Supplier Development Framework in Supply Chain Cybersecurity Evaluation of Small and Medium-sized Enterprises

by

Erh Chieh Chang

M.S. Mechanical Engineering, National Taiwan University (2015)

Submitted to the System Design & Management Program
in partial fulfillment of the requirements for the degree of

Master of Science in Engineering and Management

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2023

Authored by: Erh Chieh (Alex) Chang
System Design & Management Program
May 12, 2023

Certified by: Keri Pearlson
Executive Director, Cybersecurity at MIT Sloan (CAMS)
Thesis Supervisor

Accepted by: Joan S. Rubin
Executive Director, System Design & Management Program

Supplier Development Framework in Supply Chain Cybersecurity Evaluation of Small and Medium-sized Enterprises

by

Erh Chieh Chang

Submitted to the System Design & Management Program
on May 12, 2023, in partial fulfillment of the
requirements for the degree of
Master of Science in Engineering and Management

Abstract

Modern organizations rely on suppliers to meet customer needs and improve operations. However, the interconnectedness between organizations and their suppliers, brought about by digital transformation, has led to an increase in significant cyber breaches. To mitigate these risks, organizations use various methods and tools to both assess and monitor potential threats. Despite this, a gap exists between assessment and monitoring/improvement. The objective of this study is to address the gap between cybersecurity assessment and monitoring/improvement by developing a supplier development process in the supply chain that enhances the cybersecurity capability of small and medium enterprise (SME) suppliers. The theoretical framework is built on a literature review, anecdote evidence and best practices in supply chain management, and feedback from industry experts. The framework is a four-stage process that enhances the cybersecurity capability of SME suppliers by improving their security posture, providing training, and fostering collaboration between suppliers and clients. The study highlights the importance of collaborative capability building between client organizations and suppliers to improve cybersecurity. Future research can focus on developing this concept further and exploring its implementation in various industries.

Thesis Supervisor: Keri Pearlson
Title: Executive Director, Cybersecurity at MIT Sloan (CAMS)

Acknowledgments

The journey in research is a long one. Sometimes it also feels hard and there's no end in sight, but typing these words made me realize that no matter how hard everything seemed at first, we'll pull through no matter what.

First, I'd like to thank both Dr. Keri Pearlson and Dr. Jillian Kwang. I want to thank them for all the help, all the time they spent advising us on the right research direction. I know I am not always the best writer nor can I make a convincing academic argument, but they have always taken the time to advise me on a better direction!

Next, I'd like to acknowledge my dear mother, though she cannot provide me with technical support or offer any conclusive research insights, yet without her guidance and care, I wouldn't have made it this far in life without any major failures.

Furthermore, I'd also like to acknowledge the Sloan CAMS research group and the industry experts for their insight comments and help in formulating and refining the framework.

Lastly, I want to thank everyone who has been part of my life in these last two years, there aren't many, but thank you all for all the memories you provided me with, both good and bad, it is with these memories that made me who I am today, and I am thankful for every last pieces of those memories.

Contents

List of Figures

Chapter 1

Introduction

As digital transformation increasingly links organizations closer together in recent years, the interconnectedness between organizations and their suppliers contributed to the rising number of significant cyber breaches. There were 130 incidents in 2020 alone, which is a 14 percent increase from 114 incidents in 2019 (CSIS 2020). In 2020, SolarWinds, a software firm in the U.S. that develops business software in network, database, systems, and I.T. services management for more than 30,000 clients, experienced a cybersecurity breach in one of their monitoring software systems, Orion. Due to the nature of being a monitoring system, Orion has privileged access to the client's system to gather data. This access and widespread adoption enabled attackers to compromise services and systems far beyond SolarWinds. Another incident, while less publicized, also illustrated the vulnerability in a critical industry. In 2018, the Taiwan Semiconductor Manufacturing Company (TSMC) suffered a cyber-attack from a WannaCry variant, which spread to the wider company network when software installation for a new tool was done inappropriately. The incident brought part of the world's largest semiconductor manufacturer's production line offline, potentially costing $255 million in revenue (IT PRO 2018). These examples illustrated that while supply chain attacks are in the cyber domain, the impact of such attacks can encompass and cascade down to both the cyber and physical domain, which could cause disruptions and shutdowns of physical supply chains.

Given that small and medium-sized enterprises (SMEs) are 97% of businesses in

North America, the unprecedented threat in the supply chain cybersecurity presented an even more significant challenge to SMEs as they work to scale their business to include more prominent clients. From research conducted by both the industry and academia on the current landscape, about 40% of data security breaches arise from attacks on corporations' suppliers (Melnyk et al. 2022). Among all cybersecurity incidents, attacks against SMEs are rising (Better Business Bureau 2017). A survey conducted in October 2021 indicated that 41.8% of surveyed SMEs experienced a cyberattack in the last year, and over 69% are concerned about attacks in the coming years (Chen 2021).

In the context of investigating SMEs within the wider supply chain, for vendor selection, more than 73% of survey respondents believed a vendor's cybersecurity approach influenced the respondent's willingness to engage in business with them (Better Business Bureau 2017). This establishes the crucial interface between an organization's cybersecurity capabilities and how it impacts the wider ecosystem of organizations and processes. Thus, frameworks and processes that assess and evaluate supplier capabilities are also gaining importance as governments, regulatory bodies, industry, and academia seek to both develop and operationalize best practices and lessons learned.

The research will attempt to address some of the challenges that corporations and SMEs face by investigating challenges in supply chain cybersecurity, such as painpoints, evaluation criteria, and collaboration models.

To investigate the challenges in supply chain cybersecurity, the study is structured into four sections: The first section consists of a literature review of an overview of supply chain attacks, research and practices in supply chain cybersecurity, and general supply chain management to form a complete picture of the current landscape. The second section lays out the research methodology the study employs. The third consists of building a theoretical framework that builds on management best practices and anecdotes from the industry. The final section dives into discussion and outlines work and issues that warrant future investigations.

Chapter 2

Literature Review

This section provides a review of past literature on the current research study. Section 2.1 focuses on a general supply chain overview and supplier development practices and framework. Section 2.2 discusses the overview of various cyber supply chain attacks, supply chain cybersecurity, and the roles of SMEs within the overarching theme. In the review, both research from academia and industry practices will be discussed to provide a holistic view of the background and viewpoints.

2.1 Supply Chain

To better understand cybersecurity and its role within the supply chain, it is crucial to first gain a holistic view of the broader supply chain management practices. The review will help provide insight into how the supply chain functions as a system, the pain points, and best practices gathered by supply chain practitioners. The section will first introduce the concept and research of the supply chain to provide an overview, then explore how supply chain management (SCM) experts discuss and summarize supplier development benefits.

2.1.1 Supply Chain Management Overview

As society started collaborating on making complex goods and services, supply chain and logistics concepts have existed and are used extensively. Researchers and practitioners have proposed many different definitions and extended sub-fields for the supply chain. Christopher (1998, p. 15) offered a condensed and easy-to-understand definition: Supply chain "... is a network of organizations that are involved, through upstream and downstream linkages in the different processes and activities that produce value in the form of products and services in the hand of the ultimate consumer." It is common to visualize the supply chain in terms of flow with upstream entities such as suppliers and manufacturers and those downstream as retailers and customers. In general, there are three distinct types of flow: the flow of materials and goods, information, and money. Materials and goods usually flow downstream from suppliers to end customers, and money (cash) flows upstream from end customers to suppliers. Information, however, is bidirectional because organizations and partners need to share different information to facilitate better decision-making. The sharing of information points towards the collaborative nature of supply chain operations. Figure 2-1 shows a general concept of supply chain flow.

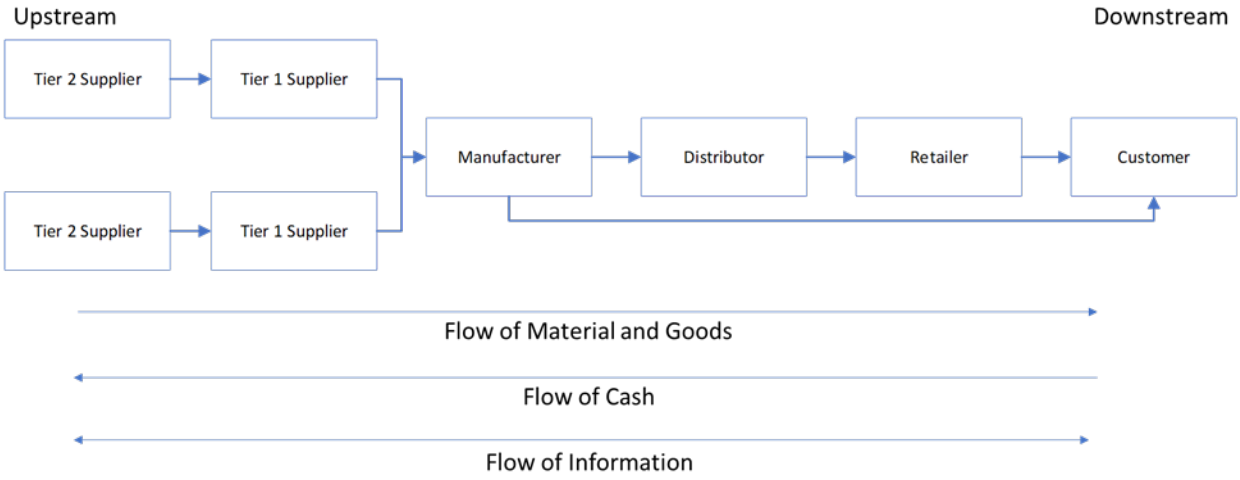

Figure 2-1: General Supply Chain Flow

Besides the aforementioned supply chain concept that offers physical goods and

products, there are other research and frameworks that focus on more specialized areas of the supply chain. One notable example is the service supply chain (SSC), which Wang et al. (2015) defined as a supply chain where a service product is the main output. They further categorized SSC into Service Only Supply Chains (SOSCs) and Product Service Supply Chains (PSSCs). In an SOSC, service is the only form of the product being offered by the system, and examples include consultancy and healthcare body checks. In a PSSC, however, physical products are offered with significant service contributions, which include but are not limited to restaurants and B2B customized product solution offerings.

Another example that has been rising in popularity in recent years is the software supply chain. In short, a software supply chain consists of everything that contributes or plays a part in an application through its entire software development life cycle (SDLC). Given the heavy reliance on digital systems and processes to develop software offerings, the security of the component, activities, and practices, such as codes, infrastructure, deployment methods, tools, and protocols, becomes crucial in such supply chains (Synopsys, n.d.). The SolarWinds case in the introduction section illustrates just how vulnerable such supply chains are.

The term supply chain management (SCM), according to Harland (1996) and Stadtler (2005), can trace its roots to the early 1980s, when Oliver and Webber (1982) coined the term and discussed integrating purchasing, manufacturing, sales, and distribution teams into a single combined function. Stadtler (2005) examined SCM using a "House of SCM" framework (Figure 2-2), where integration and coordination are two critical pillars of successful SCM efforts. Among others, a few key building blocks to note are the need for inter-organizational collaboration (integration), the use of information and communication technology or ICT (coordination), and process orientation (coordination), as these indicated that in order to manage a complex supply chain system successfully, one must work under a technology-enabled collaborative system with strong trust and a collaborative approach.

Historically, SCM had only been a topic of interest to practitioners and select researchers. With the COVID-19 pandemic and recent geopolitical issues that caused

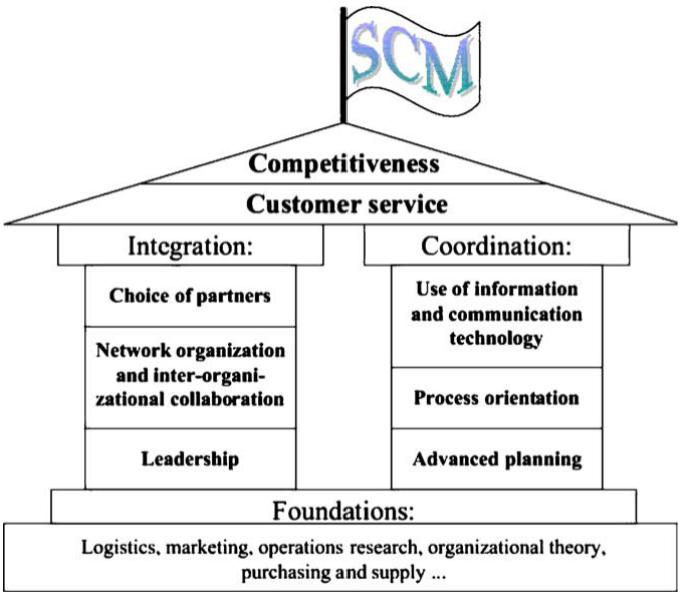

Figure 2-2: House of SCM (Stadtler 2005)

significant disruption in the supply chain, however, SCM has been increasing in importance. In their latest work, "Profit from the Source," (Schuh et al. 2022) Boston Consulting Group (BCG) examined the various industry norms and best practices in the supply chain. They have noted that traditional corporations deemed the procurement/operations function as an administrative role that does not directly contribute to revenue generation, thus relegating the procurement function to non-strategic roles. Using examples from industry leaders such as Toyota, Tesla, Apple, and Dell, the authors proposed that treating suppliers as part of the ecosystem and working with them to improve their overall capabilities can improve innovation, quality, cost, and be more agile to sudden disruptions. Additionally, by internally inviting the operations stakeholders into strategic decisions and empowering supplier engagement point-of-contacts can allow organizations to increase synergy between strategy and their entire supply chain ecosystem (Schuh et al. 2022). To better unlock the potential in working with a broad range of supplier talents and onboard suppliers to better support the business, academic researchers and industry practitioners used supplier development processes and frameworks to educate and bring supplier capability to both lower risk and increase synergy between the two parties. The topic will be

further examined in the following subsection.

2.1.2 Supplier Development Practices

For companies that intend to collaborate with the supplier and put working with them at the heart of their corporate strategy as proposed by academics and industry practitioners, then evaluating and potentially onboarding suppliers will be crucial.

In their research, Modi and Mabert (2007) investigated the improvement of supplier performance through operational knowledge transfer activities (OKTA). It is identified that evaluation and certification efforts before initiating supplier development and OKTA is crucial because it is a core foundation for initiating OKTA. This ensures that the targeted supplier has the minimum capabilities to warrant further resource expenditure and allows the identification of gaps for development. The research also highlighted incentives (promises of future business) as being a positive influence in the development process. Using OKTA, the organization can gain additional value from improved supplier performance and increased responses to exogenous shock from the more transparent sharing of information.

Operationally, organizations conduct many different types of tasks and activities during the development process. Krause (1997) surveyed National Association of Purchasing Management (NAPM) members (527 responses) and found that out of all possible activities, organizations favor activities such as supplier evaluation and feedback, site visits, requests for improved performance, and promises of increased present or future business. Other tasks that are often done but less favored are training/education of suppliers' personnel or investment in suppliers' operations. The respondents attributed much of their suppliers' increases in on-time delivery and orders received complete, as well as decreases in incoming defects and order cycle times, to their supplier development efforts.

