[title]

The Supply Chain: A Growing Source of Cyber Threat

[body copy]

Last October, *Bloomberg Businessweek* published a highly controversial, perhaps even inflammatory article on Chinese state-sponsored efforts to modify motherboards being sold by the American company Supermicro. These motherboards made their way into computers in U.S. commercial and government clients—including, it is believed, the Department of Defense. It was yet another example of the growing risk posed to enterprises through their supply chains.

While the debate continues as to the accuracy of each claim in the Bloomberg article, what is certain is that the supply chain remains among the most vulnerable elements of the attack surface for many firms. I am using a broad definition of "supply chain" here. From a security perspective, a supply chain certainly includes suppliers. But it also includes vendors, contractors, service providers—anyone who has access to any part of a company's network.

The Supermicro example is just one in a long list of costly supply chain penetrations. The fact is that attacks on organizations through third parties have become more common, and CISOs can no longer afford to ignore or downplay this risk. Recent history is replete with examples:

- In one of the biggest compromises of credit card and personal information in history, more than 70 million records were stolen from Target Inc. in late 2013—a breach that ultimately cost Target nearly $300 million. But the original intrusion did not occur on the Target network; it originated in the supply chain. It all started when an employee at Fazio Mechanical, a Target supplier with just 100 employees, was duped by a phishing email. This allowed a trojan called Citadel to be installed, enabling cybercriminals to retrieve login credentials to Target's supplier network.
- A year ago, an actor going by the name "TheDarkOverlord" infiltrated several healthcare organizations and attempted to sell the stolen data on the dark web. This cybercriminal reportedly got into the organizations' secured databases using the credentials of third-party vendors and contractors.
- Reports indicate that oil and gas pipelines, electrical grids, and even nuclear facilities are vulnerable to catastrophic disruption due to the activities of the group Dragonfly, which has connections to hostile nation-state actors. Dragonfly has successfully "trojanized" industrial control systems (ICS) software at energy companies by compromising the websites of the software providers, replacing legitimate files in their repositories with malware-infected ones.
- Corporation Service Company (CSC), which provides domain registration and agent for service of process services for customers including Fortune 500 firms, discovered in 2018 that "an unauthorized third party accessed its network and certain systems," exposing personal identifiable information on more than 5,000 customers in what seems to be a malicious attack from within the supply chain.
- As reported in Fortinet's latest Threat Landscape Report, multiple criminal groups referred to collectively as Magecart stole 185,000 payment cards this past spring from numerous high-traffic eCommerce sites. They used a lightweight JavaScript card skimmer embedded somewhere on each site, often inserted into third-party components that provide functions including content management, visitor tracking, customer support, and payment services.

[callout]
Key energy infrastructure in North America and Europe is being targeted through ICS software providers.

[body continued]
A Complex Web of Vendors and Suppliers
The supply chain is inherently complex, often consisting of globally distributed and dynamic collections of people, processes, and technologies. Such a dynamic system is constantly morphing—thus making it unpredictable, even volatile. At the same time, any chain is only as strong as its weakest link. Some of the risks cited by the National Institute of Standards and Technology (NIST) include:

- *Inferior information security practiced by lower-tier suppliers.* Like Target's vendor, smaller organizations are rightly proud of the top-tier organizations on their client list, and probably post that information publicly on their websites and social media channels. At the same time, they likely have fewer monetary and human resources available to build a robust cybersecurity program. Verizon's 2019 Data Breach Investigations Report indicates that 43% of victims of cyberattacks are categorized as small businesses—a number that is probably bolstered by the access that small businesses often have to the systems of larger organizations. And a survey by (ISC)2 found that 41% of small business respondents have had to notify a larger partner to reset a password due to a security breach in their infrastructure.
- *Third-party service providers that have virtual access to information systems.* Trusted service providers often have full access to an organization's systems—even systems they never need to access. This leaves the door open to massive intrusion, whether deliberate or accidental on the part of the individual with access.
- *Compromised hardware and software*. Dragonfly and other players have successfully contaminated files from trusted software vendors' websites. Other actors target hardware, which presents myriad opportunities for cybercriminals given the proliferation of Internet of Things (IoT) and mobile devices, such as Chinese smartphones.
- *Software vulnerabilities with supplier systems and supply chain management systems.* These security holes are often not caught in a timely manner because they lie outside the purview of the organization's IT and cybersecurity teams.

