Supply Chain Cybersecurity and Small and Medium-Sized Enterprises (SMEs): Exploring Shortcomings in Third Party Risk Management of SMEs

Jillian K. Kwong
Massachusetts Institute of Technology
jkwong1@mit.edu

Keri Pearlson
Massachusetts Institute of Technology
kerip@mit.edu

Abstract

Small and medium-sized enterprises (SMEs) have long been known to be a weak link in supply chain cybersecurity. Despite their crucial role in the global supply chain, SMEs and their struggle to increase cyber resiliency and improve their defenses is understudied in academic literature. This paper uses qualitative research methods to conduct an empirical study of the challenges SMEs encounter when participating in third party cybersecurity risk assessments. Using interviews with cybersecurity and supply chain practitioners, this study provides an overview of four major risk assessment methods (i.e., questionnaires, audits and certifications, security rating services, and direct testing) and the problems that arise when companies apply tools designed for large corporations to SMEs. Results discuss how and why traditional methods fail and offers insights on how to improve third party risk of SMEs moving forward.

Keywords: Cybersecurity, Small and Medium-Sized Enterprises, Third Party Risk Assessments, Supply Chains, Cyber Risk Management

1. Introduction

In recent years there has been an explosion of cyberattacks against key suppliers that have crippled critical infrastructure and caused major disruption to everyday life (e.g., SolarWinds, NotPetya, Colonial Pipeline, etc.). A key element in these incidents has been the global supply chain. According to CrowdStrike (2021) cyberattacks have risen 430% since 2020. The Verizon Data Breach Investigation Report (2021), a systematic forensic analysis of some 80,000 incidents worldwide, concluded that in 62% of compromises, the supply chain was key in gaining access. As organizations around the world begin to shore up their defenses, one category of businesses continues to lag behind: small and medium-sized enterprises (SMEs). SMEs have long been known to be a weak link in supply chain cybersecurity. Research has found up to 70% of SMEs struggle to keep pace with the operational demands of a continuously digitizing world while at the same time falling victim to cyberattacks and breaches at alarmingly high rates (ESET, 2023). These incidents threaten not only information technology (IT) systems and data assets but can also disrupt operational technology (OT) and physical systems as well.

One issue is that many of the major cyber risk frameworks and maturity models are not designed for SMEs (Alshboul and Streff, 2015; Javaid and Iqbal, 2017). Common frameworks used to assess and manage risk such as NIST Risk Management Framework (RMF), ISO 27000+ series, Service Organization Control Type 2 (SOC2), and Cybersecurity Capability Maturity Model (C2M2), to name a few are primarily designed for large organizations or those in critical infrastructure sectors. Compared to SMEs, these organizations have vastly different resources, business structures, budget, staffing, policies, and capabilities which complicates the application of major cybersecurity frameworks to SMEs.

SMEs are a crucial part of the global economy representing over 90% of businesses worldwide, while accounting for over 50% of the world's employment (World Bank, 2023). However, despite being the backbone of many supply chains, SMEs are vastly understudied when it comes to cyber risk management in the supply chain (Alshboul & Streff, 2015; Alahmari and Duncan, 2020; Javaid and Iqbal, 2017). This is a complex problem that even regulation has yet to fully understand. Research has shown some government efforts to introduce minimum standards and build resilience can actually have an opposite effect by introducing greater levels of risk into cybersecurity supply chains. A prominent example of this was the 2016 US Department of Defense (DoD) DFARS 252.204-7012 mandate which outlined cybersecurity

URI: https://hdl.handle.net/10125/107183
978-0-9981331-7-1

and incident reporting standards for all DoD suppliers. According to Melnyk et al. (2022), the roll-out was unsuccessful largely due to resistance by SMEs who struggled to marshal the appropriate expertise, resources, and knowledge to implement DFARS requirements. Rather than building cyber resiliency, the draconian legislation caused SMEs to leave the supply chain altogether. "The requirement was seen as imposing additional cybersecurity requirements on organizations not capable of complying, due in part to the already over-stretched resources. For some SMEs, this new requirement was a contributing factor for their decision to exit the DoD supply base […] These exiting firms may expose the entire supply to a greater level of cybersecurity risk than the firms staying in the supply chain without complying to the mandate." (Melnyk et al., p. 166).