Yawar and Seuring (2020) began with a theoretical supplier development framework (Figure 2-3a) that connects various aspects of the buyer-supplier relationship. Through contingency analysis of explored literature, the researchers found interrelationships between different aspects of the buyer-supplier relationship that revised the

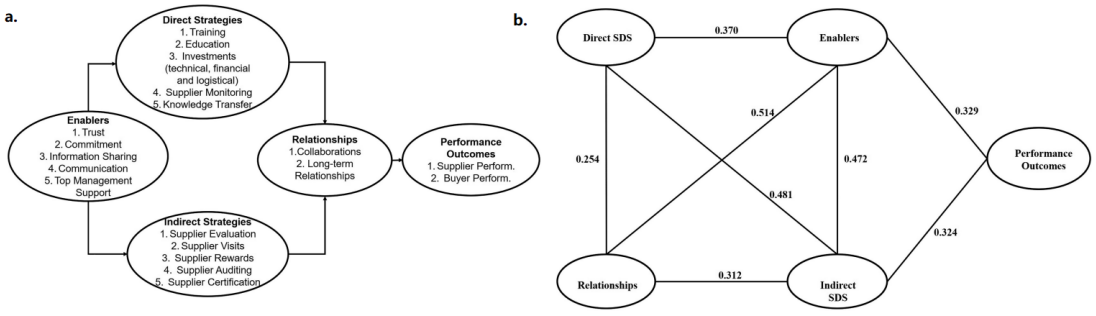

Figure 2-3: Supplier Development Conceptual Model (Yawar and Seuring 2020)

model (Figure 2-3b) with additional linkages. The revised relationship indicates that a supplier development process is a multi-faceted approach with interdependencies that is not a one-size-fits-all relation but rather a bi-directional system.

Other research focused on the organization aspect of those participating in supplier development. Quayle (2000) investigated the supplier development effort for SMEs in the U.K. In the research, it was rationalized that given larger incumbent suppliers have already reached maturity and thus might not need to be further developed or are harder to change, SMEs can benefit from observing how the larger buyer organization works, benchmarking against the best-in-class supplier in the industry, increasing its own capabilities, and gaining future preferred supplier status.

Besides committing to the incumbent supply base and conducting supplier development, other avenues of investigation focused on alternatives to the supplier development process. Li et al. (2006) and Friedl and Wagner (2012) have investigated supplier switching as an alternative as it will only incur a one-time switching cost should the new supplier meet the purchasing firm's requirements. However, the sourcing decision will be heavily dependent on other factors such as incumbent cost variance and maximum demand. It has also been pointed out that developing supplier capability to increase synergy in strategy and action coordination can maximize supply chain value, especially if the entirety of the supply chain system is considered.

Besides academic research, there are many excellent testimonies from the industry that highlights the success of supplier development framework. Dell Technologies, one of the largest U.S.-based technology conglomerates that provide computing hardware

and services to both consumer and commercial customers, works with hundreds of suppliers all over the globe to develop and ship their products to end customers.

From the research conducted in "Profit from the Source" (Schuh et al. 2022), Dell's supply chain process is renowned for its rigorousness, enabling the company to fulfill product development and customer needs with remarkable speed and efficiency. The key to this success lies in Dell's use of pre-vetted suppliers from an approved pool known as the approved vendor list (AVL). By using these approved suppliers, Dell can ensure that the supplier can deliver high-quality parts and services while complying with Dell's processes and norms to collaborate efficiently. It is this effective management that allows Dell to continuously assemble computers to serve the growing global needs during the early days of the COVID-19 pandemic.

Despite having a comprehensive list of suppliers that provide a wide range of components and services in an ever-evolving industry, Dell continues to work with existing and engage new suppliers to actively improve suppliers' capabilities. To qualify suppliers for the AVL, Dell starts by shortlisting potential candidates and providing them with a set of requirements to meet. Dell then audits, tests, and works closely with the suppliers to ensure that their components and processes satisfy all requirements before officially qualifying them for AVL status. This gives the suppliers access to future business opportunities with Dell. (Schuh et al. 2022).

In recent years, Dell has also focused on creating a more sustainable supply chain. To achieve this, the company has developed a four-stage continuous improvement model that includes risk management, audits, corrective actions, and capability building. Dell quantifies the risks associated with its suppliers, audits their operations, takes corrective actions to mitigate risks, and provides resources to help them build additional capabilities. By doing so, the company is able to ensure that its suppliers can meet the Environmental, Social, and Governance (ESG) goals set by the company (Dell 2021).

The combined academic and industry knowledge highlighted the differences in sourcing strategies and supplier collaboration approaches depending on specific contexts and industries. Despite these differences, engaging suppliers in supplier devel-

opment to increase their capability is widely recognized as a beneficial process for both client organizations and suppliers. By building capabilities together, suppliers can improve their performance and contribute to the overall supply chain value by increasing synergy in coordination and action. Thus, investing in supplier development should be considered an integral part of any organization's sourcing strategy.

2.2 Cybersecurity

The umbrella cybersecurity term encompasses many disciplines and research areas that strive to improve and innovate on existing practices and issues. Supply chain cybersecurity is fast becoming a topic that needs to be addressed in all facets of a company's business. The following sections will focus on cybersecurity as it relates to the supply chain. The literature review will draw on both academic and industry practitioner experiences. The different perspectives can allow essential insights to be gained as to the critical issues, common findings, and differing viewpoints within supply chain cybersecurity.

2.2.1 Overview of Supply Chain Attacks

Supply chain cyberattacks differ from traditional cyberattacks because instead of attacking the target organizations directly, cybercriminals target the partners and suppliers that work with these organizations. By compromising systems and services the suppliers provide or connect to the target organizations, attackers can, in turn, gain access to the target organizations. These attacks, specifically those directed at the software supply chain, are on the rise. In a survey conducted by the NCC Group, there was a 51% increase in the second half of 2021 based on the responses from 1,400 cybersecurity decision-makers in 11 countries, including the United States, the United Kingdom, China, Germany, and Singapore. (NCC Group 2022). Additionally, not only are the attacks increasing in complexity, but they are also creating a larger impact, which spans from financial loss, strategic commodity shortages, and sensitive data loss. Examples will be provided in the following subsections to illustrate the

breadth of the types and impacts of these supply chain attacks. The examples will be categorized by the business scenario they occur:

Business-to-Business (B2B) Software Supply Chain

The first type of supply chain attack occurs in a B2B setting, which can be particularly devastating as attackers target software and organizations that have direct access to business client data or networks. Two notable examples of this type of attack are the 2020 SolarWinds cyber-attack and the 2021 Microsoft Exchange server attack.

In the classic 2020 SolarWinds cyber-attack, which was referenced in numerous supply chain cybersecurity literature, the attackers targeted Orion, a network monitoring software developed by SolarWinds that had privileged access to client systems. The attackers chose SolarWinds as it is a business software firm that provides network, database, systems, and I.T. services management to more than 30,000 clients, many of them federal institutions. Attackers injected malicious code into an Orion update using bait-and-switch during the build process, which in turn made its way into client systems digitally signed. As a result, the attackers were able to compromise the systems of around 18,000 clients. The attack was particularly worrisome because it was difficult to detect, as the attackers mimicked Orion's syntax and formats to pass their traffic off as routine Orion messages. The attack had far-reaching consequences due to Orion's interconnectedness and widespread adoption (Temple-Raston 2021).

Another example is the January 2021 Microsoft on-premises Exchange servers attack, which is considered a high-value target as it can be used to access a massive pool of business and government networks. Four zero-day (previously unknown) exploits were discovered and were used to gain initial access to exchange servers, giving attackers full access to user emails and passwords, administrator privileges, and access to other devices within the network. Additional backdoors or ransomware are also installed to further the impact of the initial breach, as those cannot be patched out by fixes to the initial exploit. The number of exchange servers impacted by the attack could be higher than 250,000 in a report by Wall Street Journal (McMillan and Volz

2021).

These examples demonstrate how breaches in software that have direct access to business client information or networks can be exploited to cause extensive damage. In both cases, the attackers compromised systems far beyond their initial targets. As such, it's crucial for businesses to be vigilant about the security of the software they use and to take appropriate measures to mitigate the risks of supply chain attacks.

B2B Software Supply Chain with Physical Impact

Software supply chain attacks not only impact information on the digital system but can also create tangible damage in the physical domain. While there are many examples of such attacks, chips and fuel shortages have been placed at the forefront of national policies as a result of recent supply chain shortages and geographic conflicts. Thus, two examples from these industries will be used.

In 2018, The Taiwan Semiconductor Manufacturing Company (TSMC), the world's largest semiconductor manufacturer, suffered a cyber-attack from a WannaCry variant, shutting down three of its production facilities for up to three days. The incident occurred when an onsite operator did not follow the procedure to scan for viruses before plugging new equipment into TSMC's intranet. Once connected, the ransomware launched the attack using a Windows 7 exploit called EternalBlue to infect other TSMC plants in Taiwan. As the infected machines are part of the production line, production was halted in the three impacted plants for up to three days, potentially costing $255 million in revenue. (IT PRO 2018) Which translates to a two percent revenue shortfall for the quarter.

More recently, in May 2021, the Colonial Pipeline, the largest pipeline system for refined oil products in the United States, fell victim to a cyber attack. The attacker gained access to the company network through a VPN that was not protected with two-factor authentication using a leaked username and password. On May 7th, the attacker stole both 100GB worth of data and locked company data to demand ransom. The company paid the attacker a total of $4.4 million in ransom. While investigation showed that the attackers did not gain access to systems that actually control gas

flows, the company shut down the entire pipeline to check for breaches and did not reopen until May 12th, impacting gasoline, diesel, and jet fuel supply for the East Coast of the United States (Turton and Mehrotra 2021, Kerner 2022).

These examples demonstrate how cyber attacks on operational technologies (OT) in physical supply chains can severely impact the physical flow of goods and materials. With supply chains relying heavily on supplier collaboration, securing suppliers against attacks is crucial to minimize the risk of disruptions.

Business-to-Consumer (B2C) Software Supply Chain

Besides the B2B context, some attacks targeted software and services that serve both business and consumer segments, widening the affected group even further. Two popular consumer software examples are discussed below.

In September 2017, security researchers disclosed that CCleaner, a utility software that cleans invalid registry entries and orphaned or unwanted files developed by Piriform Software, had been compromised by cybercriminals. The issue was made more complex by the fact that the parent company Avast, is a security company. The breach occurred in March 2017, before Piriform's acquisition by Avast. Attackers were able to compromise Piriform's network through TeamViewer (remote desktop application) using stolen credentials. They used a popular malware named ShadowPad to infect numerous computers within the network. The cybercriminals waited until August (after acquisition) to start contaminating CCleaner download files. The contaminated file amassed a massive 2.27 million downloads. Despite the high download count, it is found that only a select few were targeted for a second-stage infiltration, all of which were technology and I.T. enterprises. The attackers were able to infiltrate 11 of them. Besides the long incubation period between the initial breach and the actual attacks, the targeted nature of the attack highlights the criticality of supply chain cyber-attacks being a considerable threat to organizations (Newman 2018, Lomas 2017).

Another sophisticated supply chain attack happened to ASUS, a Taiwan-based PC manufacturer, which contributed to a worldwide market share of 8.2% in Q3 of

2022 (Gartner 2022a). In June 2018, the attackers targeted the ASUS Live Update utility, a preloaded application on all ASUS computers that automatically updates BIOS, drivers, and applications. The attack, also called Operation ShadowHammer by Kaspersky researchers, used a trojan-ized updater that had a legitimate signed certificate that infected over 57,000 users' computing systems based on Kaspersky's estimate. However, the actual number is likely far bigger, given that not every computer uses Kaspersky's software. It was found that, like the CCleaner attack, the attack is aimed at a particular group of users by using a pre-coded list of unique MAC addresses to identify the target to install backdoors and download additional payloads. In a Symantec blog post, it was counted that 80% of victims were consumers, and 20% were from organizations (Symantec 2019). Kaspersky researchers stated that the complexity and techniques involved in the ASUS attack surpass that of the CCleaner (Kaspersky 2019).

The two examples illustrated that while techniques, complexity, and target of the two attacks may be different, they share a commonality in that; first, the attacks impact both consumer and corporate entities, and second, despite the high spread, the attacks were targeting a select few entities to gain high valued information.

2.2.2 Supply Chain Cybersecurity

Supply chain cybersecurity deals with the measures and processes taken to protect information within a supply chain to ensure the security and continuous uninterrupted flow of information and material. In the recent years, information and communication technologies (ICT) have been increasingly utilized within the general supply chain from advances in digital technologies and Industry 4.0 initiatives. ICTs consist of a network of digital systems, technologies, and infrastructure used to connect and share information within a supply chain (Smith et al. 2007). The use of ICTs added another layer of complexity and interconnectedness that increased the overall risk in the entire supply chain. An attack on any link within the supply chain can cause ripple effects and severe consequences to all organizations within the supply chain, causing disruption in operation, financials, and organizational trust and image.

The criticality of securing one's supply chain cybersecurity threat is never more apparent from the high-profile attacks outlined in the previous subsection. Data also showed that about 40% of data security breaches arise from attacks on corporations' suppliers (Melnyk et al. 2022), making these series of attack vectors particularly lucrative due to the impact and breadth of their reach. Organizations are increasingly becoming aware of this issue. A 2017 survey showed that in vendor selection, more than 73% of respondents believed a vendor's cybersecurity approach influenced the respondent's willingness to engage in business with them (Better Business Bureau 2017). These attacks range from physical threats such as damaging and theft of physical components, non-deliberate breakdowns of services, indirect attacks such as denial of service, direct attacks including but not limited to viruses, ransomware, and spoofing, and lastly, insider threats that are vulnerable to leakages or social engineering attacks. (Ghadge et al. 2019). In terms of the impact and consequence of the attack and breach, Ghadge et al. (2019), through the compilation of other research, categorized the impact as a series of propagation zones which radiates out from the point of penetration. These propagation zones can be defined as primary, secondary, and tertiary propagation, which impacts self, supply chain, and society, respectively.

There are many examples of corporations implementing supply chain security spanning both physical and cyber domain. An excellent example is Dell, which ships around 60 million PCs each year to 180 countries. Dell takes a rigorous approach to avoid tampering of its product from the design to sustaining phase of the product life cycle (Schuh et al. 2022). Michael Dell, the founder of Dell Inc., said at Dell Technologies World 2019, "We integrate security deeply at every step—from our supply chain to the security that's embedded deep inside our products to the network and application layer into the heart of our customers' operations." (Haranas 2019) Operationally, not only is the product secure-by-design with Secure Development Lifecycle (SDL), digital signing, BIOS protections, and so forth (Dell 2023), Dell only sources components from trusted suppliers on the approved vendor list (AVL). Additionally, to ensure no unexpected tampering during production and shipment, Dell utilizes var-

ious measures such as chassis intrusion detection, Piece Part Identification Numbers (PPID), and Secured Component Verification (SCV) to guarantee the authenticity of the hardware and services being delivered to the end customer.

