MIS Quarterly Executive

Volume 23 | Issue 4 Article 4

December 2024

How Large Companies Can Help Small and Medium-Sized Enterprise (SME) Suppliers Strengthen Cybersecurity

Jillian K. Kwong

Keri Pearlson

MIS Quarterly Executive

How Large Companies Can Help Small and Medium-Sized Enterprise (SME) Suppliers Strengthen Cybersecurity

Large companies increasingly expect small and medium-sized enterprise (SME) suppliers to meet the same cybersecurity standards that large companies follow. However, these expectations often create insurmountable burdens for SMEs, which already struggle to meet minimum levels of cybersecurity. Drawing on interviews with managers and cybersecurity executives, this article identifies four barriers that SMEs frequently encounter when implementing cybersecurity. The article also proposes five actions that large companies can take to assist their suppliers in strengthening cyber resilience.[1,2]

Jillian K. Kwong
Massachusetts Institute of Technology

Keri Pearlson
Massachusetts Institute of Technology

Small and Medium-Sized Suppliers Pose Third-Party Risk in Supply Chains

Supply chain cybersecurity is a major challenge for businesses today. Cyberattacks not only threaten information assets but can also disrupt everyday operations. While all organizations deal with the threat of ransomware and other attempts to disrupt, damage or gain unauthorized access to computer systems, networks or data, fostering cybersecurity is particularly difficult for small and medium-sized enterprises (SMEs), which can serve as "tunnels" to larger targets.

One of the most well-known examples is the 2013 data breach at Target, where hackers gained access to the company's computer network using credentials stolen from a third-party heating, ventilation and air conditioning (HVAC) vendor. Over 40 million credit and debit card accounts were stolen and approximately 70 million people had their personal information exposed.[3] SMEs are an especially attractive target for cyberattacks because SMEs often struggle to mobilize resources, develop prevention and recovery programs, and assign responsibility for cybersecurity internally.

1 Mary Sumner is the accepting senior editor for this article.

2 This research was supported by the members of the Cybersecurity at MIT Sloan (CAMS) initiative (https://cams.mit.edu/) and funded in part by the Hasso Plattner Foundation, through a grant from the HPI-MIT Designing for Sustainability Program. The authors thank Christian Doerr of the Hasso Plattner Institute for his insights during the early stages of the research. A version of this article was workshopped at the December 2023 ICIS Cybersecurity and Privacy track: MISQE Special Issue Workshop on Managing Cybersecurity to Address Increasing Digital Risk.

3 A detailed analysis of the event can be found in the U.S. Senate's Committee on Commerce, Science, and Transportation report, "A 'Kill Chain' Analysis of the 2013 Target Data Breach." *US Senate*, 2014, available at https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883.

DOI: 10.17705/2msqe.00103

Another example is the 2020 supply-chain breach of SolarWinds. The cyberattack—which involved state-sponsored hackers and a third-party network management system—infected over 18,000 SolarWinds customers in both the public and private sectors via compromised software updates. The hack was one of the most significant supply-chain attacks in history, affecting government agencies such as the U.S. Departments of Defense, State and Homeland Security, as well as thousands of companies around the world, including Microsoft, AT&T and Cisco.[4]

As cyberattacks increase, many large companies have taken steps to improve their cybersecurity defenses. Large companies, in turn, are increasingly expecting their suppliers to follow suit. However, SMEs often lack the necessary resources and funding to meet these expectations. Research has also shown that most SMEs are ill-equipped to deal with cyberattacks. For example, in 2021, 82% of ransomware attacks targeted companies with fewer than 1,000 employees.[5] Additionally, 46% of all cyber breaches in 2021 impacted SMEs, while 51% of small businesses reported having no cybersecurity measures in place.[6]

This article aims to help large companies improve the resiliency of their supply chains. The research described below—which draws on insights from 27 in-depth interviews with executives who deal with cybersecurity—is particularly relevant for managers at large companies but also applies to cybersecurity leaders, SME executives and policymakers.

In this article, we focus on third-party SME suppliers: Despite their importance and vulnerability to attack, these companies have received much less attention from researchers than large companies. By identifying the cybersecurity challenges that SME suppliers encounter and explaining how large organizations can assist SMEs in overcoming such challenges, we shine a spotlight on the unique problems that small and medium-sized enterprises face. (For more on our research methodology, please see the Appendix.)

The first section of this article provides an overview of the concept of cyber resiliency, the current literature on securing supply chains and how our research fits in. The second section highlights barriers to improving cybersecurity, implementing cyber mandates and introducing cyber best practices at SMEs. The third section provides an overview of actions that managers at large companies can take to help SME suppliers boost cyber resilience.

