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

U.S. Resilience Project

BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Cisco®
Managing Supply Chain Risks End-to-End

INTERVIEWS

Edna Conway
Chief Security Officer, Global Supply Chains

Nghi Luu
Senior Manager, Supply Chain Risk Management

Erich Shaffer
Senior Director, Supply Chain Quality Engineering

The Next New Things in Risk Management

- **Adjusting risk assessment frameworks to include mitigation efforts — both existing and potential.** On the X axis, probability measures are weighted by mitigation efforts already in place. On the Y axis, impact measures are weighted by mitigation difficulty, including level of resources and degree of control.
- **Integrate physical and cyber security requirements across the supplier network and product lifecycle.** The master security specifications document is customized to service or component, and specific site.
- **Real-time visibility into production processes of outsourced manufacturers** with the capacity to capture not only defect rates, but causes of failure and prevent a supplier's ability to shortcut testing requirements before shipment.

Company Overview

For more than 25 years, Cisco® has been a pioneer in hardware and software products used in networks around world. It was one of the first companies with a dedicated supply chain risk management (SCRM) team, and continues to innovate in practical risk management applications to protect the enterprise and its supply chain from disruption and vulnerabilities.

Organizational Approach to Integrated Supply Chain Risk

As befitting a global and complex organization, Cisco's risk management infrastructure is complex and evolving. First, there is an overall corporate risk management team. This is layered on top of functional risk management teams, including security, IT and supply chain. From a broad strokes perspective, there are multiple teams driving supply chain risk management, including:

- Resilience
- Quality
- Security, both physical and cyber
- Sustainability
- Compliance

While all elements of Cisco's risk management organization are critical to its success, this case study focuses on the resilience, quality and security processes and practices.

The focus on resilience was launched in the aftermath of Hurricane Katrina and the close call that Hurricane Rita gave Houston. Realizing that they were not fully prepared to respond systematically to a major event and could not comprehensively assess the full financial impact of the disasters, Cisco resourced a dedicated SCRM team to assess and mitigate supply chain risks and build out a better capability to respond to unpreventable incidents. Events such as the Fukushima Daiichi nuclear disaster triggered by an earthquake/tsunami and the Thai floods of 2012 validated and reinforced the importance of investment in supply chain resilience. Over the past decade, the SCRM team has tripled in size and matured its guiding principles, processes and tools — continuing to be a gold standard for organizations that have only recently begun to see SCRM as a strategic concern.

Quality is also a key team within the risk landscape, with 130 quality team members in the supply chain organization alone. This team is responsible for interfacing with the internal new product introduction (NPI) organization, external manufacturing partners, the technical assistance center and directly with customers.

Supply Chain Security has been a key part of Cisco's manufacturing supply chain for more than four years, focused on the risks of counterfeit or tainted products and misuse of intellectual property. Recently, the company established a new corporate organization focused on shifting the role security plays from "limiting damage" to enabling business. A key element of this Security and Trust Office is a broader view of supply chain security. Security will continue to be embedded throughout the product development, software, manufacturing, channel and technical service supply chains, while also addressing evolving cyber threats. To achieve its goal, the Cisco Security and Trust Office is partnering with every team that touches any part of the product lifecycle, and embedding new security capabilities into existing people, processes and tools.

Business Case for Integrated Supply Chain Risk Management

For Cisco, the drivers for continued resourcing of the SCRM effort and expansion into cyber in the supply chain come from actual events that have directly impacted the company's supply chain operations and customers. The SCRM team has proven its ability to help the company recover faster in those events, effectively demonstrating the ROI of investing in a team of dedicated resources in order to protect billions of dollars of revenue. According to Nghi Luu, Supply Chain Risk Leader:

> "Nine full-time staff and nine contractors protect literally billions in revenue. Without this team, it would take four weeks longer to get the business running after a disruption — and how much money would be lost every day during that period?"

The ability to move faster than competitors during a recovery, e.g., buying new inventory from common suppliers before a competitor can, also gives this company a competitive advantage.

In addition, risk management efforts over several years in supply chain and IT helped forge a uniquely close working partnership with the company's property insurer. For example, Cisco jointly invested with their contract manufacturers to achieve Highly Protected Risk (HPR) status from its property insurer for critical sites. This has helped the company lower its insurance premiums, while gaining higher coverage for business continuity disruptions.