Amazon Web Services (AWS), the leading cloud provider in the industry, coined the term "shared responsibility model" to describe AWS security as a service provider. In this model, AWS is responsible for the "security of the cloud" (infrastructure), and customers are responsible for "security in the cloud" (security configuration, service patches, IAMs), thus highlighting the importance of every stakeholder being important in securing the entire supply chain (Amazon, n.d.). The company also recognizes the criticality of supply chain security by investing in the Open Source Security Foundation (OpenSSF) to shore up open-source software security (Amazon 2022).

The digitalization of the supply chain increasingly connects different organizations together, making the supply chain more vulnerable to cyber-attacks. The consequences of such a breach can be severe, impacting not only the organization itself but also the wider supply chain as a whole. As a result, research and organizations are increasingly focused on securing their supply chain and how business partners play a role. The AWS shared responsibility model highlights the importance of stakeholder collaboration in securing the entire supply chain. The nature of supplier collaboration in supply chain cybersecurity will be investigated in the following sections.

2.2.3 SMEs in Supply Chain Cybersecurity

Small and medium-sized enterprises (SMEs), contributing to more than 97% of total businesses in North America (Better Business Bureau 2017), play an important role in supply chain cybersecurity. While large enterprises or organizations have more resources, established processes, and lessons learned to implement robust cybersecurity practices, SMEs do not necessarily have those and thus become frequent targets to cybercriminals. This observation is echoed by Infosec Institute (2015) in that "Whilst not always the case, it is often the smaller organizations within a supply chain who, due to more limited resources, have the weakest cyber security arrangements." With

the vital role of SMEs in providing essential products and services, their role within supply chain cybersecurity must be investigated more deeply.

SMEs are defined differently across different countries and regulatory bodies. The U.S. Small Business Administration (SBA) assigns different standards to each of the North American Industry Classification System (NAICS) codes. SBA defined most manufacturing companies with 500 or fewer employees as SMEs, and most non-manufacturing ones are capped at $7.5 million in average annual receipts. In the U.K., however, any kind of business with less than 250 employees is considered an SME. The literature review will follow the definition set by their respective research as they share similar painpoints.

SMEs face unique challenges when it comes to planning, implementing, and improving their cybersecurity capabilities compared to large enterprises (LEs). To illustrate this challenge, Heidt, Gerlach, and Buxmann (2019) with a conceptual framework. From a compilation of past literature, factors are split into three unique characteristic environments within the framework: macro, micro, and the focal SME. As shown in Figure 2-4, the macro environment consists of factors such as institutional and regional (country) influences. The micro environment consists of factors that have a direct interface with the focal firm, such as clients, consultants, and suppliers. Lastly, within the focal SME, various factors influence how the SME implements its cybersecurity, which they discussed in greater detail:

- *Limited Resource*: Many SMEs lack the financial resources, expertise, and task prioritization needed to effectively implement cybersecurity measures based on the interview conducted in the research.

- *Low Formalization Level*: A single individual within an SME is given multiple responsibilities and role-identities which may have conflicting interests. The "wearing of different hats" is found to have negatively impacted cybersecurity implementation in SMEs.

- *Ingrained Culture*: SMEs often rely on stakeholder trust, which can take a long time to build, because of their size and hierarchy. This can make it challenging

to implement cybersecurity measures when a trusted colleague's suggestion can potentially carry more weight than an expert third-party provider.

- *Geographical Insularity*: SMEs could face geographical constraints when trying to find human resources and service providers compared to their LE counterparts, who can source talents and suppliers from a wider geographical region.

- *Leadership Characteristics*: The CEO or the owner of the SME's knowledge, awareness, investment priority, and subjective opinion of the value proposition of cybersecurity capabilities can greatly influence investment in cybersecurity. The owner must balance different priorities based on limited resources, which plays into the other aforementioned factors.

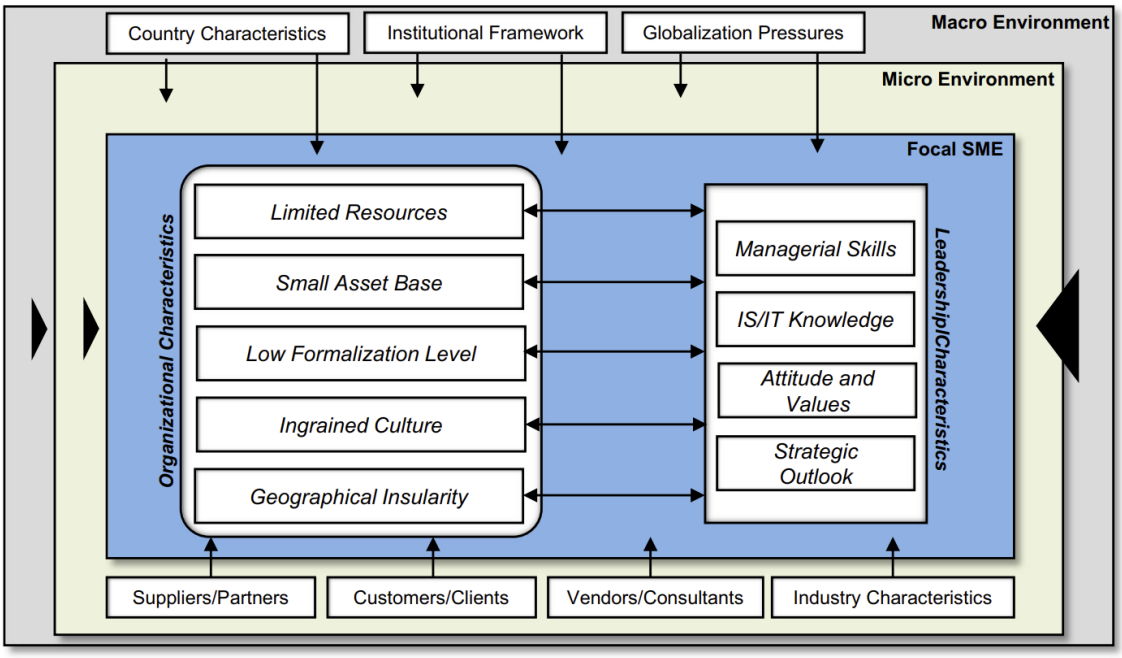

Figure 2-4: Conceptual Framework of SME Constraints (Heidt, Gerlach, and Buxmann 2019)

The research is also supported by an industry survey conducted by Better Business Bureau (2017). The respondents in the survey attributed the lack of resources, expertise, information, time, and training as top factors in hindering cybersecurity capability building. Overall, academic research and industry knowledge agree with the unique challenges SMEs face in internal cybersecurity capability development. By

recognizing these challenges, the importance of engaging in collaborative capability building is evident.

In addition to SMEs having their unique challenges because of company size, SME practices and painpoints also vary regionally. Kabanda, Tanner, and Kent (2018) explored SME cybersecurity practices in developing countries such as South Africa. Through interviews with practitioners within the South African industry, the researchers were able to classify SME cybersecurity implementation into internal and external factors (Figure 2-5). What is especially interesting is the fact that in terms of external institutional pressure, research showed evidence of coercive pressure resulting from governmental or regulatory policies. At the same time, it lacks normative (from industry associations) and mimetic (from competition) pressures. Thus, it prevents SMEs in South Africa from potentially improving their capability through professional standards, practices, and methods as set by the cybersecurity community.

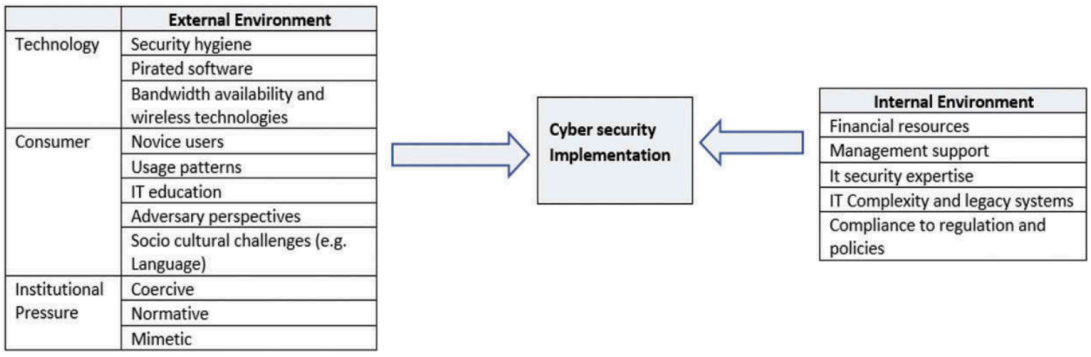

Figure 2-5: Factors in Cybersecurity Implementation of South African SMEs (Kabanda, Tanner, and Kent 2018)

From the review, it is apparent that SMEs not only suffer from unique challenges compared with their LE counterparts but also have different factors when making cross-region comparisons amongst SMEs. With SMEs being a considerable part of the total addressable market of business partners, it becomes crucial to investigate development frameworks in the context of working with these growing businesses.

2.2.4 Supply Chain Cybersecurity Assessment

When working with both internal stakeholders within the organization and external suppliers, assessment processes and best practices are often used to ensure effective communication, align expectations, and establish a common language for assessing the organization's current cybersecurity capabilities. In this subsection, the study will focus on notable regulatory frameworks, certifications, industry practices, and academic research related to cybersecurity assessment for suppliers.

One key resource for organizations seeking to improve their cybersecurity capabilities is the National Institute of Standards and Technology (NIST), which provides a range of guidelines and recommendations. For example, NIST Cybersecurity Framework (CSF) V1.1 is "a voluntary risk management framework consisting of standards, guidelines, and best practices to manage cybersecurity-related risk." (Krumay, Bernroider, and Walser 2018) This framework outlines how to assess and implement different tiers of the cyber risk management process and program within the organization and how to expand that to encompass cyber supply chain risk management (C-SCRM) with external stakeholders such as suppliers and customers (Figure 2-6).

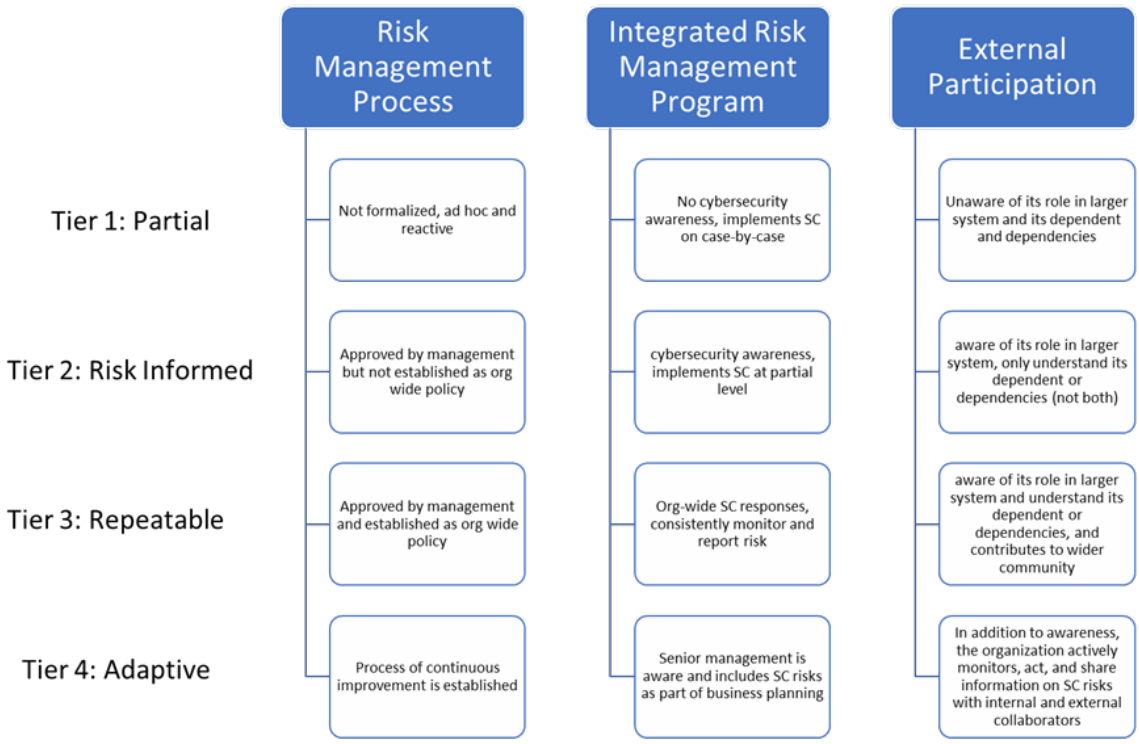

Figure 2-6: NIST v1.1 Framework (NIST 2018)

NIST has also published additional guidance specifically focused on C-SCRM. For instance, the SP 800-161 Rev. 1 (2022) "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," which "provides guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations." (Boyens et al. 2022) The document includes sections for targeted audiences in risk management, business owner, procurement, IT/cybersecurity, and system engineering professionals. In addition to specific controls and recommendations, SP 800-161 highlights the importance of enterprise, mission, and operational level activities involved in working with external suppliers. While purchasing organizations are encouraged to plan and define cybersecurity requirements as part of the procurement process, controls and requirements are typically placed as part of the contract for subsequent validation and audits rather than developing those capabilities beforehand.

Another important publication is the NISTIR 8276 "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry." The publication published insights based on 25 case studies of industry best practices and NIST's own cybersecurity guidance, which are condensed into eight key practices, they are quoted as below (Boyens et al. 2021):

1. Integrate C-SCRM Across the Organization
2. Establish a Formal C-SCRM Program
3. Know and Manage Critical Suppliers
4. Understand the Organization's Supply Chain
5. Closely Collaborate with Key Suppliers
6. Include Key Suppliers in Resilience and Improvement Activities
7. Assess and Monitor Throughout the Supplier Relationship

8. Plan for the Full Life Cycle (Boyens et al. 2021)

In these recommendations, several key points relate to supplier interaction, including the need to work closely with strategic suppliers on maintaining relationship (transparency), resilience, improvement, and continuous monitoring. The need for certification and third-party assessment of critical suppliers is also emphasized.

Figure 2-7: NCSC Supply chain cyber security summary and the individual stages (NCSC 2022)

The UK National Cyber Security Centre (NCSC) released a guideline in October 2022 to assess suppliers and manage supply chain cybersecurity risks. The guideline was developed in response to the growing threat of supply chain cyberattacks and the fact that only about "one in ten businesses review the risks posed by their immediate suppliers (13%) and the proportion for the wider supply chain is half that figure (7%)." (NCSC 2022) The guideline is split into five stages (Figure 2-7), each into different steps. The first two stages focus on understanding, mapping, and aligning internal needs, priorities, and goals. Stages 3 and 4 focus on assessing and reviewing relationships outside of the organization, mainly suppliers in pre-contract and after-contract signing. This involves monitoring supplier performance, assessing their cybersecurity posture, and embedding security controls throughout the contract duration. The final stage of the guideline is continuous improvement, emphasizing the need to improve existing controls and processes with suppliers.