The Challenge of Building Cyber Resilience in Supply Chains

Managing risk and building cyber resilience in supply chains is a topic that has been on the minds of managers for many years. While cyber risk and cyber resilience are related, they are also distinct concepts. Supply chain risks can be defined as "the likelihood of an adverse and unexpected event that can occur, and either directly or indirectly result in a supply chain disruption."[7] In contrast, supply chain resilience can be defined as "the capability of a supply chain to maintain its operational performance when faced with cyber-risk."[8]

Building cyber resilience is a complex task that requires active buy-in from all levels of an organization's leadership, including managers, executives and the board.[9] Research shows that cyber-resilient companies retain performance and operational capabilities after disruptions by employing seven principles across four distinct phases: the anticipation phase (before the breach), the absorption phase (when reducing the immediate impact of the breach),

4 Details can be found in the report, "Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents." *U.S. Government Accountability Office*, 2022, available at https://www.gao.gov/products/gao-22-104746.

5 Drapkin, A. "82% of Ransomware Attacks Target Small Businesses, Report Reveals." *Tech.co*, 2022, available at https://tech.co/news/82-of-ransomware-attacks-target-small-businesses-report-reveals.

6 For more information on cybersecurity statistics related to SMEs, see Verizon, "2021 SMB Data Breach Statistics." *Verizon Business*, 2021, available at https://www.verizon.com/business/resources/reports/dbir/2021/smb-data-breaches-deep-dive/.

7 Garvey, M.D., Carnovale, S., and Yeniyurt, S. "An Analytical Framework for Supply Network Risk Propagation: A Bayesian Network Approach." *European Journal of Operational Research*, (243), 2015, pp. 618-627.

8 McPhee, C. and Khan, O. "Editorial: Cyber-Resilience in Supply Chains." *Technology Innovation Management Review*, (5:4), pp. 3-5.

9 Huang, K. and Pearlson, K. "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture." *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019, pp. 6398-6407.

the responsiveness phase (when reducing the duration of the breach) and the shaping phase (after the breach).[10]

The academic literature on cyber resilience is largely based on studies examining large companies. However, researchers have noted that cyber resilience looks different for SMEs than for large firms because SMEs have more limited resources, including fewer technological and financial capabilities, minimal staffing levels, reduced recovery and preparedness plans, and less robust infrastructure.[11]

SMEs operate at a major disadvantage in terms of cybersecurity. SMEs are not only easy targets compared to large companies but are also more frequent victims of attack.[12] Yet despite the fact that SMEs represent a large proportion of businesses, both in the U.S. and worldwide, their cybersecurity challenges are poorly understood. To help close the knowledge gap, researchers have proposed various theoretical models and frameworks that SMEs might deploy.[13] However, the executives we interviewed noted that although many of these models and frameworks are extremely detailed, they do not meet their respective firms' needs on the ground: The models are too specific and do not take into consideration the time and resource constraints SMEs face (such as the need to balance productivity demands against security concerns).

The research described below thus investigates: 1) the challenges SME suppliers encounter when implementing cyber mandates and 2) how large organizations can help SMEs address these challenges. Answering the call by Chidukwani et al. (2022), this article seeks to expand the study of cyber resilience and supply chains by exploring the challenges that SMEs encounter in practice while shedding light on factors that hinder SME suppliers' ability to be more reliable cybersecurity partners.[14]

Four Barriers to SME Cybersecurity Implementation

It is no secret that SME suppliers struggle to dedicate adequate resources and funding to cybersecurity. Yet, as noted, very little research has investigated the specific areas where SMEs struggle and why. Drawing on interviews with nearly 30 executives, we identified four important barriers that SMEs encounter when implementing cybersecurity.

1. Unfriendly Regulation: SMEs Struggle to Meet Requirements

Cybersecurity regulation poses two significant challenges for SMEs: 1) SMEs' lack of expertise to understand and implement such regulations and 2) SMEs' need to balance competing business interests against compliance mandates.

