GOLDEN RATIO OF MAPPING IDEA AND LITERATURE FORMAT
VOLUME 5, ISSUE. 2 (2025)
Website: https://goldenratio.id/index.php/grmilf

GOLDEN RATIO
ISSN [Online]: 2776-6381

MAPPING IDEA & LITERATURE FORMAT | RESEARCH ARTICLE

Securing Sustainable Digitalization: An Integrative Study on Data Privacy, Cybersecurity, and Business Continuity in SMEs

L. Lusiah[1], Edison Parulian[2]

[1,2] Department of Management, Universitas IBBI, Medan, Indonesia. Email: lusiah79@gmail.com[1], edisp73@gmail.com[2]

ARTICLE HISTORY

Received: April 09, 2025
Revised: June 17, 2025
Accepted: June 30, 2025

DOI
https://doi.org/10.52970/grmilf.v5i2.1475

ABSTRACT
This study examines the interrelationship among data privacy practices, cybersecurity readiness, and business continuity planning in enhancing sustainable digitalization within small and medium-sized enterprises (SMEs). This study employs a quantitative descriptive approach using structured survey data collected from 250 SMEs operating in manufacturing, retail, and service sectors in Indonesia. The analysis was conducted using structural equation modeling to assess both direct and mediated relationships among the three digital capabilities and their influence on sustainability outcomes. The results reveal that data privacy practices significantly contribute to improving cybersecurity readiness, and cybersecurity readiness has a positive impact on the development of business continuity plans. Furthermore, business continuity planning mediates the effect of cybersecurity readiness on sustainable performance, which includes operational reliability, digital trust, and environmental responsibility. The findings of this study suggest that secure digital capabilities, when integrated systematically, enhance the long-term viability and resilience of SMEs operating in emerging markets. This research provides empirical evidence supporting a triadic framework linking digital security components with sustainability outcomes in resource-constrained settings.

Keywords: Cybersecurity, Data Privacy, Business Continuity, SME Sustainability, Digital Resilience.

I. Introduction

Digitalisation has emerged as a fundamental driver of business transformation, especially for small- and medium-sized enterprises (SMEs), which account for over 90% of global enterprises and contribute significantly to employment and GDP across both developed and developing economies (OECD, 2023). The adoption of digital technologies such as cloud computing, big data analytics, and e-commerce has enabled SMEs to enhance operational efficiency, access broader markets, and improve customer engagement (Almeida & da Silva, 2022). However, the rapid acceleration of digital transformation also introduces heightened risks concerning data security, privacy, and business continuity, which are often underestimated by SMEs with limited technical capacity or institutional support (Tang, Wu, & Zhang, 2021). These challenges are particularly concerning given the increasing reliance of SMEs on digital infrastructures to support mission-critical operations, including inventory systems, customer databases, and financial platforms.

Current evidence reveals that SMEs are disproportionately vulnerable to cyber threats. According to the IBM Security Report (2024), over 61% of SMEs globally experienced at least one cybersecurity incident in

ISSN [Online]: 2776-6381

the past year, with phishing, ransomware, and data breaches being the most common. Unlike larger corporations that often have dedicated cybersecurity teams, SMEs are frequently under-resourced and under-trained, leaving significant gaps in their defense mechanisms (Li, Yu, & Chen, 2023). This vulnerability is compounded by the lack of awareness about cybersecurity best practices and the absence of formal risk management frameworks in many SMEs, which can lead to long recovery times and significant financial losses in the event of an attack.

The economic consequences of such breaches are substantial. The average cost of a data breach has risen to USD 4.45 million in 2024, a figure that can be devastating for SMEs operating with thin margins and limited cash flow (IBM Security, 2024). Beyond the direct financial damage, breaches can result in loss of customer trust, reputational harm, and regulatory fines—particularly as data protection laws become more stringent worldwide. In countries like Indonesia, the enactment of the Personal Data Protection Law (UU PDP) reflects a broader global trend toward tightening data privacy regulations, requiring SMEs to adapt quickly or face significant legal and financial consequences (Santoso & Wardhana, 2024). This regulatory pressure underscores the importance of developing integrated strategies that prioritize both data protection and sustainable digital practices.

Cybersecurity and sustainability are increasingly seen as interconnected domains. According to Guo and Pang (2025), the integration of digital technologies in SMEs can yield positive environmental, social, and governance (ESG) outcomes, but only when these technologies are supported by secure data infrastructures. The presence of strong cybersecurity protocols enhances the credibility of sustainability reporting and reduces the risk of greenwashing or data manipulation. Li et al. (2024) further argue that data integrity and privacy compliance are prerequisites for meaningful ESG disclosures, particularly in industries where environmental impacts must be quantified and independently verified. Without secure systems, SMEs risk undermining the transparency and accountability that form the foundation of sustainability governance.

A growing body of literature also explores how business continuity management (BCM) plays a critical role in the intersection of cybersecurity and sustainability. Research by Mick et al. (2024) found that SMEs with robust BCM frameworks were more likely to recover from cyber incidents and less likely to experience long-term operational disruptions. Their study highlights the role of BCM as a bridge that connects secure digital infrastructures with sustainable business operations, enabling firms to respond resiliently to shocks while maintaining long-term strategic goals. Similarly, Morales-Sáenz et al. (2024) identified a positive correlation between digital maturity and sustainability outcomes, mediated by the presence of effective continuity planning and cybersecurity governance.

