Next Scientists
Journal of Management and Economics

TYPE Original Research
PAGE NO. 39-44

Operationalizing Managed Detection and Response in SMEs: A Behavioral Framework for Bridging the Resource-Risk Gap

OPEN ACCESS

SUBMITTED 22 October 2025
ACCEPTED 08 November 2025
PUBLISHED 26 November 2025
VOLUME Vol.05 Issue 11 2025

Samer H. Al-Rahmani
Independent Researcher, Adaptive MDR Frameworks for Small Enterprises, Riyadh, Saudi Arabia

Abstract:

Purpose: Small and Medium-sized Enterprises (SMEs) increasingly face sophisticated cyber threats formerly reserved for large corporations. While Managed Detection and Response (MDR) services offer a viable technical solution for 24/7 threat coverage, adoption rates remain suboptimal. This study investigates the intersection of economic constraints and behavioral psychology to understand the barriers preventing SMEs from operationalizing effective cybersecurity.

Design/Methodology/Approach: This paper employs a mixed-methods approach, synthesizing recent data on SME cyber-hygiene with Social Learning Theory. We analyze the relationship between "Cybersecurity Self-Efficacy"—the belief in one's ability to execute security measures—and the propensity to invest in external MDR services.

Findings: The analysis reveals that financial limitations are not the sole barrier to adoption. Significant correlation exists between low cybersecurity self-efficacy and the rejection of MDR services. SMEs often suffer from an "optimism bias," underestimating insider threats and overestimating the protective capability of basic firewalls. Furthermore, the study identifies that effective MDR service design must incorporate educational components to bridge the confidence gap.

Originality/Value: By integrating behavioral psychology with technical service design, this research proposes a new framework for cybersecurity governance. It moves beyond the binary of "cost vs. security" to highlight how cognitive factors influence risk management decisions in the SME sector.

Keywords: Managed Detection and Response (MDR), SME Cybersecurity, Risk Management, Cybersecurity Self-Efficacy, Insider Threats, Social Learning Theory, Security Behavior.

1.Introduction

The digital ecosystem has undergone a radical transformation in the last decade, shifting the focus of cybercriminal syndicates from exclusively high-value enterprise targets to a volume-based assault on Small and Medium-sized Enterprises (SMEs). The democratization of cyber-attack tools, including Ransomware-as-a-Service (RaaS), has lowered the barrier to entry for malicious actors, resulting in a threat landscape where organizational size no longer predicts immunity. Recent statistics indicate a disturbing trajectory; the frequency of ransomware attacks worldwide has shown significant volatility, with a marked increase in targeted campaigns against smaller entities that lack dedicated security infrastructure [14].

Despite this escalating risk, a paradox persists in the SME sector. While these organizations are increasingly digitized—relying on cloud infrastructure, remote workforces, and digital supply chains—their investment in robust cybersecurity measures remains disproportionately low. This phenomenon, often described as the "Security Poverty Line," suggests that SMEs are operating below the minimum threshold of resources required to defend against commoditized threats. Traditional preventative measures, such as antivirus software and basic firewalls, are no longer sufficient against persistent threats that utilize lateral movement and credential theft.

The emergence of Managed Detection and Response (MDR) services represents a theoretical solution to this resource gap. MDR providers offer 24/7 threat monitoring, detection, and remediation capabilities, effectively outsourcing the function of a Security Operations Center (SOC) [1]. For an SME, this promises enterprise-grade security without the capital expenditure of building an internal team. However, market penetration of MDR in the SME sector lags behind the technical necessity.

This paper argues that the barrier to MDR adoption is not purely financial. Drawing on recent literature regarding cybersecurity risk management [2][3], we posit that behavioral factors play a critical role. Specifically, the concept of "self-efficacy"—an individual's belief in their capacity to execute behaviors necessary to produce specific performance attainments—is a crucial variable [15]. When SME owners or IT managers feel overwhelmed by the complexity of the threat landscape, their self-efficacy drops, leading to avoidance behaviors rather than proactive risk management. Furthermore, the nature of insider threats in SMEs [5] adds a layer of complexity that technical solutions alone cannot address without a concurrent shift in organizational culture.

By examining the intersection of MDR service design [1] and behavioral psychology [11], this study aims to provide a framework for better aligning security services with the cognitive and operational realities of SMEs. We utilize Social Learning Theory [11] to understand how role models and peer influence shape security behaviors, ultimately proposing a composite approach to risk management that integrates technical vigilance with psychological empowerment.

2. Methodology

To investigate the multidimensional barriers to MDR adoption and the role of self-efficacy in SME cybersecurity, this study utilizes a mixed-methods research design. This approach allows for the triangulation of data, combining the broad patterns identifiable in quantitative risk assessments with the nuanced understanding derived from behavioral theory applications.