Regulations Do Not Consider the Knowledge and Constraints of SMEs

Most cybersecurity regulations are designed to apply to large companies that have the resources and ability to support experts who can understand, interpret and implement these rules in their organizations. Although SMEs are usually not directly impacted by cybersecurity regulations, SMEs that work with or supply large companies can be indirectly affected. This means that these SMEs are often expected to meet the same security standards as the large companies with which they partner. Our interviewees working at SMEs stressed that compliance is difficult not only because their companies lack the knowledge to decipher the technical details of many regulations but also because their firms do not have the internal capabilities to understand how these regulations apply to their respective organizations. For instance, a CISO at a small technology company described the confusion he encounters around password compliance:

> *"NIST [National Institute of Standards and Technology] used to say change your password every 90 days. Now you get these*

10 Coden, M. et al. "An Action Plan for Cyber Resilience." *MIT Sloan Management Review*, (64:2), 2023, pp. 1-6.

11 Bak, O. et al. "A Systematic Literature Review of Supply Chain Resilience in Small-Medium Enterprises (SMEs)." *IEEE Transactions on Engineering Management*, (70:1), 2023, pp. 328-341.

12 Faulhaber, J. and Moon, B. "Small Business Cyberattack Analysis," *CrowdStrike*, January 30, 2022, available at https://www.crowdstrike.com/blog/small-business-cyberattack-analysis-most-targeted-smb-sectors/.

13 CISA, "Securing Small and Medium-Sized Business Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks." *CISA*, 2023, available at https://www.cisa.gov/resources-tools/resources/securing-smb-supply-chains-resource-handbook.

Carías, J.F., Borges, M.R.S., Labaka, L., Arrizabalaga, S., and Hernantes, J. "Systematic Approach to Cyber Resilience Operationalization in SMEs," *IEEE Access*, (8), 2020, pp. 174200-174221.

14 Chidukwani, A., Zander, S., and Koutsakis, P. "A Survey on the Cyber Security of Small-to-Medium Businesses," *IEEE Access*, (10), 2022, pp. 85701-85719.

> *questionnaires from companies [we supply to] saying, 'Do you change your passwords every 90 days?' [Yet] NIST now says don't do that—use passphrases instead of passwords and maybe use a password manager. But instead, you have companies [still] asking, 'Do you change your password every 90 days?' If you say 'no,' you fail [their questionnaires], so you failed at compliance. …There are nuances that are lost in compliance because compliance is based on a checklist and security isn't."* (IE_2—for interviewee demographics, see Table 2)

Large companies, interviewees explained, are generally better at absorbing new regulations and mandates because their organizational structures tend to be more bureaucratic, with entire departments (legal, risk, compliance, cybersecurity, etc.) dedicated to navigating government regulations. SMEs, on the other hand, are less equipped to deal with regulatory complexity.

Regulations Do Not Encourage Prioritizing Cybersecurity

Interviewees noted that one of the best ways to make a company's leadership prioritize cybersecurity is through stronger laws and regulations. However, interviewees frequently described cybersecurity legislation as "toothless." The lack of tangible penalties for noncompliance, in turn, makes it difficult for the leadership of SMEs to mobilize resources to improve cybersecurity.[15] Given such incentives (or lack thereof), interviewees noted, there are relatively few benefits but lots of guaranteed disruption from upgrading an SME's cybersecurity capabilities.

In contrast, multiple interviewees pointed to the success of data protection legislation in motivating managers to take action and commit resources to protecting data privacy. These interviewees specifically mentioned the E.U.'s General Data Protection Regulation (GDPR),[16] which threatens fines of up to 4% of a company's global turnover for noncompliance.[17] The GDPR's aggressive penalties, for example, have raised awareness among the leadership of interviewees' firms about data protection, thus creating a stronger incentive for change. A governance, risk and compliance (GRC) and supply-chain manager told us:

> *"Now that [GDPR] is a regulatory requirement, it can't be argued with. So you get a lot more money pushed behind it. For example, my company had a lot of money and 150 people pushed in to get their GDPR uplifted. With the third-party risk-management program that I'm leading, we've got five people, but there's currently no regulation around cybersecurity that will get you fined. If there is anything, it's related to GDPR. If there's ransomware or anything like that, there's not much regulation or law around it. But if you capture any [Personal Identifiable Information] and it leaks, that's when GDPR comes in. And all hell breaks loose in regard to breach regulation and things like that. We haven't quite got the enforcement behind cyber that we need, so it's difficult."* (IE_9)

This example illustrates how, with the right incentives, regulation can tip the scales and motivate managers to make changes. Still, current cybersecurity regulations are not effective at convincing managers to make cybersecurity a priority. Yet this does not mean that large companies must wait for governments to introduce regulations that bite. Instead, by understanding the competing priorities that SMEs face, large companies can work with their SME partners to create plans that help their suppliers mobilize resources and bolster their cybersecurity.

