SourceToday
Thought Leadership Series

Issue 04.2017

Cyber Security Strategies for Today's Digital Supply Chains

For decades, the electronics industry has focused on detecting counterfeit components before they enter the supply chain by sourcing from trusted suppliers and distributors. But the threats are expanding, criminals are becoming more creative, and both hardware and software threats permeate the supply. What do companies need to do to keep their supply chains safe?

Sponsored by: tti® TE connectivity AUTHORIZED DISTRIBUTOR

Supply chains of today differ markedly from those of only a few years ago. Competition to produce affordable goods in shorter production cycles to speed time to market now compels many businesses to rely on vendors from around the globe for an increasing range of services—from design to fabrication, shipping, logistics, and more.

A multitude of connected technologies now facilitate the operation of these supply chains. The internet, GPS tracking, cloud computing, wireless sensors, radio frequency identification, and a host of applications help increase the information flow along the supply chain with the aim of boosting efficiencies and reducing the costs related to the manufacture and delivery of products.

As part of this transformation to a digital supply chain, companies are increasingly providing third-party vendors with access to their networks to enable the sharing of pertinent information. In addition to manufacturing plants, transport firms, and warehousing operations, these suppliers can include utilities, maintenance companies, and professional service firms such as accounting and law firms.

And that trend is expected to continue. A 2016 cross-industry digital transformation survey of 337 executives in 20 countries, carried out by Capgemini Consulting and GT Nexus, found that in the next five years, 95% of respondents expect more processes with suppliers to be automated and 94% expect to receive more real-time status updates from across the entire supply chain (see Figure 1).[1]

But while improved connectivity and information sharing can help enhance supply chain operations and company performance, it also dramatically boosts the risk of cyberattack. By sharing passcodes, network access, intellectual property, financial information, and other sensitive data with third-party suppliers, companies are captive to the data-security standards of these vendors. Larger companies that may have hundreds or thousands of such suppliers are potentially multiplying their vulnerability to cyber theft or malice by a similar factor.

Figure 1. More automation is coming to supply chains

Source: Capgemini Consulting and GT Nexus

Supply chain cyber risk is an increasing concern for companies not only because of the number of possible entry points for hackers, but also because of the potentially greater vulnerability of supply chain partners. In particular, smaller partners that may not have made the same level of investment in IT security as the larger enterprises they service can represent easier targets for attackers to exploit than the downstream company itself.

And while companies have managed diverse supply chain risks for many decades, these have traditionally involved safeguarding against threats such as natural disasters, labor disruptions, and sabotage against physical assets. Cyberattacks against the supply chain, while a newer peril, nonetheless can cause companies significant damage—to business property, reputation, and profit.

2013 Target Breach

Perhaps the most infamous cyberattack against a company's supply chain occurred in 2013 when hackers successfully infiltrated retailer Target's network to intercept data on 40 million credit and debit card accounts. The hackers were able to sell data from these accounts on the black market for use in creating counterfeit cards to fraudulently purchase goods and, in some cases, even steal money directly from victims' bank accounts. Non-financial personal information, including names, phone numbers, and both physical and email addresses on up to 70 million customers, was also stolen during the attack.

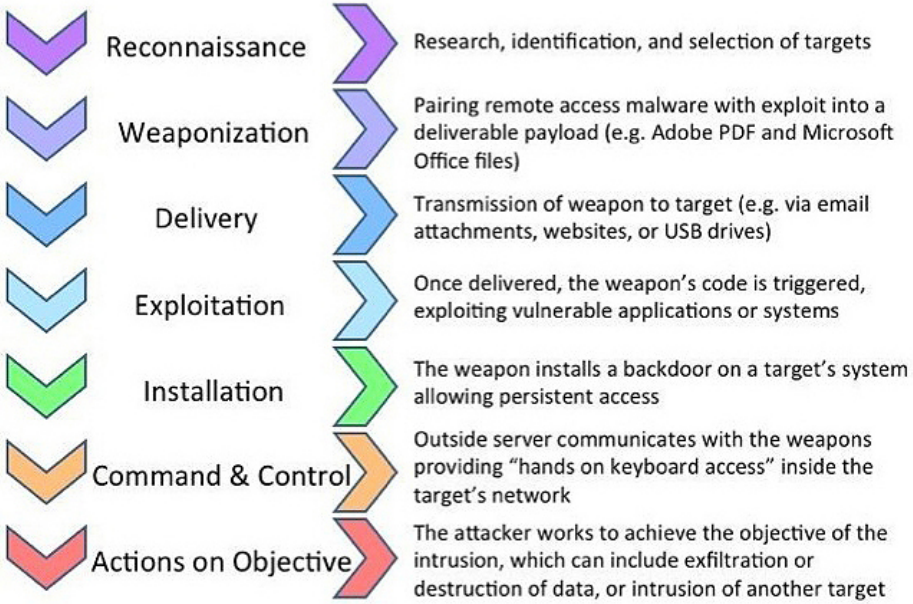
According to a 2014 "kill chain" analysis of the breach by the Senate Commerce Committee, Target had previously given network access to a third-party vendor, a small HVAC company, for "electronic billing, contract submission, and project management purposes." Attackers stole network credentials for accessing Target's network via malware-infected emails sent to the vendor, which apparently did not follow recognized information security practices.

