosters interdependence within local economies. This interconnectedness bolsters local community resilience and enhances regional economic stability (Sukumar et al. 2023; Savlovschi and Robu 2011).

However, despite their significant contributions, SMEs face unique challenges that can hinder their growth and sustainability. Access to financing is often cited as one of the most critical barriers to SME development. Many small businesses struggle to secure the funding needed to invest in new technologies, expand operations or enter new markets (Anand 2015; Song 2019; Van Haastrecht et al. 2021). Traditional financing options, such as bank loans, may be difficult to obtain due to the perceived risks of lending to smaller enterprises. Additionally, SMEs may lack the financial sophistication to navigate complex funding processes or develop compelling business cases for potential investors (Ferreira de Araújo Lima et al. 2020).

Regulatory burdens also pose significant challenges for SMEs. Navigating compliance with various regulations can be resource-intensive and disproportionately affects smaller firms, which often lack the legal and administrative capabilities of larger organizations (Ferreira de Araújo Lima et al. 2020). In some cases, regulatory requirements may hinder innovation and limit SMEs' ability to adapt quickly to market changes.

Despite these challenges, SMEs possess inherent strengths that can be leveraged for success (Walaski 2017). Their smaller size allows greater flexibility and faster decision-making, enabling them to adapt to market or consumer preferences more rapidly than larger organizations. This agility can be a significant competitive advantage, particularly in industries characterized by rapid technological advancements or shifting consumer demands (Brustbauer 2016; Walaski 2017).

Furthermore, SMEs often foster strong customer relationships, providing personalized service and fostering loyalty. This close connection to their customer base enables them to gain valuable insights into market trends and consumer preferences, helping them respond more effectively to evolving demands. By prioritizing customer satisfaction and engagement, SMEs can build a loyal customer base that sustains their operations even in challenging economic conditions (Ojiambo 2023).

Additionally, SMEs play a crucial role in promoting social and economic inclusivity. They often serve as a platform for entrepreneurship and self-employment, providing opportunities for individuals from diverse backgrounds to start and grow their businesses. This entrepreneurial spirit contributes to the overall dynamism of the economy and encourages grassroots innovation. As SMEs grow and adapt, they can empower local communities and contribute to social cohesion by creating jobs and opportunities for marginalized groups (OECD 2019).

2.2 | Cybersecurity as a Strategic Asset

Cybersecurity has evolved beyond its traditional role as a defencive mechanism in today's rapidly changing digital landscape. It is now recognized as a strategic asset essential for the sustainability and growth of organizations, particularly small and medium enterprises (SMEs). This change in thinking underscores the need for SMEs to integrate cybersecurity into their core business strategy. Doing so can enhance their resilience against cyber threats and maintain competitive advantages and growth (Ferreira de Araújo Lima et al. 2020).

Cybersecurity protects information systems, networks and data from theft, damage or unauthorized access. Historically, organizations have approached cybersecurity as a technical challenge, focusing primarily on implementing firewalls, antivirus software and other defencive measures (Renaud and Ophoff 2021). However, this narrow view has proven inadequate considering the increasing sophistication and frequency of cyberattacks. SMEs, often perceived as easier targets due to their limited resources and lack of cybersecurity expertise, must adopt a more integrated cybersecurity approach that aligns with their broader business objectives.

One of the primary reasons for framing cybersecurity as a strategic asset is its direct impact on business continuity. Cyberattacks can result in severe disruptions, financial losses and reputational damage, especially devastating for SMEs with limited resources. For SMEs, the consequences of a successful cyberattack can be devastating. Official Statistics.

The DSIT survey 2025 highlights that four in ten (43%) businesses and three in 10 charities (30%) have reported cyber breach within the last 12 months (DSIT - Department for Science and Innovation and Technology 2025). Therefore, a proactive, strategic approach to cybersecurity ensures that businesses are prepared to address potential threats and can recover quickly in the event of a breach (Rostami et al. 2015). A robust cybersecurity framework also contributes to an SME's market positioning by fostering trust and confidence among customers, partners and stakeholders. As data privacy concerns grow, customers are increasingly preferring to engage with businesses that are committed to safeguarding sensitive information. For SMEs, cybersecurity becomes a competitive advantage that helps build stronger relationships and encourages customer loyalty. By viewing cybersecurity as a strategic asset, SMEs can differentiate themselves in the market, using their security posture as a signal of reliability and responsibility (COSO 2019).

Moreover, cybersecurity serves as a critical enabler of innovation. As SMEs continue to adopt digital technologies to enhance their operations, cybersecurity ensures that these innovations can be implemented safely. Whether introducing new digital products or expanding into new markets, a strategic cybersecurity focus mitigates the risks of digital transformation, allowing SMEs to innovate without compromising security (Lloyd 2020). Embracing cybersecurity as a growth enabler rather than a limitation encourages the integration of new technologies while maintaining resilience against cyber threats.

For SMEs to fully capitalize on the strategic benefits of cybersecurity, it is essential to foster a cyber-aware organizational culture. Leadership must set the tone by prioritizing cybersecurity and integrating it into the company's core values. Employee awareness is equally important, as the workforce plays a vital role in recognizing and mitigating potential threats. Training programs that emphasize cybersecurity best practices and encourage vigilance across all levels of the organization can significantly reduce vulnerabilities (Wilson and McDonald 2023).

However, SMEs often face challenges in adopting comprehensive cybersecurity strategies due to resource constraints, such as limited access to financial and technical resources. This is where a risk-based approach becomes essential. By identifying critical assets, assessing potential threats and prioritizing mitigation efforts, SMEs can implement cybersecurity measures that align with their specific risk profiles and available resources (Ferreira de Araújo Lima et al. 2020). This approach allows SMEs to allocate resources efficiently while remaining resilient against the most pressing cyber threats.

2.3 | Secure-By-Default Architectures and the Shift in the Locus of Cyber Risk

Contemporary SMEs increasingly operate on cloud and SaaS platforms that embed security by default, including automated patching, encryption and hardened infrastructure. Under the shared-responsibility model, cloud providers secure the underlying infrastructure, whereas customers remain responsible for identity management, access configuration, data governance and operational processes (Ross and Pillitteri 2020). Consequently, cyber risk has shifted from infrastructure vulnerabilities towards failures in identity control, system configuration and human decision-making.

Empirical evidence indicates that most successful breaches now involve compromised credentials, phishing, misconfigured cloud services and abuse of legitimate access rather than exploitation of software flaws in cloud platforms (Verizon 2024). In API-enabled and supply-chain ecosystems, these organizational weaknesses are amplified, as trusted digital connections allow attacks to propagate across partners through authorized interfaces (Renaud and Ophoff 2021). Cybersecurity assurance, therefore, depends less on perimeter defence and more on how organizations regulate permissions, monitor financial and operational workflows and enforce behavioural compliance.

The proposed framework directly targets this organizational locus of risk. Fraud risk management governs financial authorization structures, segregation of duties and anomaly detection in digitally mediated transactions, addressing threats such as business email compromise and payment redirection fraud (Abdul Mumin et al. 2024; Bozkus Kahyaoglu and Caliyurt 2018). Forensic accounting enables systematic investigation of anomalous digital transactions and identification of control failures that enable cyber-fraud (Awolowo 2019; Daraojimba et al. 2023). Cyber-aware organizational culture shapes how employees interpret access privileges, comply with authentication protocols and escalate suspicious activity, which is critical in identity-centric security environments (Akter et al. 2022; Zwilling et al. 2022). Together, these mechanisms operate precisely where modern cloud-based cyber risk materializes, linking secure-by-default technologies to organizational dynamic capabilities for sensing, seizing and reconfiguring (Teece 2007; Helfat and Peteraf 2015).

3 | Conceptual Framework: Integrating Fraud Risk Management, Forensic Accounting and Organizational Culture

This study builds on the resource-based view (RBV) and dynamic capability (DC) theory to propose a conceptual framework that integrates fraud risk management, forensic accounting expertise and organizational culture into cybersecurity strategies. The framework addresses two critical dimensions of competitive advantage: what firms have (RBV) and what firms do (DC) (Helfat and Peteraf 2015; Teece 2018a, 2018b). According to the RBV, firms can achieve sustained competitive advantage by developing and leveraging resources that are valuable, rare, inimitable and nonsubstitutable (VRIN) (Barney 2001; Teece et al. 1997).

The framework adopted in this study proposes that fraud risk management systems, forensic accounting expertise and a cyber-aware organizational culture qualify as strategic resources within the RBV. However, as Helfat and Peteraf (2015) emphasize, resources alone do not constitute capabilities. Resources are assets that firms possess; capabilities are what firms can do with those assets. Furthermore, Winter (2003) distinguishes between ordinary capabilities, routine activities that enable firms to "make a living" and DCs, higher-order processes that enable firms to change how they make a living in response to environmental shifts (Teece et al. 1997). Previous evidence (e.g., H. Naseer et al. 2024; Pigola and da Costa 2025; Yeow et al. 2018) indicates that cyber threats are dynamic. Thus, they require more than static capabilities. This paper adopts a three-tier conceptual structure grounded in established DC literature:

Tier 1: Strategic resources (RBV foundation): fraud risk management systems, forensic accounting expertise and cyber-aware culture are organizational resources. These are assets the firm possesses that meet VRIN criteria (Pigola and da Costa 2025). These resources provide the foundational material for cybersecurity capability development.

Tier 2: Ordinary capabilities: When routinely deployed, these resources enable ordinary capabilities, the standardized operational activities through which SMEs conduct fraud monitoring, financial investigations and security compliance (Winter 2003). These are necessary but insufficient for sustained competitive advantage in dynamic environments.

Tier 3: Dynamic capabilities: DCs emerge when firms develop higher-order routines that strategically integrate, orchestrate and reconfigure their resource base in response to environmental changes (Eisenhardt and Martin 2000; Teece 2007). In cybersecurity contexts, DCs enable SMEs to detect emerging cyber threats, seize opportunities to mitigate risks and continuously reconfigure defences (Teece 2018a, 2018b).

In this framework (Figure 1), RBV explains why certain cybersecurity resources are strategic (they are valuable, rare and inimitable), whereas DC theory explains how those resources are activated, coordinated and recombined to remain relevant in dynamic environments (Teece 2007; Wang and Ahmed 2007). Figure 1 illustrates how three strategic resources serve as foundational inputs that, when strategically integrated through organizational routines, enable DCs. These capabilities manifest through three interrelated processes: sensing (detecting emerging threats through FRM monitoring, FA investigation

