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

CASE STUDIES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Observations from Industry

Anonymous Consumer Goods Company

February 4, 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.02042020-3

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 Goods Company is an American multinational company and one of the world's leading food manufacturers. The Consumer Goods Company's products include many of the world's most recognizable food brands and are sold in 180 different countries.

Risk Profile

The Consumer Goods Company operates over 140 factories and works with over 20,000 suppliers. Many of their products require dynamic sourcing from very small suppliers for raw materials and services, which in turn requires flexible supply chain practices. The Consumer Goods Company must facilitate this flexibility at scale without compromising rigorous product consistency and high cybersecurity and supply chain risk management standards.

Highlighted Practices in Cyber Supply Chain Management

- **Measured flexibility in contract requirements.** Rigorous cyber supply chain risk management requirements are included in all supplier contracts. However, the Consumer Goods Company is sensitive to unique supplier capabilities and may accept alternative mitigating controls if they do not introduce unacceptable risk.
- **Capture third-party expertise.** Third-party assessments are used effectively to capture cyber supply chain risks. The Consumer Goods Company engages cybersecurity and supply chain risk consultants to develop internal capabilities and processes.
- **Cross-functional training.** Education and awareness are essential elements of successful cyber supply chain risk management. The Consumer Goods Company embeds supply chain risk associates with cybersecurity associates to raise cross-functional awareness and build cohesion across teams.

Organizational Approach to Supply Chain Risk and Cybersecurity

The Consumer Goods Company works with over 20,000 suppliers globally. While over 75 % of these supplier relationships are managed by the central commercial sourcing function, the rest are managed by local factories and business units. The central commercial sourcing function operates as a service for the rest of the business. When business owners request a specific product or service, commercial sourcing will research and recommend specific vendors. Commercial sourcing owns most aspects of the supplier relationship for the entire lifecycle, including developing requests for proposals, contract negotiations, and managing compliance checks.

At the Consumer Goods Company, responsibility for risk within a domain is allocated to the business unit responsible for that domain. Because cyber risk can impact and compound other risks, the company considers cybersecurity a fundamental success factor, nearly as critical to the business as the availability of key food ingredients. The Chief Information Security Officer (CISO) works with senior risk associates from each domain to identify and manage each domain's exposure to cyber threats. Commercial sourcing is one of the CISO's most important domain partners, and the relationship between these teams is very mature.

The Board is aware of the potential brand impact of cyber and supply chain risks and considers them strategic challenges. The Board meets with the CISO and the leader of commercial sourcing quarterly and recognizes that understanding the company's risk posture and the threat landscape is an important Board responsibility. Multiple members reach out to the CISO and the leader of commercial sourcing organization to discuss specific topics on an *ad hoc* basis. The senior executive team meets with leadership from the CISO and commercial sourcing organizations monthly and maintains strong formal and informal relationships.

Supplier Management

Key Aspects of Managing Supplier Relationships

The Consumer Goods Company uses contractual requirements consistent with data privacy regulations and the NIST Cybersecurity Framework[i] (NIST CSF) as the key means for managing cyber supply chain risks. New suppliers are required to have cyber insurance and provide assurance that contractual cybersecurity controls have been met. While these requirements are present in all baseline supplier contracts, the company is sensitive to unique supplier capabilities and may accept alternative mitigating controls if they do not introduce unacceptable risk. Commercial sourcing handles contract negotiations, and the CISO's organization and legal review proposed amendments to ensure relevant risks are appropriately addressed. However, the company will not consider amending compliance-related requirements. All suppliers must demonstrate conformance with relevant data privacy laws, such as the European Union's General Data Protection Regulation (GDPR).

Measuring Supplier Risk

The Consumer Goods Company's key driver for cyber supply chain risk management is product quality. A supplier's criticality is determined by that supplier's potential impact on the consistency and availability of the company's consumer products. Cyber risks that could impact product quality include inconsistent operations technology across production facilities, contagion from suppliers experiencing a cyber-attack, and factory-specific cybersecurity risks. The company conducts regular interviews with critical suppliers to determine the relative risk of each supplier relationship. The company also performs regular NIST CSF assessments of their internal supplier management practices to determine how mature these practices are and how they may impact supplier risk.

Quality Management and Continuous Improvement

The maturity of the Consumer Goods Company's cybersecurity and supply chain risk posture is driven by a combination of internal and external expertise. Third-party assessments are an important tool to capture relevant cyber risks and identify appropriate mitigations. The Consumer Goods Company engages cybersecurity and supply chain risk consultants to evaluate and stress test existing processes and controls. Each year, third-party assessments include compliance audits, penetration tests, strategic planning, and tabletop exercises. Tabletop exercises are dynamic simulations of a complex incident with representative stakeholders from every impacted domain, including CISO organization, commercial sourcing, legal, and executive leadership. These simulations have identified a number of opportunities to improve capabilities and processes, and the company intends to include representatives from critical suppliers in future exercises.

Internally, all cybersecurity-related incidents are managed through a comprehensive incident response protocol (IRP). After each incident, the IRP requires the performance of an after action review to identify opportunities to improve the company's detection and response processes. The after action review must include input from any suppliers affected by the incident, ensuring that the company continues to evolve as a responsible and effective incident management partner.

Incident Response and Recovery

All cyber-related supply chain incidents trigger the IRP. The IRP requires the company to create a legal channel for sharing information with all affected suppliers and partners. The company works with each supplier's technical team to discover the full scope and impact of the incident. The Consumer Goods Company strongly recommends that organizations interested in developing or maturing cyber supply chain risk management programs establish relationships with each supplier's technical leadership early in the partnership. Understanding how each business approaches cyber and supply chain events will streamline multi-party collaboration and management when an incident does occur.

The Consumer Goods Company often works with individual suppliers to elevate their cybersecurity and supply chain risk management posture. For example, the CISO organization occasionally identifies deficiencies while auditing a supplier's conformance to contract

requirements. When this occurs, the CISO organization works directly with technical leadership at the supplier organization to achieve contract compliance. Many suppliers are required to implement a cybersecurity policy that covers downstream suppliers to limit the impact of a potential incident resulting from a compliance deficiency to the Consumer Goods Company.

Lessons Learned and Improvement Opportunities

The CISO considers the cyber awareness of commercial sourcing risk associates to be an essential element of successful cyber supply chain risk management. The commercial sourcing organization strives to raise their understanding of core cybersecurity principles to the level of the CISO organization's management by establishing a close partnership that includes embedding associates with the CISO's organization whenever appropriate. The experience enables the commercial sourcing team to make better informed decisions when working with suppliers and has the added benefit of building cohesion between these teams.

References

[i] Cybersecurity Framework, NIST, https://www.nist.gov/cyberframework, (retrieved September 16, 2019)