Once inside the network, hackers, undetected for several weeks, were able to install malware on point-of-sale (POS) terminals at U.S.-based Target stores to enable the theft of the credit and debit card data. The malware utilized a "RAM-scraping" attack, which allowed for the collection of unencrypted, plain-text data as it passed through the infected POS machines' memory before transfer to the company's payment-processing provider.

The attackers are believed to have obtained information on Target's third-party vendors via publicly available information on the Internet, including the company's own supplier portal and facilities management web pages. "Files available on these sites provided information for HVAC vendors and, through a metadata analysis, allowed the attacker to map Target's internal network prior to the breach," the Committee found.

To interrupt this step in the "kill chain," Target could have hidden much of its vendor information from the public (see Figure 2). The company further might have shared threat information with its service providers and encouraged collaboration on security within its supplier community. Target apparently did neither and, when the attack was under way, failed to respond to multiple automated warnings from its own anti-intrusion software that malware was being installed on its system. (Continued on page 5.)

Figure 2. Phases of the intrusion "kill chain" [2]



Source: Lockheed-Martin

Case Study: Juniper Networks

As part of its US Resilience Project, NIST published a series of case studies in 2015 profiling companies that exhibit best practices in supply chain cybersecurity. One such company is Juniper Networks, a Sunnyvale, California-based designer of high-performance internet protocol network products.

Juniper relies principally on five contract manufacturers and original design manufacturers for its fabrication services, making supply chain assurance integral to its bottom line and brand reputation. Beyond these partners, there are about 300 other suppliers with more than 2,000 sites around the world that manufacture more than 24,000 parts used in Juniper products.

Figure 3. The wheel of supplier excellence

Source: NIST/Juniper Networks

All functions that touch the supply chain are linked through a Supply Chain Risk Management Council, which meets regularly to review risk exposure. The Council continually scrutinizes the overall risk environment, including those relating to product, sourcing, and compliance, and what is needed to reduce those risks. Supply chain risks and mitigation plans receive board-level scrutiny.

Reviewing suppliers for the potential risk they could pose to the supply chain, Juniper analyzes the "percentage of risk" as well as the "percentage of spend." A supplier may be small as a percentage of total spend, but critical enough to have a major impact upon product shipment.

Prospective suppliers are vetted by a number of teams—sourcing, risk management, engineering, and security—across all categories on a Wheel of Supplier Excellence (see Figure 3). If suppliers cannot or do not want to meet the requirements, their scores likely will not be high enough to allow them to participate.

Cyber risks are managed through a number of design features and controls:

- Juniper runs one proprietary software code across all of its products lines, which allows it to embed security at the interface between software and hardware.
- Any software not digitally signed by Juniper cannot be run on its systems—and great attention is paid to protecting the signing keys and securing the digital signature process. ■

The Emerging Cyber Threat Landscape

In many large companies and organizations, the systems required to collect, organize, store, and transmit information internally constitute a significant cybersecurity challenge in and of itself. Add to that the many external information system links required to integrate third-party suppliers and the challenge is magnified considerably. The lengthier a company's supply chain is, the larger is its digital shadow—and the greater is its susceptibility to cyberattack at one or more points along that chain.