2. Organizational Culture Clashes: SME Culture Prioritizes Operational

15 While the Securities and Exchange Commission (SEC) has outlined reporting obligations for publicly traded companies and critical infrastructure, these regulations lack the same consistency and urgency across sectors that data privacy-focused legislation does. For more on the SEC reporting obligations, see "SEC.Gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," *SEC*, 2023, available at https://www.sec.gov/news/press-release/2023-139.

16 Although security was part of GDPR, interviewees stressed that security was secondary to privacy in the legislation and did not include the full scope of security areas that required attention and investment.

17 "Art. 84 GDPR – Penalties." *GDPR*, available at https://gdpr-info.eu/art-84-gdpr/.

Demands the Expense of Cybersecurity Needs

> *"The simple fact is that a security information-sharing program cannot exist without a culture. We hear this all the time. It [the right culture] has to be enforced from the top down and rigorously enforced."* (IE_1, CISO)

Just like large companies, SMEs have to balance business and operational demands against compliance and cybersecurity demands. While cybersecurity is an important concern for any organization, cybersecurity can be difficult for managers at SMEs to prioritize, especially when faced with immediate demands that are focused on keeping the business going. In fact, managers simply may not have the resources to achieve both goals simultaneously. The result is often an organizational culture that focuses on meeting operational demands above all else. A senior cybersecurity engineer at a medium-sized bank described the barriers she faces when trying to implement stronger cybersecurity controls:

> *"The first barrier is time to market. We need to balance security controls and our risk appetite versus business opportunity. We know that we are a cybersecurity team based in a bank. The main goal of the company is to be a bank. We need to deliver our products and be useful for our clients. But at the same time, we are a bank, not a grocery store. We have a responsibility with people's money that is very important to us. So we need to balance these desires and, most of the time, it is difficult to just add [more cybersecurity]."* (IE_5)

"Mismatches" in organizational culture thus occur when large companies expect their SME suppliers to match large companies' culture of cybersecurity *without* offering additional resources. As the cybersecurity engineer at the bank added:

> *"To do a security assessment of a vendor, we need to understand all scenarios. We share our questions, we have a governance interview. We have two, three, or even five security-engineer interviews to understand the scope, adjust the details and define the first version of the architecture model. This process is very hard. It lasts two or three months and takes time and money. We've had some specific situations where we've ran into trouble where it lasts almost a year to close our security report. That's [unacceptable] for our business areas and our stakeholders—and we understand it. It's the most worrying barrier for us because it's hard to adjust and to be useful [for the company] and our clients."* (IE_5)

In short, balancing an organization's operational efficiency and productivity demands with its cybersecurity requirements presents a significant challenge for many SMEs. The resulting trade-off usually produces a culture at SMEs where cybersecurity takes a back seat to building and operating the business.

Until a cyberattack occurs, interviewees stated that it is very difficult under the status quo to convince SME leadership to invest in cybersecurity. Moreover, experience also shows that companies that spend large amounts on cybersecurity can still be attacked, while others that do nothing may be spared from attacks and carry on just fine. The result: Many SMEs are very reluctant to invest heavily in cybersecurity.

3. Framework Variability: SMEs Have Difficulty Meeting the Requirements of Multiple Cybersecurity Frameworks

Cybersecurity "frameworks" are voluntary guidelines that outline standards, principles and best practices to help businesses improve their defenses by understanding and managing cyber risk.[18] There are many well-established cybersecurity frameworks, including NIST, ISO/IEC 27001/27002 and CIS Controls. While there are numerous similarities between these frameworks, there are also subtle differences that can make a certain framework a better fit for a company—depending on factors such as the firm's sector, region, business/customer needs, operational capabilities and regulatory obligations. This means that SMEs often need to

18 For more on cybersecurity frameworks, see NIST, "Understanding the NIST Cybersecurity Framework," *Federal Trade Commission*, 2018, available at https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework.

understand the specifics of multiple cybersecurity frameworks that their customers might want.

For their part, large companies routinely develop tailored approaches to evaluate vendors during third-party risk assessments. Using these frameworks, large companies pick which standards are most relevant to their firm and then orient internal processes around those standards. Though the majority of solutions are, as noted, generally similar, slight differences in each framework mean that when implemented, the framework can create additional complexity on the ground. An interviewee responsible for overseeing global supply chains at a multinational company described the situation:

> *"Typically, big companies tend to develop their own solution. They have their feeling that 'We need to develop our own tailored approach. We need our own questions. We know it better.' So they typically create their own assessment, logic and questionnaire. If you look at the content and structure, [these solutions] are typically derived out of standards. You will recognize the structure from NIST, ISO, IEC, etc. They are all alike, but it is a little bit rephrased. It's sorted a little bit differently. This is creating a huge complexity in the network, as everyone needs to sync up on the topic and make up their mind about whether it really is the same or something different. This [complexity], of course, adds to the problem."* (IE_12)

The upshot is that many SMEs are simultaneously subject to different frameworks (or even partial variations of those frameworks). It's no surprise that SMEs then tend to struggle to comply with the nuances of multiple standards at once.

