Next Scientists
Journal of Management and Economics

TYPE Original Research
PAGE NO. 16-22

Resilience by Design: An Integrative Framework for Cybersecurity Readiness, Risk Management, and Threat Mitigation in Small and Medium-Sized Enterprises

Selvion G. Harstrom

Faculty of Management, Technology & Economics, ETH Zurich, Switzerland

OPEN ACCESS

SUBMITTED 07 September 2025
ACCEPTED 18 September 2025
PUBLISHED 23 September 2025
VOLUME Vol.05 Issue 09 2025

Abstract:

Background: Small and Medium-sized Enterprises (SMEs) constitute the backbone of the global economy yet remain disproportionately vulnerable to cyber threats due to resource constraints and a lack of specialized expertise. Traditional enterprise-grade security frameworks are often too complex or costly for these entities to implement effectively.

Methods: This study employs a systematic review methodology, adhering to PRISMA-P protocols, to analyze current literature on SMB cybersecurity behaviors, risk management strategies, and technological adoption. The review synthesizes data regarding the efficacy of Managed Detection and Response (MDR) services, the "HOGO" reference framework, and the mediating role of organizational awareness.

Results: The analysis reveals that while threat awareness is increasing, it does not inextricably lead to improved security posture without structured management capabilities. The integration of outsourced MDR services significantly mitigates the technical skills gap. Furthermore, adapting ISO 27002-based frameworks (such as HOGO) provides a necessary scaffold for compliance and resilience.

Conclusion: Achieving cybersecurity resilience in the SMB sector requires a hybrid approach that combines simplified governance frameworks with cost-effective, outsourced technical solutions. Future policy must focus on incentivizing the adoption of these integrated

models to protect the digital ecosystem.

Keywords: SMB Cybersecurity, Risk Management, Managed Detection and Response, ISO 27002, HOGO Framework, Organizational Resilience, Threat Mitigation.

1.Introduction

The contemporary digital economy is characterized by a profound paradox. On one hand, Small and Medium-sized Enterprises (SMBs) are the engines of innovation and employment, representing a vast majority of global business entities. On the other hand, they represent the "soft underbelly" of the digital ecosystem—highly interconnected yet frequently under-protected. As large enterprises harden their perimeters with sophisticated defense-in-depth strategies, cybercriminal syndicates have increasingly pivoted their focus toward smaller targets. Recent data suggests that small firms suffer close to 10,000 cyber-attacks daily [14], a statistic that underscores the relentless nature of the threat landscape.

Unlike their larger counterparts, SMBs often lack the financial elasticity to absorb the costs associated with a significant data breach or ransomware attack. The "invisible hole" of information regarding SMB cybersecurity practices [21] further complicates the issue; much of the prevailing academic and industrial guidance is derived from enterprise-level case studies that do not translate effectively to the operational realities of a fifty-person manufacturing firm or a regional logistics provider. The assumption that "security through obscurity" offers protection is no longer valid in an era of automated vulnerability scanning and mass-market ransomware-as-a-service (RaaS) kits.

The regulatory environment is also shifting, placing a heavier compliance burden on smaller organizations. Initiatives such as the EU Cybersecurity Act [8] aim to standardize security certification schemes, forcing SMBs to grapple with complex compliance mandates previously reserved for critical infrastructure or financial institutions. This creates a tension between the necessity of digital transformation—adopting cloud services, IoT devices, and remote work capabilities—and the imperative to secure these expanding attack surfaces.

This paper aims to bridge the gap between high-level security theory and the pragmatic needs of the SMB sector. By synthesizing recent developments in Managed Detection and Response (MDR) services [1], risk management frameworks like HOGO [2], and behavioral analysis of management capability [4], we propose an integrative framework. This framework seeks to provide a pathway for SMBs to achieve "resilience by design," moving beyond ad-hoc fire-fighting toward a structured, sustainable security posture.