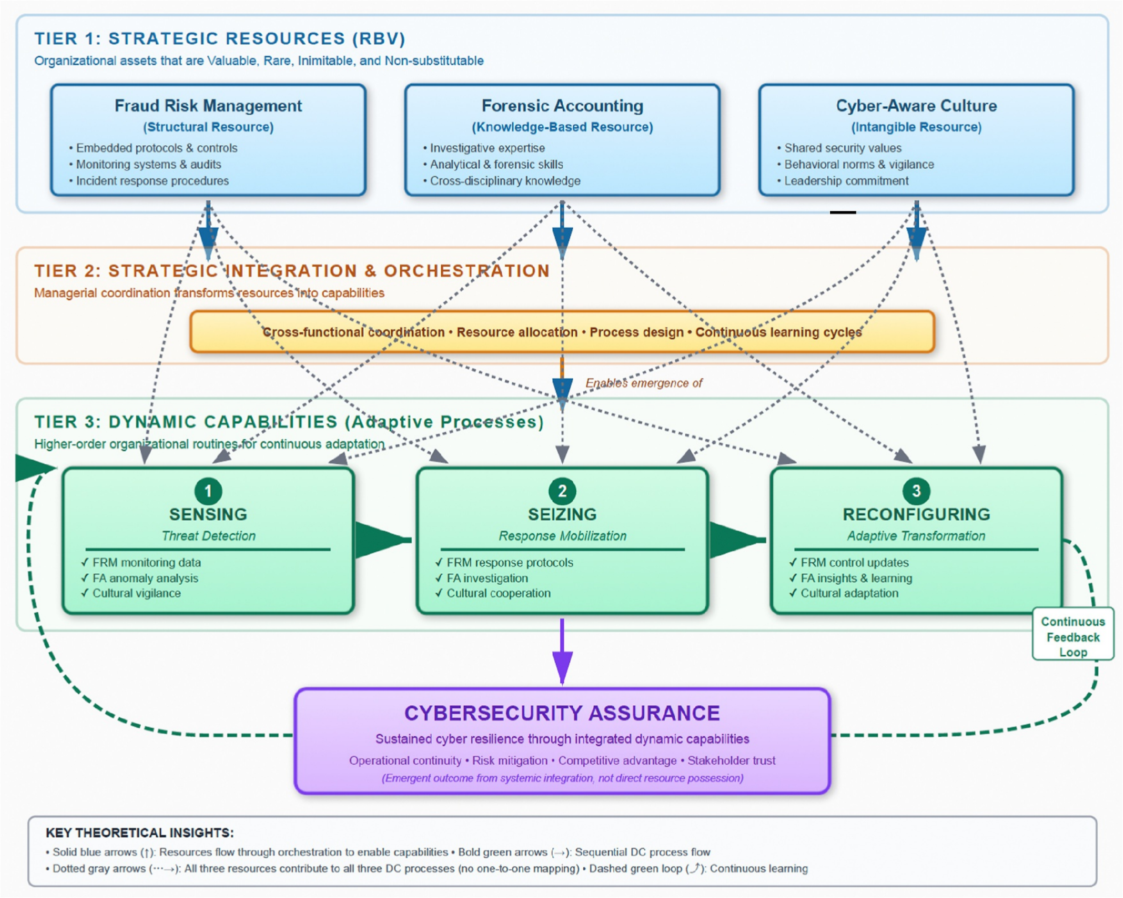
TIER 1: STRATEGIC RESOURCES (RBV)
Organizational assets that are Valuable, Rare, Inimitable, and Non-substitutable
Fraud Risk Management
(Structural Resource)
• Embedded protocols & controls
• Monitoring systems & audits
• Incident response procedures
Forensic Accounting
(Knowledge-Based Resource)
• Investigative expertise
• Analytical & forensic skills
• Cross-disciplinary knowledge
Cyber-Aware Culture
(Intangible Resource)
• Shared security values
• Behavioral norms & vigilance
• Leadership commitment
TIER 2: STRATEGIC INTEGRATION & ORCHESTRATION
Managerial coordination transforms resources into capabilities
Cross-functional coordination • Resource allocation • Process design • Continuous learning cycles
Enables emergence of
TIER 3: DYNAMIC CAPABILITIES (Adaptive Processes)
Higher-order organizational routines for continuous adaptation
1
SENSING
Threat Detection
✓ FRM monitoring data
✓ FA anomaly analysis
✓ Cultural vigilance
2
SEIZING
Response Mobilization
✓ FRM response protocols
✓ FA investigation
✓ Cultural cooperation
3
RECONFIGURING
Adaptive Transformation
✓ FRM control updates
✓ FA insights & learning
✓ Cultural adaptation
Continuous Feedback Loop
CYBERSECURITY ASSURANCE
Sustained cyber resilience through integrated dynamic capabilities
Operational continuity • Risk mitigation • Competitive advantage • Stakeholder trust
(Emergent outcome from systemic integration, not direct resource possession)
KEY THEORETICAL INSIGHTS:
• Solid blue arrows (↑): Resources flow through orchestration to enable capabilities • Bold green arrows (→): Sequential DC process flow
• Dotted gray arrows (···→): All three resources contribute to all three DC processes (no one-to-one mapping) • Dashed green loop (↗): Continuous learning

FIGURE 1 | Conceptual framework: Dynamic capabilities framework for SME cybersecurity assurance. The three organizational resources (FRM, FA, culture) function as inputs that, when strategically integrated, enable DCs (sensing, seizing reconfiguring) for cybersecurity assurance. Arrows indicate primary contributions, though all elements support all processes through systemic interaction.

and cultural vigilance), seizing (mobilizing coordinated responses through FRM protocols, FA evidence and cultural cooperation) and reconfiguring (adapting defences through FRM control updates, FA insights and cultural learning). Arrows indicate primary contributions, though all resources support all processes through systematic interaction. The framework is grounded in the Resource-Based View (resources as competitive advantage) and Dynamic Capability. Theory.

This integration of RBV and DCT demonstrates that cybersecurity is not only about the possession of resources but also about the capacity of a firm to mobilize, integrate and adapt them in the face on evolving threats (Schriber and Lowtedt 2020). Although fraud risk management represents embedded tools, routines and processes that help firms to organize, identify and mitigate internal and external risks, and thus a part of a firm's structural capital that is difficult to replicate, forensic accounting is a specialized resource that is rooted in expert knowledge (Adejumo and Ogburie 2025; Pigola and da Costa 2025). Thus, we argue that forensic accountants can detect irregularities, support investigations and assess financial damages resulting from cyber incidents (Adejumo and Ogburie 2025). As a specialized skill, it is both a valuable and a rare resource. Culture, on the other hand, is an intangible yet powerful resource that shapes behaviour (Akter et al. 2022; Reegård et al. 2019).

According to Reegård et al. (2019), when a firm's culture is attuned to cybersecurity awareness, it supports proactive employee behaviour, which can improve incident reporting and foster accountability. Such culture can create a resilient internal environment (Adejumo and Ogburie 2025; Moschella et al. 2023). Although these resources are critical, RBV alone does not explain how firms respond to fast-changing threats or adapt over time. This limitation is addressed in this research framework through the integration of the RBV and the dynamic capabilities theory (DCT). In this framework (Figure 1), although RBV explains why certain cybersecurity assets are strategic, DC theory explains how those assets and resources are activated, renewed and recombined to remain relevant in dynamic threat environments.

From the perspective of RBV, leveraging organizational capabilities is essential for firm growth (Breznik et al. 2019). Thus, capabilities describe a firm's capacity to alter its resource base to facilitate ongoing behavioural adjustments in response to environmental changes such as cyber threats (Fallon-Byrne and Brian 2017; Teece et al. 1997). Teece (2009) categorized DC into three distinct types: sensing capability (the capacity to investigate the firm's surroundings to discern opportunities or threats), seizing capability (the imperative to exploit recognised opportunities) and reconfiguration capability (the capacity to reconfigure internal and external resources). Sensing and seizing refer to relatively basic functions, whereas reconfiguration capabilities include considerable complexity and may necessitate a complete transformation of the organizational framework (Breznik et al. 2019; Teece 2009).

Seizing involves capitalizing on perceived possibilities through innovation (O. Khan et al. 2021). Efficient sensing and seizing require cohesive organizational routines aligned with the fundamental tasks (Teece 2007). Resources associated with cybersecurity, such as fraud risk management systems (structural routines), forensic accounting expertise (specialized expertise) and a cyber-aware organizational culture (intangible asset), are firm-specific advantages that enhance threat mitigation. In rapidly evolving digital environments, proactive resource management, rather than mere ownership, ensures cybersecurity assurance.

Teece's (2007) notion of seizing capability requires an internal assessment of the organization's structures to leverage and mobilize resources in response to detected threats, such as strategic investment in cybersecurity infrastructure, incident response and the deployment of expert personnel such as forensic accountants (Akter et al. 2022; H. Naseer et al. 2024).

Reconfiguring denotes the capacity to reorganize and restructure resources and organizational frameworks to align internal operations with identified opportunities or threats (Breznik et al. 2019). These capabilities involve transforming existing structures and routines, such as staff training, updating systems and learning from breaches to ensure continued security resilience (Bornay-Barrachina et al. 2025). These capabilities reflect a firm's learning orientation and flexibility. These may involve the continuous evolution of fraud risk models based on post-incident reviews, the integration of forensic insights from training and system updates and a learning culture that embeds cybersecurity into everyday practice, encouraging employees to adapt their behaviour and embrace new protocols (Adejumo and Ogburie 2025). These capabilities ensure that firms remain relevant and resilient amidst evolving threats.

The fundamental characteristic of DCs is their ability to recombine and reconfigure assets and organizational structures in response to changing markets and technologies. The reconfiguration process entails creating novel combinations of existing information or utilizing current knowledge for new purposes or in inventive ways. The ability to reconfigure is crucial for sustaining evolutionary fitness and, when necessary, for overcoming detrimental route dependencies. Reconfiguration capabilities are crucial for modifying existing resources to meet new objectives, creating new resources and rectifying current shortcomings in a firm's resource base (Yeow et al. 2018).

According to Teece's (2007) microfoundations for reconfiguration, the management of cospecialization and complementarities is crucial under certain conditions, necessitating alterations to the organization's existing routines, systems, structures and processes. Therefore, when digital change threatens a firm's current talents and resources, it must prioritize adaptation. Therefore, the proposed framework explains how internal resources (RBV) are activated and sustained through dynamic capabilities (DCs) to achieve cybersecurity assurance (S. B. M. Ahmad et al. 2021; H. Naseer et al. 2016, 2018).

This framework contributes to the theory by offering a structured understanding of how sensing, seizing and reconfiguring capabilities operationalize cybersecurity. This dynamic lens is paramount as firms are increasingly exposed to digital threats, where security does not rely in static defences but on adapting organizational intelligence. The following subsections detail each strategic resource contribution to the integrated DC system.

3.1 | Fraud Risk Management: A Structural Resource Enabling Response Mobilization

Fraud risk management (FRM) systems represent a critical structural resource for SME navigating cybersecurity threats (Eze et al. 2022; Sihombing et al. 2023).

From an RBV perspective, FRM qualifies as a strategic resource because it prevents fraud-related financial losses and reputational damage, which are essential for SME sustainability (Rostami et al. 2015; Shanmugam et al. 2012; Mishra et al. 2019). FRM systems are valuable because they directly protect a firm's assets; rare in resource-constrained SME environments where comprehensive fraud controls are not widely adopted (Abdul Mumin et al. 2024); inimitable when embedded in firm-specific organizational culture and tacit knowledge; and non-substitutable as external systems cannot replace internally tailored fraud management frameworks (Mishra et al. 2019). FRM encompasses the systems, protocols and practices an organization uses to identify, assess and mitigate fraud risks (Bozkus Kahyaoglu and Caliyurt 2018). These include internal audits, access restrictions, segregation of duties, incident monitoring and financial controls. As a structured resource, FRM provides the organizational infrastructure for risk governance, the scaffolding upon which cybersecurity defences are built (Lamptey and Singh 2018). Unlike ad hoc responses, FRM embeds fraud prevention into organizational routines, creating procedural rigour, accountability mechanisms and early warning systems (Sihombing et al. 2023).

When deployed routinely for compliance monitoring, FRM functions as an ordinary capability (the standardized processes through which firms conduct oversight) (Winter 2003). However, FRM transcends ordinary capability status when strategically integrated into a DC system. Specifically, FRM enables the seizing function within Teece's (2007) framework by providing the structural capacity to mobilize resources rapidly when threats are detected: FRM provides sensing support through FRM monitoring protocols (e.g., transaction audits, access logs) that generate data streams that feed detection; seizing enablement through preestablished FRM response protocols (e.g., incident escalation procedure, forensic investigation triggers) enables rapid resource mobilization when anomalies are identified (A. Naseer et al. 2023). FRM also provides post-incident reconfiguration of contributions by reviewing control weaknesses and informing iterative improvement cycles (Moschella et al. 2023). The key distinction is that FRM systems are resources; FRM deployment for adaptive response contributes to DC. As Helfat and Peteraf (2015) clarify, resources enable capabilities, but capability resides in the organization's capacity to deploy those resources purposefully in changing contexts.