Interviewees, moreover, noted that SMEs rarely receive guidance when deciding which framework to prioritize. One interviewee described the challenge as "trying to navigate a sea of frameworks in a rowboat, without a map or radio." SMEs, in short, have multiple frameworks they need to follow, but often lack the necessary resources and guidance to execute them efficiently.

4. Process Misalignment: Security Processes in SMEs Need to Align with Customer Process Needs

We also found process "misalignment" between large companies and their SME suppliers—cybersecurity processes were misaligned, as were the cybersecurity component of all processes. A director of cybersecurity engagement at a multinational retailer told us:

> *"You've got these regulations where the actual supplier is not required to do it, but the customer they're trying to sell to is. You get this tension of, 'We're not going to build it until we need it.' But these big companies don't always move so fast either. To prioritize it now gets really, really tough because we've got to retrofit a bunch of things. Getting compliant doesn't mean you install a software package and you're there. It's much more process and people. The tech is usually the easy part. That's another tension you see with small companies, where there isn't great guidance."* (IE_18)

Another example of process misalignment is the challenge of aligning cybersecurity practices with data governance. Interviewees observed that to properly secure data, incorporating strong data governance is essential. Yet data governance is a complex task that requires multiple processes and internal coordination. In some cases, aligning data governance processes might require organizations to recategorize/reclassify data or even rebuild certain systems to keep track of all their data. While doing this is an expensive, time-consuming process for any organization, for an SME, especially one dealing with data governance for the first time, it can be a task that is next to impossible.

Recommendations for Large Companies

While every situation and business relationship is unique, the following recommendations (summarized in Table 1) are intended to serve as a roadmap for large companies looking for actionable steps to improve SME cybersecurity in their supply chains. As with the barriers discussed above, the

following recommendations were crafted based on the insights offered by our interviewees.

1. Provide SME Suppliers with the Resources and Expertise Needed to Understand and Comply with Regulations

Regulation impacts large companies differently than SMEs. Because most cybersecurity legislation is intended for large companies, there is an implicit assumption that organizations have the requisite infrastructure (such as in-house cybersecurity, legal or GRC teams) to decipher and comply with such legislation.

We found that SME suppliers struggle to comply with cyber mandates not only because of inadequate funding but also as a result of SMEs' inability to understand and implement such rules. Large companies can thus help their SME suppliers by providing the expertise needed to help SMEs understand the intricacies of compliance mandates and how they apply to their organization. This assistance can include guidance from legal and GRC teams to review the details of regulations and discuss expected actions, outcomes and standards. In return, SMEs should come to the table with a strong understanding of their own infrastructure, internal processes and organizational capabilities. Doing this will ensure that SMEs have the proper foundation to understand what they are expected to do and how to comply.

Nevertheless, developing such an understanding is often harder than it may seem. For example, the director of a program at a cybersecurity company that provides free resources to SMEs told us:

> *"We saw a major unmet need in operational technology environments. The cybersecurity risks keep rising and many organizations are struggling with the resources or expertise to address them. And we found this to especially be a problem among small to medium-sized businesses"* (IE_11).

The curriculum the cybersecurity company developed included educational training, workshops and assessments targeted at SMEs with little to no experience in cybersecurity. The curriculum was designed to walk SMEs through the process of setting up their cybersecurity program by introducing executives and staff to key technical controls/infrastructure, assisting in the development of cyber policies and incident response plans, building awareness around compliance expectations/documentation, familiarizing employees with assessments, introducing best practices and otherwise building cyber maturity.

2. Work with SMEs to Create Incentives for Meeting Desired Benchmarks and Standards

Cybersecurity legislation, as noted, generally lacks consequences for noncompliance, especially compared to data privacy legislation. This "lack of teeth" makes it harder for cybersecurity teams to persuade management to prioritize cybersecurity and allocate additional resources to it. To help remedy this challenge, large companies can work with SMEs to develop a plan that includes incentives for meeting desired benchmarks and security standards—thereby reducing pressure on SME managers and security practitioners to "justify" cybersecurity spending. As a CTO of a small technology company told us:

> *"We need to adjust the economic incentives to make it worth the third parties' time, effort and investment to be more secure. They need to be rewarded for it, instead of being punished for it—which is what's happening today. We won't see meaningful improvements in the systemic risk environment that we live in until we can figure out how to [change the incentives]."* (IE_7)

3. Develop Programs and Processes to Help SMEs Match Their Partnering Company's Elevated Culture of Cybersecurity

Our research shows that there is often a mismatch between what supplier SMEs can deliver and where large partnering companies need them to be—in terms of people, processes and technology.

