Mitigating Cyber Security Risks in the Supply Chain

Minimizing cyber risks in the supply chain is a modern challenge needing urgent attention across industries.

Each vendor in the supply chain presents cyber vulnerabilities which must be minimized in order to mitigate the corporate cyber security risks. It is not enough to concentrate on the buyer's systems because the risks throughout the supply chain are threats to business growth and sustainability. Best practices include identification of current vendor vulnerabilities, regular assessment of vendor cyber security practices, and supplier vetting during contract negotiations.

Supply Chain of Vulnerabilities

Supply chains pose enormous technology risks because all companies rely on software, hardware and the internet today. If any vendor fails to manage cyber security, the organization is put at risk no matter how well its own cyber security risk minimization program is designed. Corporate programs can close security gaps by developing comprehensive risk management programs that incorporate supplier chain risks into consideration. That is the first best practice – integrating assessment of internal and external risks.

Specific supplier vulnerabilities around technology involve people, facilities, systems, and goods and services. Does the supplier vet the personnel who accesses the organization's sensitive, customer or proprietary data, or corporate systems? Are supplier facilities secure so that no one can hack or sabotage computer systems? Do suppliers have cyber security policies and procedures, including vetting their suppliers? How well do suppliers protect their software and technology products that will be integrated into the corporate systems or customer products?

The corporate vetting process for current suppliers utilizes a number of tools. Surveys are useful because all relevant questions can be asked in customized supplier surveys. Asking questions about product security is critical when the organization is purchasing technology from the vendor or the supplier's technology is embedded in their customer's systems. All corporate suppliers should inform their customers about security systems in place to mitigate security risks involving their suppliers, accessing their client's computer systems, and protecting their in-house computer systems. Security questions also cover security governance, incident management and reporting, physical security, and information protection.

The ideal time to establish a strong supplier relationship that addresses cyber security is during contract negotiations. The supplier contract can stipulate the vendor's cyber-security responsibilities. If this is a new supply chain risk

management program, existing contracts need review by senior leadership and legal personnel.

Meeting Standards

Industry compliance standards represent recommended and minimum standards, but vendors should also have additional standards and compliance requirements that are even more stringent. For example, the Payment Card Industry Data Security Standard (PCI DSS) is a an industry security standard that applies to any merchant that has processes, stores, or transmits credit card information. The standard is administered by the Payment Card Industry Security Standards Council, (PCI SSC) but the credit card vendors and acquirers are responsible for standards compliance. Business violations of the standards can lead to fines, but worse is the threat of data breaches that can lead to reputational damage.

Target's experience is a good example of the complexity of cyber security in supply chain. In December 2013, 40 million Target customers had their credit and debit card information, and the following year it was revealed that 70-110 million Target customers had their email and mailing addresses stolen. The negative impact of this data breach has been severe and continues to grow. So far, the breach has cost Target well over $252 million, offset by $90 million in insurance payments. However, Target is now facing additional claims from four major credit card companies because it ignored security system alerts and is facing fines and penalties from government agencies.

If the vendor is breached, but it does not impact a particular customer, the vendor is not legally obligated to inform that customer, unless language in the contract requires the reporting. It is important to get the language into existing and new contracts. The Target breach emanated from Target giving a supplier access to the Target network to monitor refrigeration units. Hackers breached the supplier's system and used that access to break into Target's system.

Using Suppliers to Test Suppliers

Effective cyber security best practices include a mix of on-site testing and security tools. Penetration tests are useful for periodic testing. A third party assesses compliance with standards and may try to hack into the vendor systems. The Open Group is a collaborative organization for customers, technology companies, supplier organizations, and government agencies to develop guidelines for "manufacturing, sourcing, and integrating trusted, secure technologies." The objective is to shape global procurement strategies and best practices to reduce vulnerabilities and threats to the global supply chain.

The Open Group standards can be incorporated into purchasing decisions for off-the-shelf technology and used by suppliers to protect the integrity of their products and services. Vendors certified by Open Group have been assessed and approved as meeting strict guidelines and security standards, contributing to supply chain security. Organizations can look for certifications like the one Open Group offers.

Bitsight has developed software that enables organizations to utilize continuous, data-driven performance to assess third party suppliers' security controls. Strategic vendors, critical to business sustainability, can go through pilot projects before being added to the supply chain. Third party providers can also offer supply chain mapping which helps identify hotspots for potential security breaches.

This is another opportunity for corporations to find and utilize diverse suppliers specializing in cyber security, and there are many. Resilient Point is a Service Disabled Veteran Owned Small Business that delivers cyber security and intelligence solutions to government and commercial organizations. Secured Sciences Group is a woman-owned business offering cybersecurity, governance, and risk and compliance services. Radiant Infotech is a minority-owned and woman-owned small business offering technology-based and cyber-security solutions.

There is no single cyber-security plan that organizations can implement in the supply chain. Best practices include developing contractual agreements that address security, performing onsite and other vendor assessments, utilizing risk management tools, and ensuring in-house controls and procedures are in place. The procurement process should be developed jointly with IT so that standard security requirements are included in RFPs and the final contract. Finally, as Target discovered, it is critical that responsible people adhere to the cyber security policies and procedures. It is true that the weakest link in the supply chain creates the greatest threats.