2. Literature Review

2.1 The Vulnerability Context and the "Invisible Hole"

The literature consistently highlights a disparity in how cybersecurity is conceptualized in large versus small organizations. Gafni and Pavel [21] describe an "invisible hole" of information, arguing that the unique constraints of SMBs—specifically the lack of dedicated IT security personnel—are often overlooked in broader security studies. This lack of visibility is dangerous because it masks the systemic risks accumulating within the supply chains of larger economies. Heikkila et al. [22] emphasize this in the context of manufacturing, noting that as Industry 4.0 connects factory floors to the internet, legacy equipment in small machine shops becomes a critical vector for intrusion.

The threat landscape for SMBs is not merely a scaled-down version of the enterprise threat landscape; it is distinct. Dickson [14] notes the sheer volume of daily attacks, which suggests that automation allows attackers to target SMBs en masse. Furthermore, the adoption of Internet of Things (IoT) devices has expanded the attack surface significantly. Eaves [17] argues that while IoT offers operational efficiency, the security standards for these devices are often lax, and SMBs lack the network segmentation capabilities to isolate insecure devices from critical business data.

2.2 Risk Management and Decision Making

Risk management in SMBs is often characterized by informality. Berry and Berry [5] provide an initial assessment of these approaches, noting that many small business owners treat cyber risk as a pure IT issue rather than a strategic business risk. This compartmentalization leads to underinvestment. Osborn and Simpson [15] explore the decision-making dialogue in UK case studies, finding that risk perception is heavily influenced by cognitive biases; if a peer organization has not suffered a

visible breach, an SMB owner is likely to underestimate their own probability of attack.

This disconnect is further explored by Cleveland and Scheg [6], who examined the intention related to cyberthreat awareness. They posit that awareness alone is insufficient to drive behavioral change without a corresponding increase in "self-efficacy"—the belief that the organization has the capability to mitigate the risk. Without this, awareness leads to fatalism rather than action. Eilts [16] reinforces this with an empirical assessment of readiness, suggesting that resilience is not just about technology, but about the organizational culture's ability to respond to disruption.

2.3 The Role of Frameworks and Standards

Standardization is a double-edged sword for SMBs. While frameworks like ISO 27001 provide a gold standard, they are often viewed as bureaucratically crushing. Cruzado et al. [2] introduce the "HOGO" reference framework, which attempts to adapt ISO 27002 and 27032 specifically for SMEs. This represents a crucial shift in the literature: moving from "light" versions of enterprise standards to bespoke frameworks designed for the SME context. Similarly, the Cloud Security Alliance's "CCM Lite" [7] represents an acknowledgement by industry bodies that the full Cloud Controls Matrix is unwieldy for smaller teams.

González et al. [11] argue that organizational practices are the true antecedents of security performance. It is not the purchase of a firewall that predicts safety, but the maintenance of the firewall and the policy governing its configuration. This aligns with the work of Oroni and Fu [4], who establish that management capability mediates the relationship between awareness and enterprise performance. In essence, a well-managed company is a secure company, regardless of the specific tools used.

2.4 Technical Solutions and Outsourcing

Given the chronic skills shortage in cybersecurity, the literature increasingly points toward outsourcing as a viability strategy. Rajgopal [1] presents a compelling case for MDR service design, arguing that 24/7 threat coverage is mathematically impossible for an SMB to achieve in-house. The shift from Capital Expenditure (CapEx) on hardware to Operational Expenditure (OpEx) on services like MDR and cloud-based Intrusion Detection Systems (IDS) [19] is a recurring theme.

Elezaj et al. [19] demonstrate that data-driven IDS can be tailored for SMEs, but the management of these alerts remains a bottleneck, reinforcing the need for managed services.

3. Methodology

3.1 Systematic Review Protocol

To ensure the rigor and replicability of this study, we adopted a systematic review methodology informed by the guidelines of Tranfield et al. [9] and the PRISMA-P statement [12]. The systematic review is the preferred instrument for synthesizing evidence in management science because it minimizes bias and allows for the aggregation of fragmented case studies.

