Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

.

Strategic Integration of Cybersecurity in IT SMEs: Developing a Lean Sociotechnical Framework

Student Name: Dan Bajenaru

Student Number: 2129380

Modul Name: **Leading and Implementing Change**

Module Code: LCLM6003

Lecturer: Nishi Ramsurrun

Table of Contents

1. Identification of a Business Problem 3
1.1 Background and Rationale 3
1.2 The Business Problem 3
1.3 Key Debates and Significance 3
2. Research Aims, Objectives, and Questions 3
2.1 Research Aim 3
2.2 Research Objectives 3
2.3 Research Question 4
3. Preliminary Literature Review 4
3.1 The Technological Context: Complexity vs. Capacity 4
3.2 The Organisational Context: Governance and Culture 5
3.3 The Environmental Context: From Compliance to Survival 5
3.4 Contribution to the Field 5
4. Research Methodology & Design 5
4.1 Research Philosophy: Interpretivism 5
4.2 Research Approach: Inductive 6
4.3 Research Strategy: Qualitative Exploratory 6
4.4 Data Collection: Secondary Data Analysis 6
4.5 Data Analysis: Reflexive Thematic Analysis 6
4.6 Ethical Considerations 7
5. Business Relevance & Practical Implications 7
5.1 Operational Resilience 7
5.2 Commercial Survival 7
5.3 Cultural Change 7
6. Plan of Work and Time Schedule 7
7.References 10

1. Identification of a Business Problem

1.1 Background and Rationale

The digital economy has shifted from large, monolithic enterprises to a decentralized ecosystem reliant on IT Small and Medium-Sized Enterprises (SMEs). Ranging from software houses to Managed Service Providers (MSPs), these firms act as critical nodes in the global supply chain, often holding privileged access to major client networks.

However, a "resource-risk asymmetry" defines this sector. While technically proficient in product delivery, IT SMEs frequently lack cybersecurity governance maturity. They face enterprise-grade threats—such as AI-driven ransomware—but operate with limited budgets and flat hierarchies, creating a dangerous contradiction where they are "too busy building" to secure their infrastructure effectively.

1.2 The Business Problem

The core problem is that cybersecurity is rarely integrated into the business processes or culture of IT SMEs. Instead, it is treated as an isolated compliance function rather than a strategic necessity. In high-velocity cultures where speed-to-market is paramount, rigid security measures are often perceived as barriers to productivity.

This friction drives "Shadow IT" and "Rational Non-Compliance," where staff bypass complex controls to maintain efficiency. Furthermore, existing frameworks like COBIT are designed for large enterprises and fail to suit the flat structures of SMEs, leaving these firms without a viable governance model that fits their operational reality.

1.3 Key Debates and Significance

This issue matters beyond the individual firm. A breach in an IT SME is a systemic risk that can compromise entire supply chains. Recent history, such as the Kaseya or SolarWinds attacks, has shown how compromising one small software provider can grant attackers access to thousands of downstream victims.

Therefore, the key debate in the industry is shifting. It is no longer about “how to make SMEs adopt enterprise security” (which has failed), but “how to design security that actually fits the SMEs.” This research addresses the urgent need to move beyond the "blame culture" of human error and investigate the structural reasons for integration failure.

2. Research Aims, Objectives, and Questions

2.1 Research Aim

The aim of this research is to develop a strategic framework to guide the holistic integration of cybersecurity into the core business processes and culture of Small and Medium-Sized Enterprises (SMEs) within the IT sector.

2.2 Research Objectives

To achieve this aim, the following specific objectives have been established:

1. **To critically examine** the current context and maturity levels of cybersecurity integration within IT SMEs. I need to understand the baseline capabilities and define the specific nature of the "resource-risk asymmetry" that prevents them from defending themselves.
2. **To identify and analyze** the specific limitations of existing enterprise-grade frameworks (e.g., COBIT, ITIL) when applied to the resource-constrained, agile environments of IT SMEs. I intend to find out *why* these standard models fail when applied to smaller teams.
3. **To evaluate** the operational and strategic impacts of fragmented security measures. specifically investigating how poor usability and governance friction drive non-compliance. I want to understand the link between "bad user experience" and "security breaches."
4. **To develop** a novel "Lean Sociotechnical Framework" that pragmatically aligns security initiatives with the agile business objectives of IT SMEs. The goal is to propose a model that ensures resilience without compromising operational speed.

2.3 Research Question

This research will be guided by the following central research question:

How can Small and Medium-Sized Enterprises (SMEs) within the IT sector strategically integrate cybersecurity into their operational processes and organizational culture to build a resilient and adaptive defence, given their unique resource constraints?

3. Preliminary Literature Review

To analyze the integration gap, this research will utilize the **Technology-Organisation-Environment (TOE) framework** (Tornatzky & Fleischer, 1990) as its theoretical lens. Preliminary reading suggests this is the most effective model for this study as it allows for the simultaneous analysis of internal constraints (Organization) and external pressures (Environment).