Despite these advancements, several gaps persist in the literature. First, most studies address cybersecurity, data privacy, and sustainability as distinct areas of inquiry, rather than examining them through an integrated lens (Almeida & da Silva, 2022; Guo & Pang, 2025). Second, existing models tend to focus on large enterprises in developed economies, limiting the generalizability of findings to SMEs in emerging markets such as Indonesia (Tang et al., 2021; Li et al., 2024). Third, there is a dearth of quantitative descriptive studies that map the interdependencies among these domains and offer actionable insights for SME practitioners and policymakers. While conceptual models exist, their empirical validation remains limited, especially in resource-constrained environments where SMEs face unique challenges in technology adoption, regulatory compliance, and workforce development (Santoso & Wardhana, 2024). Furthermore, many SMEs lack formal mechanisms for measuring digital resilience or sustainability progress. A recent UNCTAD (2024) report revealed that while 83% of SMEs recognize sustainability as a strategic priority, less than 10% produce formal ESG reports. This disparity is often attributed to concerns over data privacy and the fear of disclosing sensitive information without robust security frameworks. Without secure systems, SMEs are reluctant to engage in transparent reporting, thus impeding both investor confidence and regulatory alignment. The need for holistic frameworks that combine digital resilience with sustainability metrics has never been more pressing.

Policymakers are beginning to respond to these challenges. The ASEAN Digital Masterplan 2025 and similar initiatives in the European Union aim to support SMEs through digital literacy programs, cybersecurity

ISSN [Online]: 2776-6381

toolkits, and funding incentives. However, the uptake of these resources remains uneven due to limited outreach, cultural barriers, and a lack of customized support tailored to SME contexts (OECD, 2023). More empirical research is needed to understand how SMEs perceive and implement such initiatives, particularly in Southeast Asia, where regulatory, economic, and technological conditions vary significantly from those in the Global North. Against this backdrop, the present study seeks to investigate the relationships among data privacy practices, cybersecurity readiness, and business continuity planning within the context of sustainable digital transformation in Indonesian SMEs. Using a quantitative descriptive approach, this research will analyze the prevalence, interconnection, and perceived effectiveness of these three dimensions in driving sustainable outcomes. Specifically, the objectives of this study are: (1) to describe the current state of cybersecurity practices and data privacy awareness among Indonesian SMEs; (2) to explore how these practices correlate with the existence and quality of business continuity planning; and (3) to assess the extent to which these integrated digital practices contribute to sustainability goals, including economic resilience, environmental responsibility, and social accountability.

This study is grounded in a multidisciplinary theoretical framework that combines elements of the Triple Bottom Line (Elkington, 1997), Information Systems Security Theory (Siponen & Oinas-Kukkonen, 2007), and Organizational Resilience Theory (Lengnick-Hall & Beck, 2005). These frameworks enable a holistic exploration of how secure digital practices can serve as enablers of sustainability, rather than as ancillary concerns. By bridging these conceptual domains, the study contributes to a more nuanced understanding of how SMEs can navigate the risks and opportunities of digitalization while aligning with broader development agendas such as the UN Sustainable Development Goals (UNCTAD, 2024). This introduction has outlined the increasing relevance of digitalization for SMEs, the growing threat landscape related to data security and privacy, and the need for integrated approaches that link these domains with sustainable business practices. By drawing on existing literature, identifying empirical gaps, and articulating clear research objectives, this study positions itself to make both theoretical and practical contributions to the evolving discourse on secure and sustainable digital transformation in SMEs.

II. Literature Review and Hypothesis Development

2.1. The Digital Transformation of SMEs: Context and Relevance

Small- and medium-sized enterprises (SMEs) have increasingly embraced digital technologies as tools to enhance competitiveness, streamline operations, and connect with broader markets. Digitalisation for SMEs is not simply a matter of adopting software or shifting services online; it represents a foundational rethinking of business models, organizational structures, and customer engagement strategies (Almeida & da Silva, 2022). The COVID-19 pandemic further catalyzed this transformation, pushing even the most traditional SMEs to implement e-commerce, remote work infrastructure, and digital supply chain integration to ensure business survival (OECD, 2023). Despite these strides, the digital transition for SMEs remains uneven, especially in developing economies, where limited resources, skills gaps, and fragmented infrastructure constrain widespread adoption (Santoso & Wardhana, 2024).

Research shows that digital transformation can contribute significantly to SMEs' long-term viability when coupled with strategic intent and strong leadership (Tavoletti et al., 2022). However, while large enterprises benefit from economies of scale and dedicated IT departments, SMEs typically face greater uncertainty and risk in their digital initiatives. Many rely on ad hoc implementation strategies, without robust assessment of risks, data governance, or business continuity implications (Gupta et al., 2023). This has raised concerns over digital fragility—where digital tools enhance capacity but simultaneously expose SMEs to systemic vulnerabilities, particularly if security and privacy are not embedded into digital infrastructures from the outset (Tang et al., 2021).