But, Cisco believes that the most important driver for investment in supply chain risk management is brand reputation and customer satisfaction. The processes and practices that create confidence in the quality and integrity of the products in the supply chain and resiliency of the supply chain are a market differentiator.

Supply Chain Resilience

Mr. Luu emphasizes Cisco's comprehensive framework for supply chain risk management.

> "We've come to realize that it's not just about boxes getting from Point A to Point B. It's geopolitical risks, cyber risks, overall supply chain continuity risks. We've created a holistic framework for risk assessment that examines six overall categories of risk with over 25 subcategories."

These categories are being mapped onto a visual display that is currently in development. The X axis will show the probability of likelihood of an event based on the mitigation efforts already in place. Instead of impact on the Y axis, the measurement will showcase mitigation difficulty — the resources required, both dollars and headcounts, to mitigate the risk and level of control over the event. For example, the level of control over a natural disaster would be negligible. The resulting circles on the chart will show potential risks. The size of the bubble represents the size of threat. Some risks may be high probability and hard to mitigate, but do not represent a significant threat. That data will be used to drive annual planning efforts and budgets for risk mitigation.

Continuity of supply in the face of potential disruptions is a guiding principle for the Cisco SCRM team. Its approach focuses on mitigating vulnerabilities before a disruption — ensuring that suppliers can fulfill their committed recovery times.

Mitigation efforts are prioritized by revenue. The supply chain model spans more than 30 business units. The company uses high-powered analytics to determine which components, suppliers and manufacturing sites are most at risk, and then drives risk mitigation strategies and action plans to reduce the risk.

The SCRM team has four primary risk management strategies:

1. Incident Management
2. Supplier Business Continuity Planning (BCP)
3. Manufacturing and Test Resilience
4. Product Resilience

Incident Management

The Cisco supply chain organization has deployed a number of capabilities to improve its ability to handle disruptions:

A. Situational Awareness: The SCRM team partners with the corporate team on a multi-pronged 24/7 "sensing function" supported by a live feed of events around the world that could impact supply chain locations and operations. The SCRM team also tracks global trends that could adversely impact supply chains. Among the emerging issues on its radar include:
   - Changing legal environments (e.g. customs restrictions on shipments into Russia in response to the Ukraine situation);
   - Logistics delays (e.g. the 2014-15 Los Angeles port congestion showcased both infrastructure constraints, as well as the bottleneck from a labor action); and
   - The need for increased health and safety at suppliers (e.g. a factory explosion in China led authorities to investigate and shut down other suppliers, including three of its suppliers).

B. Tabletop and live drills: The team conducts two to three drills per year within supply chain, as well as participation in the corporate drills and exercises on "what-if" scenarios. For example, what if the border with Mexico closes? What if there were a pandemic?

C. Supply Chain Incident Management: The Supply Chain team organized a standing incident management team. These are employees from key product groups and functional teams who join the war room if an incident occurs that disrupts the supply chain. The supply team maintains key contacts, and the incident team list is refreshed annually.

D. Playbooks: The SCRM team has developed playbooks that detail different roles and responsibilities in managing an incident. The playbooks provide a framework for organizing the incident response team, key contacts related to various types of incidents, and templates and supporting materials to assist in running and managing the incident response.

Supplier BCP

The BCP component of Cisco's program starts with an annual survey administered by a third party to hundreds of suppliers to identify the exact geographic location of their manufacturers. In the event an earthquake, for example, the company would be able to map all of its components and suppliers in the affected area by location, part and spend — and forecast potential disruptions in the supply chain and revenue at risk. The database includes key information: Whether there is an alternate manufacturing site; what is the Time to Recover (TTR), who are the

key contacts that enable the company to manage the impact. Quarterly updates capture net new additions to the supply chain, as well as changes for existing partners. The company that administers the survey will conduct virtual audits and follow up with the vendors for quality control purposes. Actual supplier Business Continuity documents are collected, but only a subset of critical vendor BCPs are audited annually.

One of the areas the company is pursuing is greater visibility into lower tiers of the supply chain. What it found about a month after the Thai floods was an unexpected spike in disruptions. It turned out that lower tier suppliers had exhausted inventories, but their production capacity had been affected by the flood. Cisco continues to seek greater visibility into the supply chain, at the very least to be able to map the sub-tier suppliers geographically.