To address this mismatch, large companies with a strong cybersecurity culture need to develop programs and processes that help supplier SMEs elevate their own cybersecurity

culture—including their organizational values and attitudes—to the level of large companies. A senior director of cybersecurity at a bank explained:

> *"We still face some resistance from some partners. But due to our maturity and our security level, the other companies understand 'That's a bank. They will be really concerned with security and have a good security team. So let me use this force and this knowledge to help me to improve my security.' What really helped us is when the LGPD [Geral de Proteção de Dados Pessoais—Brazil's data protection law] or [the E.U.'s] GDPR started to be valid. Any company that handles personal data needs to have a security policy and have strong security measures. Because of that [need], we use these as a force to help them [SME suppliers] to help us."* (IE_4)

Our interviewees also provided examples of large companies partnering with SME suppliers to develop programs that: (1) help build awareness of cybersecurity issues, regulations and frameworks and (2) introduce best practices, develop buy-in and set expectations around cybersecurity. For instance, a large mining company worked with an SME supplier to build cybersecurity infrastructure from the ground up. The supplier had fewer than 10 employees and no resources to invest in cybersecurity. However, the supplier was highly specialized and difficult for the mining company to replace. Because the supplier was handling sensitive data on behalf of the mining company, the latter had no choice but to work with the supplier to help it become compliant.

The mining company began by hiring an external firm to analyze the SME and recommend the best course of action. After onsite visits and extensive information gathering with the SME, the external firm advised the mining company to provide and maintain all necessary equipment—including laptops, servers and databases—to ensure that the supplier could meet compliance mandates and continue operating securely. While not all large companies can (or will choose to) hire an external firm, this example highlights how large companies can recognize their SME suppliers' constraints and then help the SMEs build tailored solutions to address their cybersecurity problems.

4. Coordinate with Peer Organizations to Align Cybersecurity Frameworks and Streamline Assessment Procedures for SMEs

SMEs that supply more than one company are, as noted, often subject to different cybersecurity frameworks. When this happens, SMEs are forced to decide which standards to use and how to comply. An interviewee working on retainer as a virtual CISO for small companies stated:

> *"Companies need solutions that are the right balance. You can have criteria for selection, but someone still needs to dig through and separate out all the relevant information. Small companies can't get the Cadillac of solutions. I was talking to a GRC vendor that does interesting stuff. But their cheapest tier is $15k a year. If you want more than one certification/framework, like SOC2, HIPAA, ISO and GDPR, each additional one is another $7,500 a year. So you get to $30 grand before you've even started."* (IE_16)

For SMEs, navigating the complexities of each framework is a daunting task that is not only time consuming, but also opens the door to additional vulnerabilities. Large companies can assist SMEs by working with peer companies to align frameworks and coordinate assessment processes. For instance, sharing and recycling assessments between companies saves time by reducing the number of questionnaires that SMEs need to complete; sharing and recycling also harmonizes benchmarks, thus reducing the need for SMEs to choose between aligning their processes with one standard or another.

An executive at a multinational manufacturing company that we interviewed told us how his firm collaborated with peer organizations to create a standardized form that could be completed once by a supplier and then accepted by any organization it supplies to. In contrast, the current approach to SME risk assessments is akin to going to a doctor, creating a profile and enrolling in a new healthcare system: Doing that requires, among other things, filling out personal information and patient history forms

Table 1: Barriers and Actions

Barrier	Action
1: Unfriendly Regulation - Regulations do not consider the knowledge and resource constraints of SMEs. - Regulations do not encourage cybersecurity to be prioritized.	**1:** Provide SME suppliers with resources and expertise to understand and comply with regulations.
	2: Work with SMEs to create incentives for meeting desired benchmarks and standards.
2: Organizational Culture Clashes - SME culture prioritizes operational demands at the expense of cybersecurity needs.	**3:** Develop programs and processes to help SMEs match their partnering company's elevated culture of cybersecurity.
3: Framework Variability - SMEs have difficulty meeting the requirements of multiple cybersecurity frameworks.	**4:** Coordinate with peer organizations to align cybersecurity frameworks and streamline assessment procedures for SMEs.
4: Process Misalignment - Security processes in SMEs need to align with customer process needs.	**5:** Ask SMEs important cybersecurity questions and clarify expectations earlier in the procurement process.

and getting basic lab tests done, only to have to repeat the process with a visit to a different doctor. Such repetition is costly, time-consuming and introduces variance into the system because the patient is more likely to omit or change information each time.

