European International Journal of Multidisciplinary Research and Management Studies

TYPE Original Research
PAGE NO. 41-46

Check for updates

OPEN ACCESS
SUBMITTED 13 October 2025
ACCEPTED 22 October 2025
PUBLISHED 31 October 2025
VOLUME Vol.05 Issue10 2025

Operationalizing Cybersecurity Resilience in Small and Medium Enterprises: An Integrated Analysis of Adaptive Maturity Models, Managed Threat Response, and Regulatory Compliance

Daria K. Novokreshchenova
Independent Researcher, Cyber Risk Governance & Regulatory Compliance, Saint Petersburg, Russia

Abstract: Small and Medium-sized Enterprises (SMEs) increasingly face sophisticated cyber threats previously reserved for large multinational corporations. However, SMEs often lack the financial liquidity, technical expertise, and personnel required to maintain robust security postures. This article investigates the multifaceted challenges of SME cybersecurity, proposing an integrated approach that combines adaptive maturity models with Managed Detection and Response (MDR) services. Utilizing a systematic review and thematic analysis of recent literature, we examine the efficacy of current frameworks, including Situational Crime Prevention (SCP) techniques and AI-driven security solutions in the context of Industry 4.0. The study identifies a critical "resource-risk gap" where traditional, static security policies fail to address the dynamic nature of modern cybercrime. Our results suggest that static compliance is insufficient; instead, SMEs must adopt adaptive security architectures that scale with their digital footprint. Furthermore, the analysis highlights the pivotal role of MDR services in providing 24/7 threat coverage, effectively outsourcing the Security Operations Center (SOC) function that is financially unviable for most SMEs to build in-house. We also explore the human element, emphasizing that cybersecurity awareness (CSA) among management is a prerequisite for effective technical implementation. The findings culminate in a recommendation for a hybrid

resilience strategy:leveraging external expertise through MDR while fostering internal "cyber hygiene" through standardized labeling and cascading best practices. This research contributes to the field by offering a practical roadmap for operationalizing cybersecurity in resource-constrained environments.

Keywords: SME Cybersecurity, Managed Detection and Response (MDR), Adaptive Security Architecture, Situational Crime Prevention, Regulatory Compliance, Risk Management, Cyber Resilience

1.Introduction:

The digital transformation of the global economy has fundamentally altered the operational landscape for Small and Medium-sized Enterprises (SMEs). While digitalization has unlocked unprecedented opportunities for market reach and operational efficiency, it has concurrently expanded the attack surface available to malicious actors. Historically, cybersecurity discourse focused predominantly on large enterprises with significant data assets. However, recent trends indicate a strategic pivot by cybercriminals toward SMEs, which are increasingly viewed as "soft targets"—entities that possess valuable data or supply chain access but lack the sophisticated defense mechanisms of larger corporations.

The urgency of this issue is underscored by the rising cost of data breaches. As noted in global assessments, the financial impact of a breach involves not only immediate remediation costs but also long-term reputational damage and regulatory fines [17]. For an SME, the margin for error is perilously thin; a single significant ransomware attack or data exfiltration event can threaten the firm's solvency. Despite this existential risk, the adoption of comprehensive security measures in the SME sector remains inconsistent. This hesitation is often attributed to a lack of resources, specifically the prohibitive cost of maintaining an in-house Security Operations Center (SOC) and the scarcity of skilled cybersecurity professionals.

Furthermore, the threat landscape in developing and emerging economies adds another layer of complexity to this global challenge. Research into the digital business environment in regions such as Indonesia indicates that the rapid digitization of commerce has outpaced the development of security infrastructure, creating a fertile ground for cybercrime [3]. This phenomenon is not isolated; it reflects a global pattern where digital adoption acts as a double-edged sword. The integration of Industry 4.0 technologies—including the Internet of Things (IoT) and cloud computing—has introduced new vulnerabilities that require advanced detection capabilities, often leveraging Artificial Intelligence (AI) [7].

This article argues that the traditional "moat and castle" approach to cybersecurity is obsolete for SMEs. Instead, resilience requires a dynamic, adaptive approach that integrates human awareness, regulatory compliance, and outsourced advanced capabilities such as Managed Detection and Response (MDR). By synthesizing insights from recent literature on Situational Crime Prevention (SCP) [4], cybersecurity awareness (CSA) [2], and adaptive security maturity models [16], this study aims to provide a holistic framework for SME cybersecurity. We posit that the solution lies not in attempting to replicate enterprise-grade security in miniature, but in adopting flexible, service-oriented models that provide high-level protection through economies of scale and specialized external partnerships.