This lack of attention on SMEs unfortunately exists across industry, government, and academia. Efforts to reduce risk and build resiliency within supply chains will continue to struggle unless more effort is made to understand the difficulties SMEs face managing cyber risk in everyday practice. This intersection represents a perfect opportunity for academics to bridge theory and practice and produce groundbreaking research that has significant real-world impact. While many scholars have studied the technical aspects of information security (Brunner et al., 2020; Lee, 2020) and general best practices for SME cybersecurity (Cartwright et al., 2023; Lacity & Reynolds, 2014; Rawindaran et al., 2022), this article uses a qualitative approach to explore challenges SMEs face related to cybersecurity risk assessments. It should be noted that this problem is not due to shortcomings in technology and thus cannot be addressed from a purely technical perspective. Many of these challenges arise from humans interacting with each other as well as the technical systems and business processes at work. Because of this, it is important to look at the problem from a management and organizational communication perspective to prioritize the study of humans and their interactions with the world around them. This paper highlights hidden dependencies and breakdowns that occur in practice and how it impacts SME cybersecurity and risk assessment.

Answering the call by Alahmari and Duncan (2020) this research seeks to close this gap by conducting an empirical study of challenges SMEs face related to cyber risk management assessments and supply chain cybersecurity. Using interviews with cybersecurity and supply chain practitioners, the goal of this paper is to study the challenges SMEs encounter when participating in third-party cybersecurity risk assessments. Results will inform future work about how to better address cybersecurity vulnerabilities within supply chains. The research question is as follows:

RQ: What cybersecurity challenges do SMEs encounter when it comes to third party risk assessments?

2. Cyber Risk Management and Supply Chains

Academic literature has studied different aspects of cyber risk management including typologies of cyberattacks, threats, and sources of intrusion (Kumar & Mallipeddi, 2022; Lamba et al., 2017; Nygård & Katsikas, 2022). Researchers have also explored how firms responded to protect digital supply chains and the different ways cyber risks have been mitigated throughout the supply chain (Boiko et al., 2019; Boyson et al., 2022; Ghadge et al., 2020; Kumar & Mallipeddi, 2022; Nygård & Katsikas, 2022). Case studies on internal policies and programs of individual organizations have also been conducted to understand how companies addressed cyber threats to their digital supply chains (Boyson et al., 2022; Colicchia et al., 2018; Gaudenzi & Siciliano, 2017).

2.1. Cyber Supply Chain Risk Management

Cyber Supply Chain Risk Management (CSCRM) is an integrated discipline at the intersection of cybersecurity, enterprise risk, and supply chain management. Boyson (2014) defines CSCRM as the "organizational strategy and programmatic activities to assess and mitigate risks across the end-to-end processes (including design, development, production, integration, and deployment) that constitute the supply chains for IT networks, hardware, and software systems" (p. 342). However, studies have identified weaknesses in CSCRM as well as other cyber risk frameworks criticizing them as ineffective due to problems with scope or inconsistent uptake in practice (Boyson et al., 2022; Fenz et al., 2014; Javaid & Iqbal, 2017). According to Brunner, Sauerwein, Felderer, and Breu (2020) industry practitioner's reliance on informal, non-replicable approaches impedes collection of high-quality, reliable data. They found typical risk identification practices involved in-person meetings, phone calls, and emails between stakeholders to brainstorm "techniques and checklists to identify information security risks. Accordingly, these practices limit[ed] the traceability and documentation of decisions which might result in a lack of transparency" (p. 17). In response, researchers have called for greater study and alignment of risk management approaches with industry practices (Boyson et al., 2022; Brunner et

al., 2020; Fenz et al., 2014; Javaid & Iqbal, 2017; Wangen & Snekkenes, 2013; Webb et al., 2014).

