Customs-Trade Partnership Against Terrorism

Alert

Cyber Security - How to Effectively Secure a Supply Chain and Partner Ecosystem

The Customs-Trade Partnership Against Terrorism (C-TPAT) program is one layer in U.S. Customs and Border Protection's (CBP) multi-layered cargo enforcement strategy. Through this program, CBP works with the trade community to strengthen international supply chains and improve United States border security.

To enhance communication with its members, C-TPAT routinely highlights security matters for the purpose of raising awareness, renewing Partners' vigilance, and recognizing best practices implemented to address supply chain security concerns.

The purpose of this C-TPAT Alert, generated in cooperation with FireEye, a leader in cyber security solutions, is to raise awareness of C-TPAT Partners of their exposure to indirect cyber-attacks, not only through their supply chain, but through their third-party relationships; and to make them aware of available federal guidance that can help to strengthen their cyber defenses.

> *No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families … So we're making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism.*
>
> *President Barack Obama*
> *State of the Union Address*
> *January 20, 2015*

In the film *Oceans Thirteen*, a group of con men defraud a Las Vegas casino with rigged dice. How? They travel to the Mexican factory where the dice are manufactured. There, they taint the dice-making material with magnets to manipulate which numbers appear. In other words, they exploited the supply chain. As the con men explain in the film, "The dice are controlled from the manufacturer all the way to the [casino] floor. Which is why we went all the way to the manufacturer."

This is more than just Hollywood fiction. This scenario is playing out globally in many industries.

Risks to the supply chain have dramatically increased in recent years due to companies' increased outsourcing of significant responsibilities to other organizations. As enterprises have become more specialized, the need for capital investments associated with manufacturing, logistics and design, has skyrocketed, resulting in more outsourcing. And while many enterprises have consequently applied tighter controls to their expanding supply chains, these best practices traditionally include only pricing, quality, on-time delivery, market influence and a few other factors that help determine if a given partner is the right choice.

But, as supply chain management has changed with the onset of digitization, the security risks have grown, necessitating tighter security controls throughout the supply chain. The increased

reliance on electronic communications and software tools offers an ideal environment for criminals and rogue governments to conduct espionage, steal intellectual property, derail transactions or use partners as a springboard to catch a bigger fish. And, as companies partner and collaborate with other businesses to speed up product time-to-market, they share information with supply-chain partners at a level never seen before. Whether informal, unstructured information in an email inbox or via a network share over a Virtual Private Network, they are entrusting potentially sensitive and valuable information, such as intellectual property, budgets, Go-to-Market plans, roadmaps and other data, to someone else. Bad actors capitalize on the strong trust relationships and information sharing between enterprises and their third-party business partners, as well as the often relatively weaker security controls in place at the third-party organizations.

In 2014, the media reported on multiple cyber-attacks, ranging from manufacturing to retail, where bad actors reached their victims through trusted third parties. As an example, in July 2014, a highly sophisticated attack went after the shipping industry through a manufacturer of hardware and software for handheld barcode scanners used by shipping and logistics firms worldwide. The scanners work by connecting to the shipping companies' wireless networks and transmitting the package information they collect, such as origin, destination, value, and contents. The bad actor installed malware (malicious software designed to damage, disable, or gain access to computer systems) on the Windows operating systems used in the scanners at the manufacturer's location in China. Since the malware was loaded at the manufacturer, the companies buying the scanners trusted the hardware and the software. The unsuspecting companies connected the scanners to their wireless networks and installed their security certificates, used to create a secure connection with the web and protect the corporate network from unauthorized access. However, since the scanners were already infected, the scanned data was stolen by the bad actor and the companies' security certificates were compromised, allowing the bad actor to access the companies' networks, including their corporate financial data, customer data, and detailed shipping and manifest information.

These attacks can take many forms. For instance, a bad actor could steal a target victim's intellectual property and data stored with a third-party, access the target through its network connections and shared infrastructure with a third-party, or use its access to the third party to socially engineer access to a victim's systems, such as by tricking the victim to click on a link or open an email that appears to be from the trusted third party but actually installs malware. The reality of these types of attacks is that when attackers are prevented from directly accessing a target, they will use any means necessary to regain entry to the systems they fought hard to access. As organizations targeted by advanced bad actors harden their own security, vendor and supplier relationships potentially become the easiest path for bad actors to exploit when attempting to compromise their targets.

To help reduce the frequency, severity and impact of advanced cyber attacks against the supply chain, C-TPAT Partners should develop an integrated cybersecurity risk management plan that incorporates security controls and best practices that mitigate risk associated with advanced cyber threats and the use of sophisticated attack techniques. In particular, the Federal Government, through National Institute of Standards and Technology (NIST), is working with the private sector to develop resources to help organizations manage security risks to their

supply chains. To date, NIST has issued an Information and Communications Technology Supply Chain Risk Management (SCRM) Fact Sheet, which can be located at the following website: http://csrc.nist.gov/scrm/index.html. NIST is also working with industry on specific guidance on best practices for SCRM and has issued a draft version of Special Publication (SP) 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, for public comment. While this document is still under development, the draft offers specific best practices that organizations may use now to better manage supply chain risk. It may be accessed at the following link: http://csrc.nist.gov/scrm/publications.html.

In addition, C-TPAT organizations may also turn to the NIST *Framework for Improving Critical Infrastructure Cybersecurity* ("Framework") for guidance, available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. While this document does not specifically address SCRM, the Framework, created through collaboration between industry and government, identifies standards, guidelines, and practices that organizations may voluntarily adopt to better manage cybersecurity-related risk. By utilizing the risk management processes described in the Framework and other NIST documents, and encouraging their supply chain partners to do the same, C-TPAT organizations will better manage cyber-related supply chain risk.

The Framework relies heavily upon NIST Special Publication 800.53 Rev 4 *Security and Privacy Controls for Federal Information Systems and Organizations* as a source of best practices and security controls that organizations should consider implementing. A few highlights include the following security controls:

- NIST 800.53 Rev 4 SC-7 Boundary Protection
- NIST 800.53 Rev 4 SI-3 Malicious Code Protection
- NIST 800.53 Rev 4 SC-44 Detonation Chambers

By applying these best practices and other Federal Government SCRM guidance, C-TPAT Partners can mitigate the ever-evolving cybersecurity risks within their supply chains and those in their third party relationships.

C-TPAT Program

CBP.GOV/CTPAT

1300 Pennsylvania Avenue, NW
Washington, DC 20229
(202) 344-1180

Industry.partnership@dhs.gov