2. Literature Review

2.1 Situational Crime Prevention in Cyberspace

The theoretical underpinnings of cyber defense often draw from criminology. Ho, Ko, and Mazerolle [4] explore the application of Situational Crime Prevention (SCP) techniques to the digital domain. SCP theory suggests that crime can be reduced by altering the immediate environment to increase the effort and risks for offenders while reducing the rewards. In the context of SME cybersecurity, this translates to "target hardening" (e.g., multi-factor authentication), "access control" (e.g., zero-trust architectures), and "guardianship" (e.g., active monitoring). However, the literature suggests that SMEs often struggle to implement these techniques effectively due to a lack of technical understanding and the perception that security measures impede business agility.

2.2 The Human Factor and Awareness

Technology alone is insufficient if the human operators remain the weakest link. Eybers and Mvundla [2] highlight the critical importance of Cybersecurity Awareness (CSA) amongst managers. Their findings suggest that security culture trickles down from the top; if leadership views security as merely an IT issue rather than a strategic business imperative, compliance among staff wavers. This is corroborated by Cartwright, Cartwright, and Edun [11], who discuss the "cascading information" effect. They argue that IT service providers play a crucial role in disseminating best practices to micro and small businesses. However, this reliance on external providers also introduces a dependency risk—

if the IT provider fails to communicate risks effectively, the SME remains oblivious to its vulnerabilities.

2.3 Regulatory and Compliance Pressures

The regulatory environment for data protection has become increasingly stringent. In Nigeria, for instance, there is an urgent call for the reform of cybercrime regulatory agencies to better protect the digital economy [6]. Similarly, in the European context, Johannsen, Kant, and Creutzburg [9] emphasize the necessity of measuring IT security compliance and data governance. For SMEs, navigating this complex web of regulations—such as GDPR in Europe or various national data protection acts—is a significant burden. The literature indicates a tension between "tick-box" compliance, where firms aim to meet the minimum legal requirements, and genuine security maturity, which focuses on actual risk reduction.

2.4 The Technological Shift: Cloud and AI

As SMEs migrate to the cloud, the security paradigm shifts from protecting on-premise assets to securing distributed environments. Roy and Patil [12] propose frameworks specifically for cloud security initiatives in SMEs, emphasizing shared responsibility models. Concurrently, the rise of Industry 4.0 has necessitated the integration of AI-based security measures [7]. Artificial Intelligence offers the potential to automate threat detection, analyzing vast amounts of traffic data to identify anomalies that would be invisible to human analysts. This automation is particularly promising for SMEs, as it acts as a force multiplier, allowing small teams to manage complex security environments.

3. Methodology

3.1 Research Design

This study employs a qualitative research design centered on a systematic review and synthesis of peer-reviewed literature published between 2015 and 2025. The objective is to construct a composite picture of the SME security landscape, identifying common themes, challenges, and successful mitigation strategies.

3.2 Data Collection

The primary data sources include academic journals, conference proceedings, and technical reports focusing on information security, computer science, and business management. Key databases utilized include IEEE Xplore, ScienceDirect, and SpringerLink. The selection criteria prioritized studies that specifically addressed the unique constraints of SMEs (budget, size, expertise) and the implementation of specific frameworks like MDR, SCP, and maturity models. A total of 22 core references were selected for deep analysis.

3.3 Data Analysis

We applied Thematic Analysis, following the guidelines established by Braun and Clarke [18]. This method involves a six-phase process: familiarization with the data, generating initial codes, searching for themes, reviewing themes, defining and naming themes, and producing the report. This approach allowed us to move beyond a mere description of the literature to an interpretation of the underlying patterns. For instance, disparate discussions on "budget constraints" and "lack of training" were synthesized under the broader theme of "Resource Asymmetry." Similarly, discussions on "auditing," "labeling," and "regulatory reform" were grouped under "Standardization and Governance."

