World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Integration of small-scale vendors into large firms' cybersecurity frameworks: strategies, challenges, and collaborative models

Suleiman Ibrahim Salifu *

Faculty of Business and Management Studies, School of Graduate Studies, Park University, USA.

World Journal of Advanced Research and Reviews, 2026, 29(03), 427-440

Publication history: Received on 26 January 2026; revised on 06 March 2026; accepted on 06 March 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.29.3.0526

Abstract

The rapid increase in the use of computerized systems in supply chains has revealed a significant number of cybersecurity weaknesses, particularly where large enterprises interact with their small-scale vendors. This paper examines the gaps and weaknesses in cybersecurity integration across different supply chain partners. Through qualitative analysis of existing literature, case studies, and industry frameworks, the research identifies the limitations of traditional compliance-based approaches, such as the fundamental restraints faced by small vendors, limited budgets, technical expertise, and cybersecurity awareness. The study proposes a tiered, partnership-oriented framework that reframes cybersecurity integration from punitive compliance requirements to collaborative support mechanisms for large enterprises and small-scale vendors. Key findings propose that successful integration requires (1) risk-based vendor categorization, (2) proportionate security requirements, (3) shared resource models, and (4) continuous relationship management. The paper concludes that the ability to withstand, recover from, or adapt to cyber-attacks and system failures in modern supply chains depends on transforming vendor relationships from transactional compliance to strategic partnerships, with large firms assuming greater responsibility for capability building across their extended digital ecosystem. Practical recommendations include developing scalable assessment tools, creating cybersecurity knowledge sharing platforms, and establishing clear governance structures that balance security requirements with vendor sustainability.

Keywords: Supply Chain Management; Cybersecurity; Risk Management; Integration; Vendor Management

1. Introduction

The 21st-century supply chain has moved from rigid, step-by-step physical pipelines into fluid, high-tech networks. Digital technologies, including cloud computing, Internet of Things (IoT) devices, automated logistics systems, and integrated enterprise platforms have brought about remarkable improvements in efficiency gains while simultaneously creating systemic cybersecurity vulnerabilities (Humayed et al., 2020). Because our digital systems are so deeply linked, a single security breach can trigger a significant effect, moving far beyond its original target to disrupt entire supply chains and essential services. The 2020 SolarWinds attack demonstrated how a single compromised software update could cascade through thousands of organizations globally, including government agencies and Fortune 500 companies (Zetter, 2021). Such incidents highlight that in interconnected digital ecosystems, an entity's security is only as effective as the weakest link in the chain.

The scale of the problem is substantial. According to IBM's 2022 Cost of a Data Breach Report, supply chain attacks increased by 42% from the previous year, with the average breach costing $4.46 million when third-party involvement was identified (IBM Security, 2022). These attacks exploit the inherent asymmetry between large organizations with mature cybersecurity programs and their smaller partners who often lack basic security controls. The economic reality

* Corresponding author: SULIIMAN IBRAHIM SALIFU

is that while large firms may invest millions in cybersecurity infrastructure, their smaller-scale vendors usually lack the budget, expertise, and awareness necessary to secure their part of the supply chain (Ghadge et al., 2020).

1.1. Problem Statement

The core problem this paper addresses is the cybersecurity integration gap between large, well-resourced firms and their small-scale vendors. This gap creates what security experts term the "weakest link" vulnerability, which arises because, while large organizations implement robust, high-cost security, they frequently rely on smaller, less-prepared partners in their supply chain (Boyes, 2015). Attackers strategically bypass these sophisticated defenses by targeting smaller vendors, which often have direct network access or shared data. Small vendors, typically defined as having fewer than 50 employees and restricted security budgets, constitute an attractive, low-effort entry point. First, they often have direct network connections or shared systems with larger partners. Second, they possess valuable data or system access credentials. Third, due to limited resources, small vendors frequently lack 24/7 monitoring, dedicated cybersecurity staff, and robust, updated security systems. (Humayed et al., 2020).

Several factors are coming together to worsen this issue. The mass adoption of cloud computing and SaaS platforms has significantly increased the number of digital links between companies. At the same time, the rise of remote work has made organizations more vulnerable by introducing less secure home networks and personal devices into the corporate environment. While the EU's NIS2 Directive and U.S. federal orders demand better security across extended supply chains, they often create a "compliance gap." Large firms are legally required to secure their ecosystems, but the resulting technical and financial requirements can be unattainable for their smaller collaborators (European Commission, 2022; The White House, 2021).

Research Objectives

This paper aims to achieve three primary research objectives:

- Examine the economic, technical, and cultural barriers that prevent effective cybersecurity integration between large firms and small-scale vendors.
- Assess current integration models, including compliance-based frameworks, technological solutions, and partnership approaches, identifying their strengths and limitations.
- Develop a practical, scalable framework that addresses the constraints of small vendors while meeting the security requirements of large organizations.

Research Questions

- What economic, technical, and cultural barriers hinder effective cybersecurity integration between large firms and small-scale vendors?
- How effective are existing cybersecurity integration models, such as compliance-based frameworks, technological solutions, and partnership approaches, in addressing these barriers?
- What practical and scalable cybersecurity integration framework can be developed to accommodate small vendors' constraints while meeting the security requirements of large organizations?

Significance of the Study

This research contributes to both academic literature and practical cybersecurity management. Academically, it bridges gaps between supply chain management, cybersecurity studies, and organizational behavior literature by examining how differences in money and power make it hard to keep networks safe. For professionals, it offers a clear guide on how to protect their digital systems without overwhelming smaller partners or making the rules too difficult to follow.

