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

CASE STUDIES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Observations from Industry

SUMMARY OF FINDINGS AND RECOMMENDATIONS

February 4, 2020

This publication is available free of charge from:
https://doi.org/10.6028/NIST.CSWP.02042020-1

Jon Boyens
Celia Paulsen
Computer Security Division
Information Technology Laboratory

Nadya Bartol
Kris Winkler
James Gimbi
Boston Consulting Group

SERIES DESCRIPTION

This *Summary of Findings and Recommendations* summarizes the *Case Studies in Cyber Supply Chain Risk Management* series' major findings and recommendations based on expert interviews. The *Case Studies in Cyber Supply Chain Risk Management* series engaged information security, supply chain, and risk leaders across a diverse set of organizations. 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 current key practices in cyber supply chain risk management. This document describes trends, correlations, or other information garnered from an analysis of the case studies as a whole and may cover information not reported in the individual case studies. This document also contains recommendations for further research, study, and guidance development.

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

Acknowledgments

The authors—Jon Boyens of the National Institute of Standards and Technology (NIST), Celia Paulsen (NIST), Nadya Bartol of the Boston Consulting Group (BCG), Kris Winkler (BCG), and James Gimbi (BCG)—would like to acknowledge and thank a number of individuals who provided valuable insights and helped to improve this publication, especially Matthew Fallon (BCG) and Ravi Agarwal (BCG) for their contributions to the content during the document's development and review.

The authors would like to acknowledge and thank the companies that contributed to this case study series:

1. Mayo Clinic
2. Palo Alto Networks, Inc.
3. Seagate Technology PLC
4. Anonymous, Consumer Electronics Company
5. Anonymous, Consumer Goods Company
6. Anonymous, Renewable Energy Company

The authors would also like to acknowledge and thank the companies that contributed to the *Best Practices in Cyber Supply Chain Risk Management* NIST case study series published in 2015:

7. Boeing and Exostar
8. Cisco Systems
9. Deere & Company
10. DuPont de Nemours, Inc.
11. Exelon Corporation
12. FireEye
13. Fujitsu Ltd.
14. Great River Energy
15. Intel Corporation
16. Juniper Networks, Inc.
17. NetApp, Inc.
18. Northrop Grumman Corporation
19. Resilinc Corporation
20. Schweitzer Engineering Laboratories, Inc.
21. Smart Manufacturing Leadership Coalition
22. The Procter & Gamble Company
23. Anonymous, Communications Company
24. Anonymous, Utility

Executive Summary

The National Institute of Standards and Technology Computer Security Division's (CSD) Cyber Supply Chain Risk Management (C-SCRM) program collaborates with stakeholders across government, industry, and academia to identify, evaluate, and develop effective technologies, techniques, practices, and standards to secure the cyber supply chain. The program was launched in 2008 in response to Comprehensive National Cybersecurity Initiative #11, "Develop a multi-pronged approach for global supply chain risk management," and, in 2015, published its flagship guidance, Special Publication (SP) 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. NIST SP 800-161 provides guidance for identifying, assessing, and mitigating cyber supply chain risks, including counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices at all organizational levels. Later in 2015, NIST published *Best Practices in Cyber Supply Chain Risk Management,* an interview-based case study series describing how industry approaches C-SCRM, including specific tools, techniques, and processes. The C-SCRM project has informed the development of other NIST CSD publications, including:

1. NIST Cybersecurity Framework V1.1
2. NIST SP 800-37, Revision 2: *Risk Management Framework for Information Systems and Organizations*
3. Draft NIST SP 800-53, Revision 5: *Security and Privacy Controls for Information Systems and Organizations*
4. NIST Internal Report (IR) 8179: *Criticality Analysis Process Model*

This document is part of *Case Studies in Cyber Supply Chain Risk Management*—new research that builds on the CSD C-SCRM program's 2015 publications aimed at identifying how C-SCRM practices have evolved. For this case study series, NIST conducted interviews with 16 subject matter experts across a diverse set of six companies in separate industries, including: digital storage, consumer electronics, renewable energy, consumer foods, healthcare, and enterprise cybersecurity. These interviews informed the production of all documents in this series, including six individual company case studies, a summary of findings and recommendations, and a key practices document. This document summarizes findings and recommendations from the case studies. It describes trends, correlations, and novel findings garnered from an analysis of the interviews as a whole and may cover information not reported in any particular individual case study. This document also contains recommendations for further research, study, and guidance development.

The research concludes that C-SCRM is an evolving discipline that requires further attention from the user and research communities. While varied practices exist at mature organizations, less mature organizations are in need of further practical guidance and methods for implementing and evolving C-SCRM programs and practices. Proposed follow-up research opportunities include: quantitative cyber supply chain risk analysis and metrics; requirements to consider adding to supplier terms and conditions; sample supplier tiering structure (especially if an organization has a large number of suppliers) or other methods of applying criticality; and creating additional case studies that showcase mature C-SCRM programs that can be used by aspiring organizations as guidance.