By their nature, SMEs are characterized by resource constraints that limit their ability to adopt comprehensive risk management frameworks (Sukumar et al. 2023). Unlike larger organizations, which can leverage greater access to funding, human capital and advanced technologies, SMEs often operate with a narrower resource base (Ferreira de Araújo Lima et al. 2020). These constraints can make it challenging for SMEs to implement comprehensive risk management practices, particularly in the context of fraud and cybersecurity risks, which are becoming increasingly complex and sophisticated. The ability to invest in advanced fraud detection systems, cybersecurity infrastructure and continuous employee training is often beyond the financial reach of smaller enterprises.

However, despite these constraints, risk management remains essential for SMEs. Although large organizations typically formalize their cyber risk management processes, Lloyd (2020) noted that the low prevalence of formal processes is more prevalent in SMEs. Nevertheless, Moschella et al. (2023) argue that the lack of formal processes does not equate to a complete absence of risk management efforts. A comprehensive risk management system enables organizations to assess and respond to a broad spectrum of risks, ensuring they can maintain business continuity even when exposed to fraud or other disruptive events (Rostami et al. 2015). This capability is vital for SMEs, as the consequences of unmitigated risks can be disproportionately severe. Without the buffer of large financial reserves or widespread market dominance, SMEs must proactively manage their exposure to threats like fraud and cybercrime to safeguard their long-term viability.

In practice, risk management for SMEs involves assessing vulnerabilities across all business areas and developing processes to mitigate these risks. For instance, adopting fraud prevention protocols, such as regular audits, internal controls and employee monitoring, can help SMEs detect fraudulent activities before they escalate. Establishing response plans for identified risks also ensures that SMEs can act swiftly when fraud occurs, minimizing its impact on operations and finances. Moreover, incorporating technology-driven solutions such as data analytics, artificial intelligence and machine learning can support fraud detection efforts, albeit at a cost that might be prohibitive for some SMEs (Mcbride and Philippou 2022).

Although limited resources pose a significant barrier to effective risk management in SMEs, their smaller size offers strategic advantages. Unlike larger, more bureaucratic organizations, SMEs are often more agile and can quickly adapt their operations and risk management practices to changing conditions (Walaski 2017). This flexibility can enable SMEs to implement simple, cost-effective risk management frameworks that can be scaled up as the business grows. For instance, SMEs may initially adopt basic fraud detection tools and gradually increase their investment in more sophisticated systems as they achieve financial stability. Furthermore, their smaller size enables SMEs to foster closer relationships with employees and stakeholders, making it easier to cultivate a culture of vigilance and integrity, which is vital for effective fraud risk management.

However, SMEs tend to lag in sustainable risk management practices. Many SMEs do not adopt formalized systems for identifying and managing risks, leaving them vulnerable to fraud and cybersecurity threats (Brustbauer 2016). The absence of a structured risk management approach can have long-term implications, including revenue losses, legal penalties and reputational damage. As SMEs scale their operations, these risks become increasingly complex, making it even more essential to integrate fraud risk management into their overall business strategy.

SMEs' governance and regulatory environments also influence their ability to manage risks. In regions with stringent regulatory requirements, SMEs may be compelled to adopt more formal risk management practices to comply with these standards. For example, businesses operating in jurisdictions governed by data protection laws, such as the European Union's General Data Protection Regulation (GDPR), must implement robust measures to prevent data breaches and fraud. In such cases, compliance can motivate SMEs to engage in risk management practices (Rostami et al. 2015). However, where regulatory demands are more lenient, SMEs may limit their engagement with risk management, only addressing it to meet the most basic compliance standards.

Fraud risk management also plays a role in mitigating technology-enabled threats, particularly cybersecurity risks. As SMEs adopt digital tools and platforms, they expose themselves to potential fraudsters and cybercriminals who can exploit weak security systems. Cyberattacks, such as phishing, ransomware and data breaches, can have catastrophic consequences for SMEs, resulting in significant financial losses, operational disruptions and erosion of customer trust (Algamdi et al. 2025).

An effective fraud risk management system, combined with basic cybersecurity measures such as firewalls, encryption and employee training, can help small to medium-sized enterprises (SMEs) mitigate these risks.

The adoption of a risk management framework is essential for SMEs' business continuity and resilience. Although limited resources may constrain their ability to implement advanced systems, risk management should not be viewed as an optional practice but as a necessity for long-term success. An entrepreneur's ability to swiftly assess and respond to emerging risks, including fraud, is vital for the enterprise's short- and long-term survival (Farrell and Gallagher 2014). The key is for SMEs to embrace their flexibility, scale their risk management efforts as resources allow and integrate fraud prevention into their business practices as they grow.

Although SMEs face significant challenges in adopting comprehensive fraud risk management systems due to their inherent resource limitations, their agility and flexibility provide opportunities to implement scalable solutions. By embedding risk management into their organizational culture and operations, SMEs can protect themselves from fraud and cyber threats, ensuring long-term sustainability and competitiveness in an increasingly digitalized economy.

Table 1 distinguishes the conceptual elements and ties each construct to the dynamic capability process stage. In alignment with Teece (2007), the paper maps FRM as a structural resource supporting seizing, FA expertise as a resource that enhances sensing through investigative analysis and culture as a strategic resource that enables reconfiguration by fostering learning and adaptation (Teece 2007; Wang and Ahmed 2007).

The classifications above suggests that although DC can be defined as a higher-order process by which firms integrate, reconfigure and renew resources to address changing environments (Jin et al. 2024; Teece 2007; Wang and Ahmed 2007), forensic accounting aids in detecting emerging threats (sensing), fraud-risk management involves mobilizing controls to respond (seizing) and cyber-aware culture enables continuous adaptation and realignment of the organization (reconfiguring). Hence, forensic accounting, when strategically used, fits the DC definition by helping firms identify and act on new fraud threats, thus behaving dynamically rather than as a routine function (Arndt et al. 2022; S. Ahmad et al. 2025). Fraud-risk management on the other hand is presented as an internal control system (resource-based competency) which is an essential organizational resource/capability that SMEs have, but which by itself is relatively routine (an ordinary capability) unless enhanced by dynamic use (Jin et al. 2024; Sukumar et al. 2023; Vogel and Güttel 2013). Finally, cyber-aware culture is an intangible resource (part of a firm's human and social capital) that underpins the firm's ability to learn and change (Bleady et al. 2018; Chatterjee et al. 2024). Thus, culture enables DC by fostering learning and agility.

Critically, cyber threats and fraud risks are deeply interconnected. Many cyberattacks manifest as, or lead to, financial fraud, including unauthorized transactions, business email compromise, ransomware payment demands and data theft for identity fraud (Abdul Mumin et al. 2024; Zainal et al. 2022).By treating FRM as a foundational cybersecurity resource, SMEs address both financial and digital risks through integrated controls. The FRM infrastructure (e.g., monitoring stems, audit access controls) serves dual purposes, supporting both fraud prevention and cyber defence (Bozkus Kahyaoglu and Caliyurt 2018).

3.2 | Forensic Accounting: A Knowledge Resource Enhancing Threat Detection

Forensic accounting (FA) is a specialized knowledge-based resource that combines accounting, investigative, auditing, criminality and legal expertise to identify financial irregularities, quantify losses and support investigations or litigation (Awolowo 2019). Traditionally associated with post-incident fraud investigation, this framework reconceptualizes FA as a proactive knowledge resource that enhances SMEs' cybersecurity assurance capabilities. From an RBV perspective, FA expertise constitutes a valuable, rare and inimitable resource. It is valuable because FA skills enable the detection of sophisticated fraud schemes that evade automated controls (Afriyie et al. 2023); rare because specialized FA training is uncommon, particularly in SME contexts where generalist accountants dominate (Lavia López and Hiebl 2015); inimitable because FA expertise develops through accumulated experience, tacit knowledge and a cross-disciplinary integration difficult for competitors to replicate (Popoola 2014); and nonsubstitutable as algorithmic tools cannot fully replace human judgment in

TABLE 1 | Classification of framework elements.

Construct	RBV classification	Ordinary capability function	Dynamic capability role
Fraud risk management (FRM)	Structural resource: Embedded systems, protocols and processes for fraud identification and mitigation (Abdul Mumin et al. 2024; Mishra et al. 2019)	Ordinary capability when routinely deployed. Routine fraud monitoring, compliance checking and standard auditing procedure (Winter 2003)	Provides foundational infrastructures supporting all three DC processes: generating data for sensing, enabling protocol-driven seizing and facilitating systematic reconfiguration (Abdul Mumin et al. 2024; Jin et al. 2024; Teece 2007; Wang and Ahmed 2007). However, on its own, it is not a higher-order adaptive process (Sukumar et al. 2023).
Forensic accounting (FA)	Knowledge-based resource: specialized investigative, analytical and cross-disciplinary expertise (Awolowo 2019; Popoola 2014)	Standard post-incident fraud investigation following established methodologies (Winter 2003). DC when embedded in continuous learning cycles	Enhances sensing through investigative expertise; supports seizing through evidence provision; enables reconfiguration through post-incident insights and root cause analysis (Arndt et al. 2022; S. Ahmad et al. 2025). Its socially complex and path-dependent nature makes it difficult to imitate, providing a sustainable advantage (Jin et al. 2024; Teece 2007; Vogel and Güttel 2013; Wang and Ahmed 2007). It helps firms to reconfigure controls post-incident, fulfilling the criteria of a DC (sensing, seizing and reconfiguring) (Helfat and Peteraf 2015).
Cyber-aware culture	Intangible resource: shared values, norms and behavioural patterns related to cybersecurity (Akter et al. 2022; Corradini 2020; Reegård et al. 2019)	Baseline security-conscious behaviours and compliance with established protocols (Winter 2003). Intangible resource; meta-capability enabling adaptation.	Functions as meta-capability/enabler amplifies DC processes: mobilizes distributed human sensing and open communication, facilitates organizational cooperation for seizing (through rapid escalation and collective responsibility) and provides learning infrastructure for reconfiguring (through learning orientation and behavioural adaptability) (Bleady et al. 2018; Chatterjee et al. 2024). It absorbs knowledge and reorients the firm when needed (Özkul and Pamukçu 2012; Popoola 2014).

Note: This classification follows the three-tier conceptual framework: (1) resources are organizational assets the firm possesses (RBV); (2) ordinary capabilities emerge from routine deployment of resources (Winter 2003); (3) DCs arise from strategic integration and orchestration of resources to sense, seize and reconfigure in response to environmental change (Teece 2007; Helfat and Peteraf 2015). Critically, no single element exclusively maps to one DC process. Rather, the systemic integration of all three resources enables the full sensing-seizing-reconfiguring cycle (Schilke et al. 2018; Teece 2018a, 2018b).

complex fraud investigations requiring contextual interpretation (Carpenter et al. 2011).

When deployed routinely, FA functions as an operational capability, with forensic accountants conducting investigations following standardized methodologies (Winter 2003). However, when embedded into continuous organizational learning cycles, FA transcends operational status to become a DC enabler (Eisenhardt and Martin 2000). This elevation occurs through three mechanisms aligned with Teece's (2007) DC framework, first, as a sensing enhancement. FA expertise enhances organizational sensing; the capacity to scan, interpret and learn from environmental signals (Teece 2007). Forensic accountants apply investigative techniques to detect latent threats, including anomaly detection, red flag interpretation and forensic data analysis. FA-trained auditors identify irregular transaction patterns, unexpected account relationships or statistical outliers that indicate potential fraud or compromise (S. B.M. Ahmad et al. 2021). FA expertise also enables the recognition of subtle indicators that generalist accountants might overlook, such as unusual transaction timing, inconsistent documentation or behavioural warning signals (Popoola et al. 2014). Likewise, FA practitioners use specialized analytical methods to interrogate large datasets, uncovering hidden relationships or trends indicative of cyber-fraud (Daraojimba et al. 2023). Significantly, sensing through FA is not passive monitoring but active investigation, probing beyond surface-level data to uncover concealed threats (Awolowo 2019).