On the other hand, the collaborative approach of using a common form pushes back against companies that create questionnaires and assessment processes that are only applicable to their organization. With a common form, basic information can instead be shared among many stakeholders, while any additional information that is required can be handled on a case-by-case basis. The bottom line: Harmonizing frameworks allows SMEs to spend less time filling out repetitive questionnaires and more time investing in their actual cybersecurity defenses.

5. Ask SMEs Important Cybersecurity Questions and Clarify Expectations Earlier in the Procurement Process

We found that when evaluating potential new SME suppliers, large companies usually save their discussions with the SME's cybersecurity department until after initial partnership agreements are signed. However, significant delays in finalizing such agreements often happen if/when cybersecurity problems are discovered in the review process. As a result, mitigating these issues often requires redoing the entire review process, getting legal departments involved and then negotiating how problems are to be addressed. Our research shows that managers at large companies can help reduce this common bottleneck by integrating cybersecurity earlier into their procurement and business development process. For example, a senior director of supply chains at a global manufacturer told us:

> *"If you want to be part of this supply chain game, you need to speak the language of supply chain. You need a very close collaboration with your procurement team. For procurement, the claim is often, 'We need early involvement. If you involve us early enough, we can provide you all the transparency; we can provide you all the data.' For traditional cybersecurity to get a sound result with transparency, you typically need a minimum of six to eight weeks. The consequence of this is that you are not part of the game because no one can wait. Speed is highly relevant."* (IE_12)

By bringing cybersecurity into the procurement process at the start, large companies can streamline needed mitigations and ensure that SMEs prioritize cybersecurity early in the partnership—rather than treating cybersecurity as an afterthought. Table 1

summarizes how the five actions described above can help large companies address the key barriers to cybersecurity faced by SMEs.

Concluding Comments

Today's rapidly changing cyberattack landscape calls for large companies to be more proactive about cybersecurity in their supply chains. While large companies have long been aware of supply chain-related cyber risks, very little research has investigated how these risks manifest on the ground for SMEs and how large companies can help SMEs address such risks.

Drawing on interviews with cybersecurity and SME practitioners, we found that SME suppliers are generally unable to meet the security standards outlined by their large partner companies. We then identified four common barriers to SMEs becoming reliable cybersecurity partners: 1) unfriendly regulation, 2) organizational culture clashes, 3) framework variability, and 4) process misalignment.

Because it is unrealistic—for reasons discussed in this article—to expect SMEs to meet the same security standards as large companies without further support, we also proposed five actions that large companies can take to assist their SME suppliers: 1) provide SMEs with the resources and expertise needed to understand and comply with regulations, 2) work with SMEs to create incentives for meeting desired benchmarks and standards, 3) develop programs and processes to help SMEs match their partnering company's elevated cybersecurity culture, 4) coordinate with peer organizations to align cybersecurity frameworks and streamline assessment procedures for SMEs, and 5) ask SMEs important cybersecurity questions and clarify expectations earlier in the procurement process.

Appendix: Research Methodology

The research described in this article was based on 27 interviews with business executives, cybersecurity experts, supply chain managers, GRC leaders and other subject matter experts. These in-depth, semi-structured interviews allowed us to gather and probe interviewees' experience regarding 1) challenges that SMEs encounter when implementing cyber mandates and 2) how large organizations can assist in addressing these challenges. Interviews were conducted virtually and ranged from 30 to 90 minutes (with the majority lasting 60 minutes).[19] Most interviews were recorded and transcribed verbatim with the consent of the interviewee. In cases where interviewees did not wish to be recorded, the interviewer took detailed notes with the interviewee's approval.

Interviewees were recruited primarily through word of mouth and snowball sampling. Participation in the interviews was voluntary and interviewees received no compensation. Interviewees represented companies from various sectors, including banking, biotechnology, technology, insurance and financial services, manufacturing, nonprofits, retail and transportation. The organizations they represented ranged from small businesses with fewer than 50 employees to multinational corporations with over 10,000 employees. Interviewee demographics—including role, domain, industry, company size, years of job experience and gender—can be found in Table 2.