[callout]
Agile segmentation ensures that users have access only to what is necessary to do their jobs.

[body continued]
Effective Supply Chain Risk Management
Optimizing physical supply chains can be the key to profitability in many industries, and organizations have gotten better and better at ensuring that the right supplies are in the right place at the right time. They follow established procedures for mitigating dependencies and vulnerabilities in the supply chain. These risks are identified, tracked, and assigned owners in a way that increases their visibility and allows the organization to anticipate their impact.

Unfortunately, this strategic approach is seldom followed with regard to cybersecurity-related risks to the supply chain. Since these risks are several steps removed from the analysis and decision-making center of the organization, they wind up being "out of sight, out of mind." Despite this, few would disagree with the assertion that a cybersecurity failure in an organization's supply chain would be as damaging—if not more so—than an interruption in the physical supply chain. Here, the CISO needs to have a seat at the table when it comes to supply chain management, and cybersecurity needs to be a part of every organization's supply chain strategy.

[callout]
Cybersecurity in the supply chain should be a part of the overall strategy of supply chain management.

[body continued]
Recommendations for A Secure Supply Chain
A CISO certainly cannot control the security practices of an organization with which his or her organization does not even conduct business—say, a vendor of a vendor of a vendor. However, that CISO will be held accountable if a security incident originating there affects the organization's network or compromises its data. As a result, the CISO should develop a *consistent and constant agile risk assessment* of the entire supply chain.

The following are a few recommendations:

1. *Achieve ongoing visibility into every link.* Since a supply chain is a living organism that is subject to constant flux, a one-time assessment will be out of date very quickly. Every link in the supply chain must be willing to provide the organization with continual visibility into its security infrastructure, employee vetting processes, cybersecurity awareness practices, and data access patterns.
2. *Deploy intent-based segmentation.* While it is administratively easier to simply grant full access to the entire network for all third-party users, today's threat landscape requires a more sophisticated approach. Users should have access only to the resources they need to do their job. Agile segmentation can help different groups of users to have access to different resources based on need—and those needs can be adjusted on the fly. This segmentation should be supplemented with a behavior-based approach to trust that scrutinizes even trusted users.
3. *Internal awareness/education.* Senior leaders need to understand the cybersecurity risks posed by the supply chain so that they can provide input on how to minimize risk. Rank and file employees also should be educated on best practices for managing vendors in a cyber-secure way.
4. *Decision-making models.* As an organization continually assesses and reassesses the risk posed by each link in its supply chain, it is important to develop a consistent model for making decisions about how to respond to changes in the threats posed by the supply chain. Does the CISO have the authority to make immediate changes to an IT system if the threat is great enough, or does he or she have to go to the CIO for adjudication? Broad awareness of the issues involved and a strong emphasis on cybersecurity at the executive level will make such a model more effective.

The complexity of cybersecurity is often enough to overwhelm non-technical C-suite officers, and the topic of supply chain cybersecurity can be downright boring. Yet it is precisely these characteristics that make supply chains a favorite target of malicious actors. It is for this reason that CISOs must expend considerable effort in accurately calculating and visualizing their supply chains and the risk inherent to each component of the chain. Every individual and organization that interacts with your data is a part of your attack surface, and therefore needs to be a part of your integrated security strategy.

[infographic]
Supply Chain Threats

64% of companies outsource more than one-quarter of daily business tasks

95% have a process for vetting small business partners' cybersecurity

14% of enterprises were breached through a small business partner

17% of enterprises were breached through a larger partner

40% of small businesses have experienced a breach

33% have had an employee mishandle credentials of a larger partner

41% have had to notify a larger client to reset passwords due to a breach

34% of large enterprise respondents have been surprised by a partner's level of access to their network

39% of small business respondents have been surprised by their level of access to a partner's systems

55% of small businesses still had access to a client's network after the contract was completed

Source: "Securing the Partner Ecosystem: Are Small Businesses the Largest Risk to Supply Chain Cybersecurity?" (ISC)2, accessed September 5, 2019.