Second, FA serves as a source of support. When threats are detected, FA expertise supports the seizing process by providing an evidentiary foundation for response actions such as incident investigation, cross-functional coordination and decision support (Teece 2007). FA skills enable a rapid, thorough investigation of suspected breaches, documenting evidence chains, quantifying financial impact and identifying attack vectors (Fisher and Hines 2024). Forensic accountants also bridge financial, IT and legal functions during response, facilitating coordinated action (Bwerinofa-Petrozzello 2021). Moreover, FA analysis provides leadership with an accurate assessment of incident severity, guiding resource allocation during response (S. Ahmad et al. 2025).

Third, FA acts as a contributor to reconfiguration. Post-incident, FA insights inform organizational learning and control reconfiguration, such as root cause analysis, control redesign and organizational learning. FA investigations reveal not just what happened but why. Identifying control weaknesses, procedural gaps or cultural factors that enabled the breach (Awolowo 2019; Daraojimba et al. 2023). FA recommendations guide targeted improvements to FRM systems, closing specific vulnerabilities rather than implementing generic security measures (Afriyie et al. 2023; Odeyemi et al. 2024; Popoola 2014), and likewise by documenting fraud mechanisms and control failures. FA creates institutional knowledge that informs training, policy updates and cultural change (S. Ahmad et al. 2025).

The critical question is: Why classify FA as a DC rather than merely a resource? The answer lies in FA's dual nature. As expertise held by individuals, FA is a resource (human resource). However, when institutionalized through organizational routines such as regular forensic audits, embedded FA-trained internal auditors and the systematic application of forensic techniques to cybersecurity, FA becomes a capability (Eisenhardt and Martin 2000). More specifically, FA becomes dynamic when it enables continuous adaptation. As Teece (2018a, 2018b, 40) argues, "dynamic capabilities involve the capacity to renew competencies to achieve congruence with the changing business environment". Forensic accounting precisely provides this renewal function by enabling SMEs to detect, interpret and adapt to emerging fraud and cybersecurity threats that evolve faster than static controls can address (Wang and Ahmed 2007).

This framing aligns with Helfat and Peteraf's (2015) emphasis on microfoundations (i.e., the individual-level skills, processes and structures that underlie organizational capabilities). FA expertise serves as a microfoundation for cybersecurity dynamic capabilities, providing the investigative capacity necessary for effective sensing and learning. Although some studies emphasize the need for internal auditors to develop digital literacy and IT skills (Betti and Sarens 2021; Sledgianowski et al. 2017; Zhang et al. 2015), this paper argues for incorporating forensic accounting skills into SMEs' internal control mechanisms. Forensic accounting is a high-level validation of financial information that utilizes skills from various disciplines, including accounting, auditing, criminology and law (Awolowo 2019; Morgan 2020). These multifaceted skills are essential for addressing the implications of cyber threats.

Fisher and Hines (2024) highlight that forensic accountants can collaborate with cybersecurity specialists on "pre-incident processes and controls" as well as "post-incident remediation of a cybersecurity issue". Specifically, Bwerinofa-Petrozzello (2021) notes forensic accountants' involvement in organizations' fraud risk assessments, including identifying vulnerabilities to cyber risks and developing response and recovery plans. Moreover, internal auditors can leverage forensic accounting skills to prevent and detect cybercrimes and financial fraud before losses occur. This does not imply a replacement of roles but rather a collaboration that enhances the effectiveness of both functions. Internal audit functions are integral to an organization's governance practices (DeZoort and Harrison 2018). Thus, equipping internal auditors with the skills and techniques characteristic of forensic accountants can improve their sensitivity to cyber threats and vulnerabilities within their organization's internal control systems (Fisher and Hines 2024).

Studies have shown that accounting students trained in forensic accounting exhibit greater proficiency in assessing fraud risks than those who have not received such training (Carpenter et al. 2011). This suggests that traditional auditing education may inadequately prepare auditors to recognize fraud indicators and assess risk effectively. However, the multidisciplinary dimensions of forensic accounting education enhance auditors' ability to employ relevant skills and techniques in practice (Kumari Tiwari and Debnath 2017).

Daniels et al. (2013) have underscored the importance of incorporating forensic accounting and fraud-related topics into accounting curricula to equip future accountants with the necessary skills to tackle fraud. Although they did not focus specifically on cybercrime, their findings imply that strengthening forensic accounting training can enhance internal auditors' ability to identify fraud risks and provide cybersecurity assurance in SMEs.

Forensic accounting skills, including critical thinking, analytical abilities, problem-solving, communication and investigative skills, are essential for fraud prevention and detection (Abidoye et al. 2023). By incorporating these skills, internal auditors can collaborate more effectively with cybersecurity specialists to identify control weaknesses and respond to incidents more effectively. Additionally, they can support the design of control protocols that detect unusual occurrences, enhancing overall risk management.

Entrepreneurs must cultivate a culture of cyber situational awareness, recognizing the long-term value of internal auditors as a protective mechanism against cyber insecurity. For SMEs, equipping internal auditors with forensic accounting skills can improve cost efficiency while addressing resource constraints. Furthermore, whether employing in-house or outsourced auditors, SMEs should ensure that internal audit functions include forensic accounting training to bolster their technical competence and proficiency.

This approach will enable SMEs to leverage internal auditors' expertise as they navigate the complexities of fraud and cyber risk management. The potential impact of a single cyber incident on business operations, customers and the wider community is significant. Hence, SMEs must view fraud risk management and cybersecurity assurance as strategic assets essential for business continuity and socio-economic development. In summary, integrating forensic accounting skills within internal audit functions is vital for effectively enhancing SMEs' capacity to manage fraud and cybersecurity risks. By fostering collaboration between internal auditors and IT specialists, SMEs can develop a comprehensive risk management strategy that addresses immediate threats and safeguards their long-term viability. The key insight is that FA need not reside in a single individual but can be distributed across the organization through training, tools and collaborative routines (Steinbart et al. 2018).

3.3 | Cyber-Aware Organizational Culture: An Intangible Resource Fostering Organizational Adaptation

Organizational culture represents a powerful yet intangible resource that fundamentally shapes how individuals perceive, prioritize and respond to cybersecurity threats (Akter et al. 2022; Zwilling et al. 2022). For SMEs, where informal communication channels and centralized leadership amplify influence, cyber-aware culture functions as both a critical vulnerability and strategic opportunity (Wilson and McDonald 2023). From the perspective of RBV, cyber-aware organizational culture constitutes a valuable, inimitable resource. It is valuable because it shapes employee behaviour, the human element responsible for most cybersecurity failures through errors, negligence or circumvention of controls (Wilson and McDonald 2025; Zwilling et al. 2022). Culture is rare as genuine security-conscious cultures require sustained leadership commitment and behavioural change, which few SMEs achieve (Renauld and Ophoff, 2022). Culture is inimitable due to its socially complex, path-dependent nature, as competitors cannot easily replicate the accumulated norms, values and routines that define organizational culture (Barney 2001). Finally, culture is nonsubstitutable, as technical controls alone cannot compensate for an organization where employees routinely ignore security protocols or fail to report anomalies (Algamdi et al. 2025). Although culture itself is a resource, it functions as a meta-capability (an enabler that amplifies other capabilities (Doherty and Terry 2013).

Specifically, cyber-aware culture contributes to all three DC processes. First, as sensing amplifiers, employees trained to recognize phishing attempts, social engineering or unusual system behaviour serve as distributed sensors, vastly expanding detection beyond automated monitoring (A. Naseer et al. 2023). More so, cultural norms encouraging information sharing ensure that observations and concerns flow upward rather than being suppressed (Reegård et al. 2019). In addition, a learning-oriented culture encourages employees to investigate anomalies rather than dismissing them as insignificant (Akter et al. 2022). Second, as a seizing facilitator, culture enables effective seizing by ensuring organizational cooperation during response. Cultural norms mandating immediate reporting of security incidents reduce response delays (Wong et al. 2022). Also, a unified security culture facilitates coordination between IT, finance, operations and leadership during a crisis response (Steinbart et al. 2018). Moreover, when security is perceived as everyone's concern, employees actively participate in response efforts rather than deferring to specialists. Third, as a reconfiguring foundation, culture provides the adaptive capacity necessary for organizational reconfiguration. A culture that values continuous improvement treats post-incident reviews as opportunities for enhancement rather than blame exercises (Bleady et al. 2018; Chatterjee et al. 2024). Cyber-aware cultures normalize periodic changes to security practices, reducing resistance to new protocols or tools (Zhou et al. 2020). In addition, the cultural embedding of security lessons ensures that knowledge persists beyond individual turnover, thereby creating organizational resilience (Reegård et al. 2019). As Wang and Ahmed (2007) categorize DCs, "adaptive capability" describes the firm's ability to adjust to environmental changes. Cyber-aware culture embodies this adaptive capacity by fostering an organization-wide capacity to learn, adjust and evolve security practices in response to emerging threats. However, this will require organizational members to be proactive and imbibe cybersecurity awareness.

Cybersecurity awareness refers to the condition in which individuals within firms possess a comprehensive understanding of risks and security processes, bolstered by fundamental knowledge and the ability to identify and respond to security threats. This is a valuable resource that can mitigate threats when harnessed appropriately. Organizations that foster a cyber-aware culture recognize the importance of accountability in a dynamic environment. They adeptly tackle cybersecurity challenges while adhering to the policies and regulations established by their organization's security objectives, the training programs they engage in and the regulatory authorities (Akter et al. 2022; Rahim et al. 2015; Wong et al. 2022; Zwilling et al. 2022).

Cybersecurity awareness emphasizes the essential skills required to protect individuals from social engineering attacks. Social engineering occurs when an individual's psychological traits are used to facilitate a harmful cyberattack (A. Naseer et al. 2023). Kovačević and Radenković (2020) assert that cybersecurity awareness must be seen as an ongoing effort due to the possibility of both anticipated and unforeseen attacks. Capability is characterized by integrating and coordinating robust, consistent abilities that are employed efficiently and appropriately in response to diverse, both expected and unexpected, situations (Nagarajan and Prabhu 2015).

DC, based on the notion of capability, may be categorized into three essential processes: (a) coordination/integration (a static idea), (b) learning (a dynamic concept) and (c) reconfiguration (a transformational concept) (Teece et al. 1997). The DC theory extends the RBV, positing that firms possessing valuable, rare, inimitable and nonsubstitutable resources can attain a sustainable competitive advantage through the execution of innovative value-creating strategies that are challenging for competitors to imitate (Barney 2001; Schilke et al. 2018). This research defines cyber-aware organizational culture as IT-integrated dynamic capabilities characterized by an organization's capacity to assimilate, activate and employ cyber-awareness strategies and resources to respond efficiently and effectively to cybersecurity incidents and threats. The primary aim of cybersecurity awareness is to modify individuals' behaviour to ensure they respond appropriately to cyber threats (Akter et al. 2022).

Employees' comprehension of cybersecurity awareness as a valuable resource may enhance their disposition towards cybersecurity compliance (Goel et al. 2023). Gandhi (2017) characterized cybersecurity awareness as the extent to which an individual understands cybersecurity, adheres to regulations and is dedicated to an organization's objectives. Zhou et al. (2020) present empirical evidence demonstrating the significant impact of psychological factors, including self-efficacy, risk awareness and social support, on an individual's cybersecurity awareness and the technological security linked to a specific technology or asset. Poepjes and Lane (2012) emphasize the importance of understanding how individuals develop and regulate awareness through personal proficiency in decision-making contexts. A lack of cybersecurity awareness makes businesses vulnerable to cyberattacks, compromising critical resources and increasing risk. Typically, cybercriminals target individuals within organizations who are easily vulnerable. Brandenburg and Paul (2020) observed that remote or semiremote work environments have hampered a firm's ability to identify these hazards.

One of the five components of risk management, as defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), is “Governance and Culture” (COSO 2019). This concept highlights the importance of culture in fostering an agile cybersecurity approach as part of a broader organizational risk management strategy. COSO emphasizes that the SME owner or managerial lead is responsible for “defining the desired behaviours that characterize the entity's desired culture” (COSO 2019, 5). Without this top-down leadership, accountants, internal auditors and other employees may struggle to implement and enforce effective cyber-risk and fraud risk management processes.

