National Institute of Standards and Technology

Best Practices in Cyber Supply Chain Risk Management

Conference Materials

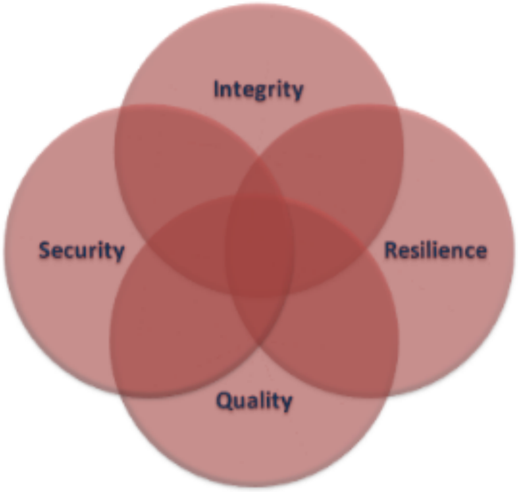
Organizational Strategies for Cyber Supply Chain Risk Management

In a Nutshell: Because cyber **s**upply chain risks cut across different risk management functions, leader companies establish organizational structures and strategies that enable them to manage risks holistically on an enterprise-wide basis.

Why Cyber Supply Chain Risk Management Needs an Enterprise Approach