Interviews with leaders responsible for C-SCRM[1]

The authors conducted in-depth interviews with six organizations that represented a variety of industry sectors and sizes. The purpose of this research was to better understand organizational viewpoints on Cyber Supply Chain Risk Management as well as the challenges faced by organizations. The goal was not to gain an understanding of the general consensus around the topic but rather to dive deeply into the experiences of a few organizations. The authors chose semi-structured interviews as the most appropriate method for collecting data about C-SCRM key practices for three reasons:

1. The status of C-SCRM key practices is often considered sensitive and is not broadly shared.
2. The subject matter is complex and non-standardized, meaning that organizations may use different terms for the same concepts.
3. Semi-structured interviews are superior to more quantitative data collection methods for studies that have these types of qualitative research goals.

The interviews were designed to capture organizations' viewpoints regarding C-SCRM key practices. Interview questions were developed and refined based on the expertise of Supply Chain Risk Management experts at NIST and Boston Consulting Group (BCG). The interviews were designed to provide a qualitative look at the organizations' C-SCRM priorities, barriers to implementing C-SCRM practices, and practical details of successful implementations without making assumptions about the practices those organizations employ.

Organizations were recruited based on their size and industry as well as whether they had previously published any material on this subject (e.g., white papers). The researchers targeted specific types of organizations that were not well represented in the case study series published in 2015. The interviewed industry verticals included: digital storage, consumer electronics, renewable energy, consumer foods, healthcare, and enterprise cybersecurity. The individuals representing the organizations interviewed were comprised of senior information security, supply chain, and risk leaders. Titles included: Chief Information Security Officer (CISO), Chair of Supply Chain Management, Vice President (VP) of Supply Chain, Office of Information Security (OIS) Director, Director of Information Technology (IT), Senior Manager, Cyber Security Manager, Product Security Officer, Senior Director of U.S. Policy, and other persons with different titles but similar responsibilities.

Notes from the interviews were reviewed for commonalities and differences, and were captured in this summary and recommendations document.

Summary of Findings

1. All of the interviewees affirmed that C-SCRM is a critical capability required for their organizations to reduce the risk of business interruption if a cyber incident were to occur.

[1] OMB control #: 0693-0043; expiration date: 03/31/2022

2. The eight C-SCRM Key Practices located in the Key Practices in Cyber Supply Chain Risk Management document can be directly correlated to the key themes noted in this document.
3. Mature C-SCRM programs exhibit close integration across functional and business lines, engage executive leadership effectively, align with business goals and objectives, foster close supplier relationships, and leverage industry standards throughout the supply chain lifecycle and plan for resilience.

Organizational Approach to Supply Chain Risk and Cybersecurity

This section outlines the trends in how the interviewed organizations approached cyber supply chain risk management in their organizational structure, policy development, and oversight.

Key Themes:

1. Integrated C-SCRM: Mature C-SCRM programs exhibit close collaboration across functional and business lines. These include supply chain risk leadership councils at the executive level, and numerous working meetings at the staff level. Collaboration across organizational lines of responsibility ensures that C-SCRM is treated as a priority, facilitates decision making with multiple perspectives, and helps organizations be proactive about their priorities. This, in turn, allows for timely responses to potential issues and more efficient engagement across the enterprise.
2. Standardized security framework: Organizations have adopted a standardized security framework (e.g., NIST Cybersecurity Framework). Frameworks allow organizations to establish a common language for C-SCRM across the enterprise, standardize internal and external assessments, and streamline incident communications and reporting.
3. Engagement of executive leadership in C-SCRM: Executives and Boards of Directors are engaged in C-SCRM through regular presentations and touchpoints. Such engagement demonstrates leadership commitment and importance of C-SCRM to the organization.
4. C-SCRM is driven by business priorities to ensure product and service delivery: C-SCRM is considered one of the critical capabilities that reduce the risks of disruption to product and service delivery if an incident were to occur. Organizations shared a variety of practices on how they identify, prioritize, and respond to cyber supply chain risks.

Integrated C-SCRM:
The level of integration of supply chain, cybersecurity, product security, and physical security increases with C-SCRM practice maturity. Other functions that participate in the process include engineering, legal, and human resources as appropriate for the specific organization's business. Mature companies have explicit roles that bridge these functions and integrate them with corporate enterprise risk management (ERM). Such internal alignment facilitates efficiency and effectiveness of delivering products and services while appropriately managing C-SCRM risks. The level and formality of C-SCRM integration varied among the interviewed organizations. Most organizations trended towards a more integrated structure, but the formality of this integration depended on the size of the organization. The following spectrum of integrated practices was observed through the interviews:

1. ***Supply chain function is responsible for C-SCRM with information security providing input:*** Traditional supply chain risk management is performed by a global sourcing team with cybersecurity-relevant inputs from information security teams to include cybersecurity threats facing the supply chain and relevant security requirements to use in sourcing. The

supply chain and information security teams perform joint post-incident reviews and hold annual conferences to discuss developments in the threat landscape.