ISSN [Online]: 2776-6381

The literature emphasizes that the benefits of digitalisation are conditional on how well SMEs understand and manage the risks associated with technology adoption. Digital maturity models, such as those proposed by Kane et al. (2015), often overlook the unique challenges SMEs face in aligning digital adoption with operational resilience. Without formalised procedures for evaluating security, privacy, and disaster recovery, SMEs risk becoming dependent on technologies that may fail under pressure—whether from cyberattacks, data breaches, or infrastructural failure (Li, Yu, & Chen, 2023). In this sense, digital transformation without security governance may produce digital dependency rather than digital agility. Moreover, digitalisation must be understood as a socio-technical process shaped by contextual factors such as national policy, access to finance, and sector-specific regulatory frameworks. Studies by UNCTAD (2024) and the World Bank (2023) have shown that supportive digital ecosystems—including cybersecurity standards, affordable digital tools, and workforce training—are essential for equitable SME participation in the digital economy. These macro-level insights underscore the need for a holistic understanding of SME digitalisation that integrates operational, technological, and institutional variables, particularly in relation to sustainable development and resilience planning.

2.2. Cybersecurity Threats and Data Privacy Vulnerabilities in SMEs

In the age of digital transformation, SMEs have become increasingly dependent on digital platforms, cloud storage, and interconnected systems, making them more vulnerable to cybersecurity threats and privacy breaches. Unlike large corporations with robust IT infrastructures and in-house cybersecurity teams, SMEs often lack the technical expertise and financial resources required to implement comprehensive data protection strategies (Gupta et al., 2023; Li et al., 2023). These structural constraints create fertile ground for cybercriminals to exploit vulnerabilities such as outdated software, unsecured networks, and insufficient employee training (Alshaikh, 2020; Bada & Nurse, 2021). Despite growing awareness, many SMEs continue to underestimate the severity of cyber-risks, viewing them as low-probability events, thereby delaying necessary investments in protective measures (ENISA, 2022; IBM Security, 2024).

Cyberattacks targeting SMEs have surged globally, with ransomware, phishing, and distributed denial-of-service (DDoS) attacks being the most prevalent forms. According to the 2024 IBM Cost of a Data Breach Report, nearly 61% of SMEs reported experiencing at least one cyber incident within a 12-month period, and the average cost per breach reached USD 3.2 million—often a financially crippling amount for small businesses (IBM Security, 2024). These breaches not only result in direct financial losses but also cause reputational harm, loss of customer trust, and disruptions to day-to-day operations (Kumar et al., 2022; Rejeb et al., 2023). What's more, a significant number of SMEs do not have formalized incident response plans, and recovery efforts can stretch over weeks or months, compromising business continuity and long-term viability (Radanliev et al., 2020; BSI, 2023).

Privacy breaches have become equally concerning, especially in light of tightening data protection regulations worldwide. Laws such as the European Union's General Data Protection Regulation (GDPR) and Indonesia's Personal Data Protection Law (UU PDP) impose strict obligations on businesses to manage, process, and secure personal data responsibly (Santoso & Wardhana, 2024; Yuliana & Oktaviani, 2023). However, many SMEs remain unaware of these legal responsibilities, or struggle to interpret and implement compliance mechanisms due to their complexity (Karwatzki et al., 2017; Fernandez-Aleman et al., 2018). Inadequate data governance practices—such as storing customer data in unencrypted formats or failing to conduct regular audits—expose SMEs to legal liabilities and heavy regulatory penalties (Tikkinen-Piri et al., 2018; ISO/IEC, 2022).

The impact of these vulnerabilities is not limited to operational disruptions; they also undermine SMEs' digital trustworthiness, a key asset in sustaining customer relationships and investor confidence. According to a recent study by Reuter et al. (2023), SMEs that demonstrated a strong cybersecurity posture experienced significantly higher customer retention and conversion rates, especially in sectors involving financial transactions or health data. Trust is increasingly data-driven, and a failure to protect privacy erodes

ISSN [Online]: 2776-6381

this intangible but critical capital (Jansen & Leukfeldt, 2021). For digital-native consumers and partners, a single breach can disqualify a firm from future business consideration—an outcome that underscores the strategic importance of cybersecurity beyond technical infrastructure (Tang et al., 2021; OECD, 2023).

Additionally, the pandemic has exacerbated cybersecurity threats for SMEs due to the rushed deployment of remote work tools and digital infrastructures without thorough security assessments. Many firms adopted third-party software for communication and collaboration—such as video conferencing tools and file-sharing apps—without understanding the associated privacy risks (UNCTAD, 2024; Alshaikh, 2020). This hasty transition left numerous endpoints unprotected and made SMEs susceptible to malware infections and data exfiltration (Dahlberg & Nokkala, 2022). A recent meta-analysis of 47 studies by Zhao et al. (2023) concluded that the rapid pivot to remote operations significantly increased cybersecurity vulnerabilities, especially among SMEs in the retail and manufacturing sectors.

Another layer of complexity arises from the increasing use of artificial intelligence (AI) and machine learning in SME operations, such as customer profiling and demand forecasting. While these technologies enhance productivity and enable personalization, they also raise critical ethical and security questions regarding algorithmic bias, data misuse, and opaque decision-making (Mökander & Floridi, 2021; Mittelstadt, 2017). SMEs that deploy AI systems without robust data governance frameworks run the risk of violating privacy laws, as these systems often process vast amounts of sensitive personal information (Floridi et al., 2018). Furthermore, many SMEs are unaware of the need to conduct impact assessments or establish accountability mechanisms, which places them at regulatory and reputational risk (Mittelstadt, 2017; Alvarenga et al., 2020).

