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

CASE STUDIES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Observations from Industry

Mayo Clinic

February 4, 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.02042020-5

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 2
Risk Profile 2
Highlighted Practices in Cyber Supply Chain Management 2
Organizational Approach to Supply Chain Risk and Cybersecurity 3
Supplier Management 3
Key Aspects of Managing Supplier Relationships 3
Measuring Supplier Risk 4
Quality Management and Continuous Improvement 4
Incident Response and Recovery 4
Lessons Learned and Improvement Opportunities 5
References 5

Company Overview

The Mayo Clinic is an academic, medical non-profit based in Rochester, Minnesota that serves over 1.2 million patients across Arizona, Florida and Minnesota each year. Patients from around the world come to their facilities for access to specialized treatment and equipment. The Mayo Clinic hosts five schools in its College of Medicine and Science, including a nationally-ranked clinical program and a leading medical research program[i].

Risk Profile

The Mayo Clinic spends over $4 billion across tens of thousands of suppliers each year. Medical centers are subject to heavy control by regulators and are responsible for ensuring that their supply chain partners comply with data management policies, such as the Drug Supply Chain Security Act and the Health Insurance Portability and Accountability Act (HIPAA). More critically, a compromised supply chain may impact the quality of patient care or cause patient harm. The Mayo Clinic makes significant investments in supply chain management to mitigate these risks, and has been recognized for their mature supply chain risk management practices by Gartner as a leader in healthcare supply chain management in their annual Healthcare Supply Chain Top 25[ii].

Highlighted Practices in Cyber Supply Chain Management

- **Centralize supply chain risk management.** Dispersed cybersecurity and supply chain risk functions may result in inconsistent and ineffective incident management. The Mayo Clinic enhanced traditional Supply Chain Risk Management (SCRM) and Cyber Supply Chain Risk Management (C-SCRM) by centralizing all supply chain risk responsibility into a single third-party risk management (TPRM) team.
- **Rigorous cybersecurity assessments and documentation.** The Mayo Clinic requires vendors in specific supply category groups to commission penetration tests and rigorous security assessments annually. The Mayo Clinic reviews vendor product design details and internal cybersecurity policies prior to contract decisions.
- **Identify and leverage supplier categories.** Many supply networks are too complex to operate a “one size fits all” approach to supply chain risk management. The Mayo Clinic classifies all suppliers into one of six supply category groups depending on the nature of the supplied product or service. Separate onboarding processes and contract terms and conditions for each group ensure that supplier requirements are commensurate with compliance and management requirements.

Organizational Approach to Supply Chain Risk and Cybersecurity

The Supply Chain Management (SCM) organization is the central body responsible for sourcing and contracting throughout the Mayo Clinic. SCM divides all suppliers into broad supply category groups—including medical devices, medical supplies, medical equipment, services, information technology, and pharmaceuticals—to support compliance obligations and particular management requirements of each category.

Within SCM, the centralized supply chain audit/controls and business continuity (SCACBC) team is responsible for managing financial, supply chain resiliency, and cyber supply chain risks across all six supply category groups. SCACBC functions as an internal audit team, and collaborates with the Mayo Clinic's Office of Information Security (OIS), IT, legal, and compliance teams to perform risk assessments of select vendors. These assessments include supplier risk profiling, operational performance metrics, external threat monitoring, and financial audits. This unified SCRM practice simplifies supplier management and empowers SCM to quickly address supply chain events or threats. The Mayo Clinic considers their centralized approach a key factor to their successful supplier risk management.

Supplier Management

Key Aspects of Managing Supplier Relationships

The Mayo Clinic's vendor onboarding process is a critical tool for cyber supply chain risk management. Suppliers are contractually obligated to comply with the Mayo Clinic's information security schedule or demonstrate mitigating controls to account for particular requirements. These requirements include cybersecurity, physical security, and ethical behavior requirements particular to their product or service category group. Many of these requirements are publicly available for potential suppliers to review before engaging the Mayo Clinic[iii,iv].

New suppliers are subject to a cybersecurity assessment by the Mayo Clinic's OIS. The OIS interviews the supplier's information security staff and reviews internal policy, cybersecurity attestations, and process documents to determine whether the vendor is conformant to the cybersecurity requirements established for the relevant supply category group. Particular emphasis is placed on the supplier's handling of regulated data, third-party network access, and secure software development practices. Moreover, complex medical devices invoke specialized requirements, such as detailed design diagrams, evidence of rigorous vulnerability assessments, and supporting documentation.

At the conclusion of the assessment, the OIS provides a cybersecurity risk report to SCM who assists the business proponent in making a procurement decision based on this report and on the supplier's bankability and regulatory status. Suppliers must conduct external information security assessments and penetration tests annually, and the Mayo Clinic reserves the right to verify conformance with site audits at the suppliers' facilities. The Mayo Clinic declines to work with suppliers that present high instability or cybersecurity supply chain risk if they cannot effectively mitigate those risks.