2.2. SMEs and Cyber Risk Frameworks

Research has found SMEs in particular struggle with the application and implementation of cyber risk frameworks due to lack of budget, management support, limited IT staff, and expertise. According to Javaid & Iqbal (2017), IT risk management in SMEs is challenging because 1) the major standards are designed for large organizations with "well-structured business processes" and IT risk management expertise and 2) fail to provide an accurate level of detail, scope, and guidance for SMEs. The authors explain, "either these standards are specific to some particular business domain or provide generic guidelines at strategic level with missing operational level details, which needs to be integrated and customized before its application to a particular enterprise business processes and environment" (p. 78). Although SMEs have been understudied in cybersecurity and risk management literature, there has been some research providing in-depth critiques of popular risk management frameworks applied to SMEs and proposal of new models specifically designed for SMEs which have not yet been rigorously tested or implemented in practice (Alahmari & Duncan, 2020; Alshboul & Streff, 2015).

3. Methodology

Data was drawn from semi-structured interviews with subject matter experts including practitioners from cybersecurity, supply chain, legal, and business departments. This included security specialists (e.g., CISOs, security consultants), supply chain managers, legal and compliance experts (e.g., governance, risk management, and compliance (GRC) teams), executive leadership, and other management personnel. Interviews were chosen for this exploratory study because unlike questionnaires, experiments, or surveys, interviews allowed the researchers to delve into the individual experiences of SMEs related to third party risk assessments (King, 1994).

Questions from the in-depth, semi-structured interviews probed practitioner knowledge, motivations, perceptions, and experiences about 1) cybersecurity supply chains, 2) cyber risk management, and 3) challenges encountered protecting their organizations and data. The primary focus was to get a better sense of how current cybersecurity systems worked at SMEs. In terms of analysis, interviews were coded using selective open coding and analyzed using thematic analysis. The first phase involved identifying emergent patterns while an iterative, inductive approach was used to identify reoccurring themes and distinguish patterns within transcripts (Charmaz, 2006; Murphy, Dingwall, Greatbatch, Parker, & Watson, 1998; Strauss & Corbin, 1990).

4. Shortcomings of Traditional Risk Assessment Methods When Applied to SMEs

Interviews with practitioners identified four of the most common risk assessment methods used to evaluate third party security specifically 1) surveys/questionnaires, 2) audits and certifications, 3) security rating systems, and 4) direct testing. Participants discussed their experiences with each method at length including strengths, weaknesses, and challenges they encountered in practice. A topic of particular salience to all interviewees was the differences between how security was *supposed* to work on paper versus how it *actually* played out on the ground.

A key weakness identified across all methods was the lack of depth or context around the resulting data. Most tools (except direct testing) only provided a snapshot of a specific aspect of an SME's security program but what was missing was a way to see how an organization's security was working in practice. One reason for this was the heavy reliance on self-report or self-attestation from the company being evaluated. While all data should be subject to scrutiny, the inability to verify information provided by a SME (or any organization for that matter) made it difficult for companies to accurately assess risk and mitigate it.

Traditional assessment methods also created additional barriers for SMEs to prove their cybersecurity maturity due to their high cost, time requirements, and disruption to regular operations. While large organizations can build the cost of regular audits, assessments, certifications, and other expenses into their budgets, SME's struggle to keep up with the ongoing costs of demonstrating cybersecurity using these traditional methods. Practitioners argued that the time and money required to demonstrate compliance under the current system using traditional assessment methods created a two-tier system that rewarded those who could "pay to play" while shutting out those who could not afford the high cost of audits and yearly certifications. They also pushed back against the idea that paying for these services actually made an organization more secure noting that compliance did not equal security. Many organizations who could demonstrate compliance and meet standards on paper were not anywhere near being secure in practice. This section discusses four of

the most common types of third-party assessment tools used to evaluate SMEs including strengths, weaknesses, and challenges in implementation. Findings are summarized below and in Table 1.

Table 1. Types of Assessment Tools.