Thesis Statement

This paper suggests that big companies and their small vendors need to change how they handle security. Instead of just forcing small partners to follow strict rules, big firms should work with them as partners and offer different levels of support based on what they need. To succeed, large companies must understand that small vendors have limited resources, set security goals that are actually reachable, and build a system that keeps the network safe without ruining the business relationship.

Organization of the Study

This paper begins with the introduction, which delves into the problem statement, research objectives, significance of the study, and thesis statement. Following this introduction, Chapter 2 reviews existing literature on supply chain cybersecurity and small business constraints. Chapter 3 outlines the research methodology, that is, the research design, data collection, and analytical frameworks. Chapter 4 analyzes integration challenges in detail. Chapter 5 proposes a summary of key findings and proposes a comprehensive integration framework.

2. Literature review

Small-scale vendors play a vital role in most economies in the world, relying on them to provide a sizable number of employment opportunities and contribute a significant part of the GDP. Moreover, these businesses remain among the businesses exposed to cyber threats because of poor financial conditions, a lack of awareness, and resources. This mapping study will delve into existing research on the types of cybersecurity threats faced by small-scale vendors, the defensive practices being used, and the challenges in fighting and preventing cybersecurity threats (Novelli et al., 2024).

2.1. Evolution of Supply Chain Cybersecurity

The concept of supply chain cybersecurity has elevated massively over the past decade. Early actions intended to deal with this problem focused primarily on securing internal systems, with little attention to external partners. Boyes (2015) identified this as a critical mistake resulting from inattention, noting that "the interconnectivity of modern supply chains means that cybersecurity can no longer be viewed as an internal matter" (p. 29). The shift toward recognizing supply chain cybersecurity as a single field gained momentum following high-profile attacks, particularly the 2013 Target breach that originated from an HVAC vendor's compromised credentials (Kaufman, 2016).

Academic literature has increasingly focused on the systemic characteristics of supply chain cyber risk. Ghadge et al. (2020), the idea of supply chain cybersecurity is a complex adaptive system where little exposure in one node creates cascading effects throughout the network. Their research identified three primary risk categories: (1) data security risks, involving theft or corruption of sensitive information; (2) operational technology risks, affecting physical systems and processes; and (3) reputational risks, damaging stakeholder trust across multiple organizations at the same time.

The National Institute of Standards and Technology (NIST) framework has become a basis for supply chain cybersecurity. NIST (2018) draws attention to the effective supply chain risk management, which requires "identifying, assessing, and reducing risks associated with the distributed and interconnected nature of information and communications technology product and service supply chains" (p. 5). However, as Rashid (2021) notes, the broad entity's nature presents implementation challenges for resource-constrained organizations.

2.2. Small-Scale Vendor Characteristics and Constraints

Understanding small-scale vendor characteristics is crucial for crafting effective integration ideas or actions intended to deal with the problem. Research by the U.S. Small Business Administration indicates that 88% of small business owners feel their company is exposed to cyberattack, yet most lack the resources to carry out detailed security measures (SBA, 2021). Humayed et al. (2020) pointed out several different characteristics of small business cybersecurity postures:

2.2.1. Economic Constraints

Insufficient investment in cybersecurity is caused by their constant inability to allocate more funds to purchase advanced security technologies. Fotis (2024b) demonstrates that organizations implementing preventive security measures may reduce the chances of a successful cyberattack by up to 70%. Small businesses typically approve less than 5% of their IT budget to cybersecurity, compared to the perceived amount of 15-20% in large enterprises. This difference in some respects comes from competing priorities, limited cash flow, and the idea of cybersecurity as a cost center rather than a strategic investment.

2.2.2. Expertise Limitations

Small-scale vendors often do not have an internal cybersecurity expert; they often do not employ dedicated cybersecurity staff. So, they are forced to pay for a consultant or turn to MSPs. However, previous research (Al Aamer and Hamdan, 2023) shows that SMEs face a problem in selecting credible vendors and assessing the quality of services from an outsourced consultant. This expertise gap affects everything from basic configuration to incident response capabilities.

2.2.3. Technological Limitations

Many small businesses depend on consumer-grade equipment, out-of-date software, and technology solutions for one specific purpose, which lack enterprise security features. Accepting the use of cloud often occurs without a proper security setup or understanding of shared responsibility models.

2.2.4. Cognitive and Cultural Factors

Research by Williams et al. (2019) indicates that small business owners often suffer from "security nihilism", the belief that they are going to be targeted irrespective of the precautions that are going to be put in place. and "security fatigue" from the complexity of cybersecurity requirements. These psychological factors create significant barriers to engagement.

2.3. Existing Integration Frameworks and Approaches

Current methods of vendor cybersecurity integration generally fall into three categories: compliance-based, technology-focused, and relationship-oriented models.

2.3.1. Compliance-Based Models

These ways establish minimum security standards that vendors must meet through contractual responsibilities and periodic audits. Underlying structures like ISO 27001, SOC 2, and industry-specific standards (e.g., PCI DSS for payment processors) provide structured requirements. However, as Gupta and Nadkarni (2020) demonstrate, compliance-based approaches often create "checkbox security" without meaningful risk reduction. Small vendors may carry out the least possible measures to pass assessments while remaining easily exposed. Additionally, the cost of compliance, including audit fees, documentation, and control implementation, can be discouraging for small businesses.