Overall, the NCSC guidance provides a good summary of an overarching supply chain cybersecurity assessment and management model. However, the guideline did not go into how to develop and improve the supplier's security posture post-assessment.

In addition to government guidelines, certifications are available for organizations to demonstrate compliance with prospective business partners. One of them is Systems and Organizations Controls 2 (SOC 2). SOC 2 certifications are not legally required and are conducted by non-government third-party auditing agencies. SOC 2 certification involves a Type 1 audit to test the process and policy of the organization at a point in time, followed by a Type 2 audit, which assesses the effectiveness of the implemented processes and policies as part of the Type 1 audit over time (McCarthy 2023). However, it is to be noted that the criteria being assessed may vary across organizations, as each organization selects those applicable to their services and defines the scope of the audit. This implies that different organizations can all be SOC 2 compliant, but only towards the specific goals that the organization defined for itself. As a result, potential business partners must review the detailed report to determine whether all the necessary controls have been met.

Another certification is ISO 28000:2022, which outlines requirements for a security management system, including those related to the supply chain. The standard mandates that the organizations assess their security environment and its supply chain dependencies and interdependencies (Figure 2-8). It also requires the organization to determine if adequate security measures are in place to effectively manage cybersecurity risks, including the relevant upstream and downstream processes and controls of the supply chain to meet the organization's objectives (ISO 2022). ISO 28001:2007 furthered the concept of security management systems by putting forth guidance for implementing security, assessments, and plans in a supply chain context (ISO 2007). While the standards highlighted the importance of managing security by considering supply chain dependencies, it is still within the context of taking supply chain risk into account rather than actively engaging and mitigating risk on the supplier's side.

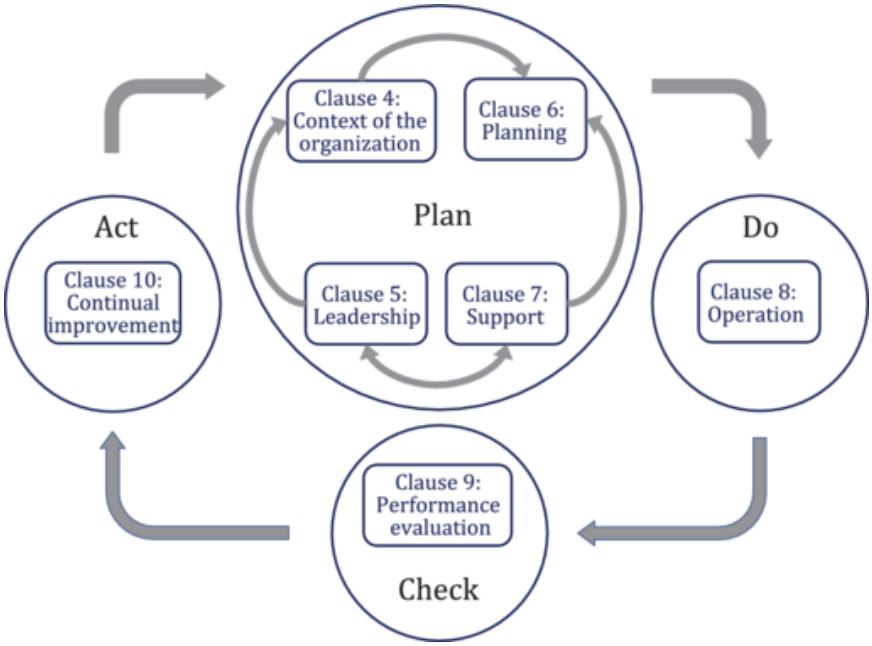

Figure 2-8: PDCA model of the security management system (ISO 2022)

The rising need for organizations to evaluate or assess their suppliers' cybersecurity capabilities has led to the emergence of various services and solutions in the cybersecurity sector. One such solution is the auditing firms that assess compliance with regulatory standards and certifications. In addition, companies that provide cybersecurity scorecards and rating services, such as BitSight and SecurityScorecard, offer aggregated scores for the cybersecurity capability of different firms they survey. However, they accomplished this by doing network mapping and risk vectors from publicly available data, information, access, and other types of commercial/open-source intelligence sources (Bitsight, n.d., SecurityScorecard 2020, Epiq, n.d.). They then compiled their initial scoring based on that information; while objective, there is no visibility or penetration of the organization's internal system. These scores are revised when the firm being scored or the client organization hires them to redo a detailed audit. While these services offer a good high-level first-pass assessment, the method may not be effective for organizations working with suppliers that have a minimal internet presence or those with unique requirements. Also, with a standardized method that spans the entire spectrum of firms, the scoring might not accurately reflect organizational needs as some organizations will emphasize different categories

or items being scored.

Besides formalized regulatory standards and industry solutions, researchers tried to build on the standard by simplifying the process and providing an aggregated scoring mechanism. For instance, Benz and Chatterjee (2020) presented a cybersecurity evaluation tool (CET) based on the NIST cybersecurity framework (CSF) for SMEs. While the NIST CSF framework theoretically allows organizations to conduct cyber risk management through best practices regardless of their initial capability or sophistication in terms of cybersecurity, it is complex and lacks a comparative rating system. The complexity gated none-experts, which in turn means that "organizations are unable to gauge the effectiveness of implementing the recommended security policies and procedures" (Benz and Chatterjee 2020). To address this, the CET tool draws upon 35 of the 96 standards set by NIST; these 35 standards are used as part of the CET tool for backend score aggregation in different categories (identify, protect, detect, respond, and recover) on a scale of five scoring categories (none, reactive, formalizing, repeatable, and role model). Based on these scores, the tool provides relevant recommendations. The research is limited in that the tool is still aimed at generalized self-assessment and isn't envisioned with both a client organization and their suppliers in mind (customized goal and baseline). There is also no formalized development process that takes the evaluatee from the current baseline to the intended goal.

Another research by Emer, Unterhofer, and Rauch (2021) also proposed an assessment tool intended for SMEs that has an even simpler visualized recommendation system. The tool splits different cybersecurity items into four quadrants with axes of importance (based on various metrics) vs. capability gap: Must haves, quick wins, money pits, and low-hanging fruit. The tool provided a simplified quadrant system to assess what capabilities to enable but is limited in both pilot scope and the discrete cut-offs between different quadrants, which makes items closer to the axis harder to judge their importance.

Surveying the industry and research landscape, it is clear that as the importance of supply chain cybersecurity grows, efforts have focused on technical capabilities to

prevent attacks and processes to prevent incidents at the single-organization level. At a multi-organization level, numerous assessment and scoring mechanisms have been proposed and tested with varying degrees of success. However, little research or industry and regulatory frameworks have explored the process that bridges evaluation and subsequent integrated cooperation. Melnyk et al. (2022) also calls attention to the need for supplier development as future work to address current supply chain cybersecurity challenges. While supplier development is an established practice in regular supply chain management, vendor oversight and development in its cybersecurity readiness is one area that lacks in-depth investigation. The study will discuss supplier development in the cybersecurity context in the following chapters.

Chapter 3

Research Methodology

The objective of this research was to develop a theoretical cybersecurity supplier development framework to guide future supplier engagement and development within the supply chain industry. The combined knowledge from the two research fields was used to develop the framework. Firstly, a literature review of the current cybersecurity landscape identified gaps in current practice. Secondly, we examined anecdotal evidence from traditional supply chain management research and industry practices to gain insight into the best practices of the supply chain industry. The developed framework was further refined through comments and suggestions from industry subject matter experts.

The first step in building the framework involved a review of the current literature on the state of supply chain cybersecurity to identify the gaps in the current cybersecurity supplier collaboration. Academic research (Benz and Chatterjee 2020, Emer, Unterhofer, and Rauch 2021) and numerous regulatory frameworks, such as NIST, ISO, and NCSC (NIST 2018, Boyens et al. 2021, ISO 2022, ISO 2007, NCSC 2022, Boyens et al. 2022), provided various approaches to assess cybersecurity capability. The same set of research also includes provisions for monitoring capability. However, the review revealed a lack of focus on capability development outside organizations, which hinders proper collaboration with partners for mutual improvement. This challenge is particularly relevant when dealing with current supply chain cybersecurity challenges (Melnyk et al. 2022), highlighting the need for further concept

development.

Next, a theoretical model was developed using Melnyk et al. (2022) framework in laying a foundation for cybersecurity across the supply chain (CASC) and supply chain research in mutual capability building in supplier development (Krause 1997, Modi and Mabert 2007). The model takes established concepts and processes utilized in traditional supply chain management industries and academic literature and applies them to a cybersecurity context. Using theories from the supply chain allowed best practices built on decades of lessons learned and iterated by experts to solidify the feasibility of the proposed managerial process. This could accelerate framework adoption and lowers the barrier of entry by practitioners. Best practices from regulatory guidelines such as Department of Energy's C2M2 maturity model and National Cyber Security Centre's (NCSC) supply chain cybersecurity guidance were used to further enhance the synergy between the classic supplier development process and the needs of supply chain cybersecurity.

Finally, the framework was refined by soliciting feedback and suggestions from industry practitioners and subject matter experts. These experts have built their expertise on years of aggregated lessons learned and insights in everyday operational work. Incorporating their specific suggestions and best practices in operationalizing the process can significantly enhance its feasibility. Feedback was gathered during presentation meetings, and the framework was revised accordingly to ensure its practicality and effectiveness in real-world scenarios.

By combining the traditional knowledge of supplier development in supply chain management with current cybersecurity assessment and management pain points, a new process was developed that integrates well within the current cybersecurity context. This approach provided a solid foundation for the process, which increased its feasibility, and decreased overall policy resistance.

Chapter 4

Supplier Development Process Framework

Assessing cybersecurity capabilities and documenting best practices in continuous improvement are abundant in research, regulatory guidelines, and industry insights from the literature review. However, a gap exists in supplier collaboration within the supply chain between assessing the cybersecurity capabilities of the supplier and contract signing with the supplier, especially when large client organizations are concerned with SME suppliers not meeting minimum cybersecurity requirements. The lack of a clear way to ensure suppliers improve their cybersecurity capabilities and close the capability gap with the client organization's requirements creates a business opportunity versus security dilemma. Business priorities may take precedence over security concerns, and contracts may be signed without suppliers demonstrating the required capabilities. This Catch-22 situation poses a challenge for both buyers and suppliers, particularly SMEs, where demonstrating and developing required cybersecurity capabilities is essential to gain business, but without an existing business opportunity, it can be challenging to do so.

This business dilemma is traditionally solved in supply chain management through the supplier development process. The research will answer the call from Melnyk et al. (2022), which recommend future research to investigate a supplier development process to shape suppliers' cybersecurity capabilities. With the critical need for co-

operation within both the physical and software supply chain, this chapter aims to develop a theoretical supplier development process framework that bridges the gap between assessment and subsequent contract signing, seeking to improve SME cybersecurity capabilities (Figure 4-1). With such a framework, it is hoped that large client organizations with their mature cybersecurity management capabilities can help SMEs build the necessary cybersecurity capabilities to meet the minimum requirements and collaborate to create better overall business value. Additionally, client organizations can have better confidence in managing supply chain cybersecurity risks, benefiting all parties involved.

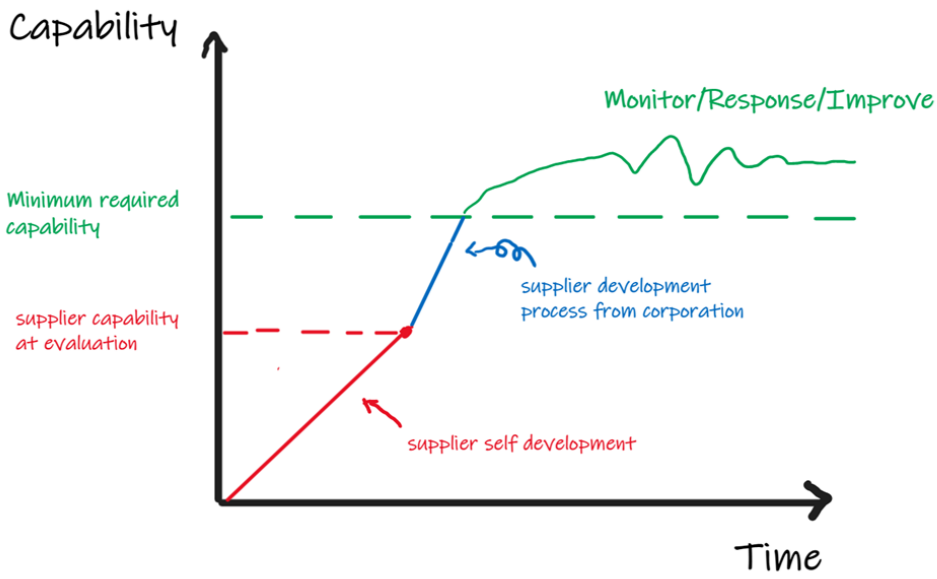

Figure 4-1: Process Gap within supplier collaboration

The supplier development process framework in supply chain cybersecurity intends to provide a guideline for procurement, cybersecurity, and risk management professionals within an organization to assess and develop software, hardware, and service suppliers on an ad-hoc and regular basis. The framework serves to augment current business processes with the best practices in supply chain management. While the framework is a managerial process for developing supplier cybersecurity capabilities during the qualification and onboarding process, it can be generalized to fit different situations and contexts. The framework is built on several key assumptions, which

will be discussed below.

Framework Assumptions

First, the framework defines the persona using this process as a larger purchasing organization (client) with mature cybersecurity and risk management programs and processes that can improve on organization's overall capability. The process is intended to augment the organization's existing processes and targets less cyber-capable suppliers, specifically SMEs within their industry, who may not have mature cybersecurity capabilities. SME suppliers make up a significant portion of overall businesses and need help securing themselves against possible attacks. While the framework serves as a client organization process, it can also help SME suppliers to better understand the larger partner's (client) requirements, process, and the value such activities offer to plan their efforts accordingly. Given the complexity of stakeholder management, each step of the framework will also be classified as an internal or external process: Those internal to the client organization and those external to the organization, such as the suppliers.

Additionally, the process will run independently of other engineering and business processes, focusing explicitly on supplier development in cybersecurity capabilities. Factors such as cybersecurity investment funding are considered an exogenous input and thus not discussed within the scope of the development process. However, the framework is built to take exogenous inputs from other cross-functional teams and processes at key checkpoints within the supplier development process to align with the broader business strategy. The process will be cognizant of exogenous inputs and aligned with other processes to ensure its effectiveness.

Lastly, businesses across different industries operate differently in terms of supplier engagement. The framework is built assuming that the purchasing organization, because of sourcing needs to support future projects and initiatives, is considering and qualifying suppliers for an approved vendors list (AVL) consisting of both larger and smaller suppliers. Supplier development will be initiated and concluded before officially going into a contractual agreement. However, the process can be modified

to fit different engagement models, such as but not limited to development efforts on existing suppliers that exhibit issue in managing their cybersecurity-related controls or suppliers already under contractual bonds but are not operationally integrated with the purchasing organization yet.