Types of Assessment Tools	Strengths	Weaknesses
Questionnaires and Surveys (e.g., based on ISO 27000+)	• Cheap • Easy to administer • Widely used and accepted throughout the industry	• Based on self-report/self-attestation • Long, time consuming (1000+ questions), and low response rates • Only as good as respondent is honest • Often too vague to be actionable or useable
Audits and Certifications (e.g., System and Organization Controls (SOC) 2 reports)	• Establishes standards to benchmark security against • Provides documentation • Signals leadership has begun to think about/invest in security	• Reflects security on the day the organization was audited or certified • Expensive and time consuming • Only as good as the person auditing/certifying • Criticized as "Pay to play" system
Security Rating Services (e.g., BitSight, SecurityScorecard, RiskRecon, etc.)	• Offers an "objective" (i.e., not a self-assessment) rating of an organization's security	• Misleading based on what is promised vs. what is actually delivered • Criticized as "Pay to play" system
Direct Testing (e.g., penetration testing and red team assessments)	• One of the best/most accurate and reliable ways of assessing 3rd party security	• Cost • Time consuming • Liability • Permissions

4.1. Questionnaires and Surveys

Questionnaires and surveys were signaled out as one of the most commonly used tools for third party risk assessment. Based on internationally recognized standards (e.g., NIST Cybersecurity Framework (CSF), ISO 27001, IEC 62443) or one developed by an individual company, this method was cheap, easy to administer, and widely accepted throughout the industry. These often involved checklist style questions asking about technical setup, configurations, processes, policies, and procedures.

Not only were questionnaires criticized as being too long, generic, and time-consuming (resulting in low completion rates), but also because they were based on self-report or self-attestation by the organization being evaluated. This meant answers are only as good as the honesty of the person filling them out. The entire assessment hinged on how truthful or forthcoming the SME in question was about their security. The inability to verify answers meant SMEs had to be taken at their word. The lack of accountability mechanisms or avenues for recourse meant not only the opportunity but incentive for SMEs to lie and get away with it were quite high.

Another major issue was that results were often too vague and general to be useful. Although questionnaires can give insights into technical capacities and how networks are configured, they often lacked detail about how systems were being used and what exactly was going on in practice. Despite being extremely time-consuming, both SMEs and large companies expressed disappointment in the effectiveness of questionnaires to help inform decisions about third party security. Not only did questionnaires take an inordinate amount of time to complete, but they also took an enormous amount of time to review. Most, if any, organizations do not have any reliable way to use information from questionnaires in a meaningful way which meant this process resulted in very few actionable insights.

Aside from these general shortcomings, questionnaires presented a barrier for SMEs who had limited staff and capability to complete them in a timely manner. While larger organizations could hire staff and build entire departments dedicated to demonstrating

compliance, SMEs were far more limited and had to divert an existing employee's attention away from their usual job or hire new staff to complete them. While some SMEs have started pushing back against the use of questionnaires by charging fees to offset the time and expense of completing lengthy questionnaires, some startups are looking to automate the process and create repositories for answers. However, some interviewees criticized these efforts as not actually addressing the underlying problem but instead putting a Band-Aid over it.

4.2. Audits and Certifications

Audits and certifications were another popular way of demonstrating cybersecurity maturity by showing compliance with major standards. This category typically involved an external third party coming in to assess the security of an organization and to see if compliance and/or security mandates were being met. These were commonly based on established standards or widely accepted criteria such as ISO 27000 series, NIST, or SOC2 frameworks. According to participants, audits and certifications were useful for benchmarking a company's security, providing documentation, and signaling to those outside the company that the SME has begun to think about and invest in cybersecurity.

However, practitioners also pointed out that because many of the assessments were checklist-based, there was ample opportunities for companies to be certified as compliant without actually being secure. Similar to questionnaires, the audit and certification process was highly subjective and dependent on the quality of answers provided by the SME as well as the proficiency of the evaluator. Participants stressed that being compliant with mandates and standards did not automatically equate to a company being mature or having good security. A company can be considered "secure" on paper and still be attacked regardless of whether they have great, average, mediocre, or poor security. They argued the purpose of audits and certifications is not necessarily to stop attacks but to provide assurance that if the company were to be attacked, there were mechanisms and processes in place to defend the organization and recover. In this sense, audits and certifications do not just document the security program in place, but also provide a layer of assurance to outsiders that the organization had reasonable protections in place and acted in a reasonable manner thus helping protect them from liability in case of a potential lawsuit.

