Best Practices in Vendor Selection and Management

In a Nutshell: When companies began extensively outsourcing and globalizing the supply chain in the 1980's and 1990's, they did so without understanding the risks suppliers posed. Lack of supplier attention to quality management could compromise the brand. Lack of physical or cybersecurity at supplier sites could result in a breach of corporate data systems or product corruption. Over time, companies have begun implementing vendor management systems – ranging from basic, paper-based approaches to highly sophisticated software solutions and physical audits – to assess and mitigate vendor risks to the supply chain.

Supplier Risks: The core set of supplier risk criteria typically includes: financial risks, location risk, business continuity and time to recovery risks, and operational risks (quality, cost, performance, capacity). These risks indicators can tell a company whether a supplier or sub-supplier is more or less likely to deliver products on time and as expected. Some companies are finding that it's not enough to evaluate risk at the supplier level. They also map and track individual components, products and equipment.

Cyber supply chain risks: More recently, cyber concerns have opened up a number of other supplier risk issues. Some companies include in their risk assessments:

- How well do suppliers vet their own personnel? Of particular concern are personnel in supplier companies that have access to the data, systems or facilities of their customers.
- How well do the vendors vet their service providers? Any service provider – from janitorial services to system maintenance – or any provider with access to company information poses a potential cyber risk.
- How well do the vendors vet their products and software? Of particular concern are products with embedded IT that will be integrated into their customer's systems.

Supplier Security Requirements: Physical and cybersecurity processes are being evaluated during supplier vetting processes. Many companies also include process requirements in supplier agreements and contract language. Key security processes evaluated for supplier vetting and included in contract requirements include:

- Security Governance
- Manufacturing/Operational Security
- Software Engineering and Architecture
- Asset Management
- Incident Management
- Transportation Security
- Physical and Environmental Security
- Personnel Security
- Information Protection
- Sub-tier partner security (lower tiers, service providers, cloud)

Examples of Vendor Management Best Practices: Companies have identified various practices that have helped their business manage their vendors more effectively. These practices include:

- A focus on brand integrity rather than brand protection. This supports life-cycle threat modeling which proactively identifies and addresses vulnerabilities in the supply chain.
- Procurement and sourcing processes are developed jointly with input from IT, security, engineering, and operations personnel; sourcing decisions receive multi-stakeholder input.
- Standard security terms and conditions are included in all requests for proposals (RFPs) and contracts, tailored to the type of contract and business needs.
- Asset or business owners must formally accept responsibility for exceptions to security guidelines and any resulting business impact.
- Since many risk assessments depend on supplier self-evaluation, a number of companies employ on-site verification and validation of these reviews. Some companies cross-train personnel to be stationed at supplier companies so that security criteria can be monitored year round.
- New suppliers enter a test and assessment period – to test the capabilities of the supplier and its compliance with various requirements -- before they actively join the supply chain. In high risk areas, for example, a supplier might go through a series of pilots before they fully enter the supply chain.
- Tier 1 suppliers are required to give their suppliers the same survey that the Original Equipment Manufacturer (OEM) requires of them.
- Approved vendor lists are established for manufacturing partners.
- Quarterly reviews of supplier performance are assessed among a stakeholder group.
- Annual supplier meetings ensure that suppliers understand the customers' business needs, concerns and security priorities.
- Mentoring and training programs are offered to suppliers, especially in difficult or key areas of concern to the company, such as cybersecurity.

Tools for Supplier Risk Management: Vetting supply chain partners beyond the first tier is a challenge for many companies. Manual methods can be difficult and do not scale for companies with hundreds or thousands of tier-one suppliers and numberless sub- tier suppliers. Plus, while large companies are often able to make suppliers adopt their preferred solutions, smaller companies don't have the deep relationships or the power to get the information they need.

To fill these gaps, third party providers are collecting, managing and centralizing supplier risk management data. This can result in increased efficiencies for analyzing the supply chain as well as reduce the burden on suppliers who may be asked to fill out similar informational forms for each customer. Third party vendors also offer supply chain mapping services which provide supplier locations, financial data, and sometimes the location of critical parts, components and equipment to ensure that critical chokepoints or security issues are apparent.