The chapter will be divided into different stages of the supplier development process (Figure 4-2): Identify (Section 4.1), Assess (Section 4.2), Develop (Section 4.3), and Continuous Improvement (Section 4.4). Within each of the four stages, the process is introduced step-by-step manner. A hypothetical case will be presented throughout the chapter to be used to depict how an organization can best utilize this framework.

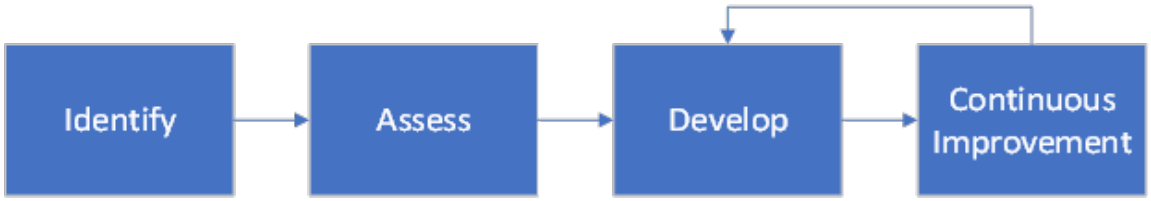

Figure 4-2: Supplier Development Process

4.1 Identify Stage

4.1.1 Framework Walkthrough

The first stage within the supplier development process is the Identify stage. For organizations that rely heavily on suppliers to deliver products and services, it can be challenging to categorize external suppliers and determine the relevant stakeholders within the organization that need to be involved in the decision-making process. Thus, the objective of the identify stage is twofold, the first is to gain an understanding of the landscape in which the organization operates, and the second is to develop an approach to assessing the suppliers based on this understanding.

Identify Stakeholders and Supplier

The stage starts with first internally **identifying key stakeholders with stakes in cybersecurity and supplier onboarding**. This should include but are not limited to the following:

- Who provides the approval necessary to move both the initiative and process forward? (e.g., executive sponsors)
- Who are the parties responsible for mapping out sourcing strategy or contract negotiations? (e.g., operations, procurement)
- Who are responsible for assessing and developing supplier's security capabilities? (e.g., cybersecurity team, IT Team)
- Who should be consulted during the development process? (e.g., engineering, regulatory)
- Who should be informed about the status of the development process? (e.g., legal team, management team)

Existing teams and programs can also be leveraged if the organization has preexisting cybersecurity incidents or risk management programs that monitor and improve on organization cybersecurity capabilities.

The organization needs to **identify suppliers the organization intends to collaborate with** after identifying internal stakeholders. These include both current and potential suppliers that the organization is or will be working with (Schuh et al. 2022). By looking at the organization's business, operation, and technology's needs, an exhaustive list of current and future suppliers can be compiled.

Categorize and Prioritize Suppliers

Next, the organization can **categorize and prioritize suppliers based on criticality to operations and cybersecurity risk**. Categorizing suppliers involves

examining the products or services they provide and their connection to the client organization. This categorization process is important to determine the types of cyber risk suppliers pose to the organization. Gartner (2022b) provides an example of supplier categorization based on risk associated with digital supply chain. These include suppliers that have 1) access to sensitive information disclosed by the client organization, 2) shared infrastructure such as networks, systems, and managed services providers, 3) commercial and open-source software used by client organizations, and 4) codebases with security flaws in digital products. This categorization is essential as it helps organizations to understand the risks associated with their suppliers and prioritize them accordingly. However, due to the complexity of the supply chain and different industries, different organizations may have their own unique way of classifying suppliers and their risks. To assist organizations, various industry guidelines provide a good overview of examples on the types of suppliers they may encounter. For example, UK NCSC (2022) supply chain cybersecurity guideline categorized suppliers based on the type of relationship the client organization has with them. This categorization process helps organizations understand their suppliers and prioritize those that pose the highest risk:

- Service providers (end-to-end, IT, Cloud Providers/Reseller, etc.)
- Equipment and system maintainers
- Manufacturers of hardware and software products
- System integrators
- Consultancies
- Managed service providers (MSPs)
- Trusted software suppliers

While different industry guidelines may have distinct conventions and categorizations for suppliers, they share commonality in having similar types of risk in each

category. This typically includes considering the nature of the relationship, such as whether the supplier is a manufacturer or service provider, as well as the level of access they have to sensitive information, networks, or codebases. These factors can provide good indicators for the controls and requirements needed to effectively manage supplier risk.

Establish Cybersecurity Requirements

After categorizing and prioritizing the suppliers, the organization can **establish supplier cybersecurity requirements based on supplier type and needs**. This critical step serves as a precursor to both Assess and Develop stage. A supplier of hardware products that has its own production line will have very different set of controls and processes when compared with a supplier of software products as risks associated with OT systems within the factory and product tampering in transit isn't common in a purely software environment. Once the requirements have been established, the organization should **document cybersecurity requirements for different supplier categories**. This documentation will enable both internal and external stakeholders to understand the process and the cybersecurity capabilities required in a more transparent manner (NCSC 2022).

A flowchart of the Identify stage can be seen in Figure 4-3.

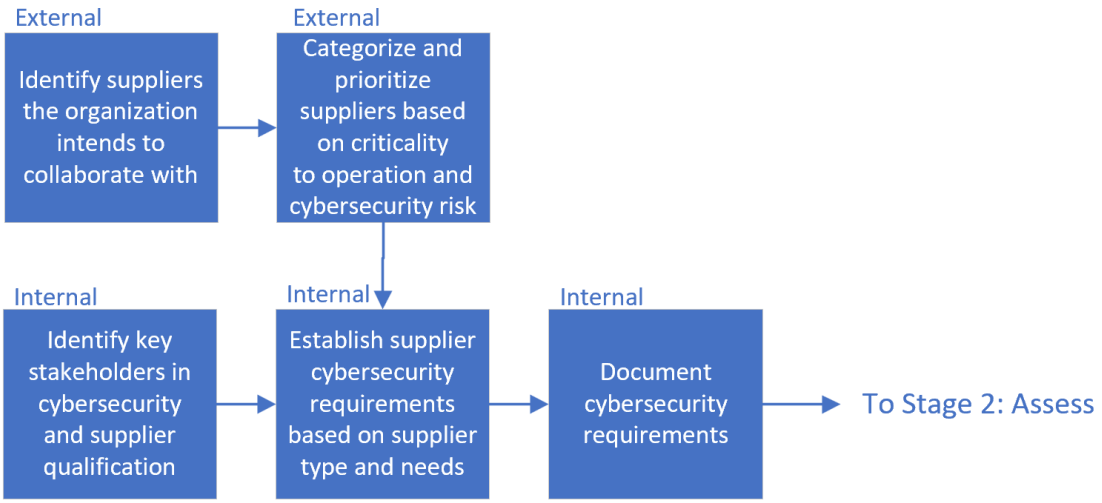

Figure 4-3: The Identify Stage

4.1.2 Identify Stage Example – Click Technologies

To provide an operational context for the process, the study uses a hypothetical company, Click Technologies. This company collaborates with suppliers for hardware product development and services. Because of the recent rising cybersecurity threat, chip shortages, and supply chain congestion, Click Technologies has decided to increase the cybersecurity capabilities of its supplier pool and qualify new suppliers for its Approved Vendor List (AVL). A program manager was assigned to facilitate discussions and document relevant processes within the supplier cybersecurity development core team, consisting of cross-functional team members such as procurement, cybersecurity, IT, finance, operation engineering, and R&D engineering.

The core team formalizes a supplier development process that identifies, assesses, and develops the supplier's cybersecurity capability. It is reasoned that Click Technologies' cybersecurity governance and best practices accrued over decades of being a leader in delivering reliable and safe product offering to its customers can be extended to its supply base. They first identified target suppliers for the development process. The procurement and IT teams took an inventory of existing Click Technologies suppliers and identified potential suppliers that are not yet qualified to be on the AVL. They then categorized all current and potential suppliers into their respective categories: Manufacturers (hardware products), software/service provider (internal systems), and software suppliers (software product codebases).

The core team aligned on a set of requirements for each of the three categories of suppliers. This is done by taking into consideration input from various functional members in areas such as supplier collaboration model, interface with the company, strategic importance of the supplier, and applicable cybersecurity controls. The requirement represents the ideal state at which Click Technologies expected their supplier pool to have in terms of cybersecurity capabilities.

4.2 Assess Stage

4.2.1 Framework Walkthrough

The second stage in the supplier development process is the Assess stage. This stage builds on the foundation laid down in the previous stage by utilizing the categorized supplier list, coupled with the aligned supplier priority and the documented requirements and criteria. The objective of this stage is to assess suppliers to understand their current cybersecurity capabilities based on the requirements set forth in the previous stage. This is crucial because the point-in-time assessment and evaluation of supplier allows organizations to establish a baseline of the supplier's capability and their susceptibility to potential attacks. This will help identify the supplier's capability gaps and serve as a starting point for subsequent development efforts.

Assess Supplier Capability

The stage starts with **conducting assessment on the targeted supplier** using a client-appropriate assessment of cybersecurity capabilities and processes that was documented in the Identify stage. This may involve various tools, methods, and third-party auditors to ensure compliance with the controls and criteria being investigated.

The purpose of a cybersecurity assessment determines the ability of an organization's security controls, processes, and programs to remediate vulnerabilities and potential attacks (Meir 2021). This is particularly important when working with a new SME supplier that may lack the expertise or experience to build and ramp up their cybersecurity capabilities. By conducting an assessment, the client organization can gain an understanding of the supplier's previously unknown cybersecurity capability. Some examples of these tools and processes were provided in the previous sections. Across industries that support public sectors or critical national initiatives, mandatory adherence to regulatory frameworks is becoming standard. However, there is no one-size-fits-all assessment criteria in the private sector. A database containing customer's personal identifiable information (PII) will be subjected to different

levels of scrutiny when compared to a physical production line database containing quality-related information.

To address this, established methods such as the NIST frameworks, Department of Defense's Cybersecurity Maturity Model Certification (CMMC), and the Department of Energy's C2M2 maturity model (Department of Energy 2022) can provide a blueprint for assessing suppliers based on an organization's specific context and needs. For example, the C2M2 model defines 10 cybersecurity domains such as risk management, cybersecurity architecture, and identity and access management. Each domain comes with its own set of objectives and practices that can be used to assess an organization's cybersecurity capability.

In addition to aforementioned frameworks and certifications such as ISO 27001, ISO 28000, or SOC2, an organization should strive to use assessment methods and requirements specific to the industry's unique needs. Firstbrook et al. (2022) provided a good example of the items that can be assessed in a digital supply chain context:

- Internal security controls based on industry best practices and standards.
- Documented secure design processes and engineering practices.
- Bill of materials (BOMs) for components, products, and services that encompasses firmware, software, and hardware that includes codes.
- Cybersecurity management programs and incidence response plan.
- Established procurement process with controlled approved vendors.

Identify and Report Capability Gap

Once the assessment is complete, the organization will need to **identify the supplier's capability gap with requirements**. This allows the organization to understand the supplier's current status and any capability gaps that the supplier may have in meeting the established cybersecurity requirements. The capability gap identified is heavily dependent on the requirements and processes used to assess the supplier in the previous step. This can come in the form of individual checklist items or an

aggregated maturity level from a group of controls, processes, and technology. For example, the client organizations may have identified an individual finding, such as physical devices and systems not being inventoried, as part of their assessment checklist. Alternatively, in the case of the C2M2 model, the supplier may have received a MIL1 for "Control logical Access" within the Identity and Access Management domain. This may be lower than the client's MIL2 requirement, as the client requires logical access to incorporate the principle of least privilege. The information gathered during this step can then be used to evaluate whether the current gap warrants further investment and capability building to mitigate any associated risks.

The final step within the Assess stage is to **report assessment result to internal stakeholders**, including cross-functional stakeholders and senior management. This step is critical to regroup and align on a decision whether to proceed with subsequent development efforts. The decision should be based on the supplier's strategic alignment with the overall business, risk associated with the supplier's cybersecurity capabilities, and the resource investment needed to develop the suppliers. This ensures that the supplier development efforts are closely aligned with the organization's business and sourcing strategy to increase overall value.

A flowchart of the Assess stage can be seen in Figure 4-4.

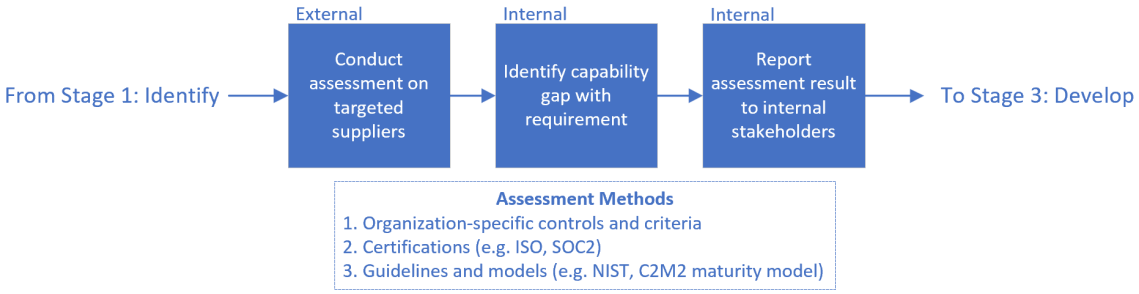

Figure 4-4: The Assess Stage

4.2.2 Assess Stage Example – Click Technologies

After aligning on a set of requirements for each of the three categories of suppliers, the core team assessed Sunlite Inc., which manufactures components that can be

used in Click Technologies' upcoming product. Sunlite Inc. was already in talks with Click Technologies' procurement team and eager to facilitate the assessment process. The core team, along with third-party auditing firm, conducted Sunlite's cybersecurity capability assessment in four key areas: certification/compliance, people and process, information technology (IT), and operational technology (OT). They found that Sunlite's OT area is at maturity level one, falling short of Click Technologies' defined maturity level two. The assessment findings were summarized, documented, and reported as part of the sourcing dashboard update to senior management. It was decided to move forward with Sunlite Inc. as it is crucial to making Click Technologies' supply chain more resilient.

4.3 Develop Stage

4.3.1 Framework Walkthrough

The Develop stage is the primary phase in which various development activities are conducted. It builds upon the success and deliverables of the Identify and Assess stages, utilizing documented requirements, categorized suppliers, and relevant assessment scoring. The stage follows an iterative process that resembles a project management approach, including planning and subsequent execution. Each step is summarized in the order they procedurally appeared.

Plan and Prioritize Development Activities

The stage begins with internal **planning development activities and schedule milestones** based on business needs and task complexity. This planning process is critical for capturing, planning, and documenting any action plans for the capability gaps identified during the Assess stage. The development plan created in this stage is aimed at closing these gaps while being mindful of the wider organizational strategy, including planned roll-in or onboard dates. This approach ensures that the development activities are feasible and aligned with the organization's overall goals.