These data collection and analytical processes from the Supplier BCP Program are so robust that they are used for risk management in other areas as well. The SCRM team effectively acts like a service model approach, providing other groups in the company with the data necessary to identify, prioritize and mitigate risks. For example, as part of their standard data collection process, the SCRM team collects supplier financial health data quarterly from the supply chain finance organization. SCRM then uses this data as part of their overall product resiliency reviews with the multiple product teams.

Manufacturing and Test Resilience

Time to Recover (TTR) is measured by how long it takes for a supplier to recover its operations or relocate to an alternate site. Most organizations focus on the inventory and people required for production. One critical element of this metric that is often either forgotten about or underestimated is the equipment used on the manufacturing floor. Replacement equipment may have lead-times of up to a year. However, given the expense of this equipment, companies are reluctant to invest in redundant equipment, which is a challenge for the Supply Chain Continuity program. Risk mitigation efforts with suppliers are continuing to evolve in this space.

Product Resilience

Product Resilience at Cisco entails a formal risk review of products to identify sole source or other risk components before a product is manufactured. Component risk ratings — mandatory for new product introductions — have three levels:

1 = some risk

2 = no risk

3 = preferred

The objective is to engage with engineering and product operations to drive resiliency upstream into the early stages of the design and development process.

Managing Supplier Risks

Cisco is a leader in managing supplier risks through a series of formalized business reviews. Suppliers are vetted up front and regularly reviewed against a number of criteria, including performance, financial stability, quality and security. Suppliers are subject to regular audits from both the security and IT security teams, as well as less frequent audits on financial and regulatory risks. Additionally, the company controls the part numbers its contract manufacturers can purchase through its Bill of Materials, which specifies an approved vendor list for each part number.

Supply Chain Quality Assurance (QA)

How does Cisco, with its 100 percent outsourced manufacturing supply chain, assure quality in its products? Answer: By innovating in quality assurance and testing methods, as well as product innovation.

Today, the supply chain quality team is focused on hardware, but is evolving toward a full product quality experience, which would include software. At the moment, there is no centralized software quality team. The teams that write the code are also responsible for managing the quality of that code. By contrast on the hardware side, design teams hand off to the supply chain quality team, which manages the quality of the incoming design, the build and the customer.

Quality assurance has been a priority for Cisco's manufacturing supply chain since inception, when certain initial phases of the manufacturing processes were outsourced. But, about a dozen years ago, test and assembly were outsourced as well. Cisco's leadership understood that, in addition to its close ties with trusted manufacturing partners, the company needed new ways to verify adherence to both technical and quality requirements. The company made significant investments in technology and collaborative processes to create a high confidence level in component quality, manufacturing process and test reliability, including:

HALT Lab (Highly Accelerated Lifecycle Testing): The processes are designed to catch potential defects as early as possible. Long before anyone is thinking about production, prototypes are tested in the HALT Lab. According Erich Shaffer, Senior Director for Supply Chain Quality: "We shake it, subject it to high and low temperatures to find out where it breaks, and strengthen the weak points to increase reliability."

Real-time Data: Cisco's unique secret weapon is a propriety software system that gives it real-time visibility into the production processes and quality controls of its outsourced manufacturers. This homegrown software system built in the 1990s was originally deployed as a shop-floor test system. As business has grown and production has been outsourced to electronic manufacturing services (EMS) partners, the system has evolved and been integrated with systems at its partner sites. The system provides the company with data on yields, component defect rates, test results and all other production information from all sites all the time. Adopting this test system is a pre-requisite to being a member of Cisco's manufacturing supply chain.

It is a workstation that is set on the factory floor at a manufacturing partner. Each of the products in production plugs into the system, and it recognizes the serial number and diagnostic tests to be run. This capability increases quality assurance on many levels.

