National Institute of Standards and Technology

Best Practices in Cyber Supply Chain Risk Management

Conference Materials

Business Case for Cyber Supply Chain Risk Management

In a Nutshell: The best practices and tools for cyber supply chain risk management (SCRM) simultaneously protect the quality and integrity of the supply chain, provide cybersecurity and resilience of products, create the capacity to meet customer expectations, and also safeguard brand reputation and shareholder value**.** In today's environment of volatility and vulnerability, cyber SCRM is not optional.

What are the Business Drivers for Cyber SCRM? The global complexity of supply chains, the increase in potential disruptions, and emerging cybersecurity risks to the supply chain - caused by threats and vulnerabilities of information systems - have dramatically increased the risks that:

- Process and product quality could be compromised by inadequately monitored suppliers.
- Lower-tier suppliers could intentionally or unintentionally introduce software, firmware, or hardware in which confidentiality, integrity or availability has been compromised.
- Supply chain disruptions could create a scramble for parts that enables poor quality or counterfeit products to enter the supply chain.
- High-value intellectual property shared with suppliers could be misused.
- Service suppliers – including contract manufacturers, outsourced legal and accounting, and repair and maintenance providers—could tamper with a company's information based on their access to a company's information system, if the data is not adequately protected.
- Adversaries can use vulnerabilities of different components within the supply chain to attack a company's information systems.

All of these risks are part of the new cyber supply chain risk landscape, and they can jeopardize business operations, the quality and integrity of products and services, and impact the bottom line, business reputation, and customer satisfaction.

Cyber Supply Chain Risks- Magnitude of Impact: The research in this area is sparse, but a few factoids help make a business case for action:

- As supply chains grow more complex and more globalized, the likelihood that a manufacturing organization will ***not*** experience a supply chain disruption in a twenty-four month period is a mere 2%. The average cost of a disruption is estimated at $360,000, without factoring in management time, lost customers, or reputational damage.[1]
- In 2014, roughly a quarter (23%) of all cyber breaches were attributed to current service providers and contractors; 45% were attributed to past partners.[2] Attacks targeted key sectors that use industrial control systems for physical processes, particularly in the manufacturing and energy sectors; the manufacturing and services industries were the most targeted for spear-phishing attacks (20% each).[3]

[1] Sourcing Innovation, *The ROI of Supply Chain Resiliency: It's More Than You Think: Attaining ROI with Supply Chain Resiliency*. Sponsored by Resilinc, November 2013. http://info.resilinc.com/roi-of-supply-chain-resiliency-resilinc-sourcing-innovation

[2] PwC, *Managing Cyber Risks in an Interconnected World*, 2014, http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

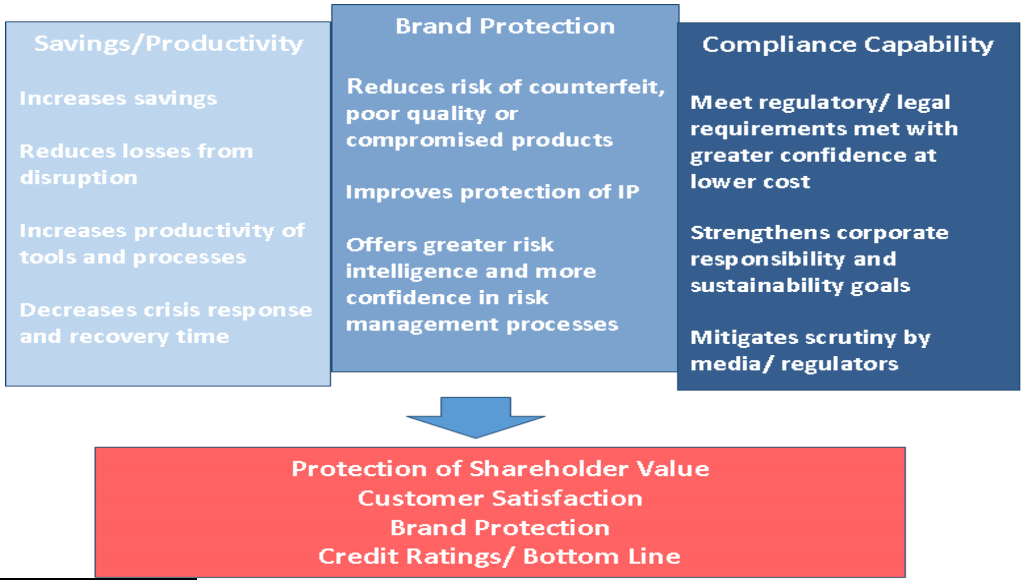
[3] Symantec. *Internet Security Threat Report*, p. 13. 2015.

- Most breaches in 2014 were a result of cyber espionage (60%) with manufacturers being the most targeted (27.4%). Cyber-espionage was used to compromise company secrets (85.8%) and as of 2013, 51% of cyber-espionage attacks involved state-affiliated actors[4]. An increasing number of cyber-espionage attacks attempt to alter processes along the manufacturing line.[5]

Questions CEOs and Boards of Directors Should Be Asking:

1. **Do we know who our suppliers and our suppliers' suppliers are?** Knowing who is in the supply chain is a prerequisite for managing every type of supply chain risk. Lack of transparency creates blind spots – unable to identify critical chokepoints, compliance problems, physical or cybersecurity vulnerabilities, financial stability or quality issues.
2. **Do we know how our suppliers and partners are managing cyber supply chain risks for the products and services we acquire?** Increased complexity and size of a supply chain accelerates the risk that a supplier can compromise the end product, business performance, reputation, and shareholder value. The importance of suppliers' security processes (both physical and cyber), the strength of its business continuity plan, its quality control and testing procedures, and employee security training programs has become a critical component of effective supply chain risk management.
3. **Have we captured the ROI from an end-to-end strategy for supply chain risk management?** Ultimately, companies will invest where the ROI is clear. Well-run supply chain risk management programs not only manage risks; they create competitive benefits. For some companies, multi-tier visibility in the supply chain has yielded cost reductions in sourcing, manpower and insurance**.** For others, that not only protects against disruptions, including cyber attacks, but it also creates a capability to ramp up supplies when demand is higher than forecast.

Competitive Benefits of Cyber Supply Chain Risk Management Diagram: In addition to traditional methods, appropriate cyber security policies, controls, and procedures should be implemented, based on cost-effective risk approach.



Savings/Productivity

Increases savings

Reduces losses from disruption

Increases productivity of tools and processes

Decreases crisis response and recovery time

Brand Protection

Reduces risk of counterfeit, poor quality or compromised products

Improves protection of IP

Offers greater risk intelligence and more confidence in risk management processes

Compliance Capability

Meet regulatory/ legal requirements met with greater confidence at lower cost

Strengthens corporate responsibility and sustainability goals

Mitigates scrutiny by media/ regulators

Protection of Shareholder Value
Customer Satisfaction
Brand Protection
Credit Ratings/ Bottom Line

[4] Verizon, *Threat Landscape: Manufacturing, Services, and Technology*, 2013.

[5] Symantec, *Internet Security Threat Report*, p. 69. 2015.