Examples of development activities includes but are not limited to the following (Department of Energy 2022):

- Establish cybersecurity risk management program.
- Improve IT and OT asset configuration.
- Establish logging and monitoring to maintain situational awareness.
- Create cybersecurity incident response plan to detect, analyze, and respond to incidents.

Next, client organizations **prioritize development activities** internally to optimize resource utilization. The step needs to take limitation imposed by resource into consideration for accurate prioritization (Purnus and Bodea 2014). The Value Triple Constraint model (Baratta 2006) defines the delivery of value as a function of scope and capability, indicating that organizations can maximize the value delivered by appropriately scoping (i.e., prioritizing) the work that needs to be done, given a fixed capability or resource. To prioritize activities, organizations may consider the criticality and severity of the risk associated with the capability being developed.

Aligning deliverables with internal and external stakeholders is conducted after planning and prioritizing development activities to get buy-ins and resources from stakeholders. This is crucial as capability development requires investment in both resources and time. Thus, it will require the buy-in from senior management on both sides to ensure collaboration success (Fortune et al. 2011). Incentives to collaborate can be based on items such as future business opportunities and fast-tracked capability building. The alignment step ensures that strategy, funding, resources, and deliverables are all in sync.

Conduct Supplier Development

To start the iterative development loop, start by **setting phase objective, tasks, and metric** with external suppliers. Clear communication of the objectives and deliverables is critical for successful collaboration and project-based initiatives (Fortune

et al. 2011), ensuring that there are measurable metrics for review and optimize resource usage. A phase is defined as a series of tasks that aggregate to a predefined objective that spans over a period of manageable timeframe. This may come in the form of expert judgment, natural breakpoints and phase gates within a standard software development process or grouping of related controls. Multiple phases can be run concurrently with multiple suppliers, provided that there are adequate resources.

Next, **conduct development tasks** based on aligned deliverables to increase supplier's capability. The client organization takes the lead and manages the process, which involves setting up regular review and status update meetings with the supplier to brainstorm solutions, track progress, and potentially pivot when faced with roadblocks. Examples of development tasks includes but are not limited to the following:

- Supplier process review such as cybersecurity management program and SDLC.
- Best practices and process sharing.
- Audits on implemented process and controls.
- Blackbox/whitebox penetration tests.
- Supplier cybersecurity team member interview.
- Physical site visits.

Given the nature of different tasks requiring different levels of involvement, client organization point of contacts will serve as multiple personas during this step, such as reviewer, auditor, and subject-matter-experts. On the subject of investment in capability development, both the client organization and SME supplier should see cybersecurity investment as a necessary business and procurement cost shared by both sides, rather than a separate administrative or compliance cost. Detailed discussion on cybersecurity investment will be done in Chapter 5.

Review Development Result

Wrapping up development, the organization must set a phase gate to **review development phase results** internally to determine and update supplier's capability. This meeting also serves as a post-mortem to review various aspects of the development phase, such as goal setting, supplier management practices, and the feasibility of metrics. This allows the organization to iterate and improve on its own supplier engagement method, development approach, and evaluation process. The phase gate review can have the following decisions:

- *Supplier has satisfied all requirements*: The decision signifies that the targeted supplier has fulfilled or met all aligned requirements and is qualified to be on the AVL or approved for contract signing from a cybersecurity perspective.
- *Further development is needed*: This implies that there are either other development activities to be completed or that further improvement in the current area is needed. The organization then internally **refines development approach** based on lessons learned. This ensures that the organization utilizes the insight gained from the post-mortem and implements a more optimized approach in the next rounds of development.

A flowchart of the Develop stage can be seen in Figure 4-5.

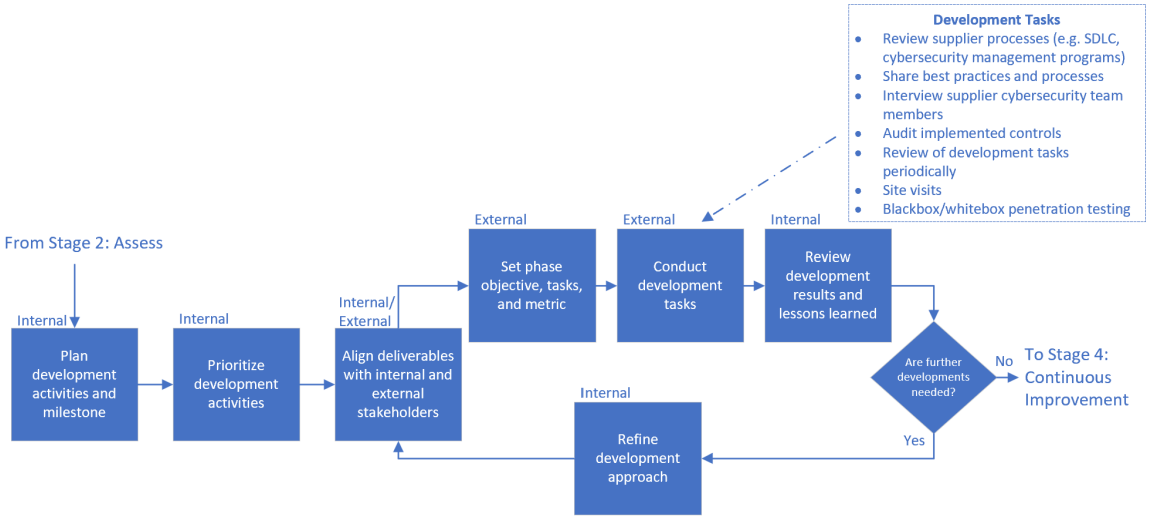

Figure 4-5: The Develop Stage

4.3.2 Develop Stage Example – Click Technologies

To conduct development, the supplier development core team planned Sunlite's capability development based on high-level business alignment between the two organizations that required Sunlite to be fully vetted and qualified in eight months. Six development activities were identified and based on prioritization from a combination of resource needs and risk presented to Click Technologies. The lack of whitelisting, source code review, and file integrity monitoring to minimize the risk of malicious code being installed and executed on OT was identified as the most critical activity to be developed and enabled. The final plan and deliverables received buy-in from both Click Technologies and Sunlite's management team.

The team at Click Technologies started working with Sunlite's point of contacts on formalizing bi-weekly dashboard meetings where status and blockers are reported and cleared. After a regular cadence was set up, among other development efforts, the team shared best practices in securing against cyberattacks on the production line with Sunlite. The team also conducted site visits/audits and penetration testing to assess Sunlite's capability improvements.

After six weeks of development, the core team at Click Technologies reviewed the phase results of the various parallel development efforts. While most efforts were successful, it was found that Sunlite had a number of older production equipment that were not easily updated to meet current cybersecurity requirements. The cross-functional team members within the core team discussed and refined the requirements with this limitation in mind and went through another cycle of development with Sunlite. This time, they ensured that the added clauses and refined approach could still mitigate cybersecurity risks.

After finishing all development activities, the core team aligned to consider the development a success and approved the cybersecurity capabilities section in Sunlite's onboarding dashboard.

4.4 Continuous Improvement Stage

4.4.1 Framework Walkthrough

The Continuous Improvement stage is the final stage of the supplier development process. It serves as an iterative process, unlike traditional continuous monitoring. This stage not only monitors, responds, and improves on current processes but also have periodic checkpoints to assess and determine any additional supplier development needs. These periodic checkpoints complete the feedback loop between supplier development and subsequent collaborative improvement efforts. They give organizations an option to reinitiate additional development activities if necessary.

The organization initiates the stage by **forming contractual agreement with suppliers**. This may be service contracts or formal recognition of approved/qualified supplier status. These agreements should include a commitment from the suppliers to uphold the cybersecurity standards and requirements established during the development process. Once suppliers are onboarded, both parties should maintain their respective development teams to ensure a single-threaded owner and point of contact for subsequent continuous improvement efforts.

Form Continuous Improvement Review Cadence

Following entry into an official collaborative relationship, the organization should **form regular review cadence on supplier's cybersecurity capabilities** to monitor their operational status. This should include determining the scope of what is being reviewed, the frequency at which those items are reviewed, and the method at which each item is tested and reviewed. These key checkpoints and metrics can be used by the organization to communicate expectations to suppliers and to determine whether additional development efforts are needed in the future. For example, the organization may choose to audit a set of agreed-upon security controls on a quarterly basis, using a combination of automated monitoring and report-based confirmation with relevant proof. With a regular review cadence, the organization can ensure that

supplier's continued efforts remain aligned with the organization's requirement and can respond quickly to any changes or developments in the supplier's cybersecurity capabilities.

Collaborate On Continuous Improvement

The process enters an iterative feedback loop after establishing and communicating the requirements and cadence. This loop commences with **periodic reviews and automated monitoring** of various metrics and the supplier's status. If the supplier is still compliant with the outlined requirements, the organization continues to **collaborate with supplier on continuous improvement in capability**, further reducing future cybersecurity risk. The organization can further **refine requirements with suppliers from lessons learned** and new needs based on newly available technology, processes, and threat landscape to keep up with the ever-evolving environment. However, if the supplier's capability falls below the outlined requirements, the Continuous Improvement stage feeds back into the Develop stage. This ensures the organization can work with their suppliers to quickly close any capability gaps identified during the Continuous Improvement stage.

The Continuous Improvement stage not only provides a feedback loop to the Develop stage, but it also has the potential to interface with an organization's existing cybersecurity incident or risk management programs to create additional value. The management programs have internal best practices for monitoring and improvement that can be leveraged by the supplier development team. Additionally, an organization's supply chain cyber risk is a crucial part of its risk management system. Therefore, status updates and audit findings from the continuous improvement efforts on the supplier side can be shared with the internal incident or risk management programs to improve risk assessment metrics. This integration of supplier development and risk management efforts can lead to a more comprehensive and effective cybersecurity strategy.

A flowchart of the Continuous Improvement stage can be seen in Figure 4-6.

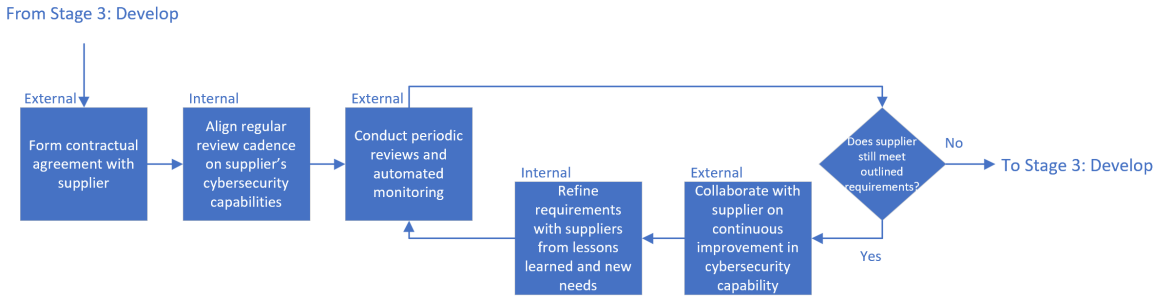

Figure 4-6: The Continuous Improvement Stage

4.4.2 Continuous Improvement Stage Example – Click Technologies

After successfully meeting various business, engineering, quality, and cybersecurity requirements, Sunlite was officially qualified as a part of the AVL. During the agreement signing, the sourcing team embedded clauses that require Sunlite to fully comply with the cybersecurity requirements set forth during the development process throughout the contract's duration and support any continuous improvement activities.

Once Sunlite was fully onboarded, the development core team set up regular review meetings and automated monitoring to work with Sunlite's team on monitoring and improving various capabilities and metrics. During one of the review meetings, it was discovered that, during a site audit, new production equipment had not been properly vetted before being connected to the factory network. This caused malware to slip into Sunlite's internal networks.

Sunlite took swift action to remove any malware within their systems. However, the team at Click Technologies decided to reinitiate another round of Sunlite capability development to improve their process in qualifying and commissioning equipment with software packages. This decision was made after internal discussions and alignment with management.

Reinitiating supplier development on an existing supplier allowed Click Technologies to conduct cyber risk reduction on a rolling basis and mutually build capability with suppliers. This approach would help Sunlite improve its cybersecurity protocols

and strengthen its position as a trusted supplier for Click Technologies.

Overall, Click Technologies' proactive approach to supplier development in cybersecurity helped prevent a potential breach and demonstrated the company's commitment to cybersecurity best practices.

Chapter 5

Discussion

The study proposes a four-stage client-side process for supplier's cybersecurity capability development. The process is used by large client organizations with mature cybersecurity capabilities when potential SME suppliers are identified and before entering into contractual agreements with these suppliers. The process bridges the gap that currently exists between supplier assessment and monitoring in cybersecurity management research and industry practices. While the framework has received positive feedback from industry experts, there are several items that warrant further discussion. These will be covered in the following sections.

Framework Application

The cybersecurity supplier development framework is designed to be modular, which allows flexibility in framework adoption to cater to unique organizational settings. While the framework is holistically designed to holistically serve as an end-to-end supplier qualification and onboarding process to assess, develop, and continuously improve supplier capability. The modularity allows each stage to be able to be utilized independently to augment established business and operation processes within an organization. Taking a holistic view can help identify key elements in an end-to-end process to facilitate adoption of the framework. With its modular design, organizations can choose to adopt certain stages of the process to address it's specific needs and challenges.

Additionally, the framework is developed with the assumption that the client organization is working to enhance supplier capability before fully integrating them into the organization's supplier ecosystem. However, the feedback loop between the Develop and Continuous Improvement stages highlights the iterative nature of this process. So, the framework can be used not only to onboard new suppliers but also to initiate capability development and improvement among the existing supply base with minimal modification. By renegotiating current contracts or documenting new statement-of-work (SOW) with the current suppliers after Develop stage, the client organization can initiate capability development with current suppliers while also documenting the updated requirements at the end of such stage.

Lastly, in addition to being a modular and iterative process, as stated above, the effectiveness and stability of the cybersecurity supplier development process heavily relies on common business goals and transparent documentation. While the Develop and Continuous Development stages are critical as they are seen as the most essential stages of the process, their success depends on the output from the Identify and Assess stages. It is crucial to ensure that the suppliers being developed are aligned with organizational goals and that documentation related to requirements, current status, and capability gaps is thoroughly validated. This ensures effective and efficient use of development resources and ultimately leads to a successful supplier ecosystem.

Cybersecurity Investment

While we assumed that supplier development is an independent process that exists in parallel to other business processes, in our conversation with industry experts, they commented investment and funding hindrances could make it difficult for any organizations to implement effective cybersecurity initiatives. The area of cybersecurity investments is also echoed by Melnyk et al. (2022) in their review of past research and highlighted as an area that requires future investigations. Looking at how businesses are run in the industry and research, we identified specific trends and best practices that can serve as a guidepost for the future.