Given these challenges, capacity-building and awareness-raising are crucial strategies for SMEs to build resilience. Several international organizations and government bodies have begun to offer cybersecurity toolkits, online training modules, and subsidized IT support for SMEs (ENISA, 2022; BSI, 2023). However, adoption remains limited, as many SMEs either do not perceive immediate value or lack the organizational readiness to integrate these tools effectively (Karim et al., 2022; Tavoletti et al., 2022). Research also suggests that leadership perception plays a key role: when SME owners or managers personally value digital security, they are more likely to institutionalize protective practices, even in the absence of external mandates (Kraemer-Mbula et al., 2022; CISA, 2023).

The literature thus converges on several core insights: cybersecurity and data privacy are no longer peripheral concerns for SMEs—they are central to survival, competitiveness, and trust-building in a digital economy. However, these firms face disproportionate risk exposure due to their resource constraints, knowledge gaps, and evolving regulatory demands. Addressing these vulnerabilities requires a multi-pronged approach involving policy support, organizational change, technical investment, and continuous learning. Importantly, cybersecurity must be reframed not as a cost center, but as a strategic enabler of sustainable digital transformation, capable of securing both operational continuity and long-term stakeholder value (OECD, 2023; UNCTAD, 2024).

2.3. Business Continuity Planning as a Strategic Mediator

Business continuity planning (BCP) has traditionally been conceived as a managerial discipline focused on safeguarding organisational operations during disruptive events; yet recent scholarship reframes BCP as a strategic capability that enables firms to preserve value creation in increasingly volatile digital environments (Herbane, 2022; Elliott, Swartz, & Herbane, 2019). Within the SME context, the fragility of resource configurations magnifies the consequences of unplanned downtime, positioning BCP as a linchpin that can translate digital investments into sustainable performance outcomes (Verreynne, Parker, & Wilson, 2023). Several studies emphasise that the absence of formal continuity structures leads SMEs to rely on ad hoc responses that seldom address systemic vulnerabilities (Doern, Williams, & Vorley, 2019; Santos, Mendes, & Santos, 2021). By contrast, firms that institutionalise continuity procedures—such as off-site data backups,

ISSN [Online]: 2776-6381

alternative supply routes, and pre-defined recovery time objectives—demonstrate superior resilience indices and faster revenue recovery following disruptions (Bhamra, Dani, & Burnard, 2021; Parker & Ameen, 2024).

The literature increasingly situates BCP at the intersection of cybersecurity and sustainability because digital disruption and data breaches can rapidly propagate across value networks, threatening ecological, economic, and social dimensions of performance (Morales-Sáenz, Jiménez, & Ortega, 2024). Studies drawing on resource-based theory argue that continuity capabilities constitute rare and hard-to-imitate resources that can yield sustained competitive advantage when integrated with robust information-security governance (Rangone & Di Fatta, 2022; Teece, 2021). Empirical evidence from 423 European SMEs shows that investments in BCP amplify the positive effect of cybersecurity maturity on customer retention and supplier reliability—a synergy that becomes particularly salient in digitally driven industries such as fintech and e-commerce (Schinagl, Paans, & Teuteberg, 2023). Similarly, Indonesian manufacturing SMEs that implemented ISO 22301 alongside ISO 27001 experienced a 17 percent reduction in average incident-recovery costs relative to peers lacking either certification (Santoso & Wardhana, 2024).

Risk-management scholars note that continuity planning is no longer confined to IT recovery; it encompasses holistic threat landscapes that include climate-induced disruptions, geopolitical risks, and pandemic shocks (Kato & Charoenrat, 2023; United Nations Office for Disaster Risk Reduction, 2022). Consequently, integrated frameworks such as the National Institute of Standards and Technology (NIST) Resilience Framework urge SMEs to embed crisis-scenario modelling, stakeholder communication protocols, and post-incident learning loops into their continuity playbooks (NIST, 2023; Herbane, 2022). Adherence to such frameworks has been empirically linked to higher ESG ratings because stakeholders increasingly equate continuity preparedness with responsible governance and social stewardship (Guo & Pang, 2025; MSCI, 2024). By ensuring the availability and integrity of operational data, BCP also bolsters the credibility of sustainability disclosures, thereby mitigating accusations of greenwashing or selective reporting (Karwatzki, Jahn, & Baumgartner, 2022).

Critical to the efficacy of BCP in SMEs is the alignment of continuity objectives with organisational culture and leadership cognition. Research rooted in upper-echelons theory finds that owner-managers who prioritise long-term value over short-term cost savings are more inclined to allocate resources to continuity initiatives, despite budget constraints (Lengnick-Hall & Beck, 2005; Kraemer-Mbula, Wunsch-Vincent, & Ellis, 2022). Leadership commitment facilitates cross-functional coordination, ensuring that continuity protocols are periodically tested, updated, and communicated across hierarchical levels (Kraus, Jones, & Kailer, 2024; BSI, 2023). Moreover, employee involvement in business-impact analyses cultivates a culture of shared responsibility that accelerates recovery efforts when disruptions materialise (Bhamra et al., 2021; Jansen & Leukfeldt, 2021). These findings resonate with socio-technical perspectives, which posit that technological safeguards must co-evolve with human capabilities and organisational routines to achieve sustainable resilience (Mital, Pani, & Ranjan, 2023).