Measuring Supplier Risk

The Mayo Clinic purchases products and services from tens of thousands of suppliers every year. Of these, just under 100 suppliers are considered primary suppliers. Potential impacts to care processes and business continuity are key factors in the criticality determination. The Mayo Clinic developed a proprietary process for determining the relative criticality between suppliers through a combination of qualitative and quantitative input. Greater criticality is also placed on the suppliers of products that contribute to long-term strategic initiatives.

Quality Management and Continuous Improvement

The pace of change in digital products and services presents a significant challenge in cyber supply chain risk management for healthcare networks. The wide range of medical devices and services creates a dynamic attack surface that requires uncommon expertise to identify how new threats might impact the organization. The Mayo Clinic will often leverage outside expertise from security audit firms to mitigate these risks and develop internal capabilities.

Executive leadership believes cyber supply chain risk management will continue to represent a significant challenge to the healthcare industry. The offices of the Chief Financial Officer, Chief Risk Management Officer, Chief Information Officer, and Chief Information Security Officer are developing the next generation of their third-party management practice to stay ahead of the threat. This third-party risk management initiative will include holistic protections throughout the entire supplier relationship lifecycle by enhancing proactive monitoring capabilities, a more comprehensive termination process, and a unified vendor onboarding process.

Incident Response and Recovery

The key focus of the Mayo Clinic's cybersecurity and supply chain incident response plans is the continuation of patient care. A dedicated business continuity team within the SCM manages supply chain resiliency events, which are often first identified by other hospitals and health networks that share the supplier. For instance, when the Illinois Environmental Protection Agency shut down the medical supply sterilization company Sterigenics[v] in February 2019, the Mayo Clinic's business continuity team proactively engaged vendors reliant on Sterigenics to identify alternative sourcing. The business continuity team stores safety reserves of critical supplies to mitigate the impact of supply chain disruptions. While most Mayo Clinic facilities leverage high-efficiency "just-in-time" operations and supply delivery, these reserves may be deployed to any facility in the network.

The business continuity team works in conjunction with the OIS to handle cyber supply chain incidents, such as mitigating the impact of ransomware on a supplier. The OIS is also responsible for detecting and responding to potential cybersecurity incidents across all suppliers and products that require access to network resources. Documents provided during the onboarding process give the OIS a detailed understanding of the potential attack surfaces exposed to a given supplier. These suppliers provide their formal incident response plans and processes, enabling effective collaboration between the supplier and the OIS during an incident.

The Mayo Clinic's leadership has been working with other integrated delivery networks and hospitals to develop a more unified approach to managing supply chain resiliency issues present in the healthcare industry. The Mayo Clinic is an active participant in the cyber supply chain risk management community, regularly contributing to conferences and other events hosted by organizations like Gartner and Vizient.

Lessons Learned and Improvement Opportunities

The Mayo Clinic recommends that companies interested in maturing or developing C-SCRM programs establish a central risk management team responsible for the entire organization. Fragmented cybersecurity and supply chain risk functions may lead to complicated and expensive management, as well as inconsistent and ineffective execution. This team should leverage existing expertise for their assessments by engaging other teams, such as the internal information security and compliance teams.

When designing a C-SCRM roadmap, the Mayo Clinic encourages organizations to be sure that their program features the following elements:

- Clearly defined governance, operational structure, policies, and procedures
- Dedicated TPRM software platform
- Business process automation to support ongoing monitoring and escalation
- Data warehouse for all third-party engagements, contracts, access, and data-sharing agreements
- Systematic supplier off-boarding and access controls
- Comprehensive inclusion of hardware, software, medical devices, networked equipment, data sharing, non-employee access, and research systems

The Mayo Clinic considers mature organizational change management and project management important enablers for successful C-SCRM implementation. Organizations should be aware that incremental, full-time equivalent investments and TPRM software licensing costs may be significant. C-SCRM can be a substantial undertaking and requires strong unity and support from executive leadership.

References

[i] Mayo Clinic School of Medicine (Alix) Overview, U.S. News & World Report, https://www.usnews.com/best-graduate-schools/top-medical-schools/mayo-medical-school-04053, (retrieved September 16, 20019)
[ii] Gartner Announces Rankings of Its 2017 Healthcare Supply Chain Top 25, Gartner, https://www.gartner.com/en/newsroom/press-releases/2017-11-16-gartner-announces-rankings-of-its-2017-healthcare-supply-chain-top-25, (retrieved September 16, 2019)
[iii] Supplier Information, Mayo Clinic, https://www.mayoclinic.org/about-mayo-clinic/supplier-information, (retrieved September 16, 2019)
[iv] Supplier Resources, Mayo Clinic, https://www.mayoclinic.org/about-mayo-clinic/supplier-information/resources, (retrieved September 16, 2019)
[v] Illinois EPA Shuts Down Suburban Sterigenics Plant, WTTW News, https://news.wttw.com/2019/02/15/illinois-epa-shuts-down-sterigenics-willowbrook, (retrieved September 16, 2019)