29

Supply chain as an attack chain

Booz Allen Hamilton – Bill Stewart, Executive Vice President; Tony Gaidhane, Senior Associate; and Laura Eise, Lead Associate

The supply chain ecosystem reaches farther and wider than ever before. The growing range of suppliers provides significant competitive advantages for companies that strategically and securely source from this global network. Yet this complex footprint comes with an equally complex range of cyberthreats, and the majority of organizations do not realize the breadth and depth of these challenges. However, hackers are well aware of existing supply chain vulnerabilities and are moving aggressively to take advantage of these exposures.

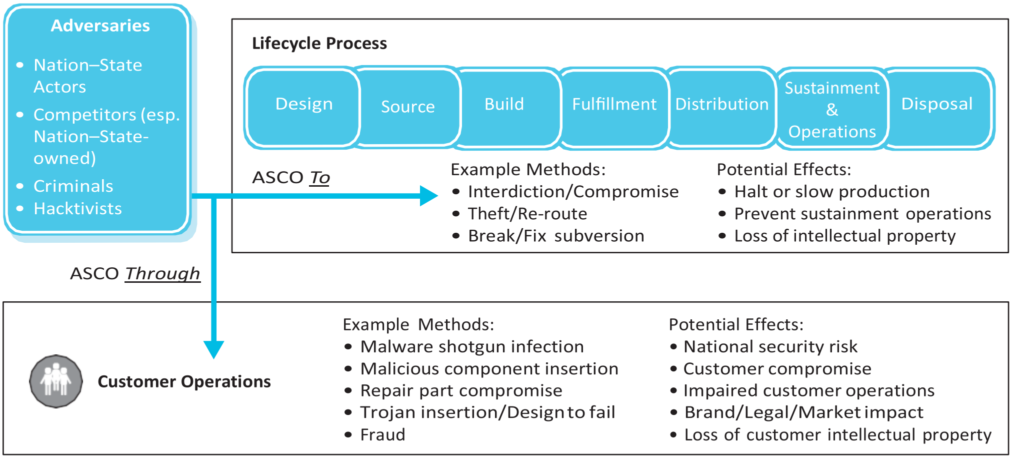
Threat actors typically target organizations' supply chains through two vectors: the first type of attack is known as "adversarial supply chain operations to," or "ASCO To," and the second is known "adversarial supply chain operations through," or "ASCO Through" (Figure 1). In an ASCO To attack, your organization is the direct target. In the latter, the adversary uses your supply chain as a means to target one of your customers. Although the intent is different, both have the potential for devastating impact to your revenue, reputation, and end consumer.

To compound this issue, today's attackers are often well funded and extremely organized. These attackers have the resources, skills, and patience to conduct sophisticated attacks on your supply chain. For example, a supply chain cyber adversary may clandestinely intercept delivery of your products and switch cyber sensitive components with a malware-infused copycat. These attacks are often so sophisticated that the end users may not realize that they did not receive the original version.

Nation-states, hacktivists, organized criminal groups, and lone wolves are constantly scanning supply chains

FIGURE 1

Attack methods on the supply chain



for weak points, and the impact of this attention has the potential to reverberate well beyond your supply chain. You inherit the risks of your suppliers. If one of your suppliers lacks security controls, you may absorb their vulnerabilities. This is particularly true if you do not comprehensively test their components during your acceptance process; once you accept their product, you accept the risks of being attacked or passing along an attack to your customers. In the event that a cyberattack occurs, you own the impacts as well. This includes brand damage, operational stoppage, legal exposure, canceled sales, and government sanctions.

Dangerous combination of hidden risks and higher expectations

Tackling cybersecurity risk in supply chain may feel like you are trapped between a virtual rock and a hard place. As companies drive to increase supply chain flexibility at the lowest overall cost, sourcing decisions expose them to the vulnerabilities of suppliers and all of their successive networks of suppliers. This ever-evolving cybersecurity threat in the multi-layered supply chain presents a number of challenges when managing cybersecurity. See Figure 2.

Supply chain traditionally has been seen as part of internal operations; it is something that happens behind the scenes for your customers. In the past, customers did not care where you made your products or how you sourced them as long as you delivered them on time, at the appropriate cost, and in good condition. However, this is all changing. Companies and governments around the world are realizing that the supply chain is an ideal way for attackers to quietly infiltrate their networks and infect a system well before customers place an order. Companies, large and small, have to begin looking at supply chain security as part of their overall supply chain risk management process.