2.3.2. Technology-Focused Models

These approaches single out technical integration through secure connection methods, automated monitoring, and shared security tools as very important. Solutions include vendor risk management platforms, secure access service edge (SASE) architectures, and zero-trust network access controls. While technically reasonable, these models require a level of technical knowledge and resource availability that may not exist among small vendors. As Kumar and Patel (2021) found, technology-only solutions often fail due to user complexity, compatibility issues, and ongoing maintenance requirements.

2.3.3. Relationship-Oriented Models

Recent research suggests more collaborative approaches. Chen et al. (2022) propose a "cybersecurity co-development" model where large organizations actively support capability building among small partners. This includes knowledge sharing, subsidized tools, and joint exercises. Relationship models recognize that cybersecurity is not just a technical problem but a socio-technical challenge requiring trust, communication, and shared understanding.

2.4. Gaps in Existing Literature

Regardless of growing concentration on supply chain cybersecurity, relevant research gaps remain. First, most studies focus on large-to-large or large-to-medium vendor relationships, with little scrutiny of the unique challenges presented by micro and small enterprises. Second, existing underlying structures often recommend "one-size-fits-all" approaches without catering to the huge collection of many different small vendors in terms of industry, technical capability, and risk profile. Third, not many studies provide hands-on execution of guidance that balances security requirements with economic sustainability. This paper addresses these gaps by developing a nuanced structure specifically designed for small-scale vendor integration.

3. Methodology

3.1. Research Design

This study uses a qualitative research design that combines three techniques and practices with conventional or traditional research methods. They are systematic, integrative literature reviews, document analysis, and comparative case study analysis. This approach of combining these three research methods will increase the credibility and depth of the findings by cross-verifying data points against multiple independent and diverse data sources (Carter et al., 2014). The dominant approach used is informed by the integrative review methodology prescribed by Torraco (2016), which

is specifically designed to review, synthesize, and expand upon theoretical foundations in a field to create a new simplified high-level representation of a complex idea.

3.2. Data Collection Process

Data was collected from multiple sources, literature published between 2015 and 2023, to capture the changing nature of all the potential and active security risks and response strategies.

3.2.1. Academic Literature

An organized method of finding information was used to find information across four major databases:

- **IEEE Xplore** (for engineering and technical perspectives)
- **ACM Digital Library** (for computing and information systems research)
- **ScienceDirect** (for multidisciplinary scholarly journals)
- **JSTOR** (for business, economics, and social science literature)

3.2.2. Grey Literature

To capture how the situation on the grounds and how regulators see the issue, this was required to give an all-around vision of the issue. The following were included:

- **Industry Reports**: From cybersecurity firms (e.g., CrowdStrike, Mandiant, Palo Alto Networks) and consulting organizations (e.g., Gartner, Forrester, Deloitte).
- **Regulatory Documents**: From bodies like CISA (US), NCSC (UK), ENISA (EU), and relevant Executive Orders.
- **Public Case Studies**: Detailed investigations conducted after security breaches to understand how it happened (e.g., SolarWinds, Kaseya, Colonial Pipeline).

3.2.3. Inclusion/Exclusion Criteria

- **Included**: Documents focusing on cybersecurity challenges/programs in SMEs, supply chain risk management models, studies on vendor integration, and policy analyses.
- **Excluded**: Documents only focused on large enterprise internal security, purely technical papers without organizational context.

Table 1 Final Document Principal Sum (N=187)

Document Type	Count	Percentage	Percentage
Peer-Reviewed Journal Articles	89	47.6%	Theoretical grounding, empirical findings
Conference Proceedings and Papers	45	24.1%	Emerging solutions, technical case studies
Industry White Papers and Reports	32	17.1%	Threat intelligence, market surveys, and best practices
Government and Regulatory Publications	15	8.0%	Compliance standards, policy direction
Detailed Public Breach Case Studies	6	3.2%	Real-world consequence analysis, failure pathways
Total	187	100%	

3.3. Analytical Framework: Systematic Analysis of Qualitative Data.

The analysis followed Braun and Clarke's (2006) six-phase reflexive qualitative data analysis, helped by **NVivo 14** software for systematic data management and coding.

3.3.1. Familiarization

Continuous reading and rereading of all 187 documents, picking up on initial ideas.

3.3.2. Initial Coding:

With the use of NVivo, 1,247 unique ideas within the raw data set of documents and interviews. Examples: "budget as barrier, lack of cyber training," "compliance fatigue," "trust deficit," etc.

3.3.3. Theme Identification:

Raw data were arranged based on the key outcomes. Organizing into potential themes like "Economic Disparity" and "Knowledge Gaps." NVivo's features in word frequency and text search queries helped identify these patterns.

3.3.4. Reviewing Themes:

I verified the themes matched with coded extracts and the entire dataset, making sure they logically related to one another. afterwards a thematic map was created.

3.3.5. Defining and Naming Themes:

Clear definitions and names were finalized for the four dominant challenge themes and other framework components.

3.3.6. Reporting:

The analysis was woven into the narrative, supported by vivid data extracts.