- First, the risk of skipping or limiting diagnostics on urgent orders is eliminated. All test results must be input before the system will authorize shipment.
- Second, the system identifies defects at the component level, but also at the repair station. That enables insight not only into failure rates, but also the reason for the failure. Accumulated across different sites and product lines, that data provides insight on whether this is a design problem, a component problem or a workflow problem. Mitigation actions might occur across multiple product lines and suppliers.
- Third, it is portable and can be deployed to address specific issues. For example, physical or electrical characteristics of a component are not usually tracked (the test is not calibrated to specific voltage but to on or off). But, if there are problems, the light touch system can be deployed for data measurement and then taken down easily.
- All of the information that is collected becomes part of a database that underpins Cisco's quality management program. It is collecting information from the factory floor on everything from yields to defect rates. That data scrolls live to headquarters and is also recorded. There are weekly meetings with cross-functional teams and with the contract manufacturers to review the data in order to understand what could have caused a down dip in yield or a spike in defects.
- Using defect rates from production and reports from customers, the company is able to identify a top ten list of problem components and work with the supplier or the design teams to correct the problem.

In addition, the system contributes to the SCRM efforts by providing massive data sets, which serve as the foundation for other teams to manage risks. Leveraging its centralized role inside the corporation, the supply chain quality assurance team interfaces with multiple organizations — from new product introduction teams and external manufacturing partners to cybersecurity and anti-counterfeiting to the customer-facing Technical Assistance Centers, and sometimes directly with the customers. For example, many counterfeit issues start off as a QA issue masked as a product failure. The systems help distinguish between the two, and QA can hand off the issue quickly to the right security forensics team.

In this era of "big data," the system is able to provide tens of millions of records a day that enables Cisco to improve quality, reduce customer returns, increase inventory turns and manage risk.

Supply Chain Security

Security requirements, originally developed for Cisco's manufacturing supply chain, are now being extended across the product lifecycle. According to Edna Conway, Chief Security Officer for Cisco's global supply chains:

> "While getting a product from the design phase through production, service and end-of-life must look seamless to customers, a number of different internal organizations actually 'own' these processes. For example, product design and development is primarily owned by engineering and supply chain operations. Planning, sourcing, fabrication, quality control and delivery is owned primarily by supply chain operations, although sales and finance also play a role. The worldwide partner organization plays a key role in the delivery of solutions to customers, while the technical services organization takes charge when the product is actually in use. And, responsibility for end-of-life management — a vulnerable time when parts can be diverted rather than decommissioned — is managed by supply chain operations and yet another group.
>
> Supply chain security is driving foundational requirements and collaborative partnerships that can be applied across the product life-cycle — from design to decommission — as well as across the supplier network. Our goal is to enhance integrity, regardless of the functional area of the company or supplier handling any aspect of that lifecycle."

In the past, requirement packages were focused very specifically — for an ASICs manufacturer or an EMS partner. But in today's complex and global supply chain, these clearly delineated cubbyholes no longer exist. An EMS partner may also be doing design work, failure analysis and warehousing. The concept of separate and independent requirements no longer works today. Cisco has developed a comprehensive supply chain security master specification with 180 requirements across 11 security domains. Some of the security requirements are applicable across the board — security governance or personnel security, for example — but others can be customized to the product, service or site. Figure 1 shows the list of Cisco's Supply Chain Security Domains.

Figure 1. Supply Chain Master Security Specification

	Domain	Description	#	Sub-domain
1	**Security Governance**	The security governance domain details requirements for supplier's overall governance strategy to manage supply chain security and compliance related risks by establishing requisite policies, standards and procedures.	1.1	Governance and Information Security Program
			1.2	Security Policies, Standards and Procedures
			1.3	Security Risk Management
2	**Security in Manufacturing and Operations**	The security in manufacturing and operations domain details requirements that a supplier must meet in their manufacturing and operating procedures in order to protect the company's material assets and IP.	2.1	Tracking and Accountability
			2.2	Security in Inventory Management
			2.3	Security in Handling Proprietary Items
			2.4	Segregation of Duties
			2.5	Scrap Management
			2.6	Tampering and Malicious Modification
			2.7	Counterfeit Mitigation
3	**Asset Management**	The asset management domain details requirements that a supplier must implement for securing IT and manufacturing assets throughout their life cycle.	3.1	Identification and Classification
			3.2	Media Protection and Disposal
			3.3	Records Management
4	**Security Incident Management**	The security incident management domain details requirements that a supplier must implement to establish a robust incident management (IM) process that should be followed for activities such as logging, recording and resolving of security incidents and anomalies.	4.1	Incident Identification and Reporting
			4.2	Incident Response