4. Results

4.1 The Barrier of Resource Asymmetry

The thematic analysis reveals that the primary impediment to SME cybersecurity is not a lack of technology availability, but a lack of accessibility driven by resource asymmetry. Mitrofan, Cruceru, and Barbu [10] identify the main causes leading to cybersecurity risks in SMEs as fundamentally economic and organizational. Unlike large enterprises that can absorb the cost of a dedicated Chief Information Security Officer (CISO) and a 24/7 SOC, SMEs often assign security responsibilities to generalist IT staff who are already overburdened with operational maintenance. This results in a reactive posture—dealing with threats only after they manifest—rather than a proactive one.

4.2 Efficacy of Adaptive Maturity Models

Traditional security models often view security as a binary state (secure vs. insecure). However, recent scholarship argues for "maturity models" that view security as a gradient of capability. Ozkan and Spruit [16] and Ozkan et al. [17] present the concept of "Adaptive Security Maturity." These models suggest that an SME's security posture should evolve relative to its specific risk profile and digital complexity. The results indicate that rigid, "one-size-fits-all" standards often fail because they overwhelm the SME. In contrast, adaptive models that prioritize critical assets first allow for a stepwise improvement that is financially sustainable.

4.3 The Role of Managed Detection and Response (MDR)

One of the most significant findings is the rising importance of service-based security models. Rajgopal [1] highlights the efficacy of MDR service design in building profitable and effective 24/7 threat coverage for SMEs. MDR bridges the resource gap by outsourcing the complex, labor-intensive work of threat hunting and incident response. The analysis suggests that for many

SMEs, subscription-based MDR is the only viable pathway to achieving a level of security comparable to larger entities. It transforms a high capital expenditure (building a SOC) into a predictable operating expenditure.

4.4 Standardization, Labeling, and Trust

How does an SME prove it is secure? How does a customer know which SME to trust? Ponsard and Grandclaudon [19] and Ponsard et al. [20] discuss the design and deployment of cybersecurity labels. Similar to energy efficiency ratings on appliances, security labels provide a simplified metric of trust. The results show that systematic auditing and feedback loops associated with these labels not only improve external trust but also drive internal process improvements.

5. Discussion

5.1 Operationalizing Resilience: The Role of MDR and Adaptive Frameworks

The synthesis of the collected data points toward a critical necessity: the operationalization of resilience. It is insufficient to merely identify risks; SMEs must possess the operational capability to respond to them. This section expands significantly on the mechanics of how Managed Detection and Response (MDR) and Adaptive Security Maturity models function in tandem to create a robust defense layer for resource-constrained entities.

The traditional paradigm of cybersecurity relies heavily on preventative controls—firewalls, antivirus software, and intrusion detection systems. While these are foundational, they are increasingly porous against modern, persistent threats. A static defense assumes that the perimeter can be sealed. However, in an era of cloud computing, remote work, and mobile device integration, the network perimeter has effectively dissolved. This is where the concept of "Resilience" supersedes "Protection." Resilience acknowledges that breaches may occur and focuses on the speed of detection and the efficacy of the recovery.

5.1.1 The Mechanics of MDR for SMEs

Rajgopal's analysis of MDR service design [1] is pivotal here. MDR differs from legacy Managed Security Service Providers (MSSPs) in a fundamental way. MSSPs typically focus on alert forwarding—sending notifications to the client when a firewall rule is breached. For an SME with no dedicated security analyst, receiving 500 alerts a day is not helpful; it is paralyzing. MDR, conversely, focuses on the "Response." It involves human analysts, augmented by AI, who investigate alerts, validate them to remove false positives, and, crucially, take action to contain threats (e.g., isolating an infected endpoint) on behalf of the client.

The operational benefit for the SME is the democratization of elite security capabilities. Through MDR, an SME with 50 employees gains access to the same threat intelligence feeds, behavioral analytics, and forensic expertise as a Fortune 500 company, but at a fraction of the cost. This shared-resource model leverages economies of scale. The MDR provider amortizes the cost of expensive SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) platforms across a large client base.

However, the integration of MDR is not "plug and play." It requires a baseline of organizational maturity. If an SME does not know what assets it has (asset management), it cannot tell the MDR provider what to monitor. This dependency links MDR directly back to the Adaptive Maturity Models proposed by Ozkan and Spruit [16].

5.1.2 Implementing Adaptive Security Maturity

The "Adaptive" aspect of security maturity is crucial for avoiding the "compliance trap"—where companies spend their budget on checking boxes rather than reducing risk. An adaptive framework begins with a granular assessment of the specific business context. For a small e-commerce retailer, the "crown jewels" are customer credit card data and website uptime. For a boutique law firm, the critical assets are client confidentiality and email integrity.