The review process involved a comprehensive search of academic databases (IEEE Xplore, ProQuest, ScienceDirect) using keywords such as "SMB Cybersecurity," "SME Risk Management," "MDR," and "ISO 27002 Adaptation." The search was restricted to papers published between 2011 and 2025 to ensure relevance to the modern threat landscape.

3.2 Inclusion and Exclusion Criteria

We prioritized studies that specifically addressed the organizational size constraint. General cybersecurity papers that did not stratify results by company size were excluded, as were purely technical papers describing cryptographic algorithms without an operational context. We also placed high emphasis on descriptive validity, as argued by Gill [3], ensuring that the studies selected provided sufficient context to determine if their findings were applicable to the general SMB population.

3.3 Theoretical Synthesis

Following the data extraction, we employed a narrative synthesis approach. We utilized the "Context-Intervention-Mechanism-Outcome" (CIMO) logic to structure the findings.

- *Context:* The resource-constrained SMB environment.
- *Intervention:* The adoption of frameworks (HOGO) and services (MDR).
- *Mechanism:* Improved management capability and risk visibility.
- *Outcome:* Enhanced resilience and business continuity.

This theoretical modeling allows us to integrate disparate findings—such as the psychological insights of Cleveland and Scheg [6] with the technical architecture

of Rajgopal [1]—into a single coherent argument.

4. Results and Analysis

4.1 The Awareness-Capability Gap

One of the most significant findings from the review is the distinction between "awareness" and "capability." Eş and Serdar [20] conducted an investigation into awareness levels in Ankara, finding that while basic awareness of terms like "phishing" was high, the practical application of this knowledge was low. Employees knew what a suspicious email looked like in theory but frequently failed to identify high-quality spear-phishing attempts in practice.

This aligns with the structural evaluation by Oroni and Fu [4], which indicates that management capability acts as a mediator. In organizations where management explicitly prioritized security metrics (e.g., included them in performance reviews), the conversion of awareness to secure behavior was significantly higher. Conversely, in organizations where security was treated solely as an IT function, high awareness scores did not correlate with a reduction in incidents. This suggests that the "human firewall" is brittle without structural support.

4.2 The Efficacy of Framework Adaptation (HOGO)

The analysis of Cruzado et al. [2] regarding the HOGO framework yields critical insights. Standard ISO 27002 implementations often fail in SMBs because they require dedicated compliance officers. HOGO simplifies this by prioritizing controls based on impact. The results indicate that SMBs using adapted frameworks show a higher maturity in "Process" and "People" domains compared to those attempting to implement the full ISO standard, who often abandon the project midway due to resource exhaustion.

The "HOGO" approach—focusing on Human, Organizational, and Governance aspects—demonstrates that security in SMBs is less about purchasing the correct appliance and more about establishing a repeatable rhythm of verification. The framework encourages a cycle of "Plan-Do-Check-Act" that is rightsized for smaller teams.

4.3 The Role of MDR in Closing the Skills Gap

Rajgopal [1] provides quantitative evidence that MDR services significantly reduce the "dwell time" of threats in SMB networks. Dwell time—the duration an attacker remains undetected—is the primary predictor of damage cost. For an SMB attempting to run an in-house Security Operations Center (SOC) during business hours only (8x5), the dwell time for attacks launching on Friday evenings is catastrophic. MDR services, by providing 24/7 coverage, reduce this dwell time from days to minutes.

Furthermore, the cost analysis suggests that for an SMB to replicate the capability of an MDR provider (SIEM licensing, threat intelligence feeds, 24/7 staffing of analysts), the cost would be approximately 6-8 times higher than the subscription cost of the service. This economic efficiency is the primary driver for the adoption of outsourced security models.

4.4 Regional Nuances and Regulatory Impact

The review of case studies from Saudi Arabia [13] and the EU [8] indicates that regulation is a primary driver of investment. In the EU, the GDPR and the Cybersecurity Act have forced a baseline of encryption and data protection. In regions with less stringent data privacy laws, SMB security investment is significantly lower, often reactive only after a breach occurs. This suggests that voluntary compliance is rarely sufficient; regulatory pressure is a necessary antecedent for widespread adoption of security practices in the SMB sector.