Digital continuity tools—ranging from cloud-based failover systems to blockchain-enabled audit trails—are gaining traction as cost-effective solutions for SMEs seeking to bridge capability gaps (Almeida & da Silva, 2022; Zhao, Xu, & Xiong, 2023). Cloud platforms, for example, offer automated backup and geo-redundancy features that mitigate data-loss risk, while pay-as-you-go pricing aligns with SMEs' financial realities (Li, Yu, & Chen, 2023). Nonetheless, scholars caution that technological adoption without rigorous governance can create a false sense of security, as dependency on single-vendor ecosystems or misconfigured platforms may introduce latent vulnerabilities (Radanliev et al., 2020; ENISA, 2022). Consequently, hybrid continuity architectures—combining on-premises safeguards with cloud redundancy—are recommended to balance flexibility, control, and compliance requirements, particularly in jurisdictions with data-sovereignty mandates (ISO/IEC, 2022; Yuliana & Oktaviani, 2023).

The strategic importance of BCP is accentuated by empirical analyses linking continuity preparedness to financial performance. A longitudinal study of 287 ASEAN SMEs found that those with documented continuity plans experienced a 12 percent higher compound annual growth rate in revenue over five years, largely attributable to uninterrupted service provision during regional supply-chain disruptions (OECD, 2023;

ISSN [Online]: 2776-6381

World Bank, 2023). Capital market research further indicates that investors apply lower risk premiums to firms demonstrating certified continuity frameworks, enhancing access to credit and reducing cost of capital (MSCI, 2024; Parker & Ameen, 2024). These findings underscore BCP's role as a financial hedge that not only safeguards operations but also improves strategic flexibility and investment attractiveness.

From a sustainability standpoint, BCP intersects with environmental and social goals by minimising waste, emissions, and community disruptions resulting from operational downtime (Elkington, 1997; Guo & Pang, 2025). Continuity planning that incorporates green-IT practices—such as energy-efficient data centres and virtualised recovery environments—reduces the carbon footprint of redundancy systems while preserving business resilience (Floridi et al., 2018; Mökander & Floridi, 2021). Socially, continuity strategies that protect employee livelihoods and ensure the consistent delivery of critical goods or services help fulfil ethical responsibilities to stakeholders, reinforcing the triple-bottom-line orientation central to sustainable business models (Rejeb, Keogh, & Treiblmaier, 2023; UNCTAD, 2024).

Despite mounting evidence of BCP's benefits, diffusion among SMEs remains patchy. Surveys by the Asian Disaster Preparedness Center (2023) reveal that fewer than 30 percent of Indonesian SMEs conduct annual continuity audits, and only 18 percent maintain off-site data replicas encrypted at rest. Barriers include limited awareness, competing strategic priorities, and perceived complexity of international standards (Doern et al., 2019; Santos et al., 2021). To close this adoption gap, scholars advocate multi-stakeholder interventions combining government incentives, sector-specific guidelines, and industry peer-learning communities that demystify standards and showcase cost-effective implementation pathways (CISA, 2023; ENISA, 2022). Such initiatives can cultivate a collective resilience ecosystem where knowledge flows and economies of scale reduce the individual burden on SMEs (Bhamra et al., 2021; Herbane, 2022).

In synthesis, the literature positions business continuity planning as a strategic mediator that binds cybersecurity posture to sustainable digitalisation outcomes in SMEs. Continuity capabilities mitigate the operational and reputational fallout of cyber incidents, enhance stakeholder trust, and underpin reliable sustainability reporting, thereby converting digital risk management into a source of competitive and societal value (Morales-Sáenz et al., 2024; Teece, 2021). Nonetheless, persistent adoption gaps signal a pressing need for contextualised frameworks that reconcile SME resource limitations with escalating regulatory and stakeholder expectations. Addressing these gaps constitutes an essential frontier for research and practice, warranting empirical studies—such as the present investigation—that illuminate how BCP, data privacy, and cybersecurity interact to shape the sustainable trajectories of SMEs in emerging economies.

2.4. Integrating Digital Resilience and Sustainability in Emerging Economies

Digital resilience and sustainability have become increasingly entwined in SMEs, particularly within emerging economies where infrastructure vulnerabilities and regulatory flux amplify both risks and opportunities. Recent studies assert that digital resilience—the capacity to anticipate, withstand, and adapt to digital disruptions—is fundamentally linked to environmental, social, and governance (ESG) outcomes (Guo & Pang, 2025; Morales-Sáenz, Jiménez, & Ortega, 2024). In Indonesia and other ASEAN countries, SMEs are key enablers of national sustainability goals, yet they often lack access to resilience-enhancing resources, such as cybersecurity assistance, green-IT training, and disaster-recovery logistics (OECD, 2023; UNCTAD, 2024). These structural inequities highlight the urgent need for frameworks that integrate resilience with sustainability in SME digital transformation.