2. ***Centralized team is responsible for C-SCRM:*** A centralized team is responsible for risk management across all supply category groups. The team functions like an internal audit team and collaborates with information security, IT, legal, and compliance teams to perform risk assessments of all vendors. This unified practice simplifies supplier management and is able to quickly address supply chain events or threats without escalation to executive leadership.
3. ***Blended approach:*** A centralized team provides guidance and oversight of C-SCRM with the business units responsible for supplier relationships. In this blended approach, all or a substantial portion of supplier relationships is managed by the centralized function, while the rest of these supplier relationships are managed by local business units. In general, the responsibilities are distributed between the centralized function and the business units as follows:
    a. The centralized team identifies cyber supply chain risks, develops security requirements for suppliers, and enforces those requirements throughout the organization. This team also approves supply chain changes, including new suppliers and contract renewals.
    b. The centralized team operates as a service for the rest of the business, which includes researching and recommending specific vendors when business owners require a specific product or service. This team owns most aspects of the supplier relationship for the entire lifecycle, including developing requests for proposals, contract negotiations, and managing compliance checks.
    c. Business unit owners are responsible for selecting and requesting their own suppliers and serving as the principal manager for those relationships.

Overall, organizations maintain a consistent and holistic approach to security and risk through a risk management council that includes participants from product security, information security, data privacy, and physical security. Additional functions that participate in the council may include engineering and legal.

Standardized security framework:

Most companies reported using a standardized framework to manage cyber supply chain risks across the organization. These frameworks are either based on standards and best practices (e.g., NIST Cybersecurity Framework (CSF), driven by regulations (e.g., North American Electric Reliability Corporation critical infrastructure protection (NERC CIP), Health Insurance Portability and Accountability Act (HIPAA)) or developed internally (e.g., through internal ERM framework). Having a standardized approach helps multiple teams across the organization to cohesively handle cyber supply chain risks. The following are some of the benefits of adopting standardized frameworks:

1. Simplifies oversight for senior leadership by providing a common playbook and response culture across separately managed teams.
2. Provides a single process for different groups that participate in C-SCRM to cohesively handle incidents that impact multiple domains (e.g., an incident involving information security and physical security concerns).
3. Establishes a unified way to identify, mitigate, and monitor risks through a policy-based approach using a single framework or standard.

4. Provides a set of secure development, IT, operational technology (OT), or physical security requirements for suppliers to meet prior to establishing a supplier relationship with the acquirer.
5. Provides a policy for supply chain to include criticality definitions, which all parties critical to digital security of the product must meet.

It should be noted that an organizational C-SCRM framework can be driven by applicable regulatory requirements.

Engagement of executive leadership in C-SCRM:
Most organizations reported that sponsorship at the executive leadership level was key to ensuring effective C-SCRM. Organizations consider broad executive attention an important component for handling supply chain risk and leadership roles with formal C-SCRM responsibilities, including the CEO, CFO, VP of Global Sourcing, CIO, CISO, Director of Information Technology, and Director of IT Security. C-SCRM is a regular topic of discussion with the Board of Directors. Observed practices for this theme are highlighted below:

1. The Board of Directors receives C-SCRM updates quarterly, semi-annually, or annually from a relevant executive (e.g., CISO). These presentations include status updates, recommendations from practitioners across the organization, challenges that need to be overcome, and business impact estimations derived from analyses of technical metrics. The common C-SCRM framework facilitates more robust communication with the Board, which is also increasingly cyber-literate.
2. The security leadership team reports to executive staff and meets quarterly to report on improvement areas. The working team meets more regularly to discuss progress on these areas.
3. The engagement by executives and Boards helps propagate the message that cybersecurity and C-SCRM are important business functions throughout the organization. As a result, employees understand that cybersecurity is a part of everyone's role.

C-SCRM is driven by business priorities to ensure product and service delivery:
Organizations view C-SCRM as a critical capability to ensure business resilience and minimize the impacts on delivery of the product and/or services to the client. The interviews captured several business goals and objectives for C-SCRM, depending on the specific businesses of the interviewees, including:

1. Minimize potential impacts to customer satisfaction, brand reputation, and shareholder value.
2. Minimize impact to cost, performance, timing, and availability of goods.
3. Ensure consistency across IT/OT platforms.
4. Meet regulatory responsibilities.
5. Ensure integrity and continuity of accounting processes (e.g., accounts receivable and accounts payable).
6. Mitigate lack of control of documents when sent to the supplier (e.g., IP theft).
7. Minimize impact to product quality.
8. Ensure visibility into how third-party Operations & Mainenance sites are built and used (i.e., no standard build out).