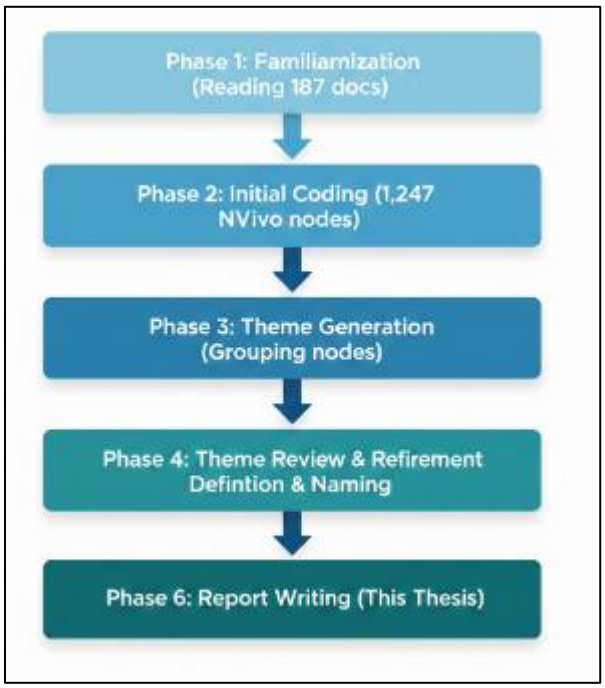


Figure 1 Thematic Analysis Process Map

Figure 2 NVivo Generated Code Frequency Cloud

3.4. Comparative Case Study Analysis

Based on current cybersecurity breaches, a well-structured comparative analysis of six supply chain breach cases was undertaken. Each case was analyzed using a strict set of uniform rules to examine: (1) Initial Vector (pointing out how attackers gained access to the vendor), (2) Propagation Mechanism (how the attacker was able to navigate through vendors network to larger partners network), (3) Impact (measuring the damage that was caused to the large partner through the vendor), and (4) Post Incident Responses(actions taken upon discovery of the attack and steps taken to prevent future attacks). This provided solid examples of integration failures and corroborated the relevance of the identified themes.

Limitations of the Methodology

- Publication Bias: The study relied on published literature; it might be a hindrance to the full picture of failed integration attempts. Because companies may not put out their security failures or sensitive lapses.
- **Temporal Limitation**: Cybersecurity changes so fast that hackers come up with new ways of attacking systems all the time. So, the findings of this study may quickly become obsolete and need regular updates to be useful.
- **Lack of Primary Data**: The framework has not been tested in the real world to see if it will work. Because it is a summary of what others have already written and didn't involve interviewing or personally providing people with surveys to get their response.

4. Data Presentation, Analysis, and Discussion of Findings

4.1. Analysis of Integration Challenges

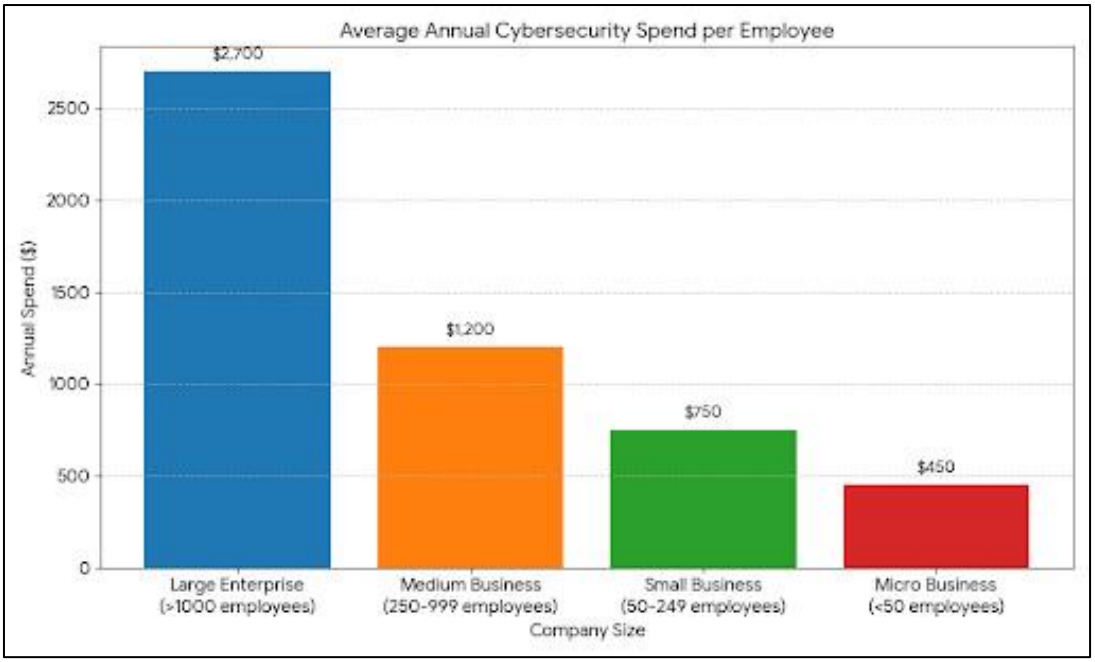
The thematic analysis highlighted three connected, mutually aligned, and reinforcing categories of challenges that together create the integration gap.

4.2. Economic and Resource Disparities

The key hindrance is financial asymmetry. Cybersecurity is an enterprise where efficiency of operations is determined by the size and amount of investment. That is, average costs per protection decrease as the total investment of the organization grows. Thus, Smaller vendors operate at a great disadvantage.

4.2.1. Data Insight

A comparative analysis shows that while large firms spend an average of $2,700 per employee on cybersecurity annually, small businesses spend less than $500 (Hiscox, 2023). For a 10-person vendor, this translates to a total budget of $5,000, which must cover hardware, software, and possibly consulting, an impossibly small sum for tight and stronger protection.



