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

U.S. Resilience Project

BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Juniper Networks
Ensuring a Remarkable Customer Experience

INTERVIEWS

Operational Excellence, Risk, and Compliance Executive

Operations Risk and Compliance Manager

Environmental, Health Safety & Security Senior Director

The Next New Things in Supply Chain Risk Management

- Forming a Supply Chain Risk Council which pulls together representatives from throughout the supply chain organization to regularly and proactively review risks, as well as mitigation plans.
- Assessing risk at multiple tiers by mapping the entire supply chain network, not just top-spend components or first-tier contract manufacturers.
- Training Juniper Networks employees co-located at vendor sites in security and continuity requirements so they become additional eyes and ears on the ground all year long.

Company Overview

Juniper Networks, Inc., founded in 1996 and headquartered in Sunnyvale, California, designs and sells high-performance Internet Protocol network products and services worldwide. The company offers network infrastructure solutions that include IP routing, Ethernet switching, security and application acceleration solutions. Its annual revenues are more than $4.6 billion.

According to the company:

> Now more than ever, the world needs network innovation to unleash our full potential. The network plays a central role in addressing the critical challenges we face as a global community. Consider the healthcare industry, where the network is the foundation for new models of mobile affordable care for underserved communities. Or the energy sector, where the network is helping to accelerate distribution of clean, renewable sources of energy. In education, the network continues to expand access to quality teaching resources, so that people of every socioeconomic background have a chance to educate themselves and participate in the global economy. At its core, the network has become a platform — one that transforms how we interact with our government institutions, conduct business on a daily basis, and connect with our family and friends.

Juniper Networks relies principally on five contract manufacturers (CMs) and original design manufacturers (ODMs) for all of its manufacturing, making supply chain assurance integral to their bottom line and brand reputation. Beyond these partners, there are about 300 other suppliers with more than 2,000 sites around the world that manufacture more than 24,000 parts used in Juniper Networks products.

Juniper Networks manages supply chain risks on an end-to-end basis — from product design to the customer dock — as part of its overall Product Integrity Program and commitment to provide a "remarkable" customer experience.

Organizational Approach to Supply Chain Risk Management

All of the functions that touch the supply chain are linked through the Supply Chain Risk Management Council, which meets on a regular basis to review risk exposure. The Council is continually scrutinizing the overall risk environment, including inherent product risks, sourcing risks, compliance risks and what is needed to reduce those risks. The team scrutinizes current activity and prioritizes areas that need attention.

The supply chain risk management team itself is lean, but it coordinates closely with the other teams to assure a holistic approach, including:

- Corporate Risk Team, with principal responsibility for financial risk, insurance risk and Foreign Corrupt Practices Act requirements;
- Physical Security Team, which has responsibility for manufacturing and product security;
- Supplier Management Team, which has responsibility for sourcing strategies and maintaining close connections to vendors;
- IT Team, which addresses both supplier IT security and supply chain cybersecurity;
- Quality Teams, which monitor component quality and manufacturing quality; and
- Engineering Teams, which participate in supplier selection.

The manager for Network Risk and Operational Compliance makes it clear that Juniper Networks has embedded an awareness of supply chain risk in the culture:

> "The awareness of the key principles — and the "to-do's" relative to risk — is always evident in our daily work life. Absent the need for posters, it's in their in box. It's on their calendar. It's the actions that we take…If you tried to separate supply chain risk management as a separate activity, you run the risk of things getting lost in the hand-off versus our integrated team approach."

Supply chain risks and mitigation plans receive board-level scrutiny. Like many other companies with a supply chain risk management program, Juniper Networks has been working hard at finding the best metric to drive desired behavior and produce a meaningful executive-level dashboard. At present, Juniper Networks is developing a new Executive Dashboard. In the meantime, it relies on a set of reports and reviews to measure progress, including monthly and quarterly reporting of actual events, percent of single and sole-sourced components with mitigation strategies in place, an SCRM business continuity maturity matrix, and current risks that pose a threat to the supply chain operations based on supplier locations and economic, political and geographic concerns. The manager for Network Risk and Operational Compliance notes: "It's my job to make sure that it's a risk concern that the board doesn't have to worry about."

Business Case for Supply Chain Risk Management

For Juniper Networks, supply chain risk management goes beyond logistics and on-time delivery. The business case rests on a broader business base of product integrity, customer service and corporate responsibility.

The security and quality programs, for example, are inextricably linked. Juniper Networks ensures that all components that go into its systems have accountability and traceability, which creates high confidence in component integrity. Those systems also create the means to do failure analysis on products or processes when quality problems arise. In fact, the same processes and tools meet a myriad of corporate objectives — from sustainability and social responsibility to supply chain continuity and security.