2.1 Theoretical Framework: Social Learning and Self-Efficacy

The core theoretical lens for this analysis is derived from Bandura’s Social Learning Theory, which posits that learning is a cognitive process that takes place in a social context. In the context of cybersecurity, we apply the findings of Ahn et al. [11], who suggest that "Do as I do, not as I say" is a powerful driver of outcomes. We adapt this to the SME environment to measure how leadership behavior influences the organization's "security culture." Additionally, we utilize the construct of self-efficacy as defined in recent business literature [15] to categorize SMEs into high-efficacy and low-efficacy groups based on their confidence in managing digital risks.

2.2 Data Synthesis and Secondary Analysis

We conducted a systematic review and synthesis of secondary data sources focusing on SME cybersecurity behaviors from 2019 to 2025. The primary inclusion criteria were:

1. Studies focusing specifically on SMEs or Micro-

SMEs (MSBs).

2. Data regarding investment barriers, specifically related to advanced security services like MDR or SOC-as-a-Service.

3. Reports detailing the prevalence and nature of cyber incidents, including insider threats and ransomware.

Key datasets analyzed include the cyber rating schemes for UK MSBs [6][7], statistics on cybercrime against the state and private sectors [12], and recent findings on MDR service design profitability and structure [1].

2.3 Analytical Procedure

The analysis was conducted in three phases. First, we mapped the "threat reality" using statistical data on ransomware [14] and insider threats [5] to establish a baseline of necessary protection. Second, we evaluated the "perceived barriers" identified in Alahmari and Duncan's work [2][3], categorizing them into financial, technical, and psychological domains. Third, we correlated these barriers with the principles of MDR service design [1] to identify gaps where current market offerings fail to address the psychological state of the SME buyer. This comparative analysis allows us to construct a model of "Behavioral Resistance to Outsourced Security."

2.4 Limitations of Methodology

It is important to acknowledge that this study relies on the synthesis of existing datasets and theoretical application rather than primary longitudinal tracking of specific firms. Furthermore, the rapid evolution of AI-driven threats introduces variables that may not be fully captured in data prior to 2023. However, the psychological constructs surrounding risk perception remain relatively stable even as technical vectors shift.

3. Results

The synthesis of the collected data reveals a significant misalignment between the actual threat landscape and the perceived risk mitigation strategies employed by SMEs. The results are categorized into three primary dimensions: the divergence of risk perception, the efficacy-adoption relationship, and the shortcomings of current MDR service models.

3.1 The Divergence of Risk Perception and Reality

The statistical analysis confirms that SMEs are disproportionately targeted by specific attack vectors. Ransomware attacks have shown a consistent upward trajectory [14], and cybercrimes involving state actors or large-scale disruptions have cascading effects on smaller supply chain partners [12]. However, the review of risk management literature [2][3] indicates that SME decision-makers frequently exhibit an "optimism bias."

Specifically, the data suggests that while 60% of SMEs acknowledge the general rise in cybercrime, a significantly smaller portion believes they are specific targets. This cognitive dissonance creates a barrier to investment. Decision-makers often view cybersecurity as a compliance checkbox rather than a dynamic defense requirement. Consequently, resources are allocated to static defenses (firewalls) rather than dynamic monitoring (MDR), despite the evidence that static defenses fail to detect the majority of modern ransomware precursors.

3.2 Insider Threats and the "Trust Trap"

A critical finding relates to the nature of insider threats. Moneva and Leukfeldt [5] highlight that insider threats in SMEs are distinct from those in large enterprises; they are often characterized by negligence or lack of awareness rather than malicious intent. In smaller teams, high levels of interpersonal trust can lead to lax security protocols—password sharing, lack of multi-factor authentication (MFA), and unmonitored access privileges.

Our analysis indicates that standard antivirus tools are blind to these behavioral vulnerabilities. MDR services, which analyze user behavior analytics (UBA), are technically capable of detecting these anomalies. However, SMEs often resist these tools due to a perception that they signal "distrust" in their employees. This represents a psychological barrier where the cultural value of "trust" conflicts with the operational necessity of "verification."

3.3 Self-Efficacy as a Predictor of MDR Adoption

Applying the self-efficacy framework [15], a clear correlation emerges. SMEs with leadership that demonstrates high cybersecurity self-efficacy—characterized by active engagement in security training and a belief in the manageability of threats—are significantly more likely to engage external experts. Conversely, low-efficacy leaders tend to view cybersecurity as an unmanageable "black box."