	Domain	Description	#	Sub-domain
5	**Security Service Management**	The service management domain details requirements, a) for the delivery of services in accordance with agreed upon delivery timeframes. b) establishing a business continuity plan/program in an event of a service disruption.	5.1 5.2	Security in Business Continuity Planning Business Continuity Plan Testing
6	**Security in Logistics and Storage**	The security in logistics and storage domain details supplier security requirements that should be followed during storage and distribution of raw materials, inventory and finished goods along the company's supply chain.	6.1 6.2 6.3	Warehousing and Storage Shipping and Receiving Packaging Security
7	**Physical and Environmental Security**	The physical and environmental security domain details requirements that a supplier must design and implement to deny unauthorized access to facilities, equipment and resources, and to protect personnel and property from damage or harm.	7.1 7.2 7.3 7.4	Physical Access Control and Monitoring Perimeter Security and Secure Areas Security During Equipment Maintenance Power and Lighting
8	**Personnel Security**	The personnel security domain details requirements to ensure that all supplier personnel who have access to any proprietary items and company IP have the required authorizations, training, and contractual agreements including appropriate clearances, if required.	8.1 8.2 8.3 8.4	Prior to and During Employment Security Training and Awareness Contracts and Enforcement Termination or Change of Employment
9	**Information Protection**	The information protection domain details requirements for protection of the company's proprietary data through its lifecycle, such as data classification, handling, cryptographic controls and disposal. It also lists the requirements to be implemented on information systems that store or process the company's IP.	9.1 9.2 9.3 9.4 9.5 9.6 9.7 9.8	Data Classification and Handling Cryptographic Controls Backup, Retention and Disposal Information Access Controls Network Security Information System Logging and Monitoring Information Exchange Information Infrastructure Security

	Domain	Description	#	Sub-domain
10	**Security Engineering and Architecture**	The security engineering and architecture domain details requirements to be followed during design, development, testing and rollout of products and services to and on behalf of the company.	10.1 10.2	Secure Design and Development Lifecycle Configuration and Change Management
11	**3rd Tier Partner Security**	The 3rd tier partner security domain details requirements focused on information security controls that must be implemented at downstream suppliers and partner (4th parties, e.g. cloud service providers) in relation to procurement of goods and services.	11.1 11.2	Security During Contract Initiation Cloud Security

This framework, originally developed for the manufacturing supply chain, will become a baseline requirement architecture for other internal and external organizations that touch the company's supply chains. Flexible application of the architecture is key to its uniform adoption and success. One area requiring a different strategy than that for the manufacturing supply chain is the company's worldwide partner ecosystem. Given the sheer number and diversity of channel partners, it would be difficult to impose a mandatory baseline of requirements uniformly. One approach under consideration is to create an "opt-in" class of channel partner. The degree of compliance with security standards will be visible to the company's customers, who can then choose a supply chain security capable channel partner at their discretion based on the nature of their purchase.

Another Cisco customer-driven pilot program seeks to extend security innovations across the company. As product engineers and supply chain managers devise new practices or technologies to improve the security in one area, the new security organization is looking for applicability to other product lines. This moves the security to a higher threshold for the whole company, and makes security a product differentiator.

Standards

Cisco has been active in a number of industry groups to help promulgate a limited set of new standards and best practices in both the supply chain security and cyber security areas. With respect to end-to-end supply chain integrity, it relies on three kinds of standards to inform its own processes:

- End-to-end Standards: At the highest level, the end-to-end standards include: NIST Cybersecurity Framework; NIST 800-161; NISTIR 7622 as guidance and the Open Trusted Technology Partner Standard, which was recently adopted as ISO 20243.

- Common Criteria: Like many off-the-shelf commercial providers, this high-tech company favors the Common Criteria standard because:
  1. Network devices are captured effectively; and
  2. A single certification is accepted by 26 nations by mutual agreement, which creates great efficiencies for COTs providers (international standards are global in creation, but not always in adoption).
- Component or System Specific: Finally, there is a subset of guidelines that are specific to products, subsystems of activities. IP guidelines for printed circuits for example as set forth in IPC 1071.

Looking to the future, Cisco believes that additional collaboration between semi-conductor manufacturers and their OEM customers can serve to enhance counterfeit protection for information and communication technology devices and the end users of those devices. Allowing an appropriate balance between protecting privacy and limited sharing of electronic chip IDs will permit OEMs to validate chip authenticity in the course of manufacturing their products.