One tangible benefit is the cost savings in meeting the regulations on conflict minerals, which require companies to disclose the country of origin of certain, designated minerals. For many companies, this requirement has proven onerous. Juniper Networks has been able to fulfill this requirement at reduced cost through an extension of its supply chain mapping system.

Guiding Principles of Supply Chain Risk Management

Juniper Networks' supply chain risk management capabilities are built upon the foundation of a solid supplier relationship management program. Relationships with these suppliers are developed and strengthened through a number of program elements, including regular performance reviews, strategy alignment sessions and performance metrics.

Supplier Risk Management: Juniper Networks outsources 100 percent of its manufacturing through top-tier contract manufacturers and outside design manufacturers. About 90+ percent of all suppliers are managed through a direct agreement (e.g. they are selected using the sourcing strategies with the engagement of the engineering teams). In reviewing suppliers for the potential risk they could pose to our supply chain, however, Juniper Networks analyzes the "percentage of risk" as well as the "percentage of spend." A supplier may be small as a percentage of total spend, but critical enough to have a major impact upon product shipment. That is why every supplier gets vetted both in terms of dollars and criticality.

Key elements of the Supplier Management Program include:

- Supplier Performance Evaluation: Juniper Networks has developed two primary tools — a Supplier Excellence Framework and Business Continuity Maturity Matrix — to evaluate suppliers.
- Verification and Audit: Juniper Networks conducts on-site audits of its major CMs and ODMs to assess and evaluate their performance.
- Certification: Each Juniper Networks supplier must certify compliance with the Juniper Networks Code of Conduct, which addresses human rights, human trafficking and other important ethical standards.
- Internal accountability: Employees at Juniper Networks re-certify their understanding of and compliance with Juniper Networks' Code of Conduct on an annual basis. Performance reviews are based in part on the principles of the Juniper Networks Way, which includes acting with integrity and respect, as well as operating as responsible corporate citizens.
- Training: Juniper Networks employees with direct responsibility for supply chain management are trained in general risk mitigation. The company also is planning to implement additional employee training related to labor standards, including freely-chosen employment.

Supplier Excellence Framework: Over the last few years, Juniper Networks has implemented a multi-point Supplier Excellence Framework to lead and measure supplier performance. These measures include many common supply chain principles, as well as measures around sustainability (carbon footprint, conflict minerals, corporate social responsibility and Code of Conduct) and risk (Business Continuity Program, responsiveness to events, etc.)

Figure 1. The Wheel of Supplier Excellence

The Wheel of Supplier Excellence breaks down Juniper Networks' expectations of its suppliers into specific metrics from leadership and management commitment to training and risk management. Prospective suppliers are rigorously vetted by a number of teams — sourcing, risk management, engineering and security — across all categories on the Wheel. If suppliers cannot or do not want to meet the requirements, their scores likely will not be high enough to allow them to participate.

Once suppliers are accepted into the Juniper Networks supplier network, a team of security specialists, often located onsite, works with them continually to strengthen brand integrity and address any gaps.

Business Continuity Maturity Matrix: Juniper Networks ranks and tracks performance, whether for its suppliers or itself, along a continuum toward World-class. For example, in the area of business continuity, Juniper Networks measures its suppliers in four areas:

- Management commitment to a business continuity program
- BCP readiness in production, key personnel and test equipment
- Selection and readiness of alternative locations
- BCP program structure, documentation and training

For each of these areas, suppliers are measured and tracked for their progress from Driving Basics to World-class in each area. Key elements that Juniper Networks tests for include:

- The degree to which management is involved and committed to demonstrating world-class performance in BCP.
- How proactive is the suppliers' planning versus just reacting when a crisis occurs.
- Are key players who would be called upon in a crisis identified, and do they know their individual roles during an event.