9. Move from detective to preventive capabilities in managing third-party cybersecurity risk.

There are a variety of ways organizations identify and prioritize cyber supply chain risks based on these goals and objectives, including:

1. Scanning the environment by deploying threat feeds, reviewing industry publications, or participating in industry groups.
2. Using assessments or audits to identify cyber supply chain risks.
3. Talent acquisition and training.
4. Establishing an initiative to improve supplier risk monitoring and potentially automating mitigation.
5. Identifying risks via regular communication and level-setting with suppliers.

Supplier Management

This section covers how the organizations determine criticality of a third-party product, component, or service, as well as the type of requirements they put in contracts and service agreements to cover security aspects such as quality, integrity, and confidentiality.

Key Themes:

1. Determining supplier criticality: Most organizations determine criticality of suppliers based on the potential impact to the business upon a failure or compromise of the supplier. Other factors include the level of supplier access, supplier stability, classification of data that supplier has access to, and strategic relevance of the supplier to the acquirer's business. Overall, acquirers need substantive insight into how suppliers operate to determine their criticality. Strong supplier relationships are helpful to getting such insight.
2. Establishing contractual cybersecurity requirements: Organizations include cybersecurity terms and conditions as part of contracts negotiations, commensurate with the criticality of the product, component, or service being procured. This helps ensure a minimum level of security on the supplier side and reduce the risk to the acquirer organization. There is variance in the extent to which such terms and conditions are enforced through contracts.

Determining supplier criticality:
There are various ways of determining the criticality of a third-party product, component, or service. For most organizations, criticality is determined based on the potential business impact of failure or compromise as well as the level of access that the supplier has to the network, facilities, and intellectual property. The following are the primary ways through which organizations determine supplier criticality:

1. **Supplier criticality based on potential business impact:** Each supplier is issued a criticality score based on the potential business impact of failure or compromise. The business impact is based on product delivery and quality, availability of alternative sourcing, and cybersecurity risks to both discreet products and the organization at large. The level of physical and logical access is also a consideration in determining criticality. Suppliers that require access to the organization's network have elevated criticality and are subject to constant security monitoring.
2. **Supplier criticality based on stability:** Supplier stability is another vital factor. If a critical supplier may not be stable or viable in coming years, organizations may find alternative suppliers, change the nature of a product, absorb production of the component provided by a supplier into the acquirer's organization, or even terminate a product's supply.
3. **Supplier criticality based on delivery impact:** Supplier criticality is also determined based on the potential delivery impact of a supply disruption and the cost to secure alternative sourcing. Strong supplier relationships are required to provide a broad understanding of how each of the critical suppliers operate. Observations from these relationships produce detailed insight into each supplier's risk profile. The relative risk of each supplier is then determined based on these risk profiles, and that decides the supplier's criticality.

4. **Other criteria to determine supplier criticality:**
    a. Suppliers with access to sensitive information, intellectual property or regulated data (e.g., protected health information [PHI]) are considered highly critical.
    b. Greater criticality is also placed on suppliers of products that contribute to long-term strategic initiatives.
    c. Supplier criticality is determined based on potential impact to the consistency and availability of the organization's products.

Establishing contractual cybersecurity requirements:

Mature organizations have established a standardized set of security requirements stratified by supplier criticality. These requirements are used in contracts, during negotiations, and for supplier onboarding. This enables organizations to incorporate security considerations early in the acquisition process, which helps establish and manage expectations in the supplier relationship. This also enables the supplier to improve their own security controls, which results in reduced risks to the acquirer. Some organizations do not have cybersecurity in contracts and/or do not consider the requirement to be comprehensive, and this is therefore an area to be improved. Compliance with cybersecurity-related terms and conditions is also a variable. While these requirements are often part of the negotiation process, they may be dismissed during the procurement process. Depending on the comprehensiveness of the requirements, level of enforcement, and supplier monitoring, organizations can expect greater or lesser transparency and visibility into cyber supply chain risks before these risks are realized. Comprehensive requirements, coupled with monitoring, can also help ensure that the security controls are maintained throughout the supplier relationship. The following are some observed practices related to incorporating cybersecurity terms and conditions in contracts:

1. Contractual terms and conditions include insurance, access requirements, and background checks.
2. Suppliers are contractually obligated to disclose component vulnerabilities, data loss, and security incidents.
3. The quality and interruption of supply are specifically mentioned in service agreements, though security is not called out.
4. Contractual terms and conditions include a specific section on information security requirements as well as consequences if there is a failure to comply with the requirements for security, quality, and integrity.
5. Contractual requirements include regular site visits, informal touchpoints, and supplier meetings.