However, many SMEs were not able to afford the costs of regular audits and certification renewals which put them at a major disadvantage when trying to demonstrate security and protect themselves from liability. For many SMEs, the cost and time required to complete these activities were out of reach. One interviewee lamented the high cost of SOC2 certifications.

4.3. Direct Testing

Participants rated direct testing as the "gold standard" of third-party risk assessments but cautioned against its widespread use citing concerns about liability and permissions. Direct testing can include the use of penetration (pen) tests or red team assessments. The purpose of each is to evaluate the security of an organization by breaching their defenses. Pen testing usually aims to find weaknesses in defense capabilities by identifying vulnerabilities and exploitable flaws in a company's cybersecurity. Since the goal is to gain maximum coverage across an organization in a minimum amount of time, these tests are done with the support of IT and senior leadership. Unlike red team exercises, pen tests primarily look for known vulnerabilities and thus are methodical in their approach (Evalian, 2022). On the other hand, the objective of red teams is to gain access or test security measures around specific area. They typically are more complex and time intensive than pen tests since they involve conducting a thorough exercise of the organization's response capabilities and security measures. Given the nature of the exercise, usually only a few key stakeholders within the organization are aware of the simulation to test real-time response and defenses (Cyderes, 2023).

Direct testing be an extremely powerful tool providing one of the best, most accurate methods of assessing third party cybersecurity and even cyber resiliency. Unlike other risk assessment methods, direct testing does not rely on self-attestations nor does it base decisions off of piecemeal metrics. Data is collected in real time measuring an organization's ability to prevent, detect, respond, and recover from attacks. Judgements about cyber maturity are grounded in real-time information about a program's strengths and weaknesses when responding to threats.

Despite the many benefits of direct testing, this method is used sparingly due to its long list of downsides. Not only is it extremely time consuming, expensive, and potentially disruptive to the target organization, it opens up serious liability concerns and potential lawsuits if the tests do not run according to plan. Getting permission to test companies can be difficult as it represents an opportunity for data breaches or other high-risk incidents to take place that could require reporting to government authorities or other administrative headaches. Direct testing of SMEs is extremely risky especially if there are not proper backups and precautions in place. This poses barriers for

SMEs since many do not have the staff and infrastructure to manage and mitigate incidents that might result from the exercises.

5. Unresolved Challenges Related to SMEs and Risk Assessments

As a whole, current assessment methods struggle to accurately and reliably measure cybersecurity in practice. Most tools were subjective and based decisions on incomplete and indirect information that was not easily verifiable or validated. The problem with these tools was that they were designed to measure mechanisms and processes on paper but not necessarily how the systems responded worked in real time. While direct testing can address many of these shortcomings, it was considered to be extremely high risk, costly, and riddled with liability concerns that limited its wider application across industry. In order to move the needle forward on third party risk assessment, tools need to evolve from checklists and subjective metrics to more dynamic measurements that allow practitioners to make decisions based on what is in front of them not just what is listed on paper.

Given the drawbacks with all four methods, participants discussed how they navigated gaps in information. Practitioners relied on interviews or simple conversations with SMEs to probe areas of weakness and inform their decision-making. Because traditional assessment tools often produced an incomplete picture, these discussions offered an efficient way to address outstanding questions or concerns by delving into problem areas, "spot check" abnormalities, discuss red flags, and coordinate response or mitigation plans. However, interviewees pointed out this required knowledgeable staff on both sides who could engage in these conversations. This research identified three key weaknesses in third party risk assessments of SMEs that should be addressed.