5. Discussion

5.1 Operationalizing the HOGO Framework and Structural Resilience

The synthesis of the literature points inevitably toward a need for structural adaptation. It is insufficient to simply tell SMBs to "be more secure"; they require a blueprint that acknowledges their limitations. The HOGO framework [2], as identified in the results, offers a compelling starting point, but to fully operationalize it, we must integrate the findings of Oroni and Fu [4] regarding management capability.

Operationalizing HOGO in an SMB requires a shift from "controls-based" thinking to "risk-based" thinking. In a controls-based model, an organization asks, "Do we have a firewall?" In a risk-based model, they ask, "What happens if our customer database is encrypted?" This shift is subtle but profound. It moves the discussion from the server room to the boardroom.

The first pillar of this operationalization is **Governance Lite**. Based on the principles of ISO 27001 but stripped of

the heavy documentation requirements, Governance Lite focuses on three core documents: an Acceptable Use Policy, an Incident Response Plan, and a Vendor Risk Assessment. These three documents cover the vast majority of liability and risk for an SMB. The Incident Response Plan is particularly critical. As noted by Weisburd et al. [10] in the context of crime prevention, the certainty of response is often a greater deterrent (or in cyber terms, a mitigator) than the severity of the defense. An SMB that knows exactly who to call and which server to unplug can reduce the cost of a breach by orders of magnitude compared to one that panics.

The second pillar is **Asset-Centric Protection**. Heikkila et al. [22] highlighted the vulnerability of manufacturing systems. Operationalizing resilience means identifying the "Crown Jewels"—the specific data or systems that, if lost, would cause the business to fail. For a law firm, this is client data; for a manufacturer, it is the CAD drawings and the production line software. Security spend must be disproportionately allocated to these assets. This aligns with the "CCM Lite" approach [7], where controls are mapped to critical cloud assets rather than applied primarily across the entire infrastructure.

The third pillar is **Continuous Human Verification**. While Cleveland and Scheg [6] discussed intention, the operationalization of this involves testing. Phishing simulations, tabletop exercises, and "war gaming" for executives are not just for the Fortune 500. A quarterly tabletop exercise where the CEO and the IT manager sit down for one hour to walk through a "ransomware scenario" creates more resilience than thousands of dollars of software. It builds the muscle memory required for decision-making under pressure. This directly addresses the "decision-making dialogue" risks identified by Osborn and Simpson [15].

5.2 The Economics of MDR and the Outsourcing Imperative

Expanding on the findings of Rajgopal [1], we must critically examine the economic architecture of modern cybersecurity for SMBs. The traditional model of IT—where a generalist system administrator handles everything from printer jams to firewall configuration—is functionally obsolete in the face of advanced persistent threats (APTs). The "Jack of all trades" is the master of none, and in cybersecurity, being a novice is a liability.

The economic argument for Managed Detection and Response (MDR) is not merely about cost savings; it is about *access to economies of scale*. A top-tier MDR provider aggregates threat intelligence from thousands of customers. If a dental clinic in London is hit by a specific strain of ransomware at 9:00 AM, the MDR provider can push a blocking rule to a logistics company in New York by 9:05 AM. An individual SMB cannot achieve this "herd immunity" in isolation. This network effect is the single greatest advantage of the outsourced model.

However, outsourcing is not a panacea. It introduces a new risk: **Vendor Supply Chain Risk**. By relying on an MDR provider, the SMB is placing its trust in a third party. If that third party is compromised (as seen in major supply chain attacks like Kaseya or SolarWinds), the SMB is vulnerable. Therefore, the *management capability* described by Oroni and Fu [4] must evolve to include *Vendor Management Capability*. The SMB owner does not need to know how to configure a SIEM, but they must know how to read the Service Level Agreement (SLA) and audit the performance of their MDR provider.