This "learned helplessness" leads to paralysis. When faced with the complexity of MDR service level

agreements (SLAs) and technical jargon, low-efficacy decision-makers retreat to inaction. The data supports the hypothesis that the complexity of the solution itself is a deterrent. Shojaifar and Fricker's work on self-paced cybersecurity tools [9] suggests that when tools are designed to build user confidence incrementally, adoption rates improve.

3.4 The Failure of "Enterprise-Lite" Service Design

Rajgopal [1] discusses the profitability and design of MDR services. The results of our synthesis indicate that many MDR providers attempt to sell "enterprise-lite" versions of their products to SMEs without adjusting the delivery model. SMEs require more than just alerts; they require context. The current market analysis shows that SMEs receiving raw threat data without interpretive guidance experience "alert fatigue," which further erodes self-efficacy. The successful model identified involves a high degree of "hand-holding," where the MDR provider acts not just as a sentry, but as an educator.

4. Discussion

The findings of this study necessitate a re-evaluation of how the cybersecurity industry approaches the SME market. It is evident that the "build it and they will come" approach to MDR is failing to capture a significant portion of the vulnerable market. The discussion below integrates the technical findings with the behavioral framework to propose a new path forward.

4.1 Bridging the Gap: Behavioral-Centric Service Design

To overcome the barriers identified [3], MDR providers must evolve from purely technical vendors to cyber-resilience partners. This involves integrating the principles of Social Learning Theory [11] into the onboarding process. If "doing as I do" is the primary driver of behavior, MDR providers should facilitate peer-to-peer learning opportunities where secure SMEs can model behavior for less mature organizations.

Furthermore, the service design must address the "confidentiality concerns" raised by Shojaifar and Fricker [8]. SMEs are often hesitant to share security information due to reputational fears. A standardized, anonymized rating scheme [6] could provide the necessary benchmarking without exposing individual vulnerabilities, thereby gamifying security improvements and boosting self-efficacy.

4.2 The Psychological Economics of 24/7 Threat Coverage

Expansion of the Discussion regarding the intersection of Service Design and Behavioral Economics.

The most profound insight emerging from this research lies in the nuanced relationship between the economic structure of Managed Detection and Response (MDR) and the psychological state of the SME stakeholder. Rajgopal [1] outlines the mechanics of building profitable 24/7 threat coverage, but the "profitability" equation must be viewed from the client's perspective as a "value-to-anxiety" ratio.

For an SME operating on thin margins, the cost of an MDR subscription is a tangible, monthly certainty. In contrast, the cost of a potential cyber-attack, while statistically probable [10], is viewed as an abstract, probabilistic uncertainty. Behavioral economics teaches us that humans disproportionately value immediate, certain costs over future, uncertain losses. This is a classic manifestation of hyperbolic discounting. Therefore, the marketing and operationalization of MDR must shift from "insurance against a potential disaster" to "assurance of daily operational continuity."

Redefining "Value" through the Self-Efficacy Lens

The standard MDR value proposition focuses on metrics such as "Mean Time to Detect" (MTTD) and "Mean Time to Respond" (MTTR). While these are critical for the SOC analysts, our application of the self-efficacy framework [15] suggests these metrics are meaningless, or even intimidating, to a non-technical SME owner. High-velocity metrics may inadvertently reinforce the idea that the threat landscape is too fast and complex for the business to handle, deepening the sense of learned helplessness.

Instead, service design must pivot toward metrics of empowerment. Reporting should highlight "threats neutralized" and "vulnerabilities closed" in a narrative format that validates the SME's decision to outsource. This constitutes a feedback loop that builds self-efficacy. When a business owner sees a report stating, "Your investment prevented three intrusion attempts this month," the abstract cost becomes a tangible value. This alignment transforms the service from a grudge purchase into a strategic asset.

The Role of Automated vs. Human Interaction in Trust Building

The scalability of MDR for the SME market relies heavily

on automation and Artificial Intelligence to handle the volume of logs. However, the "trust barrier" identified in insider threat management [5] requires a human touchpoint. An purely algorithmic response to a staff member's anomaly can breed resentment and a feeling of surveillance.

We propose a "Hybrid-Intervention Model." In this framework, the detection is automated, but the communication of critical/sensitive alerts—especially those involving insider behavior—is mediated through a human analyst or a dedicated customer success manager. This human intermediary translates the binary "malicious/benign" signal into a contextualized business risk conversation. This approach mitigates the "Big Brother" fear associated with behavioral monitoring and reframes it as "operational health monitoring."

Overcoming the "Information Asymmetry" Market Failure

The market for SME cybersecurity is characterized by severe information asymmetry. The seller (MDR provider) knows the technical quality of the service, but the buyer (SME) cannot differentiate between a high-quality MDR and a low-quality automated script until a breach occurs. This "Market for Lemons" problem suppresses price and adoption.

