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

CASE STUDIES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Observations from Industry

Seagate Technology

February 4, 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.02042020-7

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

Seagate Technology (commonly known as Seagate) is an American multinational company headquartered in Cupertino, California. Seagate is one of the world's leading manufacturers of digital storage devices, including hard disk drives, solid state drives, and storage subsystems. Digital storage is vital to the systems, data centers, and analytics that drive the increasingly data-driven economy, and Seagate's offerings are relied upon by consumers and businesses around the globe.

Risk Profile

The digital storage industry is centered on trust. Storage is vital for most digital products and services in the digital economy, and customers must trust that their storage solutions will not fail and that their data is protected. For Seagate, this means product integrity has an immense impact on the brand.

Seagate produces over 100 million highly complex products every year, necessitating a large and interdependent supply chain. The sheer scale of these relationships obliges the company to develop and maintain robust and consistent risk management processes. Seagate has been recognized and awarded for their supply chain management practices by organizations including Gartner and Supply Chain Insights.

Highlighted Practices in Cyber Supply Chain Risk Management

- **Standards-oriented requirements simplify cyber supply chain risk management (C-SCRM).** Managing risks across a large number of diverse suppliers necessitates a clear, scalable, and defensible foundation. Seagate achieves this by leveraging international standards.
- **Internal alignment streamlines incident management.** Supply chain incident response requires cross-organizational cooperation. Seagate eliminates friction between disparate functional teams by aligning incident management processes and procedures across all security and risk teams.
- **Continuous improvement.** C-SCRM processes must rapidly incorporate information about new hardware and software vulnerabilities. Seagate leverages open-source intelligence, cross-functional tabletop exercises, and post-incident reporting to improve their incident management practices.
- **Suppliers welcome C-SCRM support.** Many suppliers now recognize the value of robust cybersecurity and supply chain risk management programs. Seagate finds that most suppliers are happy to work together to mature their internal practices.

Organizational Approach to Supply Chain Risk and Cybersecurity

Seagate maintains a consistent and holistic approach to security and risk through its Enterprise Security Risk Management (ESRM) Steering Council. This organization is composed of four pillars: the Product Security Office (PSO), information security, data privacy and protection, and physical security, which is handled by Global Trust and Security. While each pillar is responsible for risk within its own domain, they share a common incident management framework based on the National Institute of Standards and Technology's Cybersecurity Framework[i] (NIST CSF). This empowers the four groups to cohesively handle incidents that impact multiple domains, such as an incident involving the IT security and Global Trust and Security teams. This consistency also simplifies administration for senior leadership, providing a common playbook and response culture across separately managed teams.

The ESRM council meets with the Seagate Board of Directors every six months to deliver bottom-up risk recommendations from practitioners in the ESRM's four pillars. These high-level recommendations are supported by business impact estimations derived from analyses of technical metrics. For instance, the IT security team determines the potential business impact of a given vulnerability by applying Common Vulnerability Scoring System (CVSS) scores and Common Vulnerability and Exposure (CVE) ratings to affected Seagate assets. The Board is increasingly cyber-literate, and the shared lexicon provided by the common incident management framework streamlines communication between executive leadership and practitioners.

A core element of Seagate's C-SCRM practice is the division of supplier management responsibilities within the company. Business unit owners select their own suppliers and serve as the principal manager for those relationships. Separately, the compliance and certifications team (CCT) is responsible for identifying supply chain cyber risks, building mitigating compliance requirements, and enforcing those requirements. All supply chain changes are approved by this team, including new suppliers and contract renewals. The CCT works with the ESRM's four pillars to design impactful security requirements for Seagate's suppliers.

Supplier Management

Key Aspects of Managing Supplier Relationships

Contractual requirements, conformant with international standards and managed by the CCT, are the cornerstone of Seagate's C-SCRM practice. While Seagate's business owners manage supply delivery and execution, they must use a global contract template with the concrete security requirements issued by the CCT. These requirements, including cybersecurity controls, are built into the global contracting process and must be met before the partnership can move forward. Suppliers must refresh compliance with these requirements annually, and the CCT ensures that all existing suppliers comply with new requirements as they are adopted. This approach also ensures consistent expectations and global compliance from all vendors.

Seagate has found that standards-oriented requirements provide a consistent and easily defensible platform to empower supplier adoption and manage downstream compliance with customer requests. The ESRM selected International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 20243[ii, iii] and ISO/IEC 15408[iv] for their comprehensive scope and clear, actionable guidance. This clarity simplifies supplier compliance and streamlines assessments and enforcement by Seagate's global audit team. Because Seagate also enforces conformance with these standards internally, the company is better positioned to comply with supply chain security requirements from downstream customers. Seagate considers standards-oriented requirements to be the key feature of their C-SCRM programs and recommends standards as the starting point for any organization looking to improve their cyber supply chain risk practice.

Seagate strives to elevate all suppliers to the company's C-SCRM maturity level through its third-party compliance program, which allows the CCT to work with suppliers to develop road maps for meeting contract requirements. The PSO has found that suppliers were often independently interested in building resilient cybersecurity and supply chain processes but lacked direction. They were, therefore, often enthusiastic about Seagate's willingness to help mature their practices and meet the instructive standards-oriented requirements.