5.1. Information Asymmetry

Information asymmetry occurs when there is an imbalance in information between two parties. In this case, a company must make decisions and grant access to their systems and infrastructure based on subjective and incomplete information about a SME's security. While information asymmetry exists in every relationship, it is especially pronounced when it comes to third party risk assessments because there are so few effective tools to vet and verify information. When a company is less than forthcoming or truthful about their security, there are not a lot of alternative options to evaluate them. While in theory companies whose suppliers do not meet their standards can go elsewhere, often times vendors with highly specialized services are difficult to replace. Switching providers presents a new slew of challenges and risk such as cost, vetting new suppliers, setup, terminating old relationships, and other disruptions to operations.

5.2. Lack of SME Knowledge about Internal Risks and Vulnerabilities

Leadership at SMEs often do not fully understand the cyber risks facing their organization and have limited knowledge about what is going on internally related to cybersecurity. This means organizational decisions are made without much regard to the vulnerabilities, risks, or threats their company faces which can exacerbate the discrepancy between how things should be done versus what is actually being done. On the other hand, even if SMEs were fully aware of the problems, many did not have the resources, expertise, staffing, or ability to fix their issues even if they wanted. This lack of knowledge combined with few means to ensure accountability and verifiability of information unfortunately created an incentive for SMEs to hide or downplay any issues regarding security.

5.3. Assessments Designed to Limit Legal Liability

Assessment tools were designed, developed, and deployed in a way that protected companies from legal liability more than cybersecurity. One of the main ways to hold a company accountable is through contracts and legal means. However, by that point the damage is already done. As mentioned above, these assessment methods were not necessarily created to stop attacks but instead provide assurances to external stakeholders that the organization in question 1) had reasonable security protections in place and 2) would act in a reasonable manner if there was an incident. This process of building a library of supporting documents was important for reducing legal liability in case of an incident but also allows companies to look like they are engaging in good cybersecurity on paper without always doing the work.

This industry norm of demonstrating outward compliance without much expectation of follow-through severely undermined the effectiveness of vital accountability measures. Aggressive testing and documentation of vulnerabilities were not necessarily desirable or encouraged. The more aggressive documentation that took place, the more obligation a company had to fix the issues which created potential liability concerns if critical issues were not addressed in

a timely manner. This was especially problematic for SMEs who struggled with the high cost of audits and certifications and thus had one less way of demonstrating compliance and cyber maturity on paper compared to larger counterparts. They also lacked the means or ability to fix problems when discovered.

6. Actionable Insights

For managers and cyber teams working with or evaluating third party risk of SMEs, there are three things to consider.

6.1. Align Processes to Standards

Aligning company processes to established standards helps decrease or at least limit variation in security postures, practices, and setup. While tailoring assessments to fit an individual company's needs might seem like a good idea in the short run, managers must understand these protections are only as good as the critical mass that adopts it. SMEs are less able to adapt their processes to comply with multiple standards. This variation, however small, could result in mistakes and confusion which increases risk and potential vulnerabilities. Communicating with SMEs about the types of standards they are subject to and how to maximize applicability across its portfolio to build towards a more robust and resilient program is key to managing risk and securing supply chains moving forward.

6.2. Determine Efficacy of New Tools and Processes

Before instituting new requirements, managers should evaluate whether existing tools and processes are actually useful and effective for all parties involved. Too often managers adopt new products and processes that promise to solve problems without critically evaluating its impact or outcomes. Creating tailored versions of surveys or programs might seem like a good idea for a company but should be done only if 1) there is capacity to review and utilize information being produced, 2) they are effective, and 3) can be implemented across multiple organizations in their supply chain. For one company to mandate additional actions that are specific and applicable only to them could potentially increase risk by adding variance into the system and creating more opportunities for mistakes failures to happen in the supply chain. In some cases, these additional steps can cause more work for employees who do not have dedicated time to make it work properly thus resulting in additional burden and bloated processes for both sides. When considering new products and processes, managers should make sure to evaluate and follow up on the new additions to ensure there is tangle value added for both sides thus increasing the likelihood of adoption and long-term adherence.