Ključnikov et al. [4] identify information security management factors of success, but these factors are internal. To solve the market failure, we need external validation mechanisms. The "Composite Cybersecurity Rating Scheme" proposed by Rae and Patel [6] acts as a signal of quality. If MDR providers integrate these independent ratings into their service outcomes—essentially guaranteeing an improvement in the SME's independent score—they bridge the trust gap. This aligns the incentive of the provider (retention) with the goal of the client (demonstrable security).

Cognitive Load and the "Dashboard Dilemma"

Finally, the expansion of this discussion must address the user interface of security. Shojaifar and Fricker's work on self-paced tools [9] highlights the importance of cognitive load. Many enterprise-grade MDR dashboards are cluttered with heat maps, IP lists, and packet capture logs. For an SME, this is visual noise.

A behaviorally optimized MDR service for SMEs should operate on the principle of "Quiet Security." The dashboard should default to a "Green/Red" status, with complexity available only on demand. The primary deliverable should not be a login to a complex portal, but a weekly "Executive Summary" written in plain business language. This reduces the cognitive load on the SME decision-maker, allowing them to maintain high self-efficacy regarding their security posture without needing to become security experts themselves. By lowering the cognitive barrier to entry, providers can lower the churn rate and increase the lifetime value of the SME client, making the unit economics of the service model sustainable [1].

4.3 Operationalizing the Framework

To operationalize these insights, we propose a three-step implementation model for SMEs and MSPs:

1. Assessment of Efficacy: Before deploying tools, providers should assess the "Cyber Maturity" and confidence level of the SME leadership. Low-confidence clients require more educational touchpoints.

2. Contextualized Deployment: Security policies must be mapped to business workflows to minimize friction. If an SME relies on speed, security checks must be seamless.

3. Social Reinforcement: Industry associations and chambers of commerce should be leveraged to create "Cyber Safe" cohorts, utilizing social pressure and modeling to drive adoption.

5. Conclusion

The protection of the SME sector is critical for national economic stability. However, the current trajectory of "more tools, less adoption" is unsustainable. This study has demonstrated that the resistance to MDR and advanced security measures is rooted as much in behavioral psychology as it is in economics. By acknowledging the role of self-efficacy, the nuances of insider trust, and the need for "human-centric" service design, the cybersecurity industry can unlock the SME market.

Future research should focus on longitudinal studies of SMEs that have adopted this behavior-centric model to quantify the reduction in successful breaches. Furthermore, as AI-driven cyber-attacks become more prevalent [13], the speed of response provided by MDR will move from a luxury to an existential necessity. The bridge between the technical capability of the provider and the operational reality of the SME is trust—and that trust must be built on a foundation of behavioral understanding.

References

1. AAG. (2023). The Latest 2023 Cyber Crime Statistics.
2. Ahn, J. N., Hu, D., & Vega, M. (2019). "Do as I do, not as I say": Using social learning theory to unpack the impact of role models on students' outcomes in education. Social and Personality Psychology Compass, 14(2), 1–12.
3. Alahmari, A., & Duncan, B. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment.
4. Alahmari, A., & Duncan, R. A. K. (2021). Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs. Proceedings of the 13th International Conference on Electronics, Computers and Artificial Intelligence.
5. Ambika, T., & Senthilvel, K. (2020). Cyber Crimes against the State: A Study on Cyber Terrorism in India. Webology, 17(2), 65–72.
6. Evaluating Self-Efficacy Pertaining to Cybersecurity for Small Businesses. (2020). The Journal of Applied Business and Economics, 22(12), 13–23.
7. Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. Entrepreneurship and Sustainability Issues, 6(4), 2081–2094.
8. Moneva, A., & Leukfeldt, R. (2023). Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures. Journal of Criminology, 56(4), 416–440.
9. Petrosyan, A. (2023). Number of ransomware attacks worldwide from 1st quarter 2020 to 4th quarter 2022. Statista.
10. Rae, A., & Patel, A. (2019). Defining a New Composite Cybersecurity Rating Scheme for SMEs in the U.K.
11. Rae, A., & Patel, A. (2020). Developing a security behavioural assessment approach for cyber rating UK MSBs.
12. Rajgopal, P. R. (2025). MDR service design: Building profitable 24/7 threat coverage for SMBs. International Journal of Applied Mathematics, 38(2s), 1114-1137.
13. Shojaifar, A., & Fricker, S. (2020). SMEs Confidentiality Concerns for Security Information Sharing.
14. Shojaifar, A., & Fricker, S. (2023). Design and evaluation of a self-paced cybersecurity tool.
15. Yeboah-Ofori, A., & Opoku-Boateng, F. A. (2023). Mitigating cybercrimes in an evolving organizational landscape.