National Institute of Standards and Technology
U.S. Department of Commerce

U.S. Resilience Project

BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

FireEye
Supply Chain Risk Management

INTERVIEWS

Craig Martin
SVP Hardware Development and Manufacturing Operations

Kip Shepard
Senior Manager of Global Logistics and Compliance

The Next New Things in Risk Management

- Securing IT systems against malicious codes that exploit unknown vulnerabilities (zero day vulnerabilities).
- Narrowing the time to trace and close supply chain breaches from 230 days to days or even hours.
- Integrating hardware development and manufacturing operations under a single executive and physical and cybersecurity under a single executive for "two in a box" risk management.

Company Overview

FireEye provides cyber security tools through its products and solutions, which include network, email and mobile security, as well forensic analysis after a breach has occurred. According to the company:

> The cyber threat landscape is evolving rapidly. Instead of broad scattershot attacks of the past, organized threat actors are laser-focused on breaching systems and stealing data using sophisticated attacks that are tailored to compromise a specific target and evade tradition signature-based defenses, a core aspect of what currently constitutes basic cyber hygiene.[1]

In parallel, the company is also growing rapidly. Founded 11 years ago, the Silicon Valley firm grew by 163 percent in 2014. According to an analyst at Forrester Research, FireEye "...ended up being the go-to people. If there's a data breach, that's a name you hear." Just in the past two years, it has been called in to investigate high-profile attacks against Target, JP Morgan Chase, Sony Pictures, Anthem and others.[2]

1 http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_fireeye_yaniv.pdf.

2 http://www.usatoday.com/story/tech/2015/05/20/fireeye-mandiant-carefirst/27659481/.

With a portfolio of 43 different products, the standard FireEye software product is built to prevent malware from being inserted into an organization's network. Other security software products focus on signature-based attacks (a known malicious code that's been identified in the wild), providing specific patches that quarantine the malicious code or pull it off the machine. According to Senior Vice President for Hardware Development and Manufacturing Operations, Craig Martin:

> "That signature-based technology worked very well for the run-of-the-mill malware threats that were more prevalent 10 years ago. The sophistication of today's cyberattacks are much more serious, however, and the threat actors better funded. Today, attacks deliberately lack a detectable pattern. A target might be pinged from multiple servers in different countries in a choreographed, time-phased attack. The attackers may go dormant for several months after an initial entry and return with malicious code that will spread throughout the targeted systems.
>
> FireEye's technology is better suited to detecting the kind of attacks that have never been seen before — "zero day" attacks. Its software creates a virtual machine with execution ware that screens incoming data on a simulated network. Anything found to be malicious is detected before it ever gets through to the live network."

In addition, with the acquisition of Mandiant and nPulse, FireEye is launching capabilities for forensic assessment of cyberattacks. Once a breach has been detected, FireEye is able to identify where that breach occurred, what end points were affected, and how to isolate the problem. Today, an estimated 230 days is required from the time a breach has been identified to the time it is remediated. FireEye executives believe that this time can be reduced to days or even hours, based on its ability to access billions of lines of network traffic data in real time.

Organizational Approach to Risk

FireEye manages two supply chains: physical and information. Due its small size, FireEye is able to manage supply chains risk through executive level collaboration. It benefits from the fact that hardware development and manufacturing operations are in the same organization. In many companies, these functions are separated — the engineering team does the hardware and software development and passes it to the manufacturing group which produces an integrated product. Putting these functions together makes it easier to integrate secure development, manufacturing and supply chain security.

Martin works closely with FireEye's Chief Information Security Officer, Craig Rosen, who is responsible for both information and physical security. Together they partner to identify, prioritize and mitigate risks on a regular basis — essentially jointly fulfilling the Chief Risk Officer role.

Supply chain risk management issues receive board-level oversight through the Subcommittee for Risk Management. The SVP for Hardware Development and Manufacturing Operations, the Chief Information Security Officer and the Security Privacy Officer participate on the subcommittee.

Business Case for Supply Chain Risk Management

In its publication, "Gazing into the Cyber Security Future: 20 Predictions for 2015," FireEye analysts predicted that cyber risks through the supply chain would only increase. Its advice to business:

> "As large organizations continue to adapt their cyber security, the gap between their best practices and mainstream practices will grow. That disparity will drive attackers to compromise less mature companies and use them as the entry points into more mature enterprises they're connected to. Consequently, understanding the supplier ecosystem will become an increasingly key part of cyber strategies.
>
> "Recommendation: Your business should require suppliers to show evidence of good security controls. Building security requirements into your master service agreements can push your suppliers to improve their security. And requiring them to demonstrate the effectiveness of their controls is a good way to make sure that your supply chain is following through on their security promises. Ask for metrics of security effectiveness such as mean time to detecting new threats, and mean time to resolving them. Most companies can't do this today, so start with requirements, then build reporting requirements into your contracts over time."[3]

3 https://www2.fireeye.com/rs/fireye/images/wp-gazing-into%20the-cyber-security-future.pdf.

This kind of insight makes the internal justification process for investments in supply chain risk management within FireEye relatively straightforward. According to Craig Martin:

> "Our message is around security. We understand the risk. We see the level of sophistication every hour of every day. So we know what's out there. We know that we might be an interesting target for someone we just caught in the act. So, internal risk management efforts often sell themselves."

Practical Applications of SCRM

In order to better support its own customers, FireEye prioritizes several areas of potential risk within its own supply chain:

- Preventing malware insertions in the componentry of programmable parts;
- Preventing malware insertions during the manufacturing process or during test and loading of operating systems;
- Preventing tampering with products in the service depots or fulfillment channels; and
- Mitigating risks of purchases from non-authorized vendors.

The company has leverages multiple mitigation strategies to counter these risks.

Standard Componentry: FireEye's manufacturing team uses standard componentry to produce limited and simple form factors for their hardware products, assembled from motherboards, processors, interface cards, drivers etc. There are no custom ASICs and few programmable components in their supply chain. Of the 40 or so system SKUs, only one is a custom design. For these reasons, it would be difficult to target FireEye's inbound flow of materials since they are generic components which come on a "first in, first out" (FIFO) basis from their suppliers, rather than dedicated or customized components. Their standardized approach to hardware manufacturing essentially serves as a first line of defense from malicious attacks.

According to Craig Martin: "We want to put the bulk of our brainpower and investment in software. That's what really differentiates us. And that is also consistent with minimizing risk in the supply chain. When you're not getting exotic with your designs, it helps to minimize SC risks."

Small supplier base: FireEye is able to maintain tighter control over its suppliers because there are only four manufacturing sites.

Stringent vendor controls: According to FireEye executives, deviations from the Approved Vendor List (AVL) pose key risks that must be managed. Because contract manufacturers often operate on thin margins, they sometime do creative things to create additional margins — for example, being tempted by cheaper parts from non-approved vendors. FireEye imposes stringent controls on suppliers to stick with suppliers on its AVL. FireEye conducts occasional site audits at all locations and also has its personnel visiting the sites on a regular basis for business purposes.

Security built into design and test processes: Security features, such as check digits, are designed into the software to prevent or detect any tampering with the code. FireEye has an iterative testing process to get the code functionally-hardened, as well as security-hardened. The formal software release process requires multiple rounds of code testing before it is tested again in the manufacturing environment. The company notifies its customers that the code is generally available (GA) for online download. But, the company typically waits for feedback from the field before it ships the software with new hardware.

Tight control on software load process and test suite: Since all of the product differentiation is in the software, FireEye is proactive in cybersecurity processes. FireEye completely owns and controls its source code through a secure portal. Contract manufacturers must download the software from a FireEye server, requiring the supplier to tap into FireEye's system rather than hosting the software resident on the supplier's systems.

Customer downloads are also tightly controlled through a license key process which requires renewal on an occasional basis (once every 1, 2 or 3 years, depending on the license purchased). This approach further helps minimize grey market issues, since non-authorized users would not have access to the new keys.

Linking security and quality systems: Given the relative simplicity of their hardware products, FireEye leverages its contract manufacturers' quality management system to identify and track every product by serial number, manufacturing assembly line and field performance. Additionally, FireEye closely monitors metrics from the field to assure quality issues are quickly addressed if anything arises. Appliances are commonly returned to FireEye for complete route cause analysis on appliances that have gone bad in the field.

Managing risks in the service depots: Another area of concern is the downstream risks where the product can be altered after final assembly. FireEye works with channel partners, but not to store product. Any appliance moving through its partners has been pre-assigned to an end user.

The company has 21 global service depots for inventory. In the event a unit fails in the field, it is replaced with a unit from the service depot. While FireEye leverages a global partner to manage all the depots, in some more remote locations, they are subcontracted to a 2nd tier vendor. In these cases, the vendor is vetted using standard selection processes. FireEye applies inventory controls in the depots, but believes that tampering risks tend to increase the longer the inventory sits in the depot. The service depots help monitor risks by assessing each returned product from the field for counterfeit or tampering.

Supply chain continuity strategies: If a product is in short supply because of unexpected demand or a disruption in supply, there is risk in going to alternative suppliers. Similarly, when products are being phased out, there are secondary markets in which to purchase those products. But, relaxing standards around the approved vendor list (AVL) creates new risks of poor quality or tampering.

FireEye uses two principal supply chain continuity strategies. The first is simply to mitigate the risk of disruption through its use of standard industry components. The company recognizes that it cannot prevent major disruptions such as earthquakes or floods, but believes it is significantly less vulnerable than other companies which may be scrambling for customized components. However, strong and trusted supplier relationships create greater confidence that Fireye's suppliers will go the extra mile to ensure that commitments to Fireye are met, even when supplies have been disrupted.

The second approach is geographic resilience. FireEye has the manufacturing and test infrastructure capacity to build product in three locations — Silicon Valley, the Midwest, and Central Europe.

Transportation Security: Kip Shepard notes that Fireye ensures that its products are moved via carriers certified to CT-PAT standards (Customs Trade Partnership Against Terrorism) in order to minimize the risk of tampering during shipment. For additional security, tamper proof seals are placed on all units at the time of manufacture.

Industry Best Practices

As a leader in solutions that help manage cyber security in their customers supply chains, FireEye is well positioned to recommend cyber security supply chain practices to complement their software.

At the component level, it is important for companies to have strict knowledge of their manufacturing and design controls and test sufficiently for malicious code. If a company uses custom components like programmable ASICs, it needs to make sure its supplier is not inserting malicious code into the components. Companies also need to keep their manufacturing operating processes tightly controlled, both at the assembly site and in transit to depots or customers.

FireEye is also proponent of standards and actively participates in the development of industry standards such as National Institute of Standards and Technology (NIST) SP 161, Supply Chain Risk Management Practices for Federal Information Systems and Organization, NIST-800 53, Federal Information Security Management Act (FISMA) and SANS Consensus Audit Guidelines (CAG), as well as EU, NATO, and the Australian Defense Signals Directorate (ASD) guidelines.[4] The company was also involved in the development of NIST's Framework for Improving Critical Infrastructure.[5]

4 https://www.fireeye.com/solutions/government.html.

5 http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_fireeye_yaniv.pdf.