Measuring Supplier Risk

This section describes how organizations are monitoring their suppliers and measuring supply chain risk. Mature acquirers establish supplier monitoring programs that cover the entire supplier relationship lifecycle, and monitor a variety of risks, including security, quality, financial, and geopolitical. This monitoring and review include validating whether or not suppliers are meeting cybersecurity and other key Service Level Agreement (SLA) requirements as well as any changes in supplier status (e.g., financial, legal, ownership, etc.).

Key Themes:

1. Measuring cyber supply chain risk: Measurement and reporting of cyber supply chain risks is an area of improvement for organizations. Limited metrics specific to cyber supply chain risks are currently being collected and reported.
2. Evaluating and prioritizing supplier risks: Each organization focuses on different risk factors depending on their business environment, but consistent focuses appear to be on minimizing the impact of disruptions in supply (including controlling costs associated with supply disruption) and mitigating the risk of compromise of the integrity of a product.
3. Communicating with suppliers: Day-to-day communication with suppliers is accomplished through traditional tools such as email, phone, and portals. Organizations also periodically survey suppliers to understand their cybersecurity posture and to monitor compliance with the contractual requirements.

Measuring cyber supply chain risk:
Most organizations do not have metrics that are specific to C-SCRM. However, several of them have planned initiatives to create and implement such metrics. An example of C-SCRM metrics that are reported is based on the Common Vulnerability Scoring System (CVSS) scores for the supply chain vulnerabilities. In that organization, the IT security team determines the potential business impact of a given vulnerability by applying CVSS scores and Common Vulnerabilities and Exposures (CVE) ratings to affected assets.

Evaluating and prioritizing supplier risks:
Risk factors for evaluating and prioritizing supplier cyber risks vary for each organization. However, the potential business impact of failure or compromise and mitigating the risk of compromise of product integrity are most common. Examples of how organizations are evaluating and prioritizing supplier cyber risks include:

1. Supplier risk identification is based on tribal knowledge and acquirer-supplier relationships.
2. Supplier risks are determined based on a self-assessment questionnaire completed by the supplier.
3. Risk assessments are performed early in the product development lifecycle to help determine the supply chain risks and feasibility of product design decisions.
4. At a minimum, suppliers go through a preliminary review process to check for sanctions against government watch lists.
5. Supplier criticality scores are utilized to prioritize supplier risks.

6. Industry standards and best practices, such as ISO/IEC 20001 and SOC 2 compliance reports, are used to evaluate supplier cyber risks.
7. NIST CSF assessments are used by the acquirers and suppliers to determine the maturity of C-SCRM practices.
8. Risks of tariffs and data regionalization are evaluated to manage supply chains that span across multiple countries.

Communicating with suppliers:

Most organizations communicate with suppliers on a regular basis via traditional enterprise communication methods, including email, phone, communications platforms (e.g., Skype, Zoom, etc.), and supplier portals (e.g., iSupplier). Organizations also survey their critical suppliers annually to ensure people, data, and policies are maintained and up to date relative to supporting the contracts. These surveys include a variety of cybersecurity practices, such as supplier personnel receiving security training, physical security measures, use of security cameras and adequacy of camera recording storage, IT and network security measures, security organizational data on external networks, and assessment of applicable compliance levels.

Quality Management and Continuous Improvement

Oversight of supplier C-SCRM practices is an important subject to every organization that was interviewed. Topics such as how to best monitor vendor quality against SLAs, company policies, and industry standards primarily drove the conversation. Additionally, organizations were focused on improving their vendors' security practices.

Key Themes:

1. Prominence of industry standards and frameworks: Whether organizations looked to international, national, or industry-specific publications, all utilize multiple frameworks to evaluate the quality of their internal and vendor-specific C-SCRM practices. Organizations also frequently supplement these frameworks with legal or certification-based requirements.
2. Inconsistent implementation of supplier security controls: Organizations often shared that the implementation of technical controls, such as enhanced monitoring and anti-virus capabilities, is not frequently validated and/or enforced for their suppliers. Acquirers are currently using compensating controls, such as education and training, but plan to augment those in the future with more comprehensive security controls.
3. Importance of supporting the supply chain: Nearly every interviewed organization shared success stories of how they were able to positively impact a supplier's security posture, for example, through mentoring and collaboration.
4. Risks of physical security outsourcing: Half of the respondents cited significant outsourcing of physical security and logistical controls, acknowledging that residual risks of this arrangement have not been consistently addressed.

Prominence of industry standards and frameworks:
Each interviewed organization uses some form of national standards or guidelines to underpin their internal C-SCRM policies and practices. A range of international standards are used in conjunction with national frameworks to ensure comprehensive coverage of controls across geographically distributed supply chains as listed in the table below.