This top-down tone is critical for the success of cybersecurity initiatives. By setting the right tone from the top, SME leaders create an environment where cybersecurity is viewed not merely as a technical requirement but as an integral part of business continuity and growth. Lloyd (2020) argues that integrating cybersecurity into the culture as a strategic opportunity rather than a burden can drive innovation and resilience. In contrast, if leaders view cybersecurity as secondary or irrelevant, employees are unlikely to prioritize it, making the organization more vulnerable to cyberattacks.

Leadership's role in shaping this culture is further underscored by research that shows SMEs often underestimate their vulnerability to cyber threats. Wilson and McDonald (2023) highlight common misperceptions among SME leaders, including the belief that their business is too small to be targeted or that their existing security measures are sufficient. These misconceptions can lead to complacency, leaving SMEs exposed to significant risks. However, when leaders recognize the importance of cybersecurity, they are more likely to allocate the necessary resources and attention to this area, thus fostering a culture of vigilance.

Promoting a cybersecurity-focused culture also positions SMEs as socially responsible entities. Lloyd (2020) notes that organizations that emphasize cybersecurity protect themselves and contribute to the broader societal and economic ecosystem. For example, an SME that falls victim to a cyberattack can experience supply chain disruptions, loss of consumer trust and negative financial impacts, which can ripple through the local and national economy. Thus, by prioritizing cybersecurity, SME owners protect their businesses, customers, partners and the broader community.

To effectively adopt such a culture, SMEs must embrace the concept of “cyber situational awareness”. Renaud and Ophoff (2021) define this as understanding an organization's cybersecurity environment, including potential risks and threats. For SMEs, developing cyber situational awareness can be constrained by resource limitations, including finances, expertise and operational capacity. However, the lack of awareness and understanding can further exacerbate their vulnerabilities. Renaud and Ophoff (2021) argue that a combination of low situational awareness and limited resources leads SMEs to adopt minimal cybersecurity measures, making them easy targets for cybercriminals.

Wilson and McDonald (2023) similarly identify that awareness, or the lack thereof, is a major challenge for SMEs regarding cybersecurity. They assert that SME leaders must be more aware of cybersecurity risks and implications than their employees because leadership drives the organization's overall risk posture. When informed and proactive, leaders set the tone for a cybersecurity-conscious culture, prioritizing vigilance and risk management. This leadership-driven awareness is crucial for encouraging employees to adopt and consistently maintain effective cybersecurity best practices.

In fostering this awareness, SME owners and managers must also view cybersecurity as part of their social responsibility. Given the interconnected nature of business in today's globalized economy, a breach in one SME can have wide-reaching effects, particularly if it is part of a larger supply chain. By embedding cybersecurity into their organizational culture, SMEs protect their interests and contribute to the stability and security of their partners, customers and the wider economy. This perspective positions cybersecurity as a strategic, ethical and practical imperative for SMEs.

To effectively implement this cultural shift, SMEs must overcome their financial and operational limitations by adopting proportionate cybersecurity measures that align with their capabilities. Although SMEs may not have the resources of larger corporations, they can still take meaningful steps to protect themselves. This could include regular employee training, robust password policies and cybersecurity tools tailored to their needs. Wilson and McDonald (2023) suggest that leaders who adopt a long-term view and commit to building a cybersecurity-conscious culture are better positioned to safeguard their businesses and contribute positively to the broader economy.

Organizational culture is a key determinant of how effectively SMEs manage cybersecurity risks. Leadership plays a pivotal role in defining and promoting this culture, setting the tone for how cybersecurity is integrated into daily operations. By embracing a proactive, socially responsible approach to cybersecurity, SME leaders can ensure the long-term sustainability and competitiveness of their businesses while also protecting their stakeholders and the broader economy from the cascading effects of cyberattacks.

The preceding sections establish that FRM, FA and culture are strategic resources. The critical insight is that DCs do not reside in individual resources but in the firm's capacity to integrate and reconfigure them (Teece 2007, 2018a, 2018b). Thus, an SME develops cybersecurity DCs when it (a) uses forensic accounting expertise and FRM monitoring and cultural vigilance to sense emerging threats, (b) activates FRM response protocols supported by FA investigation and employee cooperation to seize response opportunities and (c) updates FRM controls informed by FA insights embedded through cultural learning to reconfigure defences. This integrated system, not in any single element, constitutes the dynamic capability for cyber resilience (Helfat and Peteraf 2015; Schilke et al. 2018).

This framework advances beyond technology-centric cybersecurity models by positioning cyber resilience as an organizational capability rooted in a coordinated deployment of strategic resources. The framework emphasizes internal capability development over external tool acquisition, making it particularly relevant for resource-constrained SMEs that must maximize returns on limited security investments (Arroyabe et al. 2024; Sukumar et al. 2023). Moreover, each element aligns with established DC literature: FRM provides the structural scaffolding (organizational routines) emphasized by Eisenhardt and Martin (2000); FA supplies specialized knowledge (microfoundations) highlighted by Helfat and Peteraf (2015); and culture enables organizational transformation (adaptive capacity) central to Wang and Ahmed's (2007) DC typology. Together, they form a theoretically grounded, actionable framework for SME cybersecurity assurance.

4 | Conceptual Contributions

This paper presents a novel, integrative conceptual framework for cybersecurity assurance tailored to SMEs, combining organizational culture, fraud risk management and forensic accounting. Although prior research has explored technical or isolated approaches, this framework stands out by embedding cybersecurity within core organizational capabilities and positioning it as a strategic, cross-functional asset.

4.1 | Cybersecurity as a Strategic Asset

A key contribution of this paper is reframing cybersecurity from a reactive, compliance-based function to a proactive, strategic asset. Unlike conventional approaches that treat cybersecurity as a cost centre, our framework encourages SMEs to integrate cybersecurity into business strategy, enhancing customer trust, operational continuity and long-term competitiveness.

4.2 | Forensic Accounting as a Cyber Resilience Enabler

Although forensic accounting is typically associated with financial investigations, this paper advances its role as a DC that supports cybersecurity assurance. By applying forensic methods to detect anomalies, reconstruct events and quantify losses, SMEs can strengthen the incident response and recovery, an underexplored dimension in existing SME-focused cybersecurity models.

4.3 | Organizational Culture as a Cyber Defence Layer

The framework highlights organizational culture not just as a supporting factor but as a core defencive resource. It promotes leadership-driven awareness, accountability and employee engagement in cybersecurity practices. This socio-behavioural focus distinguishes the framework from technology-centric models.

4.4 | Integrated Fraud Risk Management

The integration of fraud risk management into cybersecurity is another distinguishing feature. Although many frameworks address these separately, this paper emphasizes their interdependence. SMEs can enhance resilience by embedding risk-based controls, audits and employee training into both financial oversight and cybersecurity processes.

4.5 | A Multidisciplinary, Holistic Approach

Most importantly, this framework offers a holistic and multidisciplinary approach, bringing together finance, audit, risk, culture and IT. This cross-functional collaboration is rarely addressed in SME cybersecurity literature, yet it is essential given SMEs' limited resources and siloed structures.

In summary, this framework transcends traditional or siloed approaches by providing SMEs with an actionable, strategy-driven model for cyber resilience, grounded in internal capabilities rather than relying solely on external tools.

5 | Conclusion

This paper proposes a novel framework for enhancing cybersecurity assurance in SMEs by integrating fraud risk management, forensic accounting and a cyber-aware organizational culture. Grounded in the resource-based view and dynamic capability theory, the study repositions cybersecurity as a strategic organizational function rather than a purely technical concern.

By identifying fraud risk management, forensic accounting and organizational culture as strategic resources and by explicating their integration as sources of dynamic capabilities, the framework offers a more holistic and adaptive approach to cyber resilience. This perspective addresses the limitations of traditional security models and provides a context-specific strategy for SMEs navigating an increasingly hostile digital environment. This study contributes to the growing literature on SME cybersecurity by highlighting the importance of internal capabilities that promote proactive threat detection, organizational learning and sustained preparedness in the face of evolving cyber risks.

5.1 | Practical and Policy Implications

This study provides a framework that offers a holistic and adaptive approach to cyber resilience by outlining concrete guidance for SME managers using illustrative examples. The conceptual framework establishes fraud risk management, forensic accounting and cyber-aware culture as strategic resources that collectively enable sensing, seizing and reconfiguring capabilities. Although FRAM infrastructure primarily supports rapid response mobilization (seizing), FA expertise primarily enhances threat detection (sensing), and culture primarily enables organizational adaptation (reconfiguring); these resources function systematically, each contributing to all three DC processes through their integration (Teece 2018a, 2018b).

This contribution offers practical guidance not only to SME leaders but also to policymakers and practitioners seeking concrete strategies to enhance cybersecurity in the SME sector. These practices align with the DC approach which emphasizes continuously adapting and reconfiguring organizational competencies to tackle evolving threats. Hence, SMEs must be agile in sensing new cyber-fraud risks, responding swiftly and learning from incidents to improve resilience.

In resource-constrained SMEs, it is recommended that they implement basic forensic accounting procedures such as periodically reviewing financial records for anomalies and training an existing finance employee in forensic methods. This can adopt cost-effective methods such as outsourcing occasional forensic audits to consultants on an as-needed basis, or by using low-cost software tools for anomaly detection, rather than maintaining a full in-house team. Although SMEs face an inherent low-budget challenge, they can leverage government-subsidized programs or university partnerships to obtain forensic expertise at minimal cost. Embracing forensic accounting leads to early fraud detection and organizational learning. Investigations have the potential to reveal control weaknesses or new fraud schemes, and these insights should feed back into improved controls and training.

In order to strengthen fraud risk management, SMEs should implement robust internal controls and clear fraud prevention policies, drawing on established frameworks such as COSO, but tailoring these frameworks to reflect their size, resources and operational complexity. They can adopt segregation-of-duties in accounting processes, using off-the-shelf accounting software features to flag unusual transactions and scheduling regular (quarterly or biannual) fraud risk assessments, with the help of external advisors if internal skills are lacking. Because SME staffs wear multiple hats which can make segregation difficult, SME owners can provide an oversight on financial reports or by rotating responsibilities. This means that simple in-house assessments can reveal critical gaps and guide where to focus limited resources. To overcome resource constraints, SMEs can leverage external guidance and support.

A strong organizational culture of security is pertinent. Cybersecurity is as much a culture as about technology, and SME leaders must make security everyone's responsibility, not just an IT issue. To enhance a cyber-aware culture, this paper recommends that SMEs should cultivate cybersecurity awareness among all employees. This can involve tangible measures such as conducting regular and brief training sessions on cybersecurity issues, and, importantly, leaders should set the tone. SME owners/managers should visibly prioritize cybersecurity in meetings and policies. Employees' buy-ins should be encouraged by explaining the importance of cybersecurity in protecting the survival of the business to motivate engagement. Creating a culture of vigilance means that employees actively watch for and report anomalies. This paper further recommends that leaders should foster a no-blame environment for reporting suspicious activities or mistakes so that personnel feel empowered to raise concerns early. This means that security concerns must be reinforced continuously. Thus, by embedding cybersecurity into daily operations, employees become a human security system, and the SMEs can adapt quickly to new threats.

Table 2 summarizes the practical recommendations. How SMEs can implement the recommendations and the expected benefits.

Specifically, policymakers could consider implementing targeted measures to address the unique vulnerabilities of Canadian SMEs, such as offering tax incentives for businesses that adopt fraud risk management systems, funding subsidized training programs in forensic accounting and cyber-risk response and creating shared cybersecurity resource centres that provide access to tools, expertise and simulation environments.

By incorporating these recommendations into policy and practice, stakeholders can develop a more adaptive, inclusive and effective cybersecurity assurance model that meets the evolving needs of SMEs, particularly in Canadian and similarly structured economies. This study contributes to the growing

TABLE 2 | Practical recommendations.

