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

U.S. Resilience Project

BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Schweitzer Engineering Laboratories, Inc.

Delivering Quality Products by Managing Supply Chain Risk

INTERVIEWS

Senior Management from Quality; Manufacturing; Security; Research and Development; and Contracts and Risk Management

The Next New Things in Supply Chain Risk Management

- SEL sources domestically to the greatest extent possible using only trusted, reputable suppliers, while delivering on the commitment to offer the lowest price anywhere in the world.
- Quality, security, and integrity enable SEL to offer a premium warranty on its products.
- SEL risk managers possess tremendous detail about the path of every component — through fabrication, packaging, testing, warehousing, shipping, and distribution.

Company Overview

Schweitzer Engineering Laboratories, Inc. (SEL) partners with customers around the world to ensure the safe, reliable and economical delivery of electric power. In 1984, SEL introduced the world's first commercially available digital relay, revolutionizing the protection of electrical power systems. Since then, SEL has developed products for the protection, monitoring, control, automation, measurement, and metering of power systems. All of these products are designed with security in mind. Headquartered in Pullman, Washington, the U.S.-based manufacturer is 100 percent employee-owned.

Supply Chain Risk Management Philosophy

Quality and security have been a part of SEL's culture since the company started. These two priorities are constantly reinforced in its operations and by management. Founder and President Edmund O. Schweitzer, III, works continually with senior management to assess emerging categories of risks and develop mitigation strategies. All employees (nearly 4,000 worldwide) attend a company meeting every Friday at which risk and supply chain security are frequent topics of discussion.

Although SEL has many supply chains, its largest and most complex is for electronic components. Despite the fact that almost 90 percent of electronic components are made outside of the United States, SEL sources domestically whenever possible in order to control quality. While conventional wisdom holds that this would put its products at a price disadvantage, SEL continually strives to offer the best price with the best functionality anywhere in the world — with a heightened level of security, continuity, and integrity.

Business Case for Supply Chain Risk Management

Customer service, supply chain security, and quality are part of the business DNA at SEL.

SEL's major customers are electric power utilities and large industrial users of electric power who demand security, quality, and integrity of the product they install on their systems. Consequently, one of the drivers for SEL's investment in supply chain risk management is the company's focus on the continuity and quality of the components and systems it provides to these customers.

SEL's business case for supply chain risk management is also tied to the company's quality assurance processes. In some cases, these products have two to three decade-long life cycles. One of the many reasons SEL offers a premium warranty (and in fact has never charged to repair or replace a defective part in its 31-year history) is that doing so provides an incentive for customers to return products which results in an ongoing quality assessment that pinpoints root causes of defects, enabling SEL to identify design process or supplier problems. That capability enables SEL to remediate problems quickly while continually improving quality.

Organizational Approach to Supply Chain Risk Management

At SEL, supply chain risk management relies on cross-functional collaboration, rather than being relegated to a separate department. The process begins with the selection of vendors, which is a team effort between product development, quality, and purchasing. Similarly, different teams weigh in on component selection, ongoing monitoring of vendors and parts, and on-site vendor audits. The approach makes risk management everyone's responsibility.

There are a number of advantages to SEL's approach. First, risk management is not an overhead function. Employees do not fear audits from a separate security department, which is sometimes perceived as adversarial in other companies. Second, it allows functional experts to bring their particular expertise to address risks that cut across the entire product life-cycle. As the senior team emphasizes:

> "People work on different pieces of supply chain risk management and provide expertise from their own areas. We collaborate together to come up with total solutions."

Best Practices in Supply Chain Risk Management

While supply chain risk management is critically important to SEL, risk is not tracked on a scorecard. Instead, the clear knowledge of threats to the supply chain — including counterfeits, Intellectual Property (IP) theft, environmental disruptions, terrorism and cybersecurity attacks and the impact such a disruption could have on their customers — drives the company to embed and execute risk management best practices as part of daily operations.

According to a senior team leader:

> "Prioritization is a moving target — changes in conditions worldwide occur, both with suppliers and with the quality of parts. We have daily meetings to re-evaluate and re-prioritize risks and mitigation strategies. We work with suppliers through quarterly supply performance reports. Every quarter we sit down with suppliers on a continuous basis."

Vendor Risk Management

SEL sets the same high expectations for its suppliers that it does for itself. The company believes that building supplier relationships is good business and has held an annual suppliers conference for the past 15 years. The goal is to ensure that SEL's suppliers understand the company's vision and objectives, its risk management priorities and expectations of its suppliers. The conference includes all supplier types: product components, service providers, insurance and equipment providers.

Supplier Risk Rating: SEL employs a supplier rating system that evaluates every supplier based on price, quality, features, innovation, delivery, and service. It also combines risk intelligence from its R&D, supplier quality, and finance and purchasing departments to evaluate supplier risks such as:

- Manufacturer location risk, based upon geographic site for all process steps;
- Supplier quality risk, based on defect data;
- R&D risk based on technology type and the length of time required for redesign should the part become unavailable;
- Financial risk, based on a manufacturer or supplier's financial health; and
- Purchasing risk, based on supplier performance for on time delivery, responsiveness, and pricing.