Measuring Supplier Risk

Seagate aims to account for the holistic risk profile of each supplier, including the business sensitivity of a given component, product integrity, and long-term stability. The PSO is principally responsible for tracking this range of cyber supply chain risks to products. This team will assign each vendor a criticality score based on the potential business impact of failure or compromise. That business impact is based on product delivery and quality, availability of alternative sourcing, and cybersecurity risks to both discrete products and Seagate at large.

The complex digital nature of Seagate's products means that the PSO has to manage disparate vectors of product quality. Beyond tracking logistics, materials, and assembly, the team must test for flawed or deliberately compromised hardware and software. Because of this, Seagate considers all suppliers providing software or complex hardware critical. The PSO works directly with suppliers to get ahead of these risks and develop incident response procedures. Likewise, suppliers that require access to the Seagate network have elevated criticality and are subject to constant security monitoring. The PSO works with the IT security team to provide these suppliers with the minimum amount of access and privileges necessary to perform their work. Beyond the standard security requirements set by the CCT, these suppliers must demonstrate that they meet Seagate's internal cybersecurity standards.

Supplier stability is another vital factor. If the PSO estimates that a critical supplier may not be viable in coming years, Seagate may find alternative suppliers, change the nature of a product, or even terminate a product.

Quality Management and Continuous Improvement

The complexity and volume of Seagate's production relies on the dependability of their large and extended direct supplier base. The PSO team considers over 45 suppliers critical, with potential disruptions representing a significant risk to product security. Those disruptions to critical suppliers can occur without actionable notice, as demonstrated in 2011 when tropical storm Nock-ten caused severe flooding in Thailand[v]. Because most hard disk manufacturers were reliant on suppliers in the affected region, the flooding materially affected the global hard disk drive supply. Consequently, Seagate requires business teams to identify alternative sourcing for all critical supply.

Beyond the risk of regional disasters like floods, alternative sourcing must consider economic and geopolitical risks. For instance, diplomatic volatility has directed Seagate's attention to potential escalations in trade tensions, such as tariffs and sanctions. Each country's domestic policy could also cause supply chain disruptions. Since more countries are considering data localization laws, Seagate is preemptively regionalizing data and service suppliers to mitigate the impact of any such mandates.

Seagate dynamically adjusts quality controls to meet new challenges. For instance, in 2017, the PSO rapidly evaluated and adjusted their quality management practices following the discovery of instruction set-level vulnerabilities called Spectre and Meltdown[vi]. Seagate leverages its global audit team to more clearly understand the impact of similar incidents on suppliers.

Incident Response and Recovery

Within the PSO, Seagate's product security operations center (PSOC) is responsible for detecting and responding to potential security incidents across more than 45 critical suppliers. While the PSOC does take advantage of automated incident detection tools, many product security events are detected and reported by employees in the CCT or the affected business teams. High-severity incidents may be escalated to the corporate incident assessment team, which is supported by the leadership of the ESRM.

This large-scale cooperation relies on clear and consistent cross-domain processes and communication. The adoption of a common incident framework across the ESRM streamlines that cooperation and results in rapid execution and response. Seagate performs a 360-degree review of incidents to improve their detection and response processes. These improvements are also informed by regular, cross-functional table-top exercises.

Information sharing and proactive collaboration has been beneficial for Seagate's C-SCRM program. Seagate participates in community-driven information sharing initiatives through programs including the CERT Coordination Center and the Department of Homeland Security's National Cybersecurity and Communications Integration Center. Internally, all four pillars of the ESRM share event information, and the incident response program establishes procedures for working with supply chain partners. Seagate establishes response and communication processes with all supply partners for incidents that may impact both parties. To effectively reach the public, Seagate.com maintains a dedicated product security advisory service[vii].

Lessons Learned and Improvement Opportunities

Seagate has found that their standards-oriented approach to supplier risk has greatly streamlined their C-SCRM processes. Leveraging external authority gives their supplier security requirements a defensible position and makes compliance attractive to suppliers and business partners concerned about their own security posture. Because of the clear assessment guidance, this approach can scale to Seagate's enormous supply chain demands and be applied to virtually every supplier on the market.

Seagate continues to develop a risk-resilient culture within their own organization and throughout their supply chain. Through investments in supply chain-oriented risk metrics and new PSO team tool development, the company aims to remain a leader in the C-SCRM space and continue to provide actionable insight for supply chain interdependencies.

References

[i] Cybersecurity Framework, NIST, https://www.nist.gov/cyberframework, (retrieved September 16, 2019)
[ii] ISO/IEC 20243 Part 1: Requirements and Recommendations, International Organization for Standardization, https://www.iso.org/standard/74399.html, (retrieved September 16, 2019)
[iii] ISO/IEC 20243 Part 2: Assessment procedures, International Organization for Standardization, https://www.iso.org/standard/74400.html, (retrieved September 16, 2019)
[iv] ISO/IEC 15408: Common Criteria, International Organization for Standardization, https://www.commoncriteriaportal.org/, (retrieved September 16, 2019)
[v] Thailand Flooding Cripples Hard-Drive Suppliers, New York Times, https://www.nytimes.com/2011/11/07/business/global/07iht-floods07.html, (retrieved September 16, 2019)
[vi] Vulnerabilities in modern computers leak passwords and sensitive data, Meltdown and Spectre, https://meltdownattack.com/, (retrieved September 16, 2019)
[vii] Seagate Security Advisories, Seagate, https://www.seagate.com/support/security/, (retrieved September 16, 2019)