6.3. Utilize Existing Resources offered by Organizations to Streamline Processes

Rather than reinvent the wheel and build a siloed risk assessment program that only meets the need of one company, managers should look to leverage and build off existing resources that would be accessible to all companies across their supply chain. Since many SMEs supply more than one customer, it is important for larger companies to try to streamline requirements whenever possible to maximize SME compliance and cooperation. There is a vast ecosystem of resources dedicated to SMEs that can inform these efforts. This includes government resources (e.g. CISA Cyber Guidance for Small Businesses, NIST Small Business Cybersecurity Corner, DoD Office of Small Business Programs, US Small Business Administration Cybersecurity trainings, FTC Cybersecurity for Small Business, etc.), industry organizations such as the National Cybersecurity Alliance, Information Sharing and Analysis Organization's (ISAO) (similar to Information Sharing and Analysis Centers (ISACs) but more general), consortiums (e.g., Charter of Trust), and NGO or non-profit organizations (e.g., Global Cyber Alliance, Cyber Readiness Institute, Cyber Peace Institute, the National Cybersecurity Society, Dragos OT-CERT, etc.). Using existing resources helps to build consistency in standards, expectations, and processes that can be understood and applied across multiple organizations in the same supply chain. This promotes uniformity in information that is useful and applicable to all organizations rather than just one. The cybersecurity of an organization is only as strong as its weakest supplier. Companies must think broader than just securing their organization and ensure that the key values, attitudes, and processes around cybersecurity proliferate throughout all organizations in their supply chain network.

7. Conclusion

Given the challenges discussed above, academic researchers have an important role to play in addressing these issues. Academics have the ability to develop better ways to understand and evaluate SME security in practice. Except for direct testing, the majority of

assessment tools are subjective, built on checklists, and based on incomplete or indirect information that cannot be easily verified. Future research should explore SME cybersecurity within supply chains and find more dynamic and responsive ways to measure risk and cyber maturity in practice.

7.1. Limitations

Results of this study are not meant to be representative of all companies or practitioners. Findings represent a snapshot or small segment of practitioner experiences and perspectives in the field related to SMEs and supply chain cybersecurity. The identification of themes and similarities across study data was important for advancing the understanding of the challenges SMEs face related to cyber risk management and third party risk assessments. Like all qualitative research, the results are not meant to be prescriptive or generalizable across every situation, company, or context. Instead, these results provide valuable insight into the overarching context that SMEs operate within. The rich description of problems and underlying factors impacting decision-making behavior is meant to advance understanding of the situation on the ground in order to help managers and researchers better account for the complexities, interdependencies, and interconnectedness that is going on in real time. The similarities in experience and lessons gleaned from analysis allow for new insights that will inform how research and management decision-making takes place in the future. Interviews are by nature subjective and based on individual experience. However, this study triangulated data to validate study results. Interviews were analyzed individually and resulting themes compared against each other. The authors compared results to existing literature and solicited feedback from practitioners to see how study findings compared to experiences of practitioners in the field.

8. References

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 (CyberSA), 1–5. https://doi.org/10.1109/CyberSA49311.2020.9139638

Alshboul, Y., & Streff, K. (2015). Analyzing Information Security Model for Small-Medium Sized Businesses. 1–9. https://www.researchgate.net/profile/Yazan-Alshboul/publication/281079574_Analyzing_Information_Security_Model_for_Small-Medium_Sized_Businesses/links/55f1929208ae0af8ee1e075e/Analyzing-Information-Security-Model-for-Small-Medium-Sized-Businesses.pdf

Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: Uncertainties, risks and cyber security. Procedia Computer Science, 149, 65–70. https://doi.org/10.1016/j.procs.2019.01.108

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation, 34(7), 342–353. https://doi.org/10.1016/j.technovation.2014.02.001

Boyson, S., Corsi, T. M., & Paraskevas, J.-P. (2022). Defending digital supply chains: Evidence from a decade-long research program. Technovation, 118, 102380. https://doi.org/10.1016/j.technovation.2021.102380

Brunner, M., Sauerwein, C., Felderer, M., & Breu, R. (2020). Risk Management Practices in Information Security: Exploring the Status Quo in the DACH Region. Computers & Security, 92, 101776. https://doi.org/10.1016/j.cose.2020.101776

Cartwright, A., Cartwright, E., & Edun, E. S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. Computers & Security, 131, 103288. https://doi.org/10.1016/j.cose.2023.103288

Charmaz, K. (2006). Constructing grounded theory: A practical guide through qualitative analysis. Sage Publications.