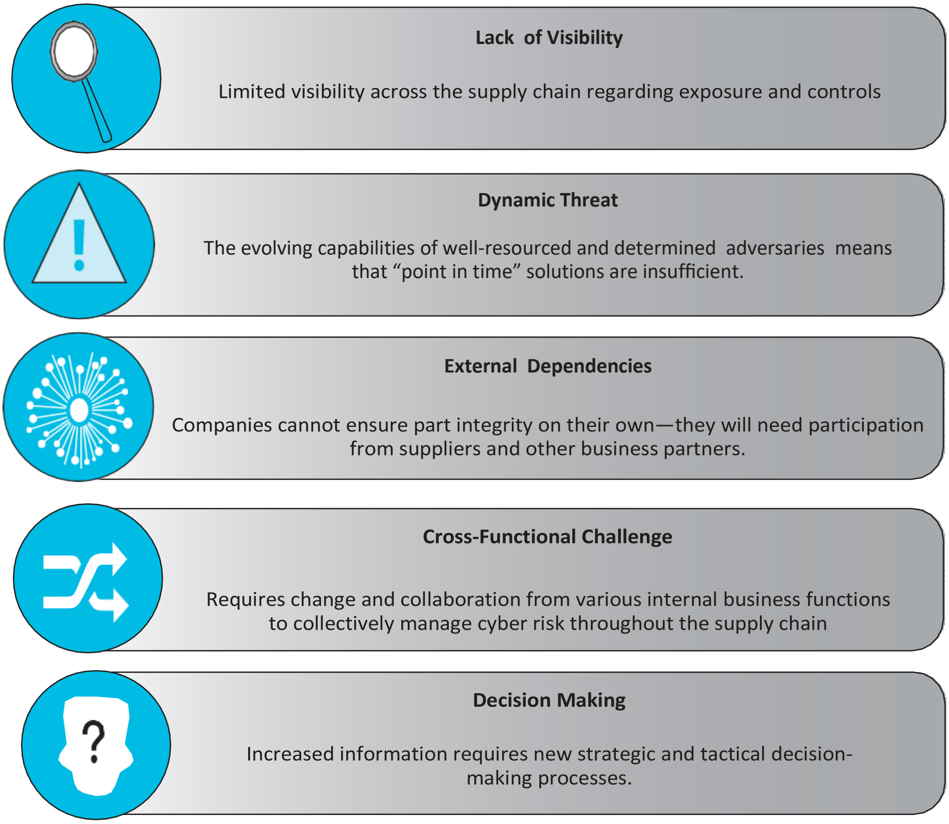
By prioritizing supply chain cybersecurity, you are well on your way to tackling this complex issue. You have an opportunity to mitigate cyber risk and transform your supply chain risk management capability into a competitive advantage to inform your broader business.

Increasing expectations

The U.S. government has been a force for driving higher-level visibility and controls across the supply chain. As the future progresses,

FIGURE 2

Cybersecurity challenges in the supply chain



Lack of Visibility

Limited visibility across the supply chain regarding exposure and controls

Dynamic Threat

The evolving capabilities of well-resourced and determined adversaries means that "point in time" solutions are insufficient.

External Dependencies

Companies cannot ensure part integrity on their own—they will need participation from suppliers and other business partners.

Cross-Functional Challenge

Requires change and collaboration from various internal business functions to collectively manage cyber risk throughout the supply chain

Decision Making

Increased information requires new strategic and tactical decision-making processes.

insurance companies will be an even larger driver for increasing supply chain standards. Business continuity policies are in place to address threats that disrupt the supply chain. Companies with weak supply chain cyber security policies and procedures could find their insurers raising their premiums or excluding claims in case of a breach. The next wave of standards could take shape with requiring you to maintain a list of all cyber sensitive supply chain components as well as develop comprehensive risk frameworks to classify, prioritize, and proactively manage the sourcing of each of those components. You need to proactively get ahead of these standards. Prove to the government, insurers, and your customers that you have a strong supply chain cyber cybersecurity capability.

It is not just the U.S. federal government that is raising the stakes. Many clients also are demanding to know more about the supply chain. Private sector clients are realizing that securing high assurance services on an untrusted hardware platform is the same as building a fort on a foundation of shifting sand. They want to know the depth of visibility into the components and services of products, and they want to be reassured that there are controls in place to manage a robust supply chain cybersecurity program. As with the government, many of these requests and requirements are at an all-time high and will become more sophisticated and comprehensive only during the next several years. If you are their supplier, they know that you are only as trustworthy as your supply chain.

■ How to create both a secure and compliant capability

Complying with standards and guidelines is not enough for securing all of the factors you need to comprehensively increase yoursecurity posture. Although standards strive to create consistency among cybersecurity programs, the fundamental truth is that there is no formula for security. Standards and frameworks can help identify the landscape of potential areas to address and may let you set a minimum level of performance, but that's it. You must move beyond merely striving to be compliant rather than noncompliant. Supply chain cybersecurity is more than an IT problem. If not used in the appropriate context, standards can be a generic solution to a highly individualized problem set. Supply chain risk is tied intimately to your business strategy and operations, and it must be tailored to your organization.

Rather than focusing on a standard, look at your program with a maturity lens. Understand the various degrees of risk you face. Then, within a well-established structure, decide where you need to invest and develop. It is up to you to prioritize the control areas to address. Focus on your current maturity in those areas and what you must do to increase your maturity. Focusing on your maturity provides you with an opportunity to identify where your program stands today, where it must be in the future, and how to get there. A maturity approach is not "one size fits all." Special considerations for your organization could necessitate that your approach be different than that of a competitor. Using a maturity model also allows you to answer the questions that are not yet asked by compliance while aligning your supply chain to your business strategy. It allows you to focus on increasing your overall security and to stay ahead of the curve.