Operationalizing this involves a phased implementation:

1. Phase 1: Hygiene and Visibility. Before deploying advanced AI hunters, the SME must implement basic hygiene. This includes patch management, multi-factor authentication (MFA), and immutable backups. Azinheira et al. [13] emphasize that assessment methodologies must start here. Without visibility into the network, advanced tools are useless.

2. Phase 2: Standardization and Policy. Once the technical baseline is set, the organizational layer must be addressed. This involves the "Cascading Information" referenced by Cartwright et al. [11]. Policies must be written not for auditors, but for employees. Using the "Security Label" concept [19], SMEs can gamify this process, striving to achieve a "Silver" or "Gold" internal rating to demonstrate progress to stakeholders.

3. Phase 3: Integration of Advanced Services (MDR). Once the SME understands its data flows and has basic controls, it integrates the MDR service. The MDR provider hooks into the SME's cloud environments (AWS, Azure, etc.) and endpoints.

4. Phase 4: Continuous Feedback Loop. Security is

not a destination. Using the metrics discussed by Katt and Prasher [14] regarding quantitative security assurance, the SME must review reports from the MDR provider. Are attacks decreasing? Are phishing attempts succeeding? This data feeds back into Phase 1, prompting new training or new controls.

5.1.3 The Intersection of Automation and Human Insight

A recurring theme in the literature is the tension between automation and human judgment. João et al. [7] discuss AI-based security in Industry 4.0. While AI is essential for parsing the terabytes of log data generated by modern networks, the "Context" is often human. An AI might flag a user logging in at 3 AM as a threat. A human manager knows that the user is travelling for business.

Operationalizing resilience requires a "Human-in-the-loop" approach. MDR provides the external human loop (the analyst), while the SME provides the internal human loop (the context). This partnership is defined by the "Service Level Agreement" (SLA) and the "Runbook." The Runbook dictates the rules of engagement: When does the MDR provider wake up the CEO? When do they unilaterally shut down a server? Developing these protocols is a governance exercise that forces the SME to think critically about its risk tolerance.

5.1.4 Addressing the "Shadow IT" and Cloud Sprawl

Roy and Patil [12] note the complexity of cloud security. SMEs often suffer from "Shadow IT"—employees using unauthorized SaaS applications (Dropbox, Trello, unauthorized PDF converters) to get work done. Operationalizing resilience requires bringing these into the light, not necessarily to ban them, but to secure them. An adaptive framework recognizes that blocking productivity tools leads to circumvention. Instead, the strategy should be "Sanction and Secure." MDR services are increasingly capable of monitoring Cloud Access Security Brokers (CASB) to detect data exfiltration through these non-corporate channels.

5.1.5 Financial Implications and the Cost of Inaction

Finally, the operational argument must always be tied to finance, as referenced by Bergthaler et al. [15] regarding problem loans and financial stability. Cybersecurity is often viewed as a cost center. However, by framing MDR and adaptive security as "Business Continuity Assurance," the narrative shifts. The cost of an MDR subscription is often less than the salary of a junior IT support tech. Yet, it provides the coverage of a full team. For an SME seeking loans or investment, demonstrating a mature, rated [19], and monitored security posture significantly reduces the perceived risk profile to lenders and investors.

In summary, operationalizing resilience is about moving from a fragmented, reactive set of tools to a cohesive, service-supported strategy. It acknowledges the limitations of the SME (budget, staff) and leverages the strengths of the market (specialized MDR providers, AI automation) to build a defense that is greater than the sum of its parts.

5.2 Policy Implications and Regulatory Reform

The findings of this study have significant implications for policymakers. Current regulations often treat all businesses as homogenous entities, applying the same stringent requirements to a ten-person startup as to a global bank. This creates a compliance burden that can stifle innovation. Idem et al. [6] argue for urgent reform in regulatory agencies. Our analysis supports a tiered regulatory framework where compliance requirements are proportional to the risk and size of the entity. Furthermore, governments should consider subsidizing MDR adoption for critical sector SMEs (e.g., healthcare, supply chain logistics) as a matter of national security.