Furthermore, the integration of MDR must be coupled with **Internal Context**. An external analyst in a Security Operations Center (SOC) halfway across the world does not know that the server labeled "SRV-04" is the backup server that hasn't been used in three years, while "SRV-02" processes all payroll. Without internal context, the MDR service generates false positives or misses the business impact of a true positive. Therefore, the most successful model is a "Hybrid" one: the SMB retains a small, knowledgeable IT liaison who bridges the gap between the business context and the external MDR technical capability.

This economic restructuring also impacts the insurance market. As noted by Berry and Berry [5], risk management approaches are maturing. Cyber insurance providers are increasingly mandating the use of MDR or equivalent monitoring services as a condition of coverage. This creates a virtuous cycle: to get insurance, an SMB must improve its posture; by improving its posture via MDR, it reduces its risk; by reducing its risk, it

lowers its premium. The "invisible hole" [21] is slowly being filled by actuarial data.

5.3 The Psychology of "Security Fatigue" and Sustainable Culture

We must also expand on the behavioral aspects touched upon by Eş and Serdar [20]. The phenomenon of "security fatigue"—where users become desensitized to constant warnings and complex password requirements—is a major threat to resilience. If security controls impede business agility, employees will find workarounds. They will use personal Dropbox accounts to transfer files if the corporate VPN is too slow; they will write passwords on post-it notes if the rotation policy is too aggressive.

Luukkonen and Sönmez [18] discuss sustainable economics; we must parallel this with **Sustainable Security**. A sustainable security culture is one that minimizes friction. This involves the adoption of technologies that are secure by default but invisible to the user, such as biometric authentication (FIDO2) which eliminates the need for complex passwords, or Zero Trust Network Access (ZTNA) which replaces clunky VPNs. By reducing the cognitive load on the employee, we improve the compliance rate.

Moreover, the narrative around security in SMBs needs to change from "Fear, Uncertainty, and Doubt" (FUD) to "Quality and Trust." Almubayedh et al. [13] highlight security issues in Saudi organizations, but the lesson is universal: security should be framed as a competitive advantage. An SMB that can prove to its clients that their data is secure (perhaps through a certification based on the HOGO framework) can win business over a competitor who cannot. Security becomes a revenue enabler, not a cost center. This reframing is essential for securing the buy-in of non-technical leadership.

5.4 Limitations and Future Research Directions

While this study synthesizes a broad range of data, several limitations exist. First, the definition of "SMB" or "SME" varies significantly across jurisdictions (e.g., the EU definition differs from the US definition), which complicates direct statistical comparison. Second, the rapid evolution of AI-driven threats (Deepfakes, AI-generated phishing) may outpace the static controls found in ISO adaptations like HOGO.

Future research should focus on longitudinal studies of SMBs that have adopted MDR services to quantify the long-term return on investment (ROI). Additionally, more empirical work is needed to validate the HOGO framework in diverse industries beyond the initial scope of Cruzado et al. [2]. The intersection of AI and SMB security—both as a threat and as a defense mechanism—remains a fertile ground for investigation.

6. Conclusion

The cybersecurity challenges facing Small and Medium-sized Enterprises are systemic, severe, and escalating. The "security through obscurity" model is dead. However, this paper argues that the situation is not hopeless. By rejecting the "enterprise-lite" approach and instead embracing frameworks and services specifically designed for the SMB context, resilience is achievable.

The integration of the HOGO reference framework provides the necessary governance structure—the "bones" of the security posture. The adoption of MDR services provides the technical muscle—the 24/7 "eyes on glass" that SMBs cannot afford to build themselves. Finally, the cultivation of management capability and awareness provides the nervous system, ensuring that the organization can react and adapt.

Policymakers must support this transition by simplifying compliance mandates and perhaps offering tax incentives for SMBs that achieve verified security standards. For the SMB owner, the path forward is clear: acknowledge the risk, outsource the complexity, and internalize the responsibility. Only through this "resilience by design" can the SMB sector continue to thrive in an increasingly hostile digital environment.

REFERENCES

1. Rajgopal, P. R. (2025). MDR service design: Building profitable 24/7 threat coverage for SMBs. International Journal of Applied Mathematics, 38(2s), 1114-1137.

2. Cruzado, C. F., Rodriguez-Baca, L. S., Huanca-Lopez, L. G., & Acuna-Salinas, E. I. (2022). Reference framework “HOGO” for cybersecurity in SMEs based on ISO 27002 and 27032.

3. Gill, C. (2011). Missing links: how descriptive validity impacts the policy relevance of randomized

controlled trials in criminology. Journal of Experimental Criminology, 7(3), 201–224.

4. Oroni, C. Z., & Fu, X. (2023). Structural evaluation of management capability and the mediation role of cybersecurity awareness towards enterprise performance.

5. Berry, C. T., & Berry, R. (2018). An initial assessment of small business risk management approaches for cyber security threats. International Journal of Business Continuity and Risk Management, 8(1).

6. Cleveland, J., & Scheg, A. (2018). Small-Medium Business Information Security Intention Related to Cyberthreat Awareness: A Quantitative Experiment. PhD thesis, Northcentral University, Ann Arbor.

7. Cloud Security Alliance. (2025). CCM Lite | CSA. https://cloudsecurityalliance.org/research/ccm-lite.

8. European Commission. (2020). The EU Cybersecurity Act: Shaping Europe's digital future. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.

9. Tranfield, D., Denyer, D., & Smart, P. (2003). Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review.

10. Weisburd, D., Farrington, D., & Gill, C. (2017). What Works in Crime Prevention and Rehabilitation: An Assessment of Systematic Reviews. Criminology and Public Policy, 16(2), 415–449.

11. González, D. P., Trigueros-Preciado, S., & González, P. S. (2019). Organizational practices as antecedents of the information security management performance.

12. Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Shekelle, P., & Stewart, L. A. (2016). Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. Revista Espanola de Nutricion Humana y Dietetica, 20(2), 148–160.

13. Almubayedh, D. A., Al khalis, M., Alazman, G., Alabdali, M., Al-Refai, R., & Nagy, N. (2018). Security Related Issues In Saudi Arabia Small Organizations: A Saudi Case Study. 21st Saudi Computer Society National Computer Conference, NCC 2018, 21, 1–6.

14. Dickson, M. (2019). Small firms suffer close to 10,000 cyber-attacks daily. FSB, The Federation of Small Businesses.

15. Osborn, E., & Simpson, A. (2018). Risk and the Small-Scale Cyber Security Decision Making Dialogue - a UK Case Study.

16. Eilts, D. (2020). An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses. ProQuest Dissertations and Theses, 11(15), 309.

17. Eaves, S. (2023). Security for Small and Medium-Sized Businesses | IoT Security Podcast | PSA Certified.

18. Luukkonen, O. A., & Sönmez, Y. Ü. (2022). Cybersecurity for Small and Medium-Sized Businesses. Journal of Sustainable Economics and Management Studies, 3(1), 21-38.

19. Elezaj, O., Yayilgan, S. Y., Abomhara, M., Yeng, P., & Ahmed, J. (2019). Data-Driven Intrusion Detection System for Small and Medium Enterprises. IEEE 24th Int. Workshop on Computer Aided Modeling and Design of Communication Links and Networks, 1–7.

20. Eş, A., & Serdar, N. (2021). SİBER Saldirilara Karşı Kobilerin Farkındalık Düzeylerini Incelenmesi: Ankara Ili Örneği. Journal of Duzce University Institute of Social Sciences, 11(1), 133–151.

21. Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB's cybersecurity. Online Journal of Applied Knowledge Management (OJAKM), 7(1), 14–26.

22. Heikkila, M., Rattya, A., Pieska, A. S., & Jansa, J. (2016). Security Challenges in Small- and Medium-Sized Manufacturing Enterprises. Int. Symp. On Small-scale Intelligent Manufacturing Systems, 25–30.