Recommendations	How to implement	Expected benefit
Establish a fraud risk management program	Perform regular fraud risk assessments; establish antifraud policies and internal controls (e.g., segregate duties, dual approvals); prepare a basic fraud response plan. Use external templates or advisors if needed.	Reduces opportunities for fraud and potential losses; ensures a proactive, structured approach to fraud prevention; improved stakeholder confidence in the business.
Integrate forensic accounting in oversight	Schedule periodic forensic audits of financial records; use data analytics tools to flag anomalies; train finance staff in forensic techniques or hire a forensic accountant for investigations as needed.	Detects fraud and errors early, before they escalate; provides evidence to support legal action if needed; deters fraud through visible oversight and scrutiny.
Build a cyber-aware culture	Provides an ongoing cybersecurity and fraud-awareness training for all employees; leadership consistently reinforces security expectations; runs periodic phishing email tests and maintains open channels for reporting incidents	SME employees act as vigilant "human sensors" catching and reporting threats that technical controls might miss; faster response to incidents limits damage; fosters an adaptive, resilient workforce.
Implement essential technical safeguards	Enforce strong passwords and multifactor authentication; keep software updated with security patches; regularly back up important data; use firewalls and anti-malware free or low-cost security tools when possible.	Mitigates common cyberattack and fraud vectors (phishing, malware); limits damage from breaches (data can be restored); improves overall cyber hygiene with minimal financial investment.
Leverage external security expertise	When possible, outsource to management security service providers for 24/7 monitoring and incident response; consult cybersecurity/fraud experts for perioding training, consider cyber insurance to transfer risks associated with major incidents	Access to specialized knowledge and round-the-clock protection without hiring full-time staff; improved ability to prevent and respond to incidents; financial protection (insurance payout) if a serious breach or fraud happens.

literature on SME cybersecurity by highlighting the importance of internal capabilities that promote proactive threat detection, organizational learning and sustained preparedness in the face of evolving cyber risks.

Funding

The authors have nothing to report.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

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

References

Abdul Mumin, M., I. O. Adam, and M. D. Alhassan. 2024. "The Impact of ICT Capabilities on Supply Chain Fraud and Sustainability–A Dynamic Capability Perspective." *Technological Sustainability* 3, no. 2: 123–146. https://doi.org/10.1108/techs-11-2023-0051.

Abidoye, A., I. F. Awolowo, and D. Chan. 2023. "Bridging the Gap: Integrating Forensic Accounting Skillsets for Enhanced Audit Quality in the Post-Pandemic Era." *Journal of Forensic Accounting Profession* 3, no. 2: 63–81. https://doi.org/10.2478/jfap-2023-0010.

Adejumo, A., and C. Ogburie. 2025. "Forensic Accounting in Financial Fraud Detection: Trends and Challenges." *International Journal of Science and Research Archive* 14, no. 3: 1219–1232. https://doi.org/10.30574/ijsra.2025.14.3.0815.

Afriyie, S. O., M. O. Akomeah, G. Amoakohene, B. C. Ampimah, C. E. Ocloo, and M. O. Kyei. 2023. "Forensic Accounting: A Novel Paradigm and Relevant Fraud Detection and Prevention Knowledge." *International Journal of Public Administration* 46, no. 9: 615–624. https://doi.org/10.1080/01900692.2021.2009855.

Ahmad, S., M. S. Ibrahim, and R. M. Abdou. 2025. "Understanding the Role of Forensic Accountants in due Diligence Within Organizations and Its Impact on Organizational Learning." *Sustainable Data Management* 1: 3–10. https://doi.org/10.1007/978-3-031-83911-5_1.

Ahmad, S. B. M., K. C. Desouza, J. Kotsias, M. T. Whitty, and R. L. Baskerville. 2021. "How Can Organisations Develop Situation Awareness for Incident Response: A Case Study of Management Practice." *Computers & Security* 101: 102–122. https://doi.org/10.1016/j.cose.2020.102122.

Akter, S., M. R. Uddin, S. Sajib, W. J. T. Lee, K. Michael, and M. A. Hossain. 2022. "Reconceptualising Cybersecurity Awareness Capability in the Data-Driven Digital Economy." *Annals of Operations Research*: 1–26. https://doi.org/10.1007/s10479-022-04844-8.

Algamdi, S. A., A. W. Khan, and J. Ahmad. 2025. "A Cyber Security Awareness Model for Distributed Teams." *Security and Privacy* 8, no. 5: 1–16. https://doi.org/10.1002/spy2.70074.

Ali, A. B. A., R. K. Ayyasamy, R. Akbar, A. K. Jebna, and K. Adnan. 2025. "Cybersecurity Infrastructure Compliance Key Factors to Detect and Mitigate Malware Attacks in SMEs: A Systematic Literature Review." *Sage Open* 15, no. 1: 21582440251314671. https://doi.org/10.1177/21582440251314671.

Al-Mutawa, B., and M. M. Saeed Al Mubarak. 2024. "Impact of Cloud Computing as a Digital Technology on SMEs Sustainability." *Competitiveness Review* 34, no. 1: 72–91. https://doi.org/10.1108/cr-09-2022-0142.

Anand, B. 2015. “Reverse Globalisation by Internationalisation of Sme’s: Opportunities and Challenges Ahead.” *Procedia - Social and Behavioral Sciences* 195: 1003–1011. https://doi.org/10.1016/j.sbspro.2015.06.359.

Arndt, F., P. Galvin, R. J. Jansen, G. J. Lucas, and P. Su. 2022. “Dynamic Capabilities: New Ideas, Microfoundations, and Criticism.” *Journal of Management and Organization* 28, no. 3: 423–428. https://doi.org/10.1017/jmo.2022.57.

Arroyabe, M. F., C. F. Arranz, I. F. De Arroyabe, and J. C. F. de Arroyabe. 2024. “Exploring the Economic Role of Cybersecurity in SMEs: A Case Study of the UK.” *Technology in Society* 78: 102670. https://doi.org/10.1016/j.techsoc.2024.102670.

Awan, M., and A. Alam. 2025. “Cybersecurity Threats and Defensive Strategies for Small and Medium Firms: A Systematic Mapping Study.” *Administrative Sciences* 15, no. 12: 481. https://doi.org/10.3390/admsci15120481.

Awolowo, I. F. 2019. *Financial Statement Fraud: The Need for a Paradigm Shift to Forensic Accounting*. Sheffield Hallam University.

Barney, J. B. 2001. “Resource-Based Theories of Competitive Advantage: A Ten-Year Retrospective on the Resource-Based View.” *Journal of Management* 27, no. 6: 643–650. https://doi.org/10.1177/014920630102700602.

Betti, N., and G. Sarens. 2021. “Understanding the Internal Audit Function in a Digitalised Business Environment.” *Journal of Accounting and Organizational Change* 17, no. 2: 197–216. https://doi.org/10.1108/JAOC-11-2019-0114.

Bleady, A., A. H. Ali, and S. B. Ibrahim. 2018. “Dynamic Capabilities Theory: Pinning Down a Shifting Concept. Academy of Accounting and Financial Studies.” *Journal* 22, no. 2: 1–16. https://www.abacademies.org/articles/dynamic-capabilities-theory-pinning-down-a-shifting-concept-7230.html.

Bornay-Barrachina, M., Á. López-Cabrales, and A. Salas-Vallina. 2025. “Sensing, Seizing, and Reconfiguring Dynamic Capabilities in Innovative Firms: Why Does Strategic Leadership Make a Difference? BRQ.” *Business Research Quarterly* 28, no. 2: 399–420. https://doi.org/10.1177/23409444231185790.

Bozkus Kahyaoglu, S., and K. Caliyurt. 2018. “Cyber Security Assurance Process From the Internal Audit Perspective.” *Managerial Auditing Journal* 33, no. 4: 360–376. https://doi.org/10.1108/MAJ-02-2018-1804.

Brandenburg, R., and M. Paul. 2020. “Cybersecurity for a Remote Workforce.” July 23, 2020, Retrieved October 17, 2021, from. https://sloanreview.mit.edu/article/cybersecurity-for-a-remote-workforce/.

Breznik, L., M. Lahovnik, and V. Dimovski. 2019. “Exploiting Firm Capabilities by Sensing, Seizing and Reconfiguring Capabilities: An Empirical Investigation.” *Economic and Business Review* 21, no. 1: 1. https://doi.org/10.15458/85451.72.

Brustbauer, J. 2016. “Enterprise Risk Management in SMEs: Towards a Structural Model.” *International Small Business Journal* 34, no. 1: 70–85. https://doi.org/10.1177/0266242614542853.

Bwerinofa-Petrozzello, R. 2021. “Helping Clients Before a Cyberattack.” *Journal of Accountancy* 232, no. 3: 24–29. https://www.journalofaccountancy.com/issues/2021/sep/help-clients-before-a-cyberattack/.

Carpenter, T. D., C. Durtschi, and L. M. Gaynor. 2011. “The Incremental Benefits of a Forensic Accounting Course on Scepticism and Fraud-Related Judgments.” *Issues in Accounting Education* 26, no. 1: 1–21. https://doi.org/10.2308/iace.2011.26.1.1.

Chatterjee, S., N. P. Rana, and Y. K. Dwivedi. 2024. “How Does Business Analytics Contribute to Organisational Performance and Business Value? A Resource-Based View.” *Information Technology & People* 37, no. 2: 874–894. https://doi.org/10.1108/itp-08-2020-0603.

Corradini, I. 2020. “Building a Cybersecurity Culture.” In *Building a Cybersecurity Culture in Organizations. Studies in Systems, Decision and Control*, 284, 63–86. Springer. https://doi.org/10.1007/978-3-030-43999-6_4.

COSO. 2019. “Managing Cyber Risk in a Digital Age.” *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*: Retrieved June 17, 2024, from. https://www.coso.org/_files/ugd/3059fc_cd21b48f95a748fb908882bb1ec96278.pdf.

Daniels, B. W., Y. Ellis, and R. D. Gupta. 2013. “Accounting Educators and Practitioners’ Perspectives on Fraud and Forensic Topics in the Accounting Curriculum.” *Journal of Legal, Ethical and Regulatory Issues* 16, no. 2: 93–106. https://www.researchgate.net/publication/289664095_Accounting_educators_and_practitioners'_perspectives_on_fraud_and_forensic_topics_in_the_accounting_curriculum.

Daraojimba, R. E., O. A. Farayola, F. O. Olatoye, N. Mhlongo, and T. T. Oke. 2023. “Forensic Accounting in the Digital Age: A US Perspective: Scrutinising Methods and Challenges in Digital Financial Fraud Prevention.” *Finance & Accounting Research Journal* 5, no. 11: 342–360. https://www.semanticscholar.org/paper/FORENSIC-ACCOUNTING-IN-THE-DIGITAL-AGE%3A-A-U.S.-AND-Daraojimba-Farayola/bf975831b0e679a1af492f1ac24fda853bf3ed8f.

Deutschland. 2023. “The Heart of the German Economy.” Accessed on March 15th, 2024. https://www.deutschland.de/en/topic/business/german-smes-facts-and-figures-relating-to-a-german-phenomenon#:~:text=56%20percent%20of%20the%20more,of%20German%20exporters%20are%20SMEs.

DeZoort, F. T., and P. D. Harrison. 2018. “Understanding Auditors’ Sense of Responsibility for Detecting Fraud Within Organisations.” *Journal of Business Ethics* 149, no. 4: 857–874. https://doi.org/10.1007/s10551-016-3064-3.

Doherty, N. F., and M. Terry. 2013. “Improving Competitive Positioning Through Complementary Organisational Resources.” *Industrial Management and Data Systems* 113, no. 5: 697–711. https://doi.org/10.1108/02635571311324151.

DSIT - Department for Science, Innovation & Technology. 2025. Official Statistics: Cyber Security Breaches Survey 2025. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025.