National		International	
1.	NIST Cybersecurity Framework (CSF)	5.	ISO/IEC 15408
2.	Sarbanes-Oxley (SOX)	6.	ISO/TS 16949
3.	Customs Trade Partnership Against Terrorism (CTPAT)	7.	ISO/IEC 20243
		8.	ISO/IEC 27000 series
4.	American Institute of Certified Public Accountants (AICPA) SOC 2	9.	ISO/IEC 28000 series

When national and international standards are perceived as too high-level or generic, both industry and technology-specific standards are used to enhance controls as listed in the table below.

Industry	Technology
1. North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC CIP) 2. Health Information Trust Alliance (HITRUST)	3. Open Web Application Security Project (OWASP) 4. SANS Institute

Inconsistent implementation of supplier security controls:
Operational enforcement of standards, guidelines, or contractual requirements across supply chains was cited by nearly all respondents as a significant area for improvement. Pain points were varied but centered on the following trends:

1. Strategic plans concerning vendor compliance were preliminary with the primary focus on assessing supplier risks in the form of surveys, self-assessments, and contract reviews.
2. Monitoring, whether automated or manual, was rarely implemented with organizations either not monitoring supplier compliance or focusing exclusively on business-related metrics.
3. The implementation of protection mechanisms, like anti-virus and enhanced logging for critical suppliers accessing acquirer networks, was not comprehensive across organizations' supply chains.

Acquirers reported progress in implementing preventive or compensating controls to address the aforementioned supplier risks with notable highlights around:

1. Organizational realignment to mitigate supplier risks, such as dedicating personnel to assess supplier risks and effectively communicating them to executive leadership.
2. Operational technology (OT) risk reduction with most instances of prevention and monitoring (e.g., network segmentation, security information, and event management [SIEM] implementation) occurring on the OT portion of the acquirer networks.
3. Strict adherence to legal and regulatory requirements was well understood by the acquirers, and consistently enforced for impacted suppliers by requesting the completion of attestation questionnaires.
4. Use of compensating controls, such as training and awareness, for less mature organizations.

One of the more notable benefits of the mitigation of cyber supply chain risks came directly from suppliers who expressed relief that the organizations were providing clear requirements in an area of risk that they did not understand very well. Overall, the interviewed organizations describe their experience of pursuing supplier monitoring and compliance activities as positive.

Importance of supporting the supply chain:
Nearly all of the interviewed organizations provided examples of preventive and corrective actions taken to improve their suppliers' baseline cybersecurity practices. The scope and methodology behind those actions varied between organizations:

1. Requiring use of standards (e.g., ISO/IEC 27002, OWASP).
2. Requiring maturity assessment against industry frameworks (e.g., NIST CSF).

3. Requiring technical controls (e.g., anti-virus and patching requirements).
4. Advocating to enhance cybersecurity maturity at a community level (e.g., industry peer groups and supplier forums).
5. Auditing and assessing suppliers' internal administrative controls, compliance posture, and pre-/post-production checks.
6. Embedding of organizations' resources with suppliers to train and spread awareness of the importance of cybersecurity.

A subset of respondents indicated that their organizations' efforts typically focused on selecting only mature suppliers to help alleviate the maturity "uplift" activities cited above.

Risks of physical security outsourcing:

Organizations were split on their approach to physical supply chain security with half outsourcing and half retaining control in-house. Organizations that had outsourced physical security and logistics acknowledged the residual risk that resulted from this arrangement without active monitoring but have indicated that they have taken steps to extend internal controls to such vendors. Organizations that secure logistical functions in-house utilize a combination of internal policies and CTPAT guidance as baseline standards.

Incident Response and Recovery

Organizations are aware of the expanded attack surface that results from an interconnected and globally complex supply chain. Greater efforts are therefore already being applied to enhance supplier resilience, but progress remains to be made on proactive incident detection, response, and recovery.

Key Themes:

1. Event visibility and response capabilities: Organizations are in need of greater visibility into cyber supply chain disruptions, both internally through a proactive formal security operations center and externally through supplier reporting requirements.
2. Redundancy and back-up supply: When unplanned events occur that cannot be addressed through enhanced visibility, critical components should be held in reserve, especially for those without an alternative supplier. For critical components, organizations consider negotiating terms to pay premiums in return for supplier assurance that critical components will be supported.
3. Comprehensive threat context: Industry organizations, threat intelligence services, and integrated delivery networks are essential to better understanding domestic and international events that may impact the supply chain, including economic and geopolitical risks.