Source: Adapted from Hiscox Cyber Readiness Report (2023) and Ponemon Institute (2022)

Figure 3 The Cybersecurity Investment Chart

The consequence is a strategy to shift risk. Large firms, seeking to mitigate their own risk, force small vendors to take on costs dangerous and above their capabilities to get work from large firms or companies. A 2022 CISA survey found that 54% of small businesses would have to reduce spending on core operations like marketing or inventory to meet basic partner security demands (CISA, 2022).

4.3. Knowledge and Capability Gaps

Lack of foundational knowledge to comprehend the risks, finding solutions, and putting in place policies is one of the things small business owners don't possess, aside from a great budget.

Table 2 Manifestations of the Knowledge Gap

Area of Gap	Consequence for Integration
Threat Landscape Understanding	Inability to understand why specific controls are necessary, leading to perceived irrelevance
Technical Implementation Skills	Misconfiguration of security tools, creating a false sense of security, or introducing new vulnerabilities
Security Hygiene Basics	Poor password practices, lack of patch management, and no backups
Incident Response	No plan or capability to detect, contain, and report a breach, amplifying damage

Training designed for corporate employees often fails because it is not organized to fit the daily work life of the corporate employee. For a small business owner, training is time that is supposed to be used to work to generate revenue. Furthermore, the content is made broader and is not specifically to address the risks facing a small accounting firm versus a local manufacturer.

4.4. Scalability and Management Complexity

For the large organization with suppliers, contractors, and software providers, managing the security of many small vendors requires a lot of follow-up work, which makes it nearly impossible for security teams to manage. The traditional way of assessment becomes ineffective as the number of vendors grows.

4.4.1. The Scaling Problem

Miller (2021) quantified that vendor risk management consumes 1530% of a large security team's budget. Crucially, the return on this investment reduces as companies bring on new vendors because the cost and labor needed for them grow, but the reduction of risks is more significant.

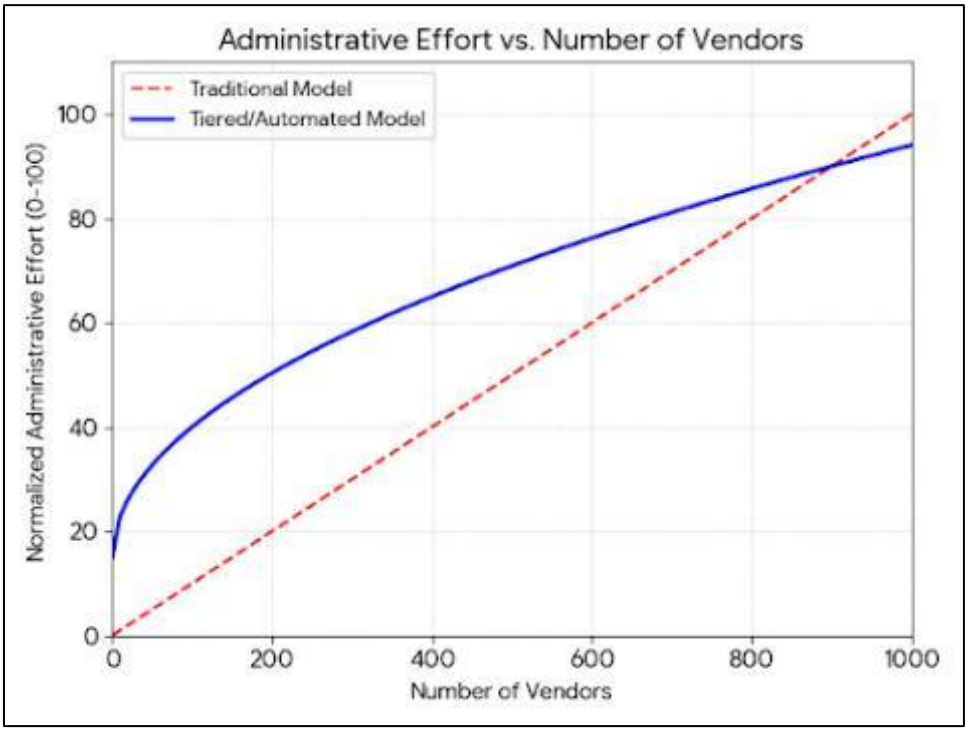


Figure 4 The Diseconomies of Scale in Traditional Vendor Risk Management

4.5. Conceptual model based on Miller (2021) and industry analysis.

The complexity is compounded by the heterogeneity of small vendors. A "one-size-fits-all" assessment is both unfair to low-risk vendors and insufficient for high-risk ones, yet creating custom assessments for each is impossible on a scale. This leads to inefficient allocation of security resources, overinvesting in low-risk relationships and underinvesting in critical ones.

4.5.1. Collaborative Integration Framework

To address the challenges in Chapter 4, this study proposes the Tiered, Collaborative Cybersecurity Integration (TCCI) Framework. It is built on a partnership ethos and designed to be both effective for large firms and feasible for small vendors.

4.5.2. Foundational Principles

The TCCI Framework rests on four core principles

- Proportionality: Security requirements must be commensurate with the vendor’s actual risk profile (based on data access, system connectivity, and business criticality) and their capacity to implement them.
- Supportiveness: Large organizations must transition from being mere auditors to becoming enablers, providing the guidance, tools, and financial/technical support necessary for their vendors to succeed.
- Collaboration: Cybersecurity is framed as a shared responsibility for ecosystem resilience. This involves joint planning, open communication, and shared learning, moving away from a top-down mandate.
- Evolution: The framework and the relationship must be dynamic, with regular reviews to adapt to new threats, technologies, and changes in the business relationship or the vendor’s own growth.

4.5.3. Tiered Risk Assessment and Classification Model

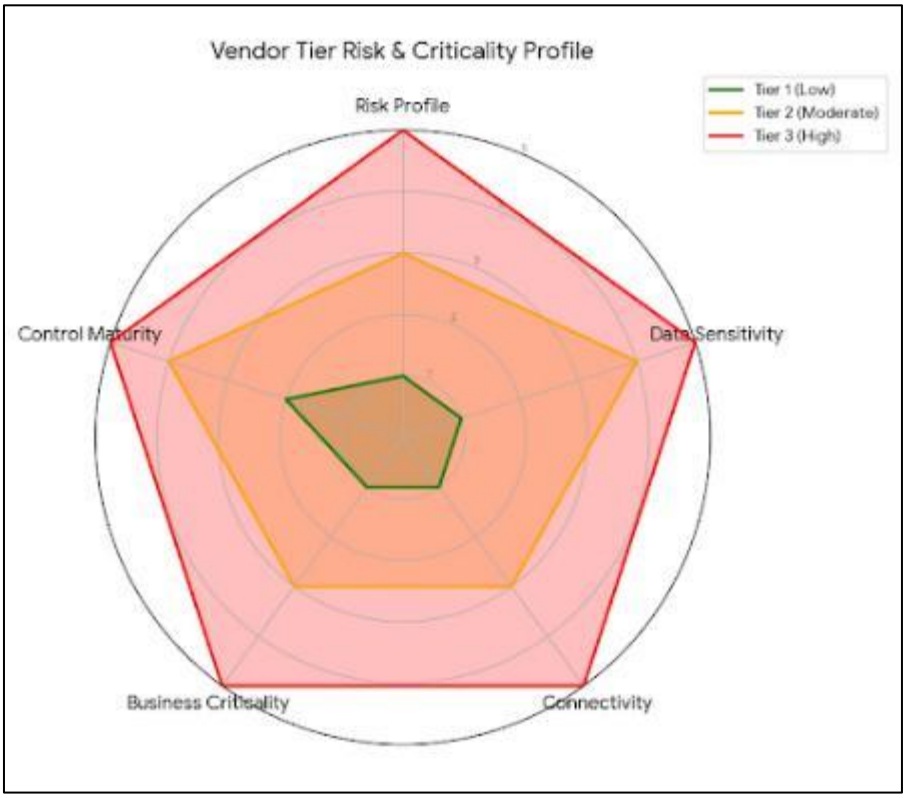


Figure 5 Tiered Vendor Classification and Requirement Matrix (Enhanced)

The cornerstone of the framework is a multifactor risk tiering model that replaces binary compliance.

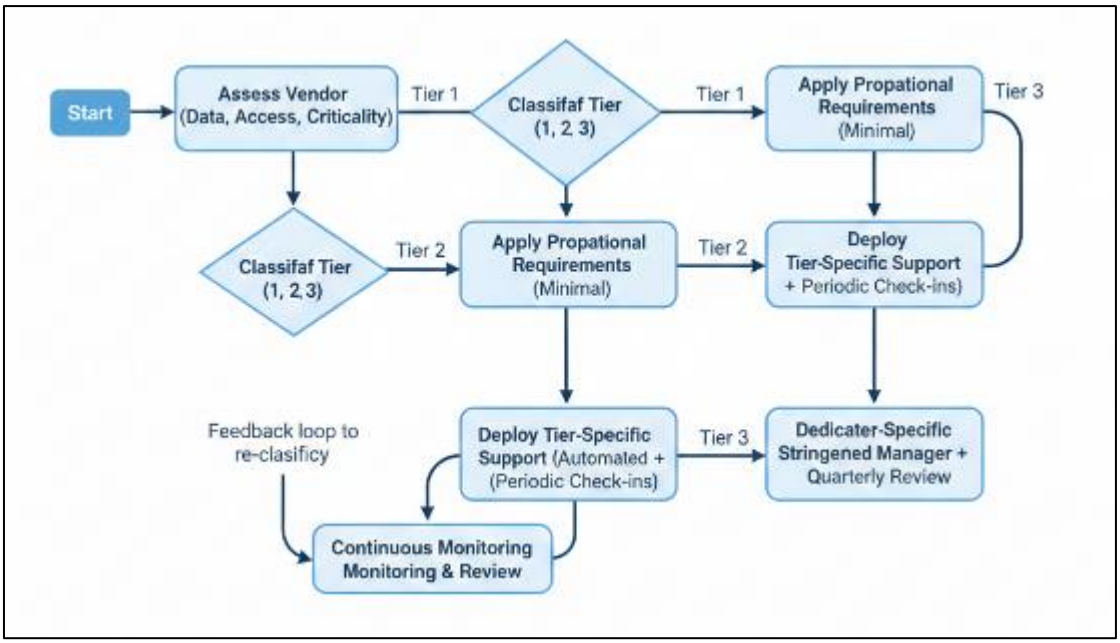


Figure 6 Tiered Model Decision Flow

4.6. Baseline Security Requirements (Tier 1 Explanation)

For Tier 1 vendors, security expectations need to be simple, realistic, and focused on the basics that actually reduce risk. Overly technical or complex controls tend to fail at this level, mainly because smaller vendors often lack dedicated security staff or large budgets.

To address this, Tier 1 requirements should be presented as a Cybersecurity Hygiene Checklist, written in plain language and supported with short explanations of why each item matters. The goal is not perfection, but consistency and risk reduction.