5.3 Limitations and Future Directions

While this study provides a comprehensive overview, it is limited by the reliance on existing literature which may lag behind the very latest threat vectors (e.g., deepfake social engineering). Additionally, the effectiveness of MDR services varies wildly between providers, and there is a lack of standardized metrics to compare MDR performance objectively. Future research should focus on longitudinal studies measuring the "Mean Time to Detect" (MTTD) and "Mean Time to Respond" (MTTR) in SMEs utilizing MDR versus those relying on internal resources.

6. Conclusion

The cybersecurity landscape for Small and Medium-sized Enterprises is characterized by a stark dichotomy: the threats are advanced and enterprise-grade, while the defenses are often rudimentary and resource-constrained. This article has argued that bridging this gap requires a fundamental shift in strategy. The era of the "generalist IT person" managing cybersecurity is over. The complexity of modern threats, driven by AI and state-sponsored actors, demands specialized defense.

Our analysis confirms that "Operational Resilience" in the SME context is achievable through a tripartite approach:

1. Adaptive Maturity: Implementing flexible frameworks that prioritize risk-based controls over static compliance checklists.

2. Managed Response: Leveraging the MDR service model to outsource the high-cost, high-skill functions of threat detection and response.

3. Human-Centric Governance: Fostering a culture of awareness and using standardized labeling to build trust and internal discipline.

By integrating these elements, SMEs can move beyond the paralysis of fear and the burden of compliance. They can construct a security posture that is not only robust enough to withstand modern attacks but also agile enough to support their continued growth and innovation in the digital economy. The future of SME security is not in buying more boxes, but in subscribing to better outcomes.

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. Eybers, S., & Mvundla, Z. (2021). Investigating Cyber Security Awareness (CSA) Amongst Managers in Small and Medium Enterprises (SMEs). Comprehensible Science, 180–191.
3. Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). Cybercrime Business Digital in Indonesia. E3S Web of Conferences, 125(21001), 21001.
4. Ho, Mr. H., Ko, P. R., & Mazerolle, P. L. (2022). Situational Crime Prevention (SCP) Techniques to Prevent and Control Cybercrimes: A Focused Systematic Review. Computers & Security, 115, 102611.
5. IBM (2019). Cost of data breach report. IBM Security.
6. Idem, U. J., Olarinde, E. S., Ikpeze, N. G., Anwana, Emem, O., Ogundele, A. T., & Awodiran, M. A. (2023). Cybercrime Regulatory Agencies need urgent Reform to Protect Nigeria. 2023 International Conference on Cyber Management and Engineering (CyMaEn).
7. João, A., Plesker, C., Klaus Schützer, Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. Electronics, 12(8), 1920–1920.
8. Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. IEEE Access, 10, 85701–85719.
9. Johannsen, A., Kant, D., & Creutzburg, R. (2020). Measuring IT security, compliance and data governance within small and medium-sized IT enterprises. Electronic Imaging, 32(3), 1–11.
10. Mitrofan, A. L., Cruceru, E. V., & Barbu, A. (2020). Determining the main causes that lead to cybersecurity risks in SMEs. Business Excellence and Management, 10(4), 38–48.
11. Cartwright, A., Cartwright, E., & Edun, E. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies.
12. Roy, A., & Patil, K. (2023). Framework for Cloud Security Initiatives in Small and Medium-Sized Enterprises.
13. Azinheira, B., Antunes, M., Maximiano, M., & Gomes, R. P. (2023). Information Security And Cybersecurity Assessment In SME – An Implementation Methodology.
14. Katt, B., & Prasher, N. (2018). Quantitative security assurance metrics: REST API case studies.
15. Bergthaler, W., Kang, K., Liu, Y., & Monaghan, D. (2015). Tackling Small and Medium Sized Enterprise Problem Loans in Europe. International Monetary Fund.
16. Ozkan, B. Y., & Spruit, M. (2023). Adaptable Security Maturity Assessment and Standardization for Digital SMEs.
17. Ozkan, B. Y., Spruit, M., Wondolleck, R., & Coll, V. B. (2020). Modelling adaptive information security for SMEs in a cluster.
18. Braun, V., & Clarke, V. (2008). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.
19. Ponsard, C., & Grandclaudon, J. (2019). Survey and Guidelines for the Design and Deployment of a Cyber Security Label for SMEs. 4th International Conference on Information Systems Security and Privacy.
20. Ponsard, C., Grandclaudon, J., & Point, N. (2020). Methodology and Feedback about Systematic Cybersecurity Experts Auditing in Belgium.