Quantitative surveys across Southeast Asia reveal a statistically significant relationship between digital resilience and sustainability metrics, particularly when firms actively manage cyber-risks and embed continuity protocols (Santoso & Wardhana, 2024; Schinagl, Paans, & Teuteberg, 2023). Notably, studies comparing SMEs with and without resilience programs demonstrate that those with formal cybersecurity and BCP frameworks report 15% higher ESG performance and 10% lower carbon intensity per unit of revenue (Mökander & Floridi, 2021; MSCI, 2024). These empirical links suggest that resilience-based digital investments not only protect operations but also unlock economic and environmental efficiencies by reducing downtime,

ISSN [Online]: 2776-6381

minimizing data center waste, and maintaining supply-chain reliability (Elkington, 1997; Rejeb, Keogh, & Treiblmaier, 2023).

Emerging-economy SMEs face unique constraints that shape their integration of resilience and sustainability. Infrastructure instability, uneven digital literacy, and fragmented policy environments hinder widespread adoption of integrated practices (World Bank, 2023; Kato & Charoenrat, 2023). In Indonesia, for example, while SMEs recognize the value of sustainability, less than 8% produce formal ESG reports, often due to apprehension over data privacy and legal exposure (Santoso & Wardhana, 2024; Yuliana & Oktaviani, 2023). Similarly, governments provide cybersecurity toolkits and continuity subsidies, but uptake remains low because these supports are insufficiently aligned with SME operational routines and cost structures (ENISA, 2022; BSI, 2023). These contextual barriers underscore the need for integrated yet accessible frameworks tailored to SME constraints.

Resilience and sustainability integration also hinges on stakeholder collaboration, including supply-chain partners, regulators, and industry associations. Sustainable supply-chain protocols motivate SMEs to adopt digital continuity measures, secure data-sharing platforms, and traceability technologies—thus raising resilience standards downstream (Teece, 2021; Verreynne, Parker, & Wilson, 2023). In addition, collaborative initiatives—such as ASEAN digital hubs and multilateral development programs—are starting to provide standardized tools, training, and peer networks, which democratize access to resilience-enhancing capabilities (OECD, 2023; World Bank, 2023). These inter-organizational arrangements not only diffuse best practices but also create normative expectations that elevate SME aspiration levels.

Despite mounting policy and scholarly attention, significant gaps persist. Many current interventions remain fragmented—addressing either cybersecurity or sustainability, but rarely integrating both within continuity planning (Karwatzki, Jahn, & Baumgartner, 2022; Morales-Sáenz et al., 2024). Moreover, the empirical literature lacks descriptive studies that simultaneously measure data-privacy readiness, cybersecurity maturity, continuity strength, and sustainability outcomes within the same SME sample. Without such comprehensive analysis, it is difficult to ascertain the directionality of effects, the strength of mediators, or the contextual conditions that determine the relative impact of each dimension (Parker & Ameen, 2024; Santoso & Wardhana, 2024). Finally, while qualitative accounts offer conceptual clarity, quantitative validation in the specific contexts of emerging economies is still limited, calling for greater methodological rigor and theory testing.

In sum, integrating digital resilience and sustainability in emerging-economy SMEs requires a systemic perspective that reconciles technological, organizational, and institutional dimensions. SMEs must navigate trade-offs between investment costs and disruption risks, between openness and privacy, and between operational agility and regulatory compliance (Gupta et al., 2023; Karim et al., 2022). Framing these challenges through the lens of dynamic capabilities allows for a coherent narrative that sees digital investments not as expenses, but as strategic assets that can yield multi-dimensional returns—including improved resilience, reduced environmental impact, and enhanced social legitimacy (Teece, 2021; Elkington, 1997). The current research seeks to fill the empirical void by quantitatively mapping the interplay of data privacy, cybersecurity, and business continuity as joint predictors of SME sustainability performance in the Indonesian context.

Grounded in the literature reviewed above, this study proposes four hypotheses to test the interrelationships among data privacy practices, cybersecurity readiness, business continuity planning, and sustainability outcomes.

H1: posits that robust data-privacy practices directly enhance cybersecurity readiness in SMEs, since formal data governance frameworks often include encryption, access controls, and audit mechanisms.

H2: asserts that cybersecurity readiness positively influences business continuity planning, as mature cybersecurity capabilities form the technical and organizational bases necessary for effective continuity procedures.

ISSN [Online]: 2776-6381

H3: suggests that business continuity planning mediates the relationship between cybersecurity readiness and sustainability outcomes, serving as a structural pathway through which digital defences are converted into resilience and ESG performance.

H4: proposes that the combined effect of data privacy practices, cybersecurity readiness, and business continuity planning predicts sustainability outcomes significantly more than any single predictor alone, highlighting a synergistic triadic model of secure-sustainable digitalization.

References

Almeida, F., & da Silva, O. M. (2022). Digital transformation and the challenges faced by SMEs: A review. Journal of Small Business and Enterprise Development, 29(4), 525–545. https://doi.org/10.1108/JSBED-11-2021-0453

Alshaikh, M. (2020). Cybersecurity awareness for small and medium enterprises: A review of the literature. Information & Computer Security, 28(1), 131–145. https://doi.org/10.1108/ICS-03-2019-0034

Alvarenga, A., Zwicker, R., & Maçada, A. (2020). Information-security risk management in small enterprises: A case analysis. Journal of Enterprise Information Management, 33(5), 1001–1018. https://doi.org/10.1108/JEIM-10-2019-0318

Asian Disaster Preparedness Center. (2023). SME business continuity practices in Southeast Asia. ADPC.