Figure 2. Business Continuity Maturity Matrix

	Dimension	Driving Basics	Mastering Basics	World-class
1	Management commitment	Management sees need for BCP preparation, but only gets involved when a crisis occurs. Delegates preparation activity to customer-facing teams.	Management begins to consolidate BCP requirements across multiple customers into one consolidated program. Specific resources are defined to lead BCP maturity and progress is reviewed by management team regularly.	Management continually sets the tone and pushes the limits of proactive BCP planning through the organization, before being requested to by customers.
2	Production, key personnel and test equipment (H/W & S/W)	Key production, personnel and test equipment has been identified for a variety of disaster modes. Plans can be generally documented, but not customer-specific and driven by whoever is in charge of the particular event.	Detailed, customer-level BCP plans are created, documented and regularly tested for relevant production, personnel and test equipment.	Alternatives are back on line before buffer inventory has been used up to fulfill pipeline demand. Alternatives are continually audited and tested for readiness. (1-2 years of prior testing and auditing.)
3	Alternate locations	Alternate locations have been identified for a variety of disaster modes. Plans can be generally documented, but not customer-specific and driven by whoever is in charge of the particular event.	Detailed, customer-level BCP plans are created, documented and regularly tested for alternative locations.	Alternatives are back on line before buffer inventory has been used up to fulfill pipeline demand. Alternatives are continually audited and tested for readiness. (1-2 years of prior testing and auditing.)
4	BCP program structure, documentation & training	Basic planning and documentation exists, driven by a community for subject-matter experts. Reviewed by other when requested	BCP programs, documentation and training are specific and driven down to the customer level. A wide scope of personnel are involved in the training. Results of training and auditing are validated.	BCP program structure is a regular part of the annual strategic planning process. Audits of capabilities, metrics and training programs are regularly reviewed by senior management.

Juniper Networks understands that its suppliers often have to start out at a basic level and develop a strategy to become World-class — and that this does not happen overnight. The maturity matrix creates a common framework for understanding what World-class means — and how to move along the continuum.

According to senior managers:

> "We meet with CM's and the ODM suppliers, and we go over the very detailed expectations we have. We review our Business Continuity Maturity Matrix with our suppliers and measure their performance along that matrix. I want to know that they have pre-qualified their back-up suppliers; thought about mitigation in case of disruption, about back-ups for their key employees; and the integrity of their test equipment. I don't want them to start that thinking process on the day we have an earthquake, fire or pandemic."

Supply Chain Continuity: From a continuity point of view, Juniper Networks is continually monitoring what is going on around the world on a 24x7x365 basis. It uses an outside vendor to monitor global events — from typhoons to port strikes to pandemics — map its supply chain and identify potential impacts. Visibility down the supply chain also enables Juniper Networks to identify and mitigate the risks of single source chokepoints.

The vendor maps Juniper Networks' entire Bill of Materials (BOM — all the products and materials, and their components that are made by suppliers in their factories) and collects that information in a central database. The tool provides the data to assess risk at a component level, supplier level, location level and financial level. Risk managers can see, at any point in time, what the supply chain impact of a disruption anywhere in the world would be.

Supply Chain Security

The Senior Director of Environment, Health, Safety & Security emphasizes three overarching drivers of Juniper Networks' security strategy:

1. **Brand Integrity rather than Brand Protection:** Brand integrity is proactive, where the more conventional brand protection strategies tend to be reactive. In conventional brand protection, for example, the focus would be on identifying and investigating counterfeit products and tracking down the criminals. This approach does not address the root causes or conditions that allowed that counterfeit to enter the marketplace in the first place. Brand integrity requires lifecycle threat modeling that identifies and proactively addresses weak points, from product development through production to shipping and warehousing.

2. **Customer Focus:** On behalf of its customers, Juniper Networks carefully manages and audits:
   - Whether those products are authorized by the manufacturer;
   - Juniper Networks' requirement that its suppliers contract only from authorized channels;
   - The documented origin of the product and who has touched the product in the distribution process; and
   - Whether the legitimacy of the product has been confirmed with the manufacturer.
3. **Life-cycle Approach:** When the design and production processes are largely invisible and finished boxes pop out, it is difficult to have a high level of certainty that nothing has been compromised or corrupted. Juniper Networks breaks the product lifecycle into smaller and more transparent pieces, each of which are tested for potential weaknesses.

This approach enables Juniper Networks to focus on how risk to product manufacturing is mitigated, rather than where its products are manufactured. Juniper Networks' primary manufacturing partners are global companies with factories all over the world, including the US, Mexico, Malaysia, Canada, Taiwan and China. Juniper Networks conducts a detailed analysis on the ability of a foreign government or foreign entity to impact the activities at the facility, no matter where it is located.

Software Design and Security

Lifecycle Approach: Juniper Networks has instituted a Software Development Lifecycle Program to improve the quality and performance of its software. Cyber risks are managed through a number of design features and controls.

- Juniper Networks runs one proprietary software code across all of its products lines, which allows it to embed security at the interface between software and hardware.
- Any software not digitally signed by Juniper Networks cannot be run on its systems — and there is a great deal of attention paid to protecting the signing keys and securing the digital signature process.
- Software and hardware have a security handshake. Secure booting processes look for security codes embedded in the hardware components. If they do not find them, the system will not boot and returns an error message: "Failed Integrity Check."
- Juniper Networks also has a secure development lifecycle training program in which all engineers are required to learn how to avoid common security mistakes and detect security flaws within software.