Organizations and businesses, even the SMEs, should start treating cybersecu-

rity capability building as part of the business and procurement cost instead of an added investment. When it comes to regulatory requirements, the cost of meeting cybersecurity standards is part of the cost of doing business as these requirements tend to be mandatory, which implies a higher barrier to entry to the market. However, in many cases of non-regulated requirements, SME suppliers can adjust their quotes based on the customer's requirements. Corporations search for suitable suppliers by releasing a request for quotation (RFQ), which is a document that requests a quote or bid for specific goods or services. The RFQ typically outlines the buyer's requirements, including the quantity and quality of the goods or services and other information needed for a quote. In the case of investment in cybersecurity capability building to meet customer needs, the SME suppliers can amortize the investment cost into the unit price of the product or service they are providing, or if provided a guaranteed business volume, amortize the cost over the contract duration. Besides the approaches mentioned above, academic research also proposed similar business-induced investments. Bandyopadhyay, Jacob, and Raghunathan (2010) noted that the implementation of a liability scheme for cybersecurity in firm-to-firm collaboration could impact cybersecurity investment. The risk of financial loss from security breaches incentivizes organizations to increase investment to a socially optimal level.

In addition to monetary returns, organizations may also derive intangible value from collaborative capability investment. SME suppliers looking to expand their market penetration sometimes work at cost parity or at a loss to engage and qualify as approved vendors for "big-name" customers. The status of being on the approved vendor list will cement the supplier's capability and reputation. Furthermore, an SME supplier could potentially gain access to resources, information, and best practices they would have otherwise not had access to. Being developed by a larger corporation will accelerate the supplier's growth to create value in the long term.

In summary, we believe that it is important to view cybersecurity investment as a necessary business and procurement cost shared by both clients and suppliers, rather than a separate administrative or compliance cost. Large client organizations can still benefit from the added cost resulting from supplier cybersecurity investment, as it

will result in lower risk and increased value generated. For SME suppliers, investing in cybersecurity can be viewed as a way to increase business value, unlocking new markets and improving their reputation.

Securing Supply Chain as a Competitive Necessity

In addition to discussion on different applications and potential funding sources to successfully conduct supplier development, the strategic importance of securing an organization's supply chain by developing a supplier's cybersecurity capability must be highlighted.

First, supplier development in cybersecurity capability is closely tied to an organization's sourcing strategy. During our conversation with a security hardware company's Chief Information Security Officer (CISO), we learned that they conduct most R&D efforts in-house and source components from various suppliers. Their approach to supply chain cybersecurity is to work on a need-to-know basis or zero-trust basis with their hardware suppliers. With less than 20 different products, this is easier to manage as there are limited potential failure points. However, as businesses grow and product offerings diversify, sourcing and co-development models will also expand and diversify. Thus, it becomes necessary to collaborate with business partners and suppliers more closely to remain competitive. Under this context, a supplier development process can increase the potential supplier pool, especially since SMEs' current cybersecurity capability will no longer be a gating factor. Large client organizations can work with SMEs on improving their capability to lower risk and ensure a standardized competency across the entire supply base.

The supplier development and continuous improvement process not only expands the organization's potential supplier pool but also provides a 360-degree view of the organization's cybersecurity capability and risk assessment. This can be achieved by integrating the data gained about the supplier during the entire four-stage process, which contains not only supplier profile and status but also continuous updates on their capabilities. This allows the organization to map out a more comprehensive cybersecurity risk management plan by considering risks associated with the

organization itself and those stemming from the interfaces with other third-party stakeholders.

Managerial Implications

Besides its theoretical contribution in bridging the procedural gap that exists between assessment and monitoring, a cybersecurity supplier development process has real-world managerial implications that contribute to benefiting managers and the broader organization in the following ways:

In the recent years, sourcing strategies have become a source of competitive advantage in the ever-evolving market. Organizations can **build a security-centric business strategy** by making the supplier cybersecurity development process an indispensable part of supplier qualification. Implementing an iterative cybersecurity development process can create a virtuous loop of security-conscious decision-making in areas such as supplier collaboration and mutual improvements both internal and external to the organization, which is crucial in today's increasingly digital landscape.

In addition to organizational strategy, organizations can have **a wider potential supplier pool** to source from, because a supplier's initial cybersecurity capability will no longer be a gating factor in supplier selection. This can lead to the organization gaining a more competitive edge within the industry. Qualified suppliers can have **more consistent supplier competency** by formalizing and documenting the development process. This allows the client organization to enact a consistent set of requirements and approaches in supply chain cybersecurity management. This ensures consistency in cybersecurity capabilities and resilience across both existing and new supply chain partners who have gone through the process. The newfound consistency can lead to more stable services and fewer shortage in physical products, which in turn increases **value generation** in the entire supply chain. This is reminiscent of the benefits highlighted in class supplier development research (Friedl and Wagner 2012).

The proactive, hands-on engagement of suppliers can also **increase transparency** and visibility into supply chain partners, improving resilience and trust between stake-

holders, which is becoming increasingly important for end customers and stakeholders who wanted to know how products are sourced and how data are protected. Additionally, it is clear that most organizational cybersecurity risk assessments and management efforts are reactionary and sometimes fragmented (Jarjoui and Murimi 2021). Through the increased transparency into its supply chain, an organization's cybersecurity management programs can conduct **better risk management** efforts because of the proactive engagement in joint decision-making with supply chain partners in the discovery and mitigation of potential negative externalities (Li and Xu 2021).

Engaging in supplier development can also help organizations **gain reputation** points by demonstrating a commitment to cybersecurity and responsible sourcing practices. This can lead to increased customer loyalty and trust. Additionally, a supplier can demonstrate cybersecurity capability by being vetted by large client organizations and committing to capability building, which increases their value as a potential business partner.

Chapter 6

Conclusion and Future Work

Organizations often collaborate and source from a wide range of suppliers and business partners to create more value for the organization and their customers. However, sometimes potential risks and side effects are overlooked in the interest of meeting business needs. As a design engineer at a major consumer electronics manufacturer, I experienced firsthand the negative impact that supplier capability issues could have on a company's reputation for quality. Often, we were forced to address design and quality issues resulting from a supplier's engineering capability not meeting our standards. The delicate balance of maintaining a sufficient number of suppliers to meet demand and delivering best-in-class quality posed a significant risk by coupling supplier capability with organization reputation. By introducing a supplier development process, we are able to front-load our efforts in developing suppliers' capabilities to deal with issues before they propagated down the supply chain. This helped us drastically reduce unplanned work and minimize organizational risk.

With those experiences in an organizational context, we developed a four-stage cybersecurity supplier development process designed to enhance the capabilities of SME suppliers and facilitate their successful onboarding into an organization's ecosystem. The process includes the Identify, Assess, Develop, and Continuous Improvement stages. It is also designed to be modular and can be easily adapted to work with different organizations and industries and supplier management practices.

Using this process, managers and executives can hope to bring value to both the

organizations and the broader supply chain ecosystem. We have identified several key actionable insights from the development of the process:

Strategic Alignment – Security Centric Business Strategy

Managers can build a culture of security-conscious business decisions by integrating supplier development process in sourcing strategies.

Reach - Increasing Potential Supplier Pool and Consistency

Increases potential supplies to source from and consistency in current supplier's cybersecurity capability for better supplier and supply chain management.

Risk Management - Gaining Visibility and Decreasing Risk

Organizations can gain visibility into supply chain cyber risks from suppliers and business partners and thus implement a more comprehensive risk management plan.

Although the framework has real-world applicability and impact, the study made some assumptions and generalizations that can benefit from further research:

Limitations and Suggestions for Future Research

First, the study assumed that the supplier development process is initiated by a larger client organization working with and developing a less mature SME supplier. While this is generally true in a capability development process, future studies could explore collaborative capability building in the context of two organizations similar in size and cybersecurity capability but with different security cultures and methodologies.

Second, an essential aspect of successful supplier development is the categorization and prioritization of suppliers within an organization's development strategy. The current model assumes the prioritization scheme to be an exogenous input based on a combination of business and risk management needs in sourcing. However, future

research could fine-tune the supplier development process by investigating prioritization methods for suppliers undergoing the development process. Suitable prioritization methods would allow organizations to optimize resource expenditure in the development process by prioritizing critical-to-security suppliers.

Lastly, further research can be conducted to compare the overall supply chain benefit gained from the mutual capability building during the supplier development process. As noted in the previous section, there isn't a clear link between cybersecurity and the overarching business strategy, with cybersecurity investment being relegated to a purely risk management and regulatory issue. By conducting investigations into the increase in value generation across the entire supply chain as a system resulting from supplier development efforts, cybersecurity co-investment across organizations can be better linked to the broader business strategy and the value security-centric strategies can bring to the table

Appendix A

Figures

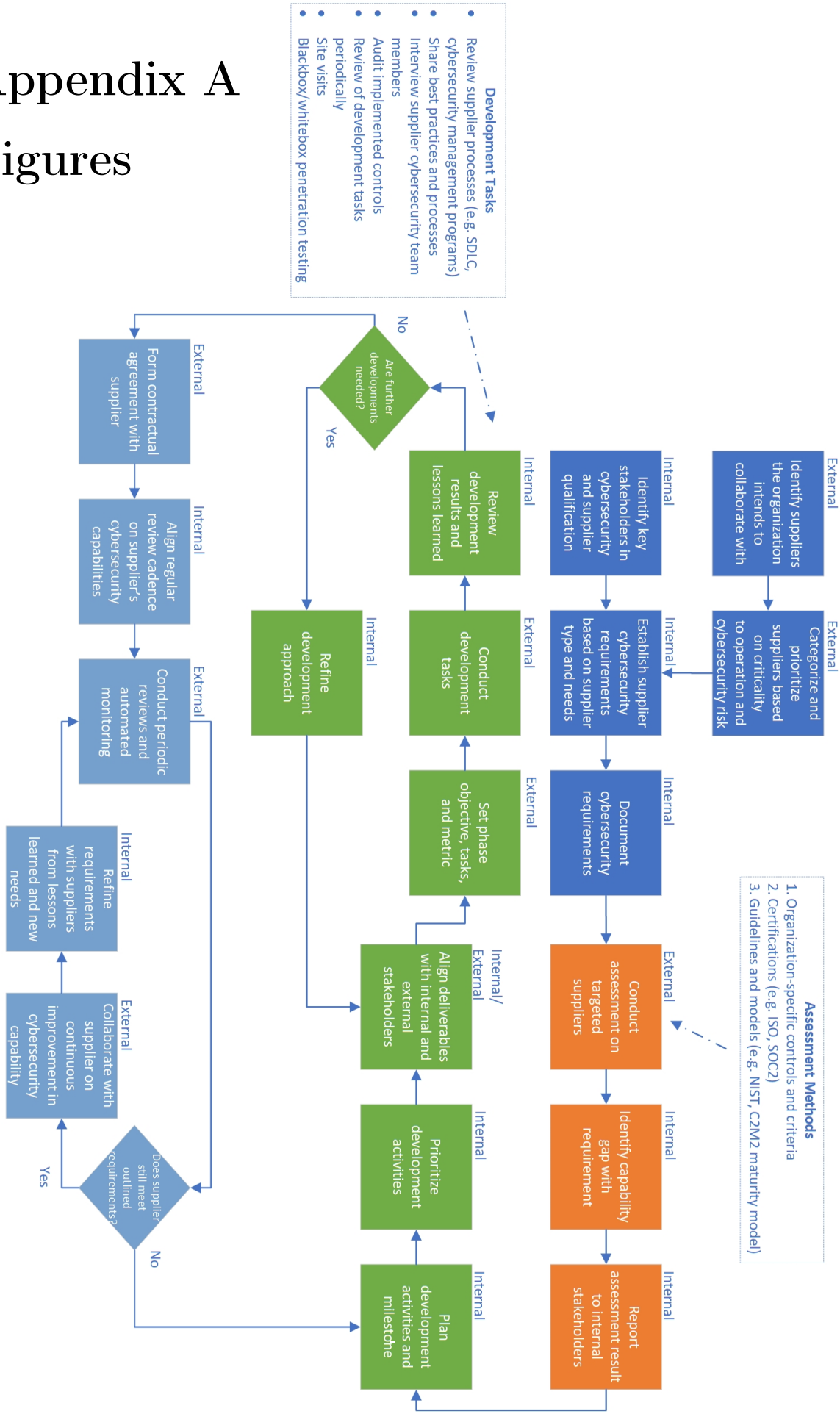

Figure A-1: Supplier Development Process Flowchart

Bibliography

Amazon. 2022. "AWS Investing an Additional $10 Million in Open Source Supply Chain Security | AWS Open Source Blog." Section: Announcements, May 13, 2022. Accessed March 23, 2023. https://aws.amazon.com/blogs/opensource/aws-investing-an-additional-10-million-in-open-source-supply-chain-security/.

———. n.d. "Shared Responsibility Model - Amazon Web Services (AWS)." Amazon Web Services, Inc. Accessed March 23, 2023. https://aws.amazon.com/compliance/shared-responsibility-model/.

Bandyopadhyay, Tridib, Varghese Jacob, and Srinivasan Raghunathan. 2010. "Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest." *Information Technology and Management* 11, no. 1 (March 1, 2010): 7–23. ISSN: 1573-7667, accessed March 18, 2023. https://doi.org/10.1007/s10799-010-0066-1. https://doi.org/10.1007/s10799-010-0066-1.

Baratta, Angelo. 2006. "The triple constraint: a triple illusion." PMI® Global Congress 2006. Seattle, WA: PA: Project Management Institute. Accessed March 14, 2023. https://www.pmi.org/learning/library/triple-constraint-erroneous-useless-value-8024.

Benz, Michael, and Dave Chatterjee. 2020. "Calculated risk? A cybersecurity evaluation tool for SMEs." *Business Horizons* 63, no. 4 (July): 531–540. ISSN: 00076813, accessed November 22, 2022. https://doi.org/10.1016/j.bushor.2020.03.010. https://linkinghub.elsevier.com/retrieve/pii/S0007681320300392.

Better Business Bureau. 2017. "2017 State of Cybersecurity Among Small Businesses in North America." Accessed October 5, 2022. https://saginllc.com/wp-content/uploads/2017/10/Cybersecurity_FINAL_LoRes_Embargoed.pdf.

Bitsight. n.d. "BitSight Security Ratings | BitSight." Accessed March 24, 2023. https://www.bitsight.com/security-ratings.

Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi. 2021. *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry.* NIST Internal or Interagency Report (NISTIR) 8276. National Institute of Standards and Technology, February 11, 2021. Accessed March 24, 2023. https://doi.org/10.6028/NIST.IR.8276. https://csrc.nist.gov/publications/detail/nistir/8276/final.

Boyens, Jon, Angela Smith, Nadya Bartol, Kris Winkler, Alex Holbrook, and Matthew Fallon. 2022. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.* NIST Special Publication (SP) 800-161 Rev. 1. National Institute of Standards and Technology, May 5, 2022. Accessed March 24, 2023. https://doi.org/10.6028/NIST.SP.800-161r1. https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final.

Chen, Patrick. 2021. "Small Business Cybersecurity Statistics: 42% attacked in last year," accessed March 2, 2023. https://advisorsmith.com/data/small-business-cybersecurity-statistics/.

Christopher, Martin. 1998. "Logistics and Supply Chain Management: Strategies for Reducing Cost and Improving Service 2e." *International Journal of Logistics Research and Applications* 2 (1): 103–104. ISSN: 1367-5567, 1469-848X, accessed March 22, 2023. https://doi.org/10.1080/13675569908901575.

CSIS. 2020. "Significant Cyber Incidents Since 2006." Accessed November 6, 2022. https://csis-website-prod.s3.amazonaws.com/s3fs-public/200626_Cyber_Events.pdf.

Dell. 2021. *Dell Fiscal Year 22 Supply Chain Sustainability Summary.* Accessed March 22, 2023. https://www.dell.com/en-uk/dt/corporate/social-impact/esg-resources/reports.htm.

———. 2023. *A Partnership of Trust: Dell Supply Chain Security.* Accessed March 23, 2023. https://i.dell.com/sites/csdocuments/CorpComm_Docs/en/supply-chain-assurance.pdf.

Department of Energy. 2022. "Cybersecurity Capability Maturity Model (C2M2)." Energy.gov. Accessed April 11, 2023. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.

Emer, Asja, Marco Unterhofer, and Erwin Rauch. 2021. "A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises." *IEEE Engineering Management Review* 49, no. 2 (June 1, 2021): 98–109. ISSN: 0360-8581, 1937-4178, accessed November 22, 2022. https://doi.org/10.1109/EMR.2021.3078077. https://ieeexplore.ieee.org/document/9424999/.

Epiq. n.d. "What is a BitSight Rating and Why Should You Consider Using It." Accessed March 24, 2023. https://www.epiqglobal.com/en-us/resource-center/articles/what-is-a-bitsight-rating.

Firstbrook, Peter, Sam Olyaei, Pete Shoard, and Katell Thielemann. 2022. "Top Trends in Cybersecurity 2022." Gartner, February 18, 2022. Accessed March 5, 2023. https://www.gartner.com/en.

Fortune, Joyce, Diana White, Kam Jugdev, and Derek Walker. 2011. "Looking again at current practice in project management." Publisher: Emerald Group Publishing Limited, *International Journal of Managing Projects in Business* 4, no. 4 (January 1, 2011): 553–572. ISSN: 1753-8378, accessed March 13, 2023. https://doi.org/10.1108/17538371111164010. https://doi.org/10.1108/17538371111164010.

Friedl, Gunther, and Stephan M. Wagner. 2012. "Supplier development or supplier switching?" *International Journal of Production Research* 50, no. 11 (June 1, 2012): 3066–3079. ISSN: 0020-7543, accessed March 15, 2023. https://doi.org/10.1080/00207543.2011.588804. https://doi.org/10.1080/00207543.2011.588804.

Gartner. 2022a. "Gartner Says Worldwide PC Shipments Declined 19.5% in Third Quarter of 2022." Gartner. Accessed March 22, 2023. https://www.gartner.com/en/newsroom/press-releases/2022-10-10-gartner-says-worldwide-pc-shipments-declined-19-percent-in-third-quarter-of-2022.

———. 2022b. "The 2022 Strategic Supply Chain Technology Themes." Gartner, March 25, 2022. Accessed March 5, 2023. https://www.gartner.com/en.

Ghadge, Abhijeet, Maximilian Weiß, Nigel D. Caldwell, and Richard Wilding. 2019. "Managing cyber risk in supply chains: a review and research agenda." *Supply Chain Management: An International Journal* 25, no. 2 (November 17, 2019): 223–240. ISSN: 1359-8546, 1359-8546, accessed November 22, 2022. https://doi.org/10.1108/SCM-10-2018-0357. https://www.emerald.com/insight/content/doi/10.1108/SCM-10-2018-0357/full/html.

Haranas, Mark. 2019. "Michael Dell's 5 Biggest Statements At Dell Technologies World." CRN, April 29, 2019. Accessed March 23, 2023. https://www.crn.com/slide-shows/storage/michael-dell-s-5-biggest-statements-at-dell-technologies-world.

Harland, C.M. 1996. "Supply Chain Management: Relationships, Chains and Networks - Harland - 1996 - British Journal of Management - Wiley Online Library." *British Journal of Management,* accessed March 22, 2023. https://doi.org/https://doi.org/10.1111/j.1467-8551.1996.tb00148.x. https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-8551.1996.tb00148.x.

Heidt, Margareta, Jin P. Gerlach, and Peter Buxmann. 2019. "Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments." *Information Systems Frontiers* 21, no. 6 (December 1, 2019): 1285–1305. ISSN: 1572-9419, accessed March 23, 2023. https://doi.org/10.1007/s10796-019-09959-1. https://doi.org/10.1007/s10796-019-09959-1.

Infosec Institute. 2015. "Cyber Security Risk in Supply Chain Management: Part 1." Infosec Resources. Accessed March 11, 2023. https://resources.infosecinstitute.com/topic/cyber-security-in-supply-chain-management-part-1/.

ISO. 2007. *ISO 28001:2007.* Accessed April 4, 2023. https://www.iso.org/standard/45654.html.

———. 2022. "ISO 28000:2022(en), Security and resilience — Security management systems — Requirements." Accessed March 24, 2023. https://www.iso.org/obp/ui/#iso:std:iso:28000:ed-2:v1:en.

IT PRO. 2018. "TSMC cyber attack was apparently caused by WannaCry." IT PRO. Accessed March 3, 2023. https://www.itpro.com/security/31629/tsmc-cyber-attack-was-apparently-caused-by-wannacry.

Jarjoui, Samir, and Renita Murimi. 2021. "A Framework for Enterprise Cybersecurity Risk Management." In *Advances in Cybersecurity Management,* edited by Kevin Daimi and Cathryn Peoples, 139–161. Cham: Springer International Publishing. ISBN: 978-3-030-71381-2, accessed March 16, 2023. https://doi.org/10.1007/978-3-030-71381-2_8. https://doi.org/10.1007/978-3-030-71381-2_8.

Kabanda, Salah, Maureen Tanner, and Cameron Kent. 2018. "Exploring SME cybersecurity practices in developing countries." *Journal of Organizational Computing and Electronic Commerce* 28, no. 3 (July 3, 2018): 269–282. ISSN: 1091-9392, 1532-7744, accessed November 22, 2022. https://doi.org/10.1080/10919392.2018.1484598. https://www.tandfonline.com/doi/full/10.1080/10919392.2018.1484598.

Kaspersky. 2019. "Operation ShadowHammer," March 25, 2019. Accessed March 22, 2023. https://securelist.com/operation-shadowhammer/89992/.

Kerner, Sean M. 2022. "Colonial Pipeline hack explained: Everything you need to know." WhatIs.com. Accessed March 22, 2023. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

Krause, Daniel R. 1997. "Supplier Development: Current Practices and Outcomes." *International Journal of Purchasing and Materials Management* 33, no. 1 (March): 12–19. ISSN: 10556001, accessed November 22, 2022. https://doi.org/10.1111/j.1745-493X.1997.tb00287.x. https://onlinelibrary.wiley.com/doi/10.1111/j.1745-493X.1997.tb00287.x.

Krumay, Barbara, Edward W. N. Bernroider, and Roman Walser. 2018. "Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework." In *Secure IT Systems,* edited by Nils Gruschka, 369–384. Lecture Notes in Computer Science. Cham: Springer International Publishing. ISBN: 978-3-030-03638-6. https://doi.org/10.1007/978-3-030-03638-6_23.

Li, Sali, Anoop Madhok, Gerhard Plaschka, and Rohit Verma. 2006. "Supplier-Switching Inertia and Competitive Asymmetry: A Demand-Side Perspective*." _Eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1540-5414.2006.00138.x, *Decision Sciences* 37 (4): 547–576. ISSN: 1540-5915, accessed March 15, 2023. https://doi.org/10.1111/j.1540-5414.2006.00138.x. https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1540-5414.2006.00138.x.

Li, Yanhui, and Lu Xu. 2021. "Cybersecurity investments in a two-echelon supply chain with third-party risk propagation." Publisher: Taylor & Francis _eprint: https://doi.org/10.1080/00207543.2020.1721591, *International Journal of Production Research* 59, no. 4 (February 16, 2021): 1216–1238. ISSN: 0020-7543, accessed March 19, 2023. https://doi.org/10.1080/00207543.2020.1721591. https://doi.org/10.1080/00207543.2020.1721591.

Lomas, Natasha. 2017. "CCleaner supply chain malware targeted tech giants." TechCrunch, September 21, 2017. Accessed March 22, 2023. https://techcrunch.com/2017/09/21/ccleaner-supply-chain-malware-targeted-tech-giants/.

McCarthy, Justin. 2023. "SOC 2 Compliance: 2023 Complete Guide | StrongDM." Accessed March 24, 2023. https://www.strongdm.com/soc2/compliance.

McMillan, Robert, and Dustin Volz. 2021. "China-Linked Hack Hits Tens of Thousands of U.S. Microsoft Customers." *Wall Street Journal* (March 6, 2021). ISSN: 0099-9660, accessed March 22, 2023. https://www.wsj.com/articles/china-linked-hack-hits-tens-of-thousands-of-u-s-microsoft-customers-11615007991.

Meir, Miryam. 2021. "What is a Cybersecurity Assessment? (Definition & Types)." SecurityScorecard, January 19, 2021. Accessed April 11, 2023. https://securityscorecard.com/blog/what-is-a-cybersecurity-assessment-definition-types/.

Melnyk, Steven A., Tobias Schoenherr, Cheri Speier-Pero, Chris Peters, Jeff F. Chang, and Derek Friday. 2022. "New challenges in supply chain management: cybersecurity across the supply chain." *International Journal of Production Research* 60, no. 1 (January 2, 2022): 162–183. ISSN: 0020-7543, 1366-588X, accessed November 22, 2022. https://doi.org/10.1080/00207543.2021.1984606. https://www.tandfonline.com/doi/full/10.1080/00207543.2021.1984606.

Modi, Sachin B., and Vincent A. Mabert. 2007. "Supplier development: Improving supplier performance through knowledge transfer." *Journal of Operations Management* 25, no. 1 (January): 42–64. ISSN: 02726963, accessed November 22, 2022. https://doi.org/10.1016/j.jom.2006.02.001. http://doi.wiley.com/10.1016/j.jom.2006.02.001.

NCC Group. 2022. *Insight Space: Supply Chain Risk: A back door for hackers?* -. Accessed March 22, 2023. https://www.nccgroup.com/media/jj4ln5so/105503_ncc_insight_space_issue_6_no_dividers_v3.pdf.

NCSC. 2022. "How to assess and gain confidence in your supply chain cyber security." Accessed March 24, 2023. https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security.

Newman, Lily Hay. 2018. "Inside the Unnerving Supply Chain Attack That Corrupted CCleaner." Section: tags, *Wired,* ISSN: 1059-1028, accessed March 22, 2023. https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/.

NIST. 2018. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.* NIST CSWP 04162018. Gaithersburg, MD: National Institute of Standards and Technology, April 16, 2018. Accessed March 24, 2023. https://doi.org/10.6028/NIST.CSWP.04162018. http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Oliver, R. K., and M.D. Webber. 1982. "Supply-chain management: logistics catches up with strategy." *Outlook* 5 (1).

Purnus, Augustin, and Constanta-Nicoleta Bodea. 2014. "Project Prioritization and Portfolio Performance Measurement in Project Oriented Organizations." *Procedia - Social and Behavioral Sciences,* Selected papers from the 27th IPMA (International Project Management Association), World Congress, Dubrovnik, Croatia, 2013, 119 (March 19, 2014): 339–348. ISSN: 1877-0428, accessed March 14, 2023. https://doi.org/10.1016/j.sbspro.2014.03.039. https://www.sciencedirect.com/science/article/pii/S1877042814021302.

Quayle, Michael. 2000. "Supplier Development for UK Small and Medium-sized Enterprises." Publisher: Routledge _eprint: https://doi.org/10.1080/713674361, *Journal of Applied Management Studies* 9, no. 1 (June 1, 2000): 117–133. ISSN: 1360-0796, accessed March 22, 2023. https://doi.org/10.1080/713674361. https://doi.org/10.1080/713674361.

Schuh, Christian, Wolfgang Schnellbacher, Alenka Triplat, and Daniel Weise. 2022. *Profit from the Source: Transforming Your Business by Putting Suppliers at the Core.* Boston, Massachusetts: Harvard Business Review Press, June 21, 2022. ISBN: 978-1-64782-139-5.

SecurityScorecard. 2020. "A Deep Dive in Scoring Methodology." SecurityScorecard. Accessed March 24, 2023. https://securityscorecard.com/resources/deep-dive-scoring-methodology/.

Smith, G. E., K. J. Watson, W. H. Baker, and J. A. Pokorski II. 2007. "A critical balance: collaboration and security in the IT-enabled supply chain." Publisher: Taylor & Francis _eprint: https://doi.org/10.1080/00207540601020544, *International Journal of Production Research* 45, no. 11 (June 1, 2007): 2595–2613. ISSN: 0020-7543, accessed March 23, 2023. https://doi.org/10.1080/00207540601020544. https://doi.org/10.1080/00207540601020544.

Stadtler, Hartmut. 2005. "Supply chain management and advanced planning—basics, overview and challenges." *European Journal of Operational Research,* Supply Chain Management and Advanced Planning, 163, no. 3 (June 16, 2005): 575–588. ISSN: 0377-2217, accessed March 22, 2023. https://doi.org/10.1016/j.ejor.2004.03.001. https://www.sciencedirect.com/science/article/pii/S0377221704001183.

Symantec. 2019. "ASUS Software Updates Used for Supply Chain Attacks." Accessed March 22, 2023. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/asus-supply-chain-attack.

Synopsys. n.d. "What Is Software Supply Chain Security and How Does It Work?" Accessed March 22, 2023. https://www.synopsys.com/glossary/what-is-software-supply-chain-security.html.

Temple-Raston, Dina. 2021. "A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack." *NPR* (April 16, 2021). Accessed March 22, 2023. https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

Turton, William, and Kartikay Mehrotra. 2021. "Hackers Breached Colonial Pipeline Using Compromised Password." *Bloomberg.com* (June 4, 2021). Accessed March 22, 2023. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

Wang, Yulan, Stein W. Wallace, Bin Shen, and Tsan-Ming Choi. 2015. "Service supply chain management: A review of operational models." *European Journal of Operational Research* 247, no. 3 (December 16, 2015): 685–698. ISSN: 0377-2217, accessed March 22, 2023. https://doi.org/10.1016/j.ejor.2015.05.053. https://www.sciencedirect.com/science/article/pii/S0377221715004646.

Yawar, Sadaat Ali, and Stefan Seuring. 2020. "Reviewing and conceptualizing supplier development." Publisher: Emerald Publishing Limited, *Benchmarking: An International Journal* 27, no. 9 (January 1, 2020): 2565–2598. ISSN: 1463-5771, accessed March 22, 2023. https://doi.org/10.1108/BIJ-01-2020-0018. https://doi.org/10.1108/BIJ-01-2020-0018.