Event visibility and response capability:
Organizations primarily learn of potential supply chain incidents through reactive measures like self-reporting, internal security testing results, and third-party notifications. Potential incidents are also uncovered during business-driven investigative activities like site inventory reviews for quantity or tampering and analysis of billing records for evidence of fraud or theft. Such means of detection are widely utilized and a step in the right direction but are infrequently augmented by proactive detection efforts like network monitoring of supplier-acquirer connections. When it comes to live incident response and mitigation, organizations are typically willing to support their suppliers directly with in-house cyber incident response or product security teams following incident notification. These teams possess a broad array of capabilities in the fields of incident evaluation, technical mitigation, and process improvements.

Redundancy and back-up supply:
Interviewed organizations understand that resilience must be supported, not only by response and mitigation but also recovery capabilities. To that end, organizations plan extensively to minimize the impacts of unforeseen supply chain disruptions. Such preparations come in the form of:

1. Introducing slack into their inventories to accommodate 60- to 90-day supply chain disruptions.
2. Defining internal protocols, triggers, and event escalation criteria.
3. Paying premiums for high availability or redundant supply chains.
4. Deploying emergency operations centers that address any emerging risks to redundancy and back-up supplies.

Comprehensive threat context:
Though threat intelligence and supply chain risk context are generally noted as areas for improvement, organizations in the industry have begun to embrace the importance of information forums or industry groups like Gartner and the Group Purchasing Organization, respectively. It is also common for organizations to subscribe to publicly available threat intelligence services like Computer Emergency Response Team Coordination Center (CERT/CC) and US-CERT. Finally, organizations are also more willing to pay a premium for private threat intelligence services that specialize in supply chain, compliance, and geopolitical risks.

Lessons Learned and Improvement Opportunities

Organizations have much to offer in the way of experience with C-SCRM topics, including lessons learned and ongoing challenges. Sharing those experiences can help less mature organizations avoid common pitfalls while also indicating the future direction of C-SCRM practices.

Key Themes:

1. Challenges in implementing C-SCRM: Organizations continue to struggle with the rapid change of pace and adapting to threats in a defensible, quantifiable, and actionable manner.
2. Lessons learned for organizations wanting to improve C-SCRM: A combination of people, process, and tools initiatives can help organizations avoid some of the common pitfalls in C-SCRM, especially early in the maturity journey.
3. Opportunities for continuous improvement in C-SCRM: C-SCRM practices will further incorporate technological integration, automation, and cross-functional risks to more holistically and dynamically assess an organization's exposure to cyber supply chain threats.

Challenges in implementing C-SCRM:
The challenges that organizations face in implementing C-SCRM take many forms but can generally be categorized into three types:

1. Keeping pace with technological change and evolving threats.
2. Hiring, training, and retaining expertise to identify and remediate risks.
3. Better understanding the return on investment for risk mitigating activities.

Efforts to address these challenges continue to evolve, but organizations found that various tools and techniques were useful in addressing them, including:

1. Using standards to provide an understandable and manageable structure, which emphasizes the benefit that requirements provide to suppliers.
2. Conducting open communication to the entire organization regarding potential risks.
3. Delivering tailored C-SCRM training, including phishing exercises.
4. Incorporating insurance into supplier negotiations, especially for data privacy or other violations that may result in fines.
5. Centralizing C-SCRM functions.
6. Using software to proactively monitor supply interruptions, support recall policies, and allocate resources for business continuity.
7. Using third-party assessment firms to gauge cyber risk.

Lessons learned for organizations wanting to improve C-SCRM:
All interviewed organizations had distinct lessons learned for organizations that are less mature in C-SCRM:

1. **Implement a standards-oriented approach to supplier risk to streamline C-SCRM processes**: Start with available standards, such as NIST guidance, ISO/IEC 20243, ISO/IEC 27001 series, ISO/IEC 15408, and Federal Information Processing Standard (FIPS)-140. Leveraging an external authority gives the acquirer's supplier security requirements a defensible position and makes compliance attractive to suppliers and business partners concerned about their own security posture. This approach can scale to supply chain demands and be applied to virtually every supplier in every market.
2. **Uplift cyber hygiene practices for vendors**: Instead of focusing exclusively on manufacturing or logistics processes, work with suppliers to improve their security posture so that they appreciate and fully benefit from enterprise controls such as multi-factor authentication and logical segmentation. Similarly, organizations should evaluate cybersecurity alongside business considerations like financial stability.
3. **Invest in unified secure platforms for exchanging information 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.
4. **Develop a central risk management team responsible for the entire organization**: The team would be comprised of roles such as Chief Risk Officer, Chief Security Officer, Chief Supply Chain Officer, or other similar roles. This group would work together to address cyber supply chain risks and be responsible for communication and engagement with executive leadership. This team should leverage existing organizational expertise, like information security and compliance functions, when holistically assessing risk.
5. **Do not wait to build deep supplier relationships**: Direct points of contact and familiarity with a supplier's business are essential to understanding risks and ensuring rapid incident response. Strengthening such relationships can also foster loyalty, ensure effective supplier management, and support operational efficiencies. Organizations should also regularly stress test their Incident Response Plans and perform tabletop exercise simulations with their suppliers.