Component Integrity: Component integrity is a key aspect of the security program. For component sourcing, Juniper Networks will only purchase components from authorized manufacturers and distributors. While the secondary markets may be less expensive, neither Juniper Networks nor its suppliers are allowed to source from the grey market. Components are categorized into A, B and C based on their value: A components are high value; B components are medium value; and C components are low value, such as nuts and bolts. The various categories have different layers of protection, including cycle counts, scrap management processes, etc.

Manufacturing partners are allowed to purchase components only from those vendors that have been specified and approved. In fact, when buyers pull up part numbers for purchase, they only see the approved vendors authorized to supply that product.

For every product serial number, Juniper Networks can identify what components went into the product all the way back to the data code or lot code in some cases. This process provides not only a high level of security, but traceability for failure analysis to ensure top quality.

Facility Security: Juniper Networks maintains stringent physical security standards, both around physical security of the facility itself and the security of the production line. Every part of the production process is dissected — from the basic breadboard to the components that get soldered and tested — looking for and addressing areas of potential vulnerability.

On the IT security side, Juniper Networks has reduced the risk of tainted software by automating the process so there is no human intervention. When someone plugs a product into a test system, the system downloads and executes the appropriate routines without an individual being able to introduce new vulnerability.

Shipping and Warehousing: Packaging, storage and secure methods of transportation are a growing concern for Juniper Networks. When Juniper Networks controls the shipment, it uses specific carriers who agree to specific carrying requirements — and Juniper Networks tracks and monitors shipments to their destination. One key concern is what happens when customers select their own carrier to move the products. At that point, Juniper Networks loses visibility and control. Juniper Networks has been working with customers on a secure shipment mechanism to identify and detect signs of tampering in the distribution chain.

An additional benefit of a robust supply chain security program is compliance with the Customs-Trade Partnership Against Terrorism (C-TPAT) in the United States and Authorised Economic Operator (AEO) Program in the European Union. Implementing these security standards in the import supply chains not only enhances the security of cargo entering the United States and European Union, but also shortens customs clearance times and results in fewer customs inspections, reducing the time to the customer.

Figure 3. End-to-end Supply Chain Security Program, which includes component integrity and traceability

Audit: Suppliers get a soup-to-nuts inspection across a whole gamut of risk areas. Juniper Networks recently has begun engaging its onsite teams at supplier facilities in audit roles. Once trained in what to look for, they can be the eyes and ears on the ground all year long, not just for the few days of an audit.

Juniper Networks does physical audits on the contract manufacturers and original design manufacturers — often a combination of security and business continuity. The audits vary in length of time based on the vendor and encompass a broad range of issues, including:

- Where the incoming components are coming from
- Security processes at the gate
- Are employees vetted and monitored; passes swiped
- Physical route that components take when they enter the front gate
- Where locked high value or security / quality-critical components are kept stored and how they are accounted for
- Where and how Juniper Networks' software is loaded
- Monitoring processes in the plant and inspection of the cameras
- Fire protection processes
- Business continuity
- Emergency preparedness

Supplier audits are announced and conducted by Juniper Networks using audit protocols designed to assess supplier performance relative to the Electronics Industry Code of Conduct (EICC), Not For Sale, and the Juniper Networks Supplier Code of Conduct, all of which address issues of ethics, human trafficking and forced labor.

Standards: The Juniper Networks Standard is a corporate standard that incorporates best practices and standards from across the standards universe. Its standards and best practices address everything from component integrity assurance; traceability of products and components; anti-counterfeit features within its products; supplier selection (including an evaluation of foreign interests, relationships, and potential for foreign control); physical security; information and IP security; and channel monitoring and incident response.

On the software security side, the company was a founding member of organizations established for supply chain security, including the Software Assurance Forum for Excellence in Code (SAFECode) and the Open Group trusted supplier program.

Juniper Networks complies with numerous international standards in the operation of its supply chain and brand integrity programs, including:

- ISO 27001 for information security
- ISO 9001/ TL9000 Quality management system (Certified)
- Common Criteria product certifications
- ISO14001 Environmental management
- C–TPAT and AEO supply chain security criteria (Certified Tier 3 C–TPAT and AEO-Security)

For shipping and transportation security, Juniper Networks has developed customs standards based on CTPAT and AEO and is certified by the regulatory bodies that oversee CTPAT and AEO. The company is supportive of these efforts since they help prevent the introduction of contraband into the supply chain. The company also is a member of the Transported Asset Protection Association (TAPA).

Juniper Networks also regularly works with industry partners and the government to identify new and emerging risks, and collaborate on best practices to mitigate those risks.