3.1 The Technological Context: Complexity vs. Capacity

A distinct contradiction appears in the literature regarding technology. On paper, we have better security tools than ever before. Concepts like Zero Trust Architecture (ZTA) and AI-driven threat detection offer immense protection. However, the literature suggests these tools are often too complex for SMEs to manage effectively.

Al-Ahbabi et al. (2024) describe the phenomenon of "tool sprawl." This occurs when an SME, in a panic to be secure, purchases multiple disconnected security products—an antivirus here, a firewall there, an email filter somewhere else. Because these tools do not "talk" to each other, they create a fragmented alert system. A small IT team of three people might receive 500 alerts a day. This leads to "alert fatigue," where critical warnings are missed simply because the noise level is too high.

Therefore, the challenge identified in the literature is not the *absence* of technology, but the *absence of integration readiness*. The tools exist, but the capacity to configure, monitor, and respond to them is missing in resource-constrained teams.

3.2 The Organisational Context: Governance and Culture

The Organizational context refers to the internal structures and culture of the firm. A key debate in the field revolves around the conflict between governance and agility.

Hadžiosmanović & Rindell (2023) argue that traditional governance models like COBIT (Control Objectives for Information and Related Technologies) are fundamentally designed for large hierarchies. They rely on "segregation of duties"—the idea that the person who writes the code should not be the person who approves the code. In an IT SME with five staff members, this segregation is impossible. Everyone does everything. When an SME tries to implement these rigid rules, it stifles agility. Since agility is the primary competitive advantage of an IT SME, the business culture rejects the security rules.

Additionally, Ktorza & Bace (2022) highlight the "human factor" in this organizational context. They argue that poor usability in security tools is a primary driver of risk. If a security control is "unusable" (e.g., requiring a 20-character password that changes every month), employees will naturally find a workaround. This is not malicious; it is a rational attempt to get work done. This study will contribute by exploring how organizational culture impacts the acceptance of security controls.

3.3 The Environmental Context: From Compliance to Survival

The Environmental context looks at the external pressures forcing an organization to change. Historically, the main driver for security was regulation (e.g., avoiding GDPR fines).

However, recent literature confirms a massive shift. The pressure is moving from regulatory compliance to commercial necessity (Supply Chain Security). Large enterprise clients (like banks or government bodies) are now terrifyingly aware of the risk posed by their smaller vendors. As a result, they are demanding that SMEs demonstrate "enterprise-grade" security as a condition of the contract.

This changes the game entirely. It shifts the motivation for integration from "avoiding fines" to "winning revenue." This is a critical distinction that existing frameworks often miss. An SME might ignore a regulator, but they cannot ignore their biggest client. This research will explore how this "commercial pressure" can be harnessed to drive better security integration.

3.4 Contribution to the Field

This study will contribute to the field by bridging the gap between high-level governance theory and the messy reality of SME operations. By proposing a framework that is specifically tailored to resource-constrained technical environments, it challenges the isomorphism of "best practice" and offers a pragmatic alternative.

4. Research Methodology & Design

4.1 Research Philosophy: Interpretivism

This study will adopt an **Interpretivist** philosophy. An epistemological perspective was chosen because the core problem is not about the physical existence of security tools, but about understanding how they are perceived, implemented, and valued by humans within an organization. The success or failure of integration depends on how security is interpreted by

the employees—whether as a "blocker" or an "enabler". Interpretivism allows the researcher to understand these subjective realities and the social dynamics of the workplace.

4.2 Research Approach: Inductive

Consistent with the interpretivist philosophy, I will use an **Inductive** approach. A Deductive approach would require me to start with a hypothesis (e.g., "ISO 27001 reduces risk") and test it. However, since I am arguing that current frameworks *don't* work for SMEs, testing them seems counter-productive.

Instead, I want to build a new theory from the ground up. By using an Inductive approach, I can observe specific instances of integration failure and success in the data and use those observations to *induce* a broader framework. I want the solution to emerge from the reality of the SME experience, rather than trying to force-fit a pre-existing theory onto them.

4.3 Research Strategy: Qualitative Exploratory

A **Qualitative Exploratory** strategy will be employed. Given the complexity of the sociotechnical interactions in SMEs and the lack of existing frameworks for this specific context, qualitative methods are best suited to provide the necessary "thick description" and contextual understanding. Exploratory research is ideal for clarifying the exact nature of the "integration gap" and identifying variables that have not yet been codified in current theory.

4.4 Data Collection: Secondary Data Analysis

The study will rely on **Secondary Data Analysis** using a **purposive sampling** technique.