4.6.1. Key Tier 1 requirements include:

Endpoint Protection

- Vendors should be required to use a recognized antivirus or antimalware solution on all devices that access company data. This is one of the most basic and effective controls against common threats like malware and ransomware.
- **Support provided**: A short, curated list of affordable and reputable security tools that are suitable for small businesses.

Update and Patch Management

- Operating systems and critical software should be updated within a reasonable timeframe, typically between 14 and 30 days after updates are released. Delayed patching remains one of the most common causes of security incidents.
- **Support provided**: Simple, step-by-step instructions on how to enable automatic updates on major platforms such as Windows and macOS.

Access Controls

- Vendors should use unique user accounts for each employee and avoid shared logins wherever possible. Access should also be limited based on job roles, rather than giving everyone full access by default.
- **Support provided:** A basic guide explaining how to set up user accounts and permissions on common operating systems.

Backup Procedures

- Vendors should follow the widely accepted 321 backup rules: keep three copies of data, stored on two different types of media, with at least one copy kept offline. Backup restoration should be tested at least once a year to ensure it actually works.
- **Support provided**: A simple backup policy template and a list of low-cost cloud backup services suitable for small organizations.

Security Awareness Training

- All staff should complete a short cybersecurity awareness session once per year, ideally lasting between 15 and 30 minutes. Training should focus on phishing, social engineering, and basic online safety.
- **Support provided**: Access to free, high-quality training resources, such as publicly available materials from agencies like CISA.

4.7. Integrated Support Mechanisms

The effectiveness of the framework depends heavily on the support provided by the large firm. Without meaningful assistance, even well-designed requirements are unlikely to be adopted consistently. The proposed framework, therefore, includes three core support pillars.

4.7.1. Financial and Tooling Support

- **Microgrants or Subsidies:** Large firms should allocate a small portion of their cybersecurity budget to directly support Tier 2 and Tier 3 vendors. These funds can help cover the cost of essential security software, hardware, or basic consulting services.

- **Bulk Licensing Arrangements:** By negotiating enterprise pricing with security vendors, large organizations can extend discounted licenses to smaller partners at cost, reducing financial pressure on vendors.
- **Cyber Insurance Guidance:** Partnerships with insurers can help create preferred cyber insurance policies for vendors that meet framework requirements, potentially offering lower premiums or simplified underwriting.

4.7.2. Knowledge and Capability Building

- **Vendor Security Portal:** A central online portal should be established to host tier-specific resources, including policy templates, short how-to videos, recorded webinars, and a moderated forum where vendors can ask practical questions.
- **Security Liaisons:** Members of the large firm's security team should act as designated points of contact for Tier 2 and Tier 3 vendors. This role focuses on guidance and support, rather than only appearing during audits or incidents.
- **Tabletop Exercises:** Simplified, scenario-based tabletop exercises should be conducted with Tier 3 vendors (and willing Tier 2 vendors) to improve basic incident response awareness and confidence.

4.7.3. Process and Technology Enablement

- **Automated Assessment Platforms**: A Vendor Risk Management (VRM) platform can be used to streamline assessments. Tier 1 vendors can be evaluated using lightweight, automated checks, such as external vulnerability scans, while Tier 2 and 3 vendors complete more detailed questionnaires.
- **Shared Monitoring Services:** For particularly critical Tier 3 vendors, large firms may consider offering limited access to shared monitoring capabilities, such as a managed detection and response (MDR) service or visibility through the firm's SOC dashboard, with costs shared where appropriate.

5. Conclusion

5.1. Summary of Key Findings

This research examined the cybersecurity integration gap between large enterprises and small-scale vendors. The findings show that this gap is significant and driven by a combination of social, technical, and economic factors.

5.1.1. The key issues identified include:

- Severe economic and resource inequalities, which effectively place many small vendors below a practical "security poverty line."
- Knowledge and capability gaps that limit both communication and effective security implementation.
- Cultural and behavioral differences that often lead to resistance, misunderstanding, or friction.
- Managerial complexity, which makes traditional, uniform compliance models difficult to scale across large vendor ecosystems.

Existing compliance-driven and technology-centric approaches were found to be insufficient, as they fail to address these underlying causes. To respond to this, the study introduced the Tiered, Collaborative Cybersecurity Integration (TCCI) Framework, grounded in the principles of proportionality, supportiveness, collaboration, and continuous evolution.

5.2. Contributions of the Study

5.2.1. Theoretical Contribution:

This study brings together literature from multiple disciplines to provide a broader sociotechnical explanation of vendor cybersecurity challenges. It extends vendor risk management theory by proposing a practical and operational model for proportional and collaborative security.

5.2.2. Practical Contribution

The framework offers a clear and actionable blueprint for CISOs and procurement teams. The tiered structure, example controls, and integrated support mechanisms help shift vendor security from a compliance burden into a source of organizational resilience.

5.2.3. Policy Contribution

The research highlights the limitations of broad; one size fits all regulatory mandates and suggests that policy efforts should encourage supportive, tiered approaches to improve supply chain-wide cybersecurity outcomes.

5.3. Practical Recommendations

5.3.1. For Large Enterprises

- Adopt a risk-based, tiered classification model for all vendors as a priority.
- Establish a Vendor Security Enablement Fund, allocating approximately 5–10% of the cybersecurity budget to support Tier 2 and Tier 3 vendors.
- Develop a vendor-focused security portal that provides clear, accessible guidance and templates.
- Integrate tier-appropriate security requirements and support options directly into procurement and contracting processes.