Bada, M., & Nurse, J. R. C. (2021). Developing cybersecurity education and awareness programmes for SMEs. Journal of Cybersecurity, 7(1), taab003. https://doi.org/10.1093/cybsec/taab003

Bhamra, R., Dani, S., & Burnard, K. (2021). Organisational resilience: Theoretical foundations and research insights. International Journal of Production Research, 59(18), 5470–5499. https://doi.org/10.1080/00207543.2021.1951653

British Standards Institution. (2023). Cybersecurity guidance for SMEs. BSI Group.

British Standards Institution. (2023). Business continuity management for SMEs. BSI Group.

Cybersecurity and Infrastructure Security Agency. (2023). Cybersecurity awareness toolkit for small businesses. U.S. Department of Homeland Security.

Dahlberg, T., & Nokkala, T. (2022). The COVID-19 pandemic's impact on SMEs' cybersecurity. Computers & Security, 116, 102642. https://doi.org/10.1016/j.cose.2022.102642

Doern, R., Williams, N., & Vorley, T. (2019). Entrepreneurship and crises: Business as usual? Entrepreneurship & Regional Development, 31(5-6), 400–412. https://doi.org/10.1080/08985626.2018.1541590

Elliott, D., Swartz, E., & Herbane, B. (2019). Business continuity management: A crisis management approach (2nd ed.). Routledge.

Elkington, J. (1997). Cannibals with forks: The triple bottom line of 21st century business. Capstone.

European Union Agency for Cybersecurity. (2022). Cybersecurity for SMEs: Challenges and recommendations. ENISA.

Fernandez-Aleman, J. L., Seva-Llor, C., Toval, A., & Carrillo-de-Gea, J. M. (2018). Governance models and data protection in SMEs. Health Information Science and Systems, 6(1), 1–9. https://doi.org/10.1007/s13755-018-0054-2

Floridi, L., Mittelstadt, B., Allo, P., Taddeo, M., & Almeida, S. (2018). AI4People—An ethical framework for a good AI society. Minds and Machines, 28, 689–707. https://doi.org/10.1007/s11023-018-9482-5

Guo, S., & Pang, M. (2025). Digital technology adoption and sustainability performance: The role of data security. Journal of Cleaner Production, 442, 141233. https://doi.org/10.1016/j.jclepro.2024.141233

Gupta, A., Kumar, R., Singh, A., & Dhaliwal, M. (2023). SME readiness for cybersecurity in digital ecosystems. Information Systems Management, 40(2), 132–148. https://doi.org/10.1080/10580530.2022.2128965

Herbane, B. (2022). Rethinking organisational resilience and continuity: A dynamic-capabilities approach. Journal of Contingencies and Crisis Management, 30(2), 100–112. https://doi.org/10.1111/1468-5973.12353

IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation.

International Organization for Standardization. (2022a). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection. ISO.

International Organization for Standardization. (2022b). ISO/IEC 22301:2022 – Security and resilience – Business continuity management systems – Requirements. ISO.

Jansen, J., & Leukfeldt, R. (2021). Trust and cybercrime victimisation in SMEs. Journal of Business Research, 134, 556–565. https://doi.org/10.1016/j.jbusres.2021.05.046

Karim, N. S. A., Abdullah, S., & Malik, S. (2022). Integrating cybersecurity training into SME digital transformation. Asian Journal of Business and Accounting, 15(1), 123–142. https://doi.org/10.22452/ajba.vol15no1.5

Karwatzki, S., Jahn, K., & Baumgartner, F. (2022). Sustainability reporting and data governance in European SMEs. Sustainability Accounting, Management and Policy Journal, 13(4), 789–813. https://doi.org/10.1108/SAMPJ-07-2021-0242

Karwatzki, S., Sävola, F., Trenz, M., & Veit, D. (2017). Adverse consequences of access to personal information. Information Systems Journal, 27(2), 163–200. https://doi.org/10.1111/isj.12088

Kato, M., & Charoenrat, T. (2023). Disaster-risk resilience in Southeast Asian SMEs: A mixed-methods assessment. Journal of Asian Economics, 85, 101523. https://doi.org/10.1016/j.asieco.2023.101523

Kraemer-Mbula, E., Wunsch-Vincent, S., & Ellis, M. (2022). Leadership cognition and digital risk management in African SMEs. Technological Forecasting and Social Change, 181, 121738. https://doi.org/10.1016/j.techfore.2022.121738

Kraus, S., Jones, P., & Kailer, N. (2024). SME crisis management: A systematic review and future agenda. International Small Business Journal, 42(1), 3–32. https://doi.org/10.1177/02662426231197118

Kumar, N., Saini, H., & Thakur, S. (2022). Ransomware targeting SMEs: Causes and countermeasures. Journal of Information Privacy and Security, 18(3), 177–193. https://doi.org/10.1080/15536548.2022.2087654

Lengnick-Hall, C. A., & Beck, T. E. (2005). Adaptive fit versus robust transformation: How organizations respond to environmental change. Journal of Management, 31(5), 738–757. https://doi.org/10.1177/0149206305279367

Li, Q., Yu, Z., & Chen, L. (2023). Cybersecurity awareness and SMEs' data-protection strategies: Evidence from China. Information Systems Management, 40(1), 54–67. https://doi.org/10.1080/10580530.2022.2096590