Opportunities for continuous improvement in C-SCRM:

As organizations look to the future of C-SCRM, opportunities for continued improvement across the industry were shared:

1. **Expand supply chain-oriented risk metrics**: Tools that track quantitative metrics per supplier in real time may help highlight supply chain interdependencies and provide actionable insights for mitigating supply chain risks.
2. **Incorporate geopolitical volatility:** While supplier relationships have been reliable, political trends are drawing attention to potential escalations in trade tensions. Accounting for the risks of such instability may help organizations diversify supply chain operations.
3. **Investing in emerging security solutions**: Machine learning-powered monitors for the manufacturing floor can provide predictive risk indicators and help organizations better understand their product lifecycles.

Future Study, Research, and Guidance

The research concludes that C-SCRM is an evolving discipline that requires further attention across user and research communities. Though less mature organizations can benefit from the foundational guidance and methods presented here, more mature organizations continue to experiment with evolving key practices. Recommended follow-up research opportunities related to these evolving key practices include:

1. Quantitative cyber supply chain risk analysis and metrics, including returns on investment for risk-mitigating activities.
2. Generic security controls to consider adding to supplier terms and conditions.
3. Guidance on determining supplier criticality as well as applying existing criticality guidance; sample supplier tiering criteria.
4. Success stories from supplier mentoring.
5. Anonymized case studies on cyber supply chain incidents.
6. Research on continuously evolving technological changes and threats that continue making C-SCRM a challenge.
7. Workforce knowledge, skills, and abilities required for addressing C-SCRM within acquirer and supplier organizations.

Investigation of the above will further understanding of C-SCRM and provide additional key practices which aspiring organizations can seek to emulate.

References

American Institute of Certified Public Accountants, SOC 2® - SOC for Service Organizations: Trust Services Criteria. Available at https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html.

Boyens J, Paulsen C, Bartol N, Winkler K, Gimbi J (2020), Case Studies in Cyber Supply Chain Risk Management. (National Institute of Standards and Technology, Gaithersburg, MD). Available at https://csrc.nist.gov/projects/cyber-supply-chain-risk-management/key-practices

Boyens J, Paulsen C, Bartol N, Winkler K, Gimbi J (2020) Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Interagency or Internal Report (IR) 8276. https://doi.org/10.6028/NIST.IR.8276-draft

Electric Reliability Council of Texas (ERCOT) (2020) *Market Rules*. Available at http://www.ercot.com/mktrules

Health Information Trust Alliance (HITRUST) (2018) *Key Considerations of a Data Protection, Information Risk Management and Compliance Program*. Available at https://hitrustalliance.net/the-hitrust-approach/

International Organization for Standardization/International Electrotechnical Commission (2009) *ISO/TS 16949:2009 — Quality management systems — Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/52844.html

International Organization for Standardization/International Electrotechnical Commission (2009) *ISO/IEC 15408-1:2009 — Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/50341.html

International Organization for Standardization/International Electrotechnical Commission (2014) *ISO/IEC 28000:2007 — Specification for security management systems for the supply chain* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/44641.html

International Organization for Standardization/International Electrotechnical Commission (2018) *ISO/IEC 20000-1:2018 — Information technology — Service management — Part 1: Service management system requirements* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/44641.html

International Organization for Standardization/International Electrotechnical Commission (2018) *ISO/IEC 20243-2:2018 — Information technology — Open Trusted Technology ProviderTM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 2: Assessment procedures for the O-TTPS and ISO/IEC 20243-1:2018* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/74400.html

International Organization for Standardization/International Electrotechnical Commission (2018) *ISO/IEC 27000:2018 — Information technology — Security techniques — Information security management systems — Overview and vocabulary* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/73906.html

Paulsen C, Boyens J, Bartol N, Winkler K (2018) Criticality Analysis Process Model: Prioritizing Systems and Components. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8179. https://doi.org/10.6028/NIST.IR.8179

National Institute of Standards and Technology (2001) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-2, Change Notice 2 December 03, 2002. https://doi.org/10.6028/NIST.FIPS.140-2.

National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

North American Electric Reliability Corporation (NERC) (2019) *Enforcement Actions 2019*. Available at https://www.nerc.com/pa/comp/CE/Pages/Actions_2019/Enforcement-Actions-2019.aspx

Sarbanes-Oxley Act of 2002, Pub. L. 107-204, 116 Stat. 745. https://www.govinfo.gov/app/details/PLAW-107publ204

U.S. Customs and Border Protection (2020) *CTPAT: Customs Trade Partnership Against Terrorism*. Available at https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat