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

CASE STUDIES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Observations from Industry

Anonymous Consumer Electronics Company

February 4, 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.02042020-2

Jon Boyens
Celia Paulsen
Computer Security Division
Information Technology Laboratory

Nadya Bartol
Kris Winkler
James Gimbi
Boston Consulting Group

SERIES DESCRIPTION

The *Case Studies in Cyber Supply Chain Risk Management* series engaged with several companies that are mature in managing cyber supply chain risk. These case studies build on the Best Practices in Cyber Supply Chain Risk Management case studies originally published in 2015 with the goals of covering new organizations in new industries and bringing to light any changes in cyber supply chain risk management practices.

For information on NIST's Cyber Supply Chain Risk Management project, see https://csrc.nist.gov/projects/cyber-supply-chain-risk-management.

DISCLAIMER

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose.

Contents

Company Overview

The Consumer Electronics Company is a major American manufacturer of high-end audio equipment including amplifiers, subwoofers, speakers, processors, and source units. The company's research and development support the production of advanced original equipment manufacturer (OEM) and aftermarket systems for automobiles, off-road vehicles, and marine vehicles.

Risk Profile

Performance and reliability are key competitive factors in the high-end consumer electronics market. Successful products require consistently sourced components and rigorous quality assurance. Customer confidence in the performance and reliability of their brands is a significant asset for the Consumer Electronics Company. The principal driver for the company's cybersecurity and supply chain risk management practices is preventing supply chain incidents that may negatively impact that confidence, such as quality control failures, retail availability issues, and counterfeit products.

Highlighted Practices in Cyber Supply Chain Risk Management

- **Public-private partnerships.** The Consumer Electronics Company participates in the U.S. Customs and Border Protection's Customs-Trade Partnership Against Terrorism. The program provides cost-reduction incentives to the company and their suppliers to develop robust supply chain and cybersecurity practices.
- **Collaborative supplier relationships.** Successful supply chain risk management (SCRM) and cyber supply chain risk management (C-SCRM) increasingly require thoughtful coordination between suppliers and acquirers. The Consumer Electronics Company deliberately fosters personal relationships with their suppliers with regular on-site visits and informal touchpoints to build mutual trust and understanding of each business, empowering robust risk management over time.
- **Dedicated platforms for supplier management.** The Consumer Electronics Company strongly recommends implementing dedicated platforms to securely and consistently manage supplier activities. These platforms help the company avoid inconsistent and *ad hoc* supplier management processes which may be vulnerable to business email compromise, sophisticated spear phishing, and other cyber-attacks.

Organizational Approach to Supply Chain Risk and Cybersecurity

The Global Sourcing team is responsible for traditional SCRM. While SCRM is formally dedicated to this team, the Consumer Electronics Company encourages open communication for concerns relating to product integrity and risk. The company considers broad executive attention an important component for handling supply chain risk and leadership roles with formal SCRM responsibilities, including the CEO, CFO, VP of Global Sourcing, and Director of Information Technology. In particular, the internal information technology team works directly with Global Sourcing to mitigate potential cybersecurity threats presented by suppliers and upstream components.

The Consumer Electronics Company fosters a strong security culture. Employees are trained on basic cybersecurity hygiene, regularly experience controlled phishing exercises, and are encouraged to actively participate in managing cybersecurity risk. Several employees have leveraged the company’s open door policy to report potential risks to leadership. The information security team enforces the principle of least privilege, and the user base has historically been enthusiastic about new security tools and processes.

Supplier Management

Key Aspects of Managing Supplier Relationships

Strong supplier relationships are a core element of the Consumer Electronics Company’s supply chain management. The company deliberately fosters formal and personal relationships with all partners and suppliers and has worked with some suppliers for over a decade. This personal approach helps build a better mutual understanding of each business and strong trust over time. To maintain these relationships, the company’s employees perform informal touchpoints and attend regular on-site meetings with each supplier. These meetings occur quarterly for some critical suppliers.

Relationships are managed directly by the development team responsible for the ultimate product. Whenever possible, the Consumer Electronics Company will source new components from existing suppliers to minimize complexity and strengthen existing relationships. When new vendors are required, the Global Sourcing team will perform an assessment of the new supplier’s security practices. These assessments are largely driven by the company’s experience with supply chain incidents, cyber hygiene best practices, and conformance with security requirements from the U.S. Customs and Border Protection’s (CBP) Customs-Trade Partnership Against Terrorism[i] (CTPAT) program.

CTPAT is the Department of Homeland Security’s largest public-private partnership for supply chain risk management. The voluntary program grants the Consumer Electronics Company a low-risk customs designation for demonstrating compliance with a broad range of supply chain security assurances, including secure transit and storage, personnel controls, and IT security. This special customs designation significantly reduces overhead and delay for the company and their suppliers. To maintain this certification, the Consumer Electronics Company's logistics partners and suppliers must demonstrate that they meet all of the program's security requirements. In addition to the assessment performed by the internal team, all contracts require these partners and suppliers to complete an annual survey about their security practices.

Measuring Supplier Risk

The Consumer Electronics Company's principal driver for managing supply chain risks is getting their products to their customers. For this reason, the potential delivery impact of a supply disruption and the cost to secure alternative sourcing determines the criticality of each supplier. The company's strong supplier relationships provide a broad understanding of how each of those suppliers operate. Observations from these relationships produce detailed insight into each supplier's risk profile. The Consumer Electronics Company derives the relative risk of each supplier from these risk profiles and that supplier's criticality to the company.

Suppliers with access to the Consumer Electronics Company's sensitive intellectual property are considered highly critical. Many suppliers require protected material, such as proprietary engineering diagrams, to produce their components. The Consumer Electronics Company has no direct control once a supplier receives that material and depends on the supplier to protect their intellectual property from theft or unlicensed use. While such incidents are rarely attributed to formal suppliers, the potential for counterfeit production is considered a significant competitive risk and is closely monitored.

The Consumer Electronics Company prefers to work with small businesses. Representing a significant portion of a supplier's revenue allows the company to more effectively impact supplier cybersecurity posture and supply chain risk management practices. The company has observed that this leverage lowers the risk of contract compliance violations, component quality issues, and counterfeit devices on the market.

Quality Management and Continuous Improvement

As the Consumer Electronics Company's business as an automobile OEM supplier continues to grow, downstream customer requirements are driving the company to mature their supply chain program. In 2015, Fiat Chrysler recalled 1.4 million cars[ii] after Wired Magazine[iii] revealed that a cybersecurity vulnerability exposed affected vehicles to remote control, allowing an attacker to manipulate steering, braking, and audio systems. The resulting public attention led to greater investment in C-SCRM throughout the auto industry. The industry's enhanced requirements for the Consumer Electronics Company and other suppliers include stronger controls for upstream supply partners, highlighting the value of the company's CTPAT participation.

More generally, all supplier components are subject to pre-production and post-production testing. While most tests are performed internally, supplier contracts grant the Consumer Electronics Company the right to engage third-party evaluators. Serial numbers cannot be assigned to products until devices pass the full battery of tests.

Incident Response and Recovery

The Consumer Electronics Company formally reviews incident details to mature their security posture and incident resilience. In one instance, a supplier's email system was compromised by a remote attacker. The attacker observed emails between the supplier and the Consumer Electronics Company's employees for several months before crafting a fraudulent payment request, leveraging the cadence of an existing business relationship. While ultimately unsuccessful, the attack highlighted the need to secure and formalize interactions with business partners. The company has since enforced the use of a controlled vendor web portal, added formal approvals to potentially impactful business processes, and extended limited access to their product data management platform to a select subset of vendors. These controls are designed to limit the potential impact of a successful cybersecurity attack against critical suppliers.

Alternate sourcing is key to the Consumer Electronics Company's supply chain incident management. Because their products are built on established technologies, several of their existing suppliers are capable of manufacturing components produced by other suppliers. This allows the company to rapidly switch providers in the event that any one supplier is disrupted or compromised. To facilitate the migration to an alternate supplier after a supply disruption, two- to three-month reserves are held for each component involved in manufacturing.

Lessons Learned and Improvement Opportunities

The Consumer Electronics Company recommends that companies interested in maturing or developing C-SCRM programs invest in unified secure platforms for all formal information exchanges with suppliers. The added confidentiality and authentication provided by these platforms protect the inherently sensitive material in supplier communications, limiting the potential for fraud, theft, and cybersecurity breaches. These platforms also streamline supplier management, simplifying sourcing functions beyond risk management.

The Consumer Electronics Company is evaluating approaches to mitigating exposure to geopolitical volatility. While supplier relationships have been reliable, current events are drawing attention to potential escalations in trade tensions. As a result, the company is working with their suppliers to diversify operations into multiple countries.

References

[i] CTPAT: Customs Trade Partnership Against Terrorism, U.S. Customs and Border Protection, https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat, (retrieved September 16, 2019)

[ii] Fiat Chrysler recalls 1.4 million cars after Jeep hack, British Broadcasting Corporation, https://www.bbc.com/news/technology-33650491, (retrieved September 16, 2019)

[iii] Hackers Remotely Kill a Jeep on the Highway—With Me in It, Wired, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, (retrieved September 16, 2019)