■ Where do I start?

Developing a robust supply chain cybersecurity program is complex, but that doesn't mean your approach has to be. It requires a risk-based prioritization approach to changes in policy, supplier contracts, resource allocation, and investment. Most companies do not have the appetite or the budget forwholesale, drastic changes. If you are like most organizations, you face the dilemma of not knowing where to begin.

So the best place to start is to get your arms around what has to be done.

1. Conduct a maturity assessment and build a roadmap.
   Your organization needs a plan for the path forward in securing your supply chain. Before you transition to developing a roadmap, you must begin with a maturity assessment. Supply chain cybersecurity program maturity assessments are simply gap analyses between how well your program operates today compared with how it should operate in a target state. To evaluate this, you must identify the key controls that apply to supply chain risk management—either controls you already use as part of your corporate cybersecurity program or controls that may be more unique to supply chain. Even if you use existing controls, you should modify them to apply to your supply chain operations.

Maturity Assessment Tip

The set of controls you select for your maturity assessment should incorporate the compliance standards that customers might use as part of their Request for Proposal requirements (e.g., NIST SP 800-161). You likely will cover more controls than these standards, but mapping them will allow you to kill two birds with one stone.

Five Common Early Wins

Below are five common ways you can gain early traction with your supply chain cybersecurity program:

- Integrate/enhance component tracking
- Include cyber in your supply chain risk management framework
- Enhance acceptance testing
- Conduct supply chain vulnerability penetration testing
- Enhance monitoring of supplier network access points

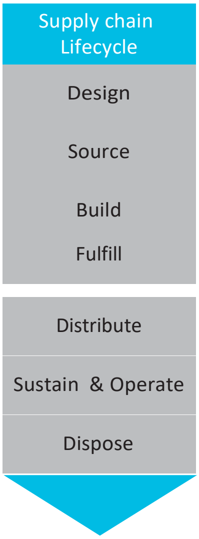
Next, identify key objectives for each control you plan to evaluate. Threat intelligence, for example, may have data collection, analysis, and distribution as key control objectives. For each objective, define a scale as well as the key characteristics for each step in that scale. Taking the threat intelligence example, a low maturity rating for data collection could be the ad hoc collection of threat data via unstructured sources, such as email. A higher maturity implementation of data collection would be a comprehensive ingestion of multiple formal data feeds that can be analyzed automatically and efficiently.

Next, conduct a baseline assessment of your current state – an honest assessment, backed by examples. This will help you surface risks associated with each control. After the baseline, define the target state for each control. The target state should be a balance between high effectiveness and practical costs, keeping in mind that not all controls need the highest level of maturity. Comparing the target state with the baseline provides you the gap you need to address.

The outcome of your maturity assessment will be a robust roadmap designed to transform your supply chain cybersecurity program. This equates to quick wins and key priorities for your organization. It should also help address the key requirements your customers demand.

2. Identify key risks throughout your supply chain lifecycle.

Breaking down your supply chain lifecycle into discrete phases can help you identify key risks for each phase. Each phase presents its own vulnerabilities and risks. For example, during the distribution phase, threat actors can intercept physical deliveries of products, place malware in cyber sensitive components, and allow the shipments to continue to end customers. As you identify risks for each phase, you have to assess the likelihood and impact of each risk. This prioritized list becomes your risk agenda and helps determine what to address first to enhance your supply chain cybersecurity program.



Supply chain Lifecycle

Design

Source

Build

Fulfill

Distribute

Sustain & Operate

Dispose

3. Decompose your key product lines.

To assess the visibility, control, and risks in your supply chain, select a few key product lines and decompose them into their cyber sensitive components. Then see how much information you can collect on their manufacturing sources, acceptance testing, suppliers, and intended customers. You will likely find that your internal systems and policies are prohibiting you from this level of visibility; however, it is this level of visibility that customers will be demanding in *the future, if not already. Once you can obtain this kind of visibility, you can then assess the processes, controls, and risks associated with those cyber sensitive components.*

- **Supply chain cybersecurity as a differentiator** The risks and expectations of your supply chain cybersecurity are increasing as threats become more sophisticated and customers' expectations rise. As you inherit the vulnerabilities from your suppliers and the risks of your customers, you have to be more aware of how your supply chain can become an attack chain. Compliance is not enough; you must develop a robust maturity model to help identify your vulnerabilities and develop a roadmap to reduce your risks.

Companies that are able to effectively manage their supply chain risks will have the advantage in the market. Understanding how to identify risk and then effectively manage those risks will allow you to be in greater control of your supply chain. A robust supply chain cyber risk management program will allow you to close vulnerabilities, making you less of a target for attackers while helping you meet and even shape your customer expectations. The trust in your brand and the quality of your product depend on the strength of your supply chain cybersecurity.
Creating the right balance of security and resilience in your supply chain will allow you to build a foundationally stronger supply chain cybersecurity program. This not only will differentiate you from your competitors but also will allow you to better understand the opportunities and advantages that are key to your success .