Eisenhardt, K. M., and J. Martin. 2000. “Dynamic Capabilities: What Are They?” *Strategic Management Journal* 21, no. 10–11: 1105–1121. https://doi.org/10.1002/1097-0266(200010/11)21:10/11<1105::aid-smj133>3.0.co;2-e.

Eze, C. U., E. C. Ebe, I. M. Okwo, et al. 2022. “Effect of the Capability Component of Fraud Theory on Fraud Risk Management in Nigerian Banks.” *International Journal of Financial Research* 13, no. 1: 90–95. https://doi.org/10.5430/ijfr.v13n1p90.

Falch, M., H. Olesen, K. E. Skouby, R. Tadayoni, and I. Williams. 2023. “Cybersecurity Strategies for Smes in the Nordic Baltic Region.” *Journal of Cyber Security and Mobility* 11, no. 6: 727–754. https://doi.org/10.13052/jcsm2245-1439.1161.

Fallon-Byrne, L., and H. Brian. 2017. “Microfoundations of Dynamic Capabilities for Innovation: A Review and Research Agenda.” *Irish Journal of Management, Sciendo* 36, no. 1: 21–31. https://doi.org/10.1515/ijm-2017-0004.

Farrell, M., and R. Gallagher. 2014. “The Valuation Implications of Enterprise Risk Management Maturity.” *Journal of Risk & Insurance* 82, no. 3: 625–657. https://doi.org/10.1111/jori.12035.

Ferreira de Araújo Lima, P., M. Crema, and C. Verbano. 2020. “Risk Management in SMEs: A Systematic Literature Review and Future Directions.” *European Management Journal* 38, no. 1: 78–94. https://doi.org/10.1016/j.emj.2019.06.005.

Fisher, N. D., and E. Hines. 2024. “Cybersecurity and Forensic Accounting Join Forces to Combat Criminals.” StoneTurn. https://stoneturn.com/insight/cybersecurity-and-forensic-accounting-join-forces-to-combat-criminals/.

Gandhi, A. 2017. “Quantitative Assessment of Information Security Awareness on Informatics Students in a University.” In *Proceedings of the 2017 International Conference on Information Technology*, 346–350.

Gašpar, G., R. Budjač, M. Valášek, M. Bartoň, T. Meravý, and M. Strémy. 2025. “Digitizing SMEs in the EU: A Scalable Model for Retrofitting Machinery to Industry 4.0.” *Applications in Engineering Science* 23: 100230. https://doi.org/10.1016/j.apples.2025.100230.

Ghaderi, Z., L. Beal, and L. Houanti. 2024. “Cybersecurity Threats in Tourism and Hospitality: Perspectives From Tourists Engaging With Sharing Economy Services.” *Current Issues in Tourism*: 1–16. https://doi.org/10.1080/13683500.2024.2353327.

Goel, L., D. Russell, S. Williamson, and J. Z. Zhang. 2023. “Information Systems Security Resilience as a Dynamic Capability.” *Journal of Enterprise Information Management* 36, no. 4: 906–924. https://doi.org/10.1108/jeim-07-2022-0228.

Helfat, C. E., and M. A. Peteraf. 2015. “Managerial Cognitive Capabilities and the Microfoundations of Dynamic Capabilities.” *Strategic Management Journal* 36, no. 6: 831–850. https://doi.org/10.1002/smj.2247.

Innomesanghan, D., E. Kiwamu, S. Butakov, and E. G. AbdAllah. 2025. “Ensuring Information Security in Inclusive Digital Environments.” In *International Conference on Computer Safety, Reliability, and Security*, 240–252. Springer Nature Switzerland.

Jin, X., D. Yang, and M. Rhee. 2024. “How Do Dynamic Capabilities Enable a Firm to Convert the External Pressures into Environmental Innovation? A Process-Based Study Using Structural Equation Modeling.” *Systems* 12, no. 12: 1–20. https://doi.org/10.3390/systems12120561.

Khan, N., S. Furnell, M. Bada, M. Rand, and J. R. Nurse. 2025. “Investigating the Experiences of Providing Cyber Security Support to Small-and Medium-Sized Enterprises.” *Computers & Security* 154: 104448. https://doi.org/10.1016/j.cose.2025.104448.

Khan, O., T. Daddi, and F. Iraldo. 2021. “Sensing, Seizing, and Reconfiguring: Key Capabilities and Organizational Routines for Circular Economy Implementation.” *Journal of Cleaner Production* 287: 125565. https://doi.org/10.1016/j.jclepro.2020.125565.

Kovačević, A., and S. D. Radenković. 2020. “SAWIT—Security Awareness Improvement Tool in the Workplace.” *Applied Sciences* 10, no. 9: 3065. https://doi.org/10.3390/app10093065.

Kumari Tiwari, R., and J. Debnath. 2017. “Forensic Accounting: A Blend of Knowledge.” *Journal of Financial Regulation and Compliance* 25, no. 1: 73–85. https://doi.org/10.1108/JFRC-05-2016-0043.

Lamptey, E. K., and R. P. Singh. 2018. “Fraud Risk Management over Financial Reporting: A Contingency Theory Perspective.” *Journal of Leadership, Accountability and Ethics* 15, no. 4: 66–75. https://doi.org/10.33423/jlae.v15i4.171.

Lavia López, O., and M. R. Hiebl. 2015. “Management Accounting in Small and Medium-Sized Enterprises: Current Knowledge and Avenues for Further Research.” *Journal of Management Accounting Research* 27, no. 1: 81–119. https://doi.org/10.2308/jmar-50915.

Le, T. D., T. Le Dinh, and S. Uwizeyemungu. 2025. “A Cybersecurity Framework for Enhancing Small and medium-sized Enterprises (SMEs) Security Posture Using User Behaviour Analytics.” *Enterprise Information Systems* 19, no. 10: 2529282. https://doi.org/10.1080/17517575.2025.2529282.

Le, T. D., T. Le-Dinh, and S. Uwizeyemungu. 2024. “Search Engine Optimisation Poisoning: A Cybersecurity Threat Analysis and Mitigation Strategies for Small and Medium-Sized Enterprises.” *Technology in Society* 76: 102470. https://doi.org/10.1016/j.techsoc.2024.102470.

Lloyd, G. 2020. “The Business Benefits of Cyber Security for SMEs.” *Computer Fraud & Security* 2020, no. 2: 14–17. https://doi.org/10.1016/S1361-3723(20)30019-1.

Mcbride, K., and C. Philippou. 2022. ““Big Results Require Big Ambitions”: Big Data, Data Analytics, and Accounting in Master's Courses.” *Accounting Research Journal* 35, no. 1: 71–100. https://doi.org/10.1108/ARJ-04-2020-0077.

Mishra, B. K., E. Rolland, A. Satpathy, and M. Moore. 2019. “A Framework for Enterprise Risk Identification and Management: The Resource-based View.” *Managerial Auditing Journal* 34, no. 2: 162–188. https://doi.org/10.1108/maj-12-2017-1751.

Morgan, S. 2020. “Cybercrime to Cost the World $10.5 Trillion Annually by 2025.” *Cybercrime Magazine* 13, no. 11. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/.

Moschella, J., E. Boulianne, and M. Magnan. 2023. “Risk Management in Small- and Medium-Sized Businesses and How Accountants Contribute.” *Contemporary Accounting Research* 40, no. 1: 668–703. https://doi.org/10.1111/1911-3846.12819.

Nagarajan, R., and R. Prabhu. 2015. “Competence and Capability: A New Look.” *International Journal of Management* 6, no. 6: 7–11. https://www.semanticscholar.org/paper/COMPETENCE-AND-CAPABILITY-A-NEW-LOOK-R.Nagarajan-R.Prabhu/a82f5b94d76a14f4fbbf406a5ba459b2f86b6588.

Naseer, A., H. Naseer, A. Ahmad, S. B. Maynard, and A. M. Siddiqui. 2023. “Moving Towards Agile Cybersecurity Incident Response: A Case Study Exploring the Enabling Role of Big Data Analytics-Embedded Dynamic Capabilities.” *Computers & Security* 135: 103525. https://doi.org/10.1016/j.cose.2023.103525.

Naseer, H., A. Ahmad, S. Maynard, and G. Shanks. 2018. “Cybersecurity Risk Management Using Analytics: A Dynamic Capabilities Approach.” *ICIS 2018 Proceedings*. 4. https://aisel.aisnet.org/icis2018/governance/Presentations/4.

Naseer, H., K. Desouza, S. B. Maynard, and A. Ahmad. 2024. “Enabling Cybersecurity Incident Response Agility Through Dynamic Capabilities: The Role of Real-Time Analytics.” *European Journal of Information Systems* 33, no. 2: 200–220. https://doi.org/10.1080/0960085x.2023.2257168.

Naseer, H., G. Shanks, A. Ahmad, and S. Maynard. 2016. “Enhancing Information Security Risk Management With Security Analytics: A Dynamic Capabilities Perspective.” *ACIS 2016 Proceedings*. 61. https://aisel.aisnet.org/acis2016/61.

Obi, J., A. S. Ibidunni, A. Tolulope, et al. 2018. “Contribution of Small and Medium Enterprises to Economic Development: Evidence From a Transiting Economy.” *Data in Brief* 18: 835–839. https://doi.org/10.1016/j.dib.2018.03.126.

Odeyemi, O., C. V. Ibeh, N. Z. Mhlongo, O. F. Asuzu, K. F. Awonuga, and F. O. Olatoye. 2024. “Forensic Accounting and Fraud Detection: A Review of Techniques in the Digital Age.” *Finance & Accounting Research Journal* 6, no. 2: 202–214. https://doi.org/10.51594/farj.v6i2.788.

OECD 2019. *Strengthening Social Inclusion Through Inclusive Entrepreneurship. Strengthening SMEs and Entrepreneurship for Productivity and Inclusive Growth: OECD 2018 Ministerial Conference on SMEs*. OECD.

Office of National statistics. 2023. “Business Population Estimates for the UK and Regions.” Accessed on March 14th, 2024. https://www.gov.uk/government/statistics/business-population-estimates-2023/business-population-estimates-for-the-uk-and-regions-2023-statistical-release.

Ojiambo, S. 2023. *Small Businesses are Key to a More Sustainable and Inclusive World*. Here’s why. World Economic Forum. https://www.weforum.org/stories/2023/03/small-businesses-sustainable-inclusive-world/.

Özkul, F. U., and A. Pamukçu. 2012. “Fraud Detection and Forensic Accounting.” In *Emerging Fraud: Fraud Cases from Emerging Economies*, 19–41. Springer Berlin Heidelberg.

Perano, M., A. Cammarano, V. Varriale, C. Del Regno, F. Michelino, and M. Caputo. 2023. “Embracing Supply Chain Digitalization and

Unphysicalization to Enhance Supply Chain Performance: A Conceptual Framework." *International Journal of Physical Distribution & Logistics Management* 53, no. 5/6: 628–659. https://doi.org/10.1108/ijpdlm-06-2022-0201.

Petzold, S., V. Barbat, F. Pons, and M. Zins. 2019. "Impact of Responsive and Proactive Market Orientation on SME Performance: The Moderating Role of Economic Crisis Perception." *Canadian Journal of Administrative Sciences* 36, no. 4: 459–472. https://doi.org/10.1002/cjas.1514.

Pigola, A., and P. R. da Costa. 2025. "Cybersecurity Management: An Empirical Analysis of Dynamic Capabilities Framework for Enhancing Cybersecurity Intelligence." *Information and Computer Security* 33, no. 4: 473–498. https://doi.org/10.1108/ICS-08-2024-0185.

Poepjes, R., and M. Lane 2012. An Information Security Awareness Capability Model (ISACM). https://www.semanticscholar.org/paper/An-information-security-awareness-capability-model-Poepjes-Lane/fed86021a363d29a6d86a86d5ccf059c53fc37ec.

Popoola, O. M. J. 2014. "Forensic Accountants, Auditors and Fraud Capability and Competence Requirements in the Nigerian Public Sector." *Doctoral dissertation, Universiti Utara Malaysia*. https://etd.uum.edu.my/4531/1/s94614.pdf.