Data was analyzed using thematic analysis, specifically Miles, Huberman and Saldana's two-cycle coding approach.[20] The first cycle consisted of initial and in vivo coding to explore the data that generated codes organically from the interview transcripts. Researchers also engaged in comparative analysis to examine new codes in relation to old codes; in addition, codes were continually updated and redefined.

The second cycle grouped codes into categories based on themes. Analyzing similar content across interview data eventually resulted in the generation of common themes. The goal was to identify the most salient categories within a corpus of data.[21]

19 Interviews were primarily conducted over Zoom, but researchers occasionally used Google Meet or Microsoft Teams if the interview participant's organization did not allow Zoom.

20 For more information on two-cycle coding, see Miles, M. B., Huberman, A. M., and Saldana, J. *Qualitative Data Analysis*, Sage Publications, 2014.

21 Charmaz, K. *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*, Sage Publications, 2006.

Table 2: Interviewee Demographics

Interview ID	Role	Domain	Industry	Company Size	Job Experience	Gender
IE_1	CISO	Cybersecurity	Technology	Medium	15+ Years	Male
IE_2	CISO	Cybersecurity	Technology	Small	15+ Years	Male
IE_3	CISO	Cybersecurity/ Supply Chain	Manufacturing	Large	25+ Years	Male
IE_4	Senior Director	Cybersecurity	Banking	Medium	15+ Years	Male
IE_5	Senior Director	Cybersecurity/GRC	Banking	Medium	8 Years	Female
IE_6	CISO	Cybersecurity	Insurance and Financial Services	Large	10+ Years	Female
IE_7	CTO	Management (Executive)	Technology	Small	10+ Years	Male
IE_8	Director	GRC/Supply Chain	Biotechnology	Medium	15+ Years	Male
IE_9	Manager	GRC/Supply Chain	Technology	Small	10+ Years	Male
IE_10	CEO	Management (Executive)	Technology	Small	15+ Years	Male
IE_11	Director	Cybersecurity/ GRC/Supply Chain	Technology	Medium	25+ Years	Female
IE_12	Senior Director	GRC/Supply Chain	Manufacturing	Large	10+ Years	Male
IE_13	CEO	Management (Executive)	Nonprofit	Small	15+ Years	Male
IE_14	Director	Cybersecurity	Technology	Small	15+ Years	Male
IE_15	Senior Vice President	Cybersecurity/GRC	Manufacturing	Large	15+ Years	Male
IE_16	Virtual CISO	Cybersecurity	Technology	Small	15+ Years	Male
IE_17	Governance Specialist	GRC	Nonprofit	Small	10+ Years	Male
IE_18	Director	Cybersecurity/ Supply Chain	Retail	Large	15+ Years	Male
IE_19	VP	Cybersecurity	Insurance and Financial Services	Medium	15+ Years	Male
IE_20	CTO	Management (Executive)	Technology	Medium	10+ Years	Male
IE_21	CISO	Cybersecurity	Technology	Small	20+ Years	Female
IE_22	Program Manager	GRC/Supply Chain	Technology	Large	5 Years	Male
IE_23	CISO	Cybersecurity	Banking	Medium	15+ Years	Male
IE_24	CISO	Cybersecurity/ Supply Chain	Transportation	Large	20+ Years	Male
IE_25	Managing Director	Management (Executive)	Technology	Small	6 Years	Male
IE_26	CEO	Management (Executive)	Technology	Small	20+ Years	Male
IE_27	Senior Director	Cybersecurity/GRC	Technology	Medium	10+ Years	Male

About the Authors

Jillian K. Kwong

Dr. Kwong (jkwong1@mit.edu) is a research scientist at MIT Sloan (CAMS), where she specializes in the cybersecurity challenges faced by small and medium-sized enterprises (SMEs) within supply chains. An expert in qualitative and mixed methods research, Dr. Kwong leverages her background in communication, data protection, human behavior and organizational studies to explore the human aspects of cybersecurity. Dr. Kwong earned her Ph.D. from the University of Southern California's Annenberg School for Communication and Journalism and has shared her research with academics, policymakers and practitioners from around the world.

Keri Pearlson

Dr. Pearlson, an expert in managing and using information, specializes in cybersecurity leadership. Her current position is executive director of CAMS, a research consortium at MIT Sloan focused on the leadership, governance and management of cybersecurity. Dr. Pearlson is a thought leader in cybersecurity culture, resilience, supply chain and board leadership. Her work has been published in *Harvard Business Review*, *MIT Sloan Management Review*, *Wall Street Journal* and many academic outlets. She is also the coauthor of a popular textbook on information systems management. She has a doctorate from Harvard Business School and master's and bachelor's degrees from Stanford.