Colicchia, C., Creazza, A., & Menachof, D. A. (2018). Managing cyber and information risks in supply chains: Insights from an exploratory analysis. Supply Chain Management: An International Journal, 24(2), 215–240. https://doi.org/10.1108/SCM-09-2017-0289

Crowdstrike. (2021). What is a Supply Chain Attack? - CrowdStrike. Crowdstrike. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/

Cyderes. (2023). Understand Pentesting vs. Red Teaming. Cyderes. https://www.cyderes.com/blog/penetration-testing-vs-red-teaming/

ESET. (2023, February 21). ESET SMB Digital Security Sentiment Report: The damaging effects of a breach. WeLiveSecurity. https://www.welivesecurity.com/2023/02/21/eset-smb-digital-security-sentiment-report-damaging-effects-breach/

Evalian®. (2022, October 31). What is the difference between red teaming and pen testing? Evalian®. https://evalian.co.uk/penetration-testing-vs-red-team-testing/

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. Information Management & Computer Security, 22(5), 410–430. https://doi.org/10.1108/IMCS-07-2013-0053

Gaudenzi, B., & Siciliano, G. (2017). Just do it: Managing IT and Cyber Risks to Protect the Value Creation. Journal of Promotion Management, 23(3), 372–385. https://doi.org/10.1080/10496491.2017.1294875

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and

research agenda. Supply Chain Management, 25(2), 223–240. https://doi.org/10.1108/SCM-10-2018-0357

Javaid, M. I., & Iqbal, M. M. W. (2017). A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). 2017 International Conference on Communication Technologies (ComTech), 78–90. https://doi.org/10.1109/COMTECH.2017.8065754

King, N. (1994). The qualitative research interview. In Qualitative methods in organizational research: A practical guide (pp. 14–36). Sage Publications, Inc.

Kumar, S., & Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. Production and Operations Management, 31(12), 4488–4500.

Lacity, M. C., & Reynolds, P. (2014). Cloud Services Practices for Small and Medium-Sized Enterprises. MIS Quarterly Executive, 13(1), 31–44.

Lamba, A., Singh, S., Singh, B., Dutta, N., & Muni, S. S. R. (2017). Analyzing and Fixing Cyber Security Threats for Supply Chain Management. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3492687

Lee, I. (2020). Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet, 12(9), 157. https://doi.org/10.3390/fi12090157

Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: Cybersecurity across the supply chain. International Journal of Production Research, 60(1), 162–183.

Murphy, E., Dingwall, R., Greatbatch, D., Parker, S., & Watson, P. (1998). Qualitative research methods in health technology assessment: A review of the literature. Health Technology Assessment (Winchester, England), 2(16), iii–ix, 1–274.

Nygård, A. R., & Katsikas, S. (2022). SoK: Combating threats in the digital supply chain. Proceedings of the 17th International Conference on Availability, Reliability and Security, 1–8. https://doi.org/10.1145/3538969.3544421

Rawindaran, N., Jayal, A., & Prakash, E. (2022). Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime. Computers, 11(12), Article 12. https://doi.org/10.3390/computers11120174

Strauss, A., & Corbin, J. M. (1990). Basics of qualitative research: Grounded theory procedures and techniques (p. 270). Sage Publications, Inc.

Verizon. (2021, May 13). Data Breach Investigations Report 2022—Master's Guide. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/

Wangen, G. B., & Snekkenes, E. (2013). A Taxonomy of Challenges in Information Security Risk Management. 76–87.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. Computers & Security, 44, 1–15. https://doi.org/10.1016/j.cose.2014.04.005