- **Justification for Secondary Data:** Investigating cybersecurity failures is notoriously difficult using primary methods. If I were to interview SME owners and ask, "Do you bypass your security controls?", they would likely lie or underreport their negligence due to "social desirability bias" or fear of reputational damage.
- **Source Selection:** To get a truthful picture, I will access high-quality secondary sources. These include aggregated industry reports (like the Verizon Data Breach Investigations Report or the IBM Cost of a Data Breach Report), government policy papers (from DSIT or NCSC), and detailed academic case studies (post-mortem analyses of breaches). These sources provide a more objective, candid view of failure patterns across thousands of incidents, without the filter of an embarrassed interviewee.
- **Sampling Strategy:** I will use purposive sampling to select a minimum of 12 high-quality sources. I will filter these based on their relevance to the IT sector, the SME context, and recency (focusing on 2020-2025 to ensure the data reflects the current AI threat landscape).

4.5 Data Analysis: Reflexive Thematic Analysis

Data will be analyzed using **Reflexive Thematic Analysis**. The analysis will involve coding the textual data against the three contexts of the TOE framework (Technological, Organisational, Environmental). This method allows for the identification of recurring barriers (e.g., "Governance-Agility Conflict") and enablers (e.g., "Usability First"), which will form the pillars of the proposed framework.

4.6 Ethical Considerations

As the study uses secondary data available in the public domain, traditional ethical risks regarding human participants (informed consent, harm) are minimized. However, academic integrity will be maintained through rigorous referencing, the accurate representation of original sources, and the avoidance of plagiarism. The study will objectively report findings, even if they contradict initial assumptions.

5. Business Relevance & Practical Implications

The proposed research has significant practical value for the IT sector, offering a roadmap for survival in a hostile digital environment.

5.1 Operational Resilience

By providing a framework for "Lean Governance," the study will help SMEs implement security controls that do not stifle their primary competitive advantage: agility. It offers a way to embed security checks into existing workflows (like DevOps pipelines) rather than adding bureaucratic layers on top. This reduction in friction is vital for reducing "Shadow IT" and ensuring consistent policy application.

5.2 Commercial Survival

The framework will help IT SMEs meet the rigorous vendor risk requirements of their enterprise clients. By framing security as a "Trust Asset," the research transforms cybersecurity from a cost center into a sales enabler, helping SMEs win and retain high-value contracts in a supply chain that demands security assurance.

5.3 Cultural Change

By highlighting the role of usability, the research will help managers reduce "Rational Non-Compliance". It provides actionable guidance on how to select tools that align with user needs, fostering a culture where security is embraced rather than bypassed. This shift from "blame" to "enablement" is critical for the long-term viability of IT SMEs.

6. Plan of Work and Time Schedule

The research will be conducted over a period of 12 weeks. The following table details the various stages of development, deliverables, and timeline.

Phase	Activity	Timeline	Key Tasks & Deliverables
1	**Topic Selection & Proposal**	Weeks 1-2	• Finalization of Research Proposal • Initial literature scoping

Phase	Activity	Timeline	Key Tasks & Deliverables
			• Definition of the "Resource-Risk Asymmetry"
2	**Literature Review**	Weeks 3-5	• Systematic search for sources (IEEE, ScienceDirect) • Draft of Chapter 2 (Lit Review) • Establishing the TOE theoretical lens
3	**Methodology & Data Collection**	Weeks 6-7	• Draft of Chapter 3 (Methodology) • Collection and filtering of 12 high-quality secondary data sources • Organization of data for analysis
4	**Data Analysis**	Weeks 8-9	• Reflexive Thematic Analysis of data • Coding data against Technological, Organizational, and Environmental contexts • Draft of Chapter 4 (Results & Discussion)
5	**Synthesis & Framework Design**	Week 10	• Development of the "Lean Sociotechnical Framework"

Phase	Activity	Timeline	Key Tasks & Deliverables
			• Draft of Chapter 5 (Conclusion & Recommendations) • Synthesis of findings into actionable strategy
6	**Review & Submission**	Weeks 11-12	• Proofreading and formatting • Reference check and academic integrity review • Final Submission of Dissertation

7.References

- Al-Ahbabi, S., & Bendiab, K. (2024). *Advances in Cybersecurity: A Literature Review*. ResearchGate.
- Braun, V., & Clarke, V. (2021). *Thematic Analysis: A Practical Guide*. Sage Publications.
- DSIT (UK Department for Science, Innovation and Technology). (2023). *Emerging technologies and their effect on cyber security*. Gov.uk.
- Hadžiosmanović, D., & Rindell, K. (2023). A Systematic Review on Cyber Security Integration in Information Technology Governance. *IEEE*.
- IBM. (2025). *Cost of a Data Breach Report 2025*. IBM Security.
- Ktorza, S., & Bace, J. (2022). Integration of Cybersecurity, Usability, and Human-Computer Interaction for Securing Energy Management Systems. *Journal of Cybersecurity and Privacy*.
- Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research Methods for Business Students* (8th ed.). Pearson.
- Tornatzky, L. G., & Fleischer, M. (1990). *The Processes of Technological Innovation*. Lexington Books.
- Verizon. (2025). *2025 Data Breach Investigations Report*. Verizon Business.
- von Solms, R., & von Solms, S. H. (2018). Cybersecurity and information security: what goes where? *Information and Computer Security*.