Supplier Survey: SEL is working to better understand its suppliers' own supply chains, ensuring all aspects of those supply chains are covered. Additionally, SEL is working on enhanced processes that scrutinize risk at lower tiers of the supply chain. Going forward, Tier 1 suppliers will need to evaluate their own supply chains for risks that could impact SEL, including:

- Suppliers of key materials for SEL parts;
- Primary risks and mitigation strategies for each supplier;
- Supplier locations; and
- Methods for forecasting demand and primary replenishment strategies.

Supplier Audits/Inspections

SEL maintains tight oversight of its supply base. Teams from R&D, quality, purchasing, and security visit top suppliers for annual audits and inspections. Suppliers also visit SEL to exchange best practices, innovative ideas, and provide mutual guidance. Collaborating with its suppliers on manufacturing process improvements helps SEL improve quality, efficiency, and cost.

This level of oversight is not limited to product providers. Other service-level partners participate in audits and inspections as well.

Quality Risk Management

In addition, SEL's parts risk system, tools and processes help provide end-to-end supply chain visibility so that customers can be assured that the products are legitimate and have not been outside of the SEL demand chain. SEL is also able to utilize these tools to assess and respond to supply chain disruptions.

This information allows SEL buyers to respond quickly in case of supply chain disruptions. In the aftermath of the 2011 Japanese earthquake and tsunami, SEL was able to quickly identify where its supply chain might be impacted. To minimize the impact of disruptions, SEL generally works with its suppliers to ensure six months of inventory is continually secured for high risk components.

Product Integrity

- SEL goes to great lengths to assure product integrity — to ensure that what its customers get is what they have been promised.
- Every prospective supplier undergoes a qualification process. Component purchases must be qualified by SEL's R&D group and are procured directly from the manufacturer or from officially franchised suppliers. When parts are purchased outside this prescribed path, the parts do not enter the supply chain until they pass a rigorous inspection process, which includes X-ray, packaging and part marking verification, and part de-encapsulation when necessary. If anything seems out of place, the manufacturer of the parts is consulted.

SEL's Product Database

- Product ID, firmware ID and serial number
- Sub-assembly data and work instructions
- Who built it?
- When it was built?
- Where was it built?
- What line was it built on?
- What test station was used?
- Who bought it?
- Who is the end-user?
- How was it shipped?
- Who was the sales representative?

Avoid Interdiction

- Buy and sell direct, avoid brokers
- Inspect packaging, track lot numbers
- Doubts? X-Ray, unpack
- Keep inventory close
- Select shipping methods with care
- Support customer with installation and commissioning

- Testing is done continuously and rigorously throughout the manufacturing process. Any variation in performance leads to a stop shipment call.
- All third party SEL suppliers work on a 'one strike and you are out' rule. If a third party source sends a counterfeit component, or components that do not meet SEL specified requirements, that supplier will be flagged in the supplier qualification database as unapproved, and SEL will not order from them again.

Supply Chain Cyber Risk Management

Given its holistic approach to integrity, SEL has established tight requirements to prevent cybersecurity incidents — from embedding cybersecurity at the earliest stages of product development, to strict physical security requirements for employees and visitors alike, and stringent rules on maintenance and upgrade services by their vendors. For example, it would be an extreme exception for a vendor to be allowed to connect remotely to SEL's systems for maintenance or upgrade. Anyone, employees included, coming on-site with USB keys are required to run them through a company-designed scanning system prior to use on SEL's system. Additionally, personal devices are not allowed to connect to SEL's network.

On the hardware side, SEL is vertically integrated. It manufactures as much as it can in-house and sources domestically to the greatest extent possible. SEL has found that this strategy generates shorter lead times (with an average 12-day turnaround) and enables rapid adjustments to supply chain disruptions and creates more confidence in the ability to secure not just the continuity of products in the supply chain, but also their integrity.

On the software side, SEL develops much of its own code. When third party code is used, the source code is always acquired. According to a cybersecurity team lead:

> "Acquiring source code is not an inexpensive venture for us. The price is always a negotiating point, but the requirement to provide us the source code is not. We will not use a third party library without having the source code. It's the right thing to do for many reasons — only one of which is cybersecurity. Another reason for paying a price premium is quality. When there's a problem, SEL can troubleshoot the code — and that is important in an industry in which the products are likely to be used for decades and often in rough environments. The fact that SEL can build a quality product that's going to last decades — and hold up from a security perspective because of these secure development practices — is a competitive strength."

Transportation Security: In terms of transportation security, SEL manages its transportation partners the same as its material providers. There are site visits to transportation providers to verify that high quality standards and policies are in place. Audits are conducted to monitor security and inventory controls. All carriers are CT-PAT certified and TSA-compliant. Air freight is routed through TSA-approved screening facilities.

Standards

At this time, SEL leverages industry standards such as ISO 27001, the NIST Cybersecurity Framework, and ITIL to reinforce their own best practices. SEL uses the best practices in multiple standards and applies them as they best fit to enhance the overall quality, security, and integrity of the products and processes.

The NIST Cyber Framework created a useful guideline for SEL to understand WHAT they needed to worry about rather than HOW to address that concern. SEL believes in sensible security, clearly understands the full range of supply chain risks, reassesses and reprioritizes as risks change and evolve, and makes sure that the response is appropriate to the risk.