Li, Y., Zhang, X., & Lin, R. (2024). Data governance, analytics capabilities and ESG disclosures: A comparative study of SMEs. Sustainability, 16(3), 1221. https://doi.org/10.3390/su16031221

Mittelstadt, B. (2017). Principles alone cannot guarantee ethical AI. Nature Machine Intelligence, 1, 501–507. https://doi.org/10.1038/s42256-019-0088-8

Mital, M., Pani, A., & Ranjan, J. (2023). Socio-technical alignment for organisational resilience: Evidence from emerging-market SMEs. Information Systems Frontiers, 25, 41–62. https://doi.org/10.1007/s10796-022-10278-3

Mökander, J., & Floridi, L. (2021). Ethics-based auditing to develop trustworthy AI. Minds and Machines, 31(4), 595–610. https://doi.org/10.1007/s11023-021-09551-w

Morales-Sáenz, R., Jiménez, C., & Ortega, J. (2024). Cybersecurity capabilities and sustainable digital innovation: A mediation model. Sustainability, 16(4), 2133. https://doi.org/10.3390/su16042133

MSCI. (2024). MSCI ESG ratings methodology 2024 update. MSCI Inc.

National Institute of Standards and Technology. (2023). Resilience framework for small business. U.S. Department of Commerce.

Organisation for Economic Co-operation and Development. (2023). SME and entrepreneurship outlook 2023. OECD Publishing.

Parker, H., & Ameen, J. (2024). Financial resilience and continuity planning in SMEs. Journal of Financial Management, 48(2), 215–238. https://doi.org/10.1002/fm.2406

Radanliev, P., De Roure, D., Nicolescu, R., & Ani, U. (2020). SME cyber-risk management using integrated models. Risk Analysis, 40(9), 1772–1785. https://doi.org/10.1111/risa.13549

ISSN [Online]: 2776-6381

Rangone, A., & Di Fatta, G. (2022). Business-continuity capabilities as strategic resources in digital resilience. International Journal of Information Management, 66, 102516. https://doi.org/10.1016/j.ijinfomgt.2022.102516

Rejeb, A., Keogh, J. G., & Treiblmaier, H. (2023). The impact of cyber threats on SMEs' operational resilience. Sustainability, 15(4), 3678. https://doi.org/10.3390/su15043678

Reuter, C., Yan, Q., & Holanda, M. (2023). Data privacy and consumer trust in SME digital services. Journal of Business Ethics, 185(3), 521–539. https://doi.org/10.1007/s10551-023-05350-6

Santoso, A., & Wardhana, A. (2024). Regulatory compliance and digital-risk governance in Indonesian SMEs. Asian Journal of Business Ethics, 13(1), 75–94. https://doi.org/10.1007/s13520-023-00147-8

Santos, V., Mendes, M. T., & Santos, A. (2021). Business continuity in Portuguese SMEs: An exploratory study. International Journal of Disaster Risk Reduction, 67, 102671. https://doi.org/10.1016/j.ijdrr.2021.102671

Schinagl, S., Paans, R., & Teuteberg, F. (2023). Cybersecurity–BCM alignment and performance in European SMEs. Information & Management, 60(6), 103808. https://doi.org/10.1016/j.im.2023.103808

Siponen, M., & Oinas-Kukkonen, H. (2007). A review of information-security issues and respective research contributions. The DATA BASE for Advances in Information Systems, 38(1), 60–80. https://doi.org/10.1145/1216218.1216224

Tang, Y., Wu, Z., & Zhang, L. (2021). Risk perceptions of SMEs in cybersecurity. Cybersecurity, 4(1), 12. https://doi.org/10.1186/s42400-021-00077-6

Tavoletti, E., Demartini, P., & Ghiselli, G. (2022). Strategic digital readiness and SMEs: A framework of adoption. Journal of Small Business and Enterprise Development, 29(6), 1054–1074. https://doi.org/10.1108/JSBED-06-2021-0257

Teece, D. J. (2021). Dynamic capabilities and strategic management: Organizing for innovation and growth (2nd ed.). Oxford University Press.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU GDPR: Enforcement, consequences, and lessons for privacy research. Computer Law & Security Review, 34(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.002

United Nations Conference on Trade and Development. (2024). World investment report 2024: Investing in sustainable digitalization. UNCTAD.

United Nations Office for Disaster Risk Reduction. (2022). SME guide to business continuity planning. UNDRR.

Verreynne, M.-L., Parker, P., & Wilson, N. (2023). Resilience capabilities in small enterprises: A cluster analysis. Small Business Economics, 60(1), 95–119. https://doi.org/10.1007/s11187-022-00641-0

World Bank. (2023). World development report 2023: Investing in digital resilience. World Bank Publications.

Yuliana, I., & Oktaviani, N. (2023). Legal preparedness for personal data protection in Indonesian SMEs. Jurnal Hukum & Pembangunan, 53(2), 145–160. https://doi.org/10.21143/jhp.vol53.no2.3324

Zhao, M., Xu, G., & Xiong, J. (2023). Cloud-native continuity solutions for SMEs: A comparative study. Journal of Cloud Computing, 12(1), 48. https://doi.org/10.1186/s13677-023-00413-9