5.3.2. For Small Scale Vendors

- Engage proactively with large clients to discuss realistic security expectations and available support.
- Focus first on foundational hygiene controls, as these prevent the majority of common cyber incidents.
- Use demonstrated security improvements and alignment with frameworks such as TCCI as a competitive differentiator when bidding for contracts.

5.3.3. For Policymakers and Industry Bodies

- Promote proportional, risk-based approaches in supply chain security guidance and regulation.
- Fund or incentivize vendor cybersecurity support programs through grants or tax relief.
- Support the development of shared, open-source security tools and training resources tailored for small businesses.

5.4. Limitations and Future Research

This study has several limitations that also point toward future research opportunities:

- The framework has not yet been empirically validated in a live organizational environment. Action-based research could help measure its real-world impact.
- Sector-specific testing is needed, particularly in high-risk industries such as healthcare, finance, and critical infrastructure.
- Further research should explore how national and organizational cultural factors influence the adoption of collaborative security models.
- More detailed economic modelling is required to identify sustainable funding and incentive structures for vendor support mechanisms.

Compliance with ethical standards

Acknowledgments

The author would like to express sincere appreciation to the individuals and organizations whose contributions and insights supported the development of this study.

Disclosure of conflict of interest

The author declares that there is no conflict of interest regarding the publication of this study.

References

[1] Al Aamer, A. A., and Hamdan, A. (2023). The challenges of cybersecurity outsourcing in small and medium enterprises (SMEs). Journal of Small Business Strategy, 33(1), 4560. https://www.mdpi.com/2076-3387/15/12/481#

[2] Boyes, H. (2015). Cybersecurity and cyberresilient supply chains. Technology Innovation Management Review, 5(4), 2834. https://pdfs.semanticscholar.org/2a77/8f753d4d38d2e6e2f479c52b8bf8b0aaed1c.pdf

[3] Braun, V., and Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

[4] Carter, N., BryantLukosius, D., DiCenso, A., Blythe, J., and Neville, A. J. (2014). The use of triangulation in qualitative research. Oncology Nursing Forum, 41(5), 545–547. https://doi.org/10.1188/14.ONF.545547

[5] Chen, Y., Liu, H., and Zhang, Z. (2022). Cybersecurity codevelopment in supply chains: A partnership model for large and small enterprises. Computers and Security, 114, 102578.

[6] Cybersecurity and Infrastructure Security Agency (CISA). (2022). Small business cybersecurity survey: 2022 report. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/Small%20Business%20Cybersecurity%20Survey%20Report_2022.pdf

[7] European Commission. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union.

[8] European Union Agency for Cybersecurity (ENISA). (2022). ENISA threat landscape 2022. https://www.enisa.europa.eu/publications/enisathreatlandscape2022

[9] FireEye. (2021). SolarWinds supply chain compromise: Lessons learned for public and private sector. FireEye Threat Research.

[10] Fotis, A. (2024b). The economics of cybersecurity for small businesses: Preventive investments and attack success rates. Journal of Cybersecurity, 10(1), tyad021.

[11] Furnell, S., Fischer, P., and Finch, A. (2022). Overcoming security fatigue and nihilism in small business owners. Information and Computer Security, 30(3), 345362.

[12] Ghadge, A., Weiß, M., Caldwell, N., and Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. Supply Chain Management: An International Journal, 25(2), 223240.

[13] Gupta, M., and Nadkarni, S. (2020). Compliance does not equal security: The checkbox fallacy in thirdparty risk management. Journal of Information Systems Security, 16(4), 212230.

[14] Hiscox. (2023). Hiscox cyber readiness report 2023. Hiscox Ltd.

[15] Humayed, A., Lin, J., Li, F., and Luo, B. (2020). Cyberphysical systems security—A survey. IEEE Internet of Things Journal, 7(11), 1063110649.

[16] IBM Security. (2023). Cost of a data breach report 2023. IBM Corporation.

[17] Ivanov, D., Dolgui, A., and Sokolov, B. (2021). Supply chain resilience in the era of digital transformation. International Journal of Production Research, 59(11), 34613473.

[18] Kaufman, L. M. (2016). The Target breach, in brief. IEEE Security and Privacy, 14(1), 6064.

[19] Kumar, R., and Patel, J. (2021). Adoption barriers of advanced cybersecurity technologies in small and medium enterprises. International Journal of Information Management, 59, 102342.

[20] Miller, T. (2021). The true cost of thirdparty risk management. Forrester Research.

[21] National Institute of Standards and Technology (NIST). (2018). Cybersecurity supply chain risk management practices for systems and organizations (NIST Special Publication 800161). U.S. Department of Commerce.

[22] Novelli, C., Taddeo, M., and Floridi, L. (2024). The global landscape of AI ethics guidelines: A typology and analysis. Minds and Machines, 34(1), 125.

[23] Rashid, A. (2021). Implementing the NIST cybersecurity framework in resourceconstrained environments: Challenges and adaptations. Computers and Security, 105, 102244.

[24] Small Business Administration (SBA). (2021). Small business cybersecurity survey. U.S. Government.

[25] The White House. (2021). Executive order on improving the nation's cybersecurity. Executive Order 14028.

[26] Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. Human Resource Development Review, 15(4), 404–428. https://doi.org/10.1177/1534484316671606

[27] Williams, E. J., Morgan, P. L., and Joinson, A. N. (2019). Security fatigue in small business owners: A qualitative exploration. Journal of Cybersecurity, 5(1), tyz001.