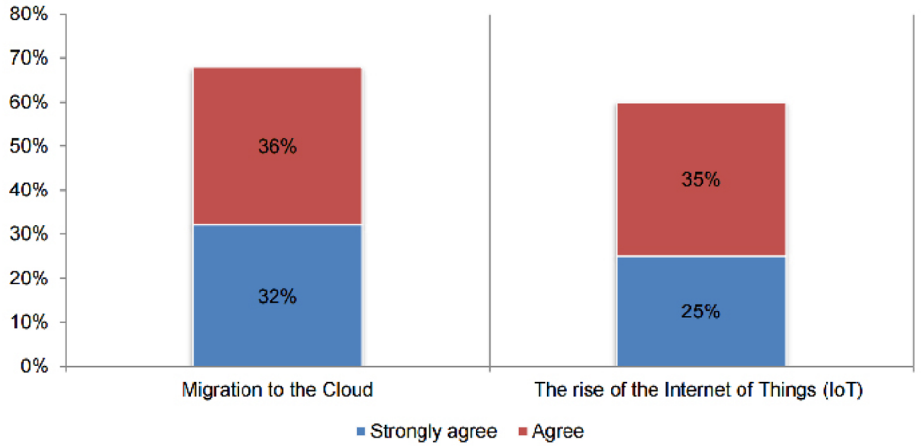
For their part, hackers are motivated to attack the supply chain for any of several reasons. With many companies more focused on preventing a direct cyberattack on their own operations, suppliers—particularly smaller ones—may represent a softer target, the weak link in the cyber defense chain. Moreover, successfully hacking a third-party vendor may capture network access to more than one downstream company to which the company supplies services.

For all the damage that can be incurred via a supply chain cyberattack—in Target's case, at least $200 million in expenses—risk managers arguably are somewhat lacking in concern for supply chain cybersecurity. A 2016 survey of 617 risk management professionals by the Ponemon Institute found that only 27% of those surveyed ranked cyber risk among their top two worries—trailing minimization of downtime (56%) and minimization of business disruptions (37%).[3]

"Most C-level executives are not engaged in their organization's third-party risk management process," the study's authors concluded. Accountability for the third-party risk management program is instead dispersed throughout the surveyed organizations.

And yet those surveyed nonetheless expect third-party risk to increase as a result of the evolving threat landscape. Large majorities of respondents believe that disruptive technologies, such as migration to the cloud (68%) and the rise of the Internet of Things (60%), will increase their exposure to third-party risk (see Figure 4). 3D printing, while not covered in the Ponemon survey, adds another emerging threat to the cyber landscape—as intellectual property in the form of product designs will be made increasingly available in digital form throughout the supply chain and subject to potential theft.

Figure 4. IoT and cloud migration increase third-party risk



Source: Ponemon Institute LLC

Summing up the emerging threat landscape, in September 2015 then-Director of National Intelligence James Clapper noted in testimony before the House Intelligence Committee:

"Despite ever-improving network defenses, the diverse possibilities available through remote hacking intrusion, supply chain operations to insert compromised hardware or software, actions by malicious insiders, and mistakes by system users will hold nearly all ICT networks and systems at risk for years to come. In short, the cyber threat cannot be eliminated; rather, cyber risk must be managed."

How, then, should companies "manage" their diverse cyber threats?

Best Practices in Supply Chain Cyber Risk Management

An array of standards and guidelines have been published that cover supply chain risk management. According to the National Institute of Standards and Technology (NIST)—a non-regulatory agency of the US Department of Commerce that develops measurement science, standards, and technology to promote industrial competitiveness—selecting the standard(s) that pertain to a specific company involves settling on an overall risk management framework, understanding one's sector and customers, and determining a company's specific role within the supply chain.

Why multiple standards? Cyber supply chain risk management is a multidisciplinary problem, and successfully addressing it requires blending practices from different industries. Organizations commonly do not fall neatly within the clear-cut designations established by standards bodies, and they often are subject to multiple regulatory standards for compliance, e.g., HIPAA, PCI DSS, and NERC CIP.

In January 2017, NIST published for comment an updated draft of its Framework for Improving Critical Infrastructure Cybersecurity—a standard widely recognized and used by multinational corporations. Reflecting the growing concerns over supply chain cyber risk, the new framework, which is due to be finalized and published later this year, incorporates language specific to this emerging cyber threat.