Popoola, O. M. J., A. Che-Ahmad, and R. S. Samsudin. 2014. "Forensic Accounting and Fraud: Capability and Competence Requirements in Malaysia." *Journal of Modern Accounting & Auditing* 10, no. 8: 825–834. https://mpra.ub.uni-muenchen.de/66664/.

Rachinger, M., R. Rauter, C. Müller, W. Vorraber, and E. Schirgi. 2019. "Digitalization and its Influence on Business Model Innovation." *Journal of Manufacturing Technology Management* 30, no. 8: 1143–1160. https://doi.org/10.1108/jmtm-01-2018-0020.

Rahim, N. H. A., S. Hamid, M. L. Mat Kiah, S. Shamshirband, and S. Furnell. 2015. "A Systematic Review of Approaches to Assessing Cybersecurity Awareness." *Kybernetes* 44, no. 4: 606–622. https://doi.org/10.1108/k-12-2014-0283.

Rawindaran, N., A. Jayal, E. Prakash, and C. Hewage. 2023. "Perspective of Small and Medium Enterprise (sme's) and Their Relationship With Government in Overcoming Cybersecurity Challenges and Barriers in Wales." *International Journal of Information Management Data Insights* 3, no. 2: 100191. https://doi.org/10.1016/j.jjimei.2023.100191.

Reed, J. 2024. "IBM: Cybersecurity Dominates Concerns Among the C-suite small businesses, and the nation." https://www.ibm.com/think/insights/cybersecurity-dominates-concerns-c-suite-small-businesses-nation.

Reegård, K., C. Blackett, and V. Katta. 2019. The Concept of Cybersecurity Culture. Proceedings of the 29th European Safety and Reliability Conference (ESREL).

Renaud, K., and J. Ophoff. 2021. "A Cyber Situational Awareness Model to Predict the Implementation of Cyber Security Controls and Precautions by SMEs." *Organisational Cybersecurity Journal: Practice, Process and People* 1, no. 1: 24–46. https://doi.org/10.1108/OCJ-03-2021-0004.

Ribau, C. P., A. C. Moreira, and M. Raposo. 2018. "SME Internationalisation Research: Mapping the State of the Art." *Canadian Journal of Administrative Sciences - Revue Canadienne des Sciences de l Administration* 35, no. 2: 280–303. https://doi.org/10.1002/cjas.1419.

Ross, R., and V. Pillitteri. 2020. "Security and Privacy Controls for Information Systems and Organizations, Special Publication (NIST SP)." National Institute of Standards and Technology. Accessed, January 16, 2026. https://doi.org/10.6028/NIST.SP.800-53r5.

Rostami, A., J. Sommerville, I. L. Wong, and C. Lee. 2015. "Risk Management Implementation in Small and Medium Enterprises in the UK Construction Industry." *Engineering Construction and Architectural Management* 22, no. 1: 91–107. https://doi.org/10.1108/ECAM-04-2014-0057.

Savlovschi, L. I., and N. R. Robu. 2011. "The Role of SMEs in Modern Economy." *Economia, Seria Management* 14, no. 1: 277–281. https://www.researchgate.net/publication/227490106_The_role_of_SMEs_in_modern_economy.

Schilke, O., S. Hu, and C. E. Helfat. 2018. "Quo Vadis, Dynamic Capabilities? A Content-Analytic Review of the Current State of Knowledge and Recommendations for Future Research." *Academy of Management Annals* 12, no. 1: 390–439. https://doi.org/10.5465/annals.2016.0014.

Schriber, S., and J. Lowtedt. 2020. "Reconsidering Ordinary and Dynamic Capabilities in Strategic Change." *European Management Journal* 38, no. 3: 377–387. https://doi.org/10.1016/j.emj.2019.12.006.

Shanmugam, J. K., A. Ali, M. Hassan, and C. Haat. 2012. "Internal Control, Risk Management, and Fraud Prevention Measures on SMEs: Reliability and Validity of Research Instrument." *Small* 100: 12–18. https://www.academia.edu/23260154/Internal_Control_Risk_Management_and_Fraud_Prevention_Measures_on_Smes_Reliability_and_Validity_of_Research_Instrument.

Sihombing, R. P., N. Soewarno, and D. Agustia. 2023. "The Mediating Effect of Fraud Awareness on the Relationship Between Risk Management and Integrity System." *Journal of Financial Crime* 30, no. 3: 618–634. https://doi.org/10.1108/jfc-02-2022-0058.

Sledgianowski, D., M. Gomaa, and C. Tan. 2017. "Toward Integration of Big Data, Technology, and Information Systems Competencies into the Accounting Curriculum." *Journal of Accounting Education* 38: 81–93. https://doi.org/10.1016/j.jaccedu.2016.12.008.

Song, A. K. 2019. "The Digital Entrepreneurial Ecosystem: A Critique and Reconfiguration." *Small Business Economics* 53, no. 3: 569. https://doi.org/10.1007/s11187-019-00232-y.

Steinbart, P. J., R. L. Raschke, G. Gal, and W. N. Dilla. 2018. "The Influence of a Good Relationship Between the Internal Audit and Information Security Functions on Information Security Outcomes. Accounting." *Organisations and Society* 71: 15–29. https://doi.org/10.1016/j.aos.2018.04.005.

Sukumar, A., H. A. Mahdiraji, and V. Jafari-Sadeghi. 2023. "Cyber Risk Assessment in Small and Medium-Sized Enterprises: A Multilevel decision-making Approach for Small e-tailors." *Risk Analysis* 43, no. 10: 2082–2098. https://doi.org/10.1111/risa.14092.

Teece, D. J. 2007. "Explicating Dynamic Capabilities: The Nature and Microfoundations of (Sustainable) Enterprise Performance." *Strategic Management Journal* 28, no. 13: 1319–1350. https://doi.org/10.1002/smj.640.

Teece, D. J. 2009. *Dynamic Capabilities and Strategic Management: Organising for Innovation and Growth*. Oxford University Press.

Teece, D. J. 2018a. "Business Models and Dynamic Capabilities." *Long Range Planning* 51, no. 1: 40–49. https://doi.org/10.1016/j.lrp.2017.06.007.

Teece, D. J. 2018b. "Dynamic Capabilities as (Workable) Management Systems Theory." *Journal of Management and Organization* 24, no. 3: 359–368. https://doi.org/10.1017/jmo.2017.75.

Teece, D. J., G. Pisano, and A. Shuen. 1997. "Dynamic Capabilities and Strategic Management." *Strategic Management Journal* 18, no. 7: 509–533. https://doi.org/10.1002/(sici)1097-0266(199708)18:7<509::aid-smj882>3.0.co;2-z.

Türen, S. H., K. Eustace, R. Islam, and G. Fellows. 2025. "Near Realtime Attack Detections With Weka Framework." In *International Conference on Advances in Computing Research*, 331–345. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-87647-9_29.

Ungureanu, M. A., E. Gavan, and C. Gasparotti. 2024. "Securing Innovation at Sea: Cyber Risk Management for SMEs in Ship Design." *Annals of" Dunarea de Jos" University of Galati. Fascicle XI Shipbuilding* 47: 89–100. https://doi.org/10.35219/AnnUgalShipBuilding/2024.47.11.

US Chamber of Commerce. 2024. "Small Business Statistics." Accessed March 14th, 2024. https://www.chamberofcommerce.org/small-businessstatistics/#:~:text=The%20number%20of%20small%20businesses,businesses%2C%20according%20to%20the%20SBA.

Van Haastrecht, M., B. Yigit Ozkan, M. Brinkhuis, and M. Spruit. 2021. "Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics." *Applied Sciences* 11, no. 15: 1–28. https://doi.org/10.3390/app11156909.

Verizon. 2024. "Data Breach Investigations Report (DBIR)." https://www.verizon.com/business/en-gb/resources/reports/2024/dbir/2024-dbir-data-breach-investigations-report.pdf?msockid=33490dccb95b6f731bfb1f6fb8e06ee4.

Verma, A., and C. Shri. 2025. "Cyber Security: A Review of Cyber-Crimes, Security Challenges, and Measures to Control." *Vision* 29, no. 4: 478–492. https://doi.org/10.1177/09722629221074760.

Vogel, R., and W. H. Güttel. 2013. "The Dynamic Capability View in Strategic Management: A Bibliometric Review." *International Journal of Management Reviews* 15, no. 4: 426–446. https://doi.org/10.1111/ijmr.12000.

Walaski, P. 2017. "Rightsizing Risk Management: For Small & Medium Enterprises." 62, no. 6: 62–69. https://nibmehub.com/opac-service/pdf/read/Risk%20Management%20In%20Small%20And%20Medium%20Enterprises%20by%20Chiara%20Crovini%20(z-lib.org).pdf.

Wang, C. L., and P. K. Ahmed. 2007. "Dynamic Capabilities: A Review and Research Agenda." *International Journal of Management Reviews* 9, no. 1: 31–51. https://doi.org/10.1111/j.1468-2370.2007.00201.x.

Williams, A. 2025. UK SMEs Face Rise in Cyber-Attacks With Average Cost GBP £7,960. https://securitybrief.co.uk/story/uk-smes-face-rise-in-cyber-attacks-with-average-cost-gbp-7-960.

Wilson, M., and S. McDonald. 2023. "SME Cybersecurity Misconceptions: A Guide for Decision Makers." In *Cybersecurity for Decision Makers*, edited by N. R. Vajjhala and K. D. Strang. 1st ed., 293–316. CRC Press. Retrieved from. https://doi.org/10.1201/9781003319887-17.

Wilson, M., and S. McDonald. 2025. "One Size Does Not Fit all: Exploring the Cybersecurity Perspectives and Engagement Preferences of UK-Based Small Businesses." *Information Security Journal: A Global Perspective* 34, no. 1: 15–49. https://doi.org/10.1080/19393555.2024.2357310.

Wilson, M., S. McDonald, D. Button, and K. McGarry. 2023. "It Won'T Happen to me: Surveying SME Attitudes to cyber-security." *Journal of Computer Information Systems* 63, no. 2: 397–409. https://doi.org/10.1080/08874417.2022.2067791.

Winter, S. G. 2003. "Understanding Dynamic Capabilities." *Strategic Management Journal* 24, no. 10: 991–995. https://doi.org/10.1002/smj.318.

Wong, L. W., V. H. Lee, G. W. H. Tan, K. B. Ooi, and A. Sohal. 2022. "The Role of Cybersecurity and Policy Awareness in Shifting Employee Compliance Attitudes: Building Supply Chain Capabilities." *International Journal of Information Management* 66: 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520.

Yeow, A., C. Soh, and R. Hansen. 2018. "Aligning With New Digital Strategy: A Dynamic Capabilities Approach." *Journal of Strategic Information Systems* 27, no. 1: 43–58. https://doi.org/10.1016/j.jsis.2017.09.001.

Zainal, S. F., H. A. Hashim, A. M. Ariff, and Z. Salleh. 2022. "Research on Fraud: An Overview From Small Medium Enterprises (SMEs)." *Journal of Financial Crime* 29, no. 4: 1283–1296. https://doi.org/10.1108/jfc-09-2021-0205.

Zhang, J., X. Yang, and D. Appelbaum. 2015. "Toward Effective Big Data Analysis in Continuous Auditing." *Accounting Horizons* 29, no. 2: 469–476. https://doi.org/10.2308/acch-51070.

Zhou, G., M. Gou, Y. Gan, and R. Schwarzer. 2020. "Risk Awareness, self-efficacy, and Social Support Predict Secure Smartphone Usage." *Frontiers in Psychology* 11: 1066. https://doi.org/10.3389/fpsyg.2020.01066.

Zwilling, M., G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim. 2022. "Cyber Security Awareness, Knowledge, and Behavior: A Comparative Study." *Journal of Computer Information Systems* 62, no. 1: 82–97. https://doi.org/10.1080/08874417.2020.1712269.