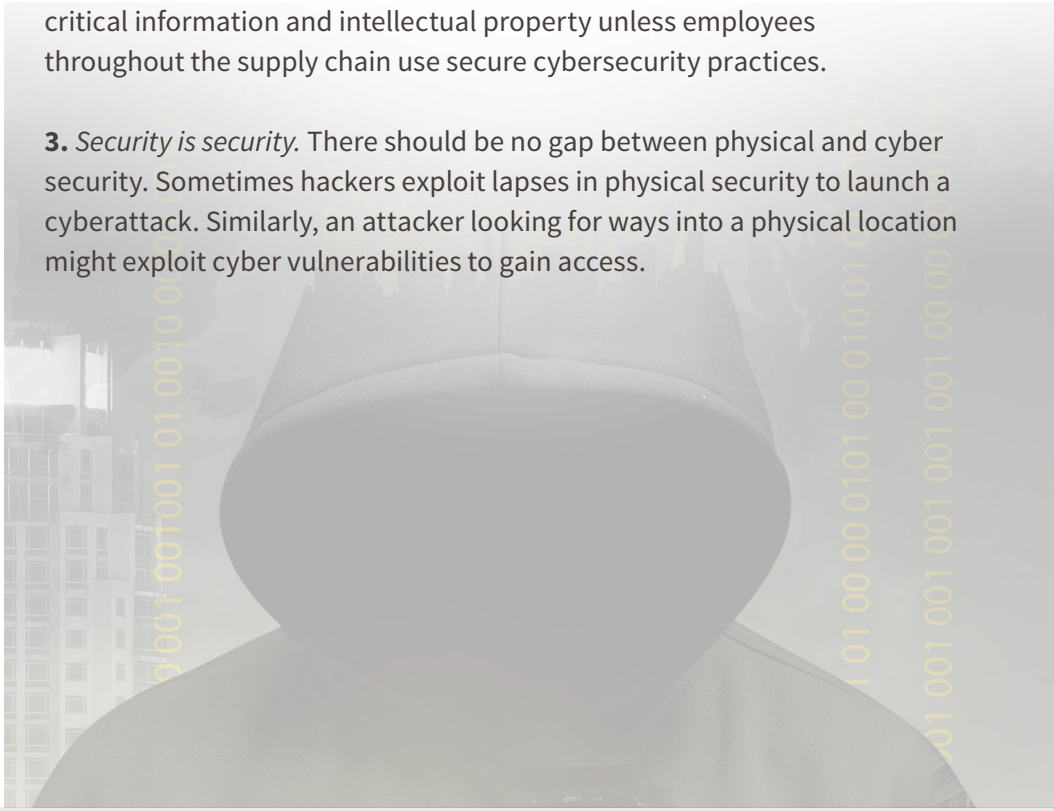
Cybersecurity in the supply chain, NIST says, cannot be viewed exclusively as an IT problem. Cyber supply chain risks touch sourcing, vendor management, supply chain continuity and quality, transportation security, and many other functions across the enterprise that require a coordinated effort to address.

NIST advances the following supply chain cybersecurity principles:

1. *Develop company cyber defenses based on the assumption that information systems will be breached*. When one starts from the premise that a breach is inevitable, it changes the decision matrix on next steps. The question becomes not just how to prevent a breach, but how to mitigate an attacker's ability to exploit the information they have accessed and how to recover from the breach.

2. *Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem*. Breaches tend to be less about a technology failure and more about human error. IT security systems won't secure critical information and intellectual property unless employees throughout the supply chain use secure cybersecurity practices.

3. *Security is security.* There should be no gap between physical and cyber security. Sometimes hackers exploit lapses in physical security to launch a cyberattack. Similarly, an attacker looking for ways into a physical location might exploit cyber vulnerabilities to gain access.



NIST cites the following examples of supply chain cybersecurity best practices:

- Include security requirements in every RFP and contract.
- Once a vendor is accepted in the formal supply chain, assign a security team to work with them on-site to address any vulnerabilities and security gaps.
- "One strike and you're out" policies with respect to vendor products that are either counterfeit or do not match specification.
- Prequalification of component purchases from approved vendors; parts purchased from other vendors should be unpacked, inspected, and X-rayed before accepted.
- Establishment of secure software lifecycle development programs and training for all engineers in the lifecycle.
- Obtain source code for all purchased software.
- Software and hardware should have a security "handshake." Secure booting processes should look for authentication codes, with the system unable to boot if codes are not recognized.
- Use track-and-trace programs to establish the provenance of all parts, components, and systems.
- Programs should capture "as built" component identity data for each assembly and automatically link the component identity data to the sourcing information.
- Personnel in charge of supply chain cybersecurity should partner with every team that touches any part of the product during its development lifecycle and ensure that cybersecurity is part of suppliers' and developers' employee processes.
- Ensure legacy support for end-of-life products and platforms, as well as continued supply of authorized intellectual property and parts.
- Impose close control over access to software by service vendors. Hardware vendors should be limited to mechanical systems with no access to control systems. All vendors should be authorized and escorted.[4]

By John Simpson

1 "The Current and Future State of Digital Supply Chain Transformation," Capgemini Consulting and GT Nexus, 2016.
2 Lockheed-Martin, as published in "A 'Kill Chain' Analysis of the 2013 Target Data Breach," Senate Commerce Committee, March 26, 2014.
3 "Tone at the Top and Third Party Risk," Ponemon Institute LLC, May 2016.
4 "Best Practices in Cyber Supply Chain Risk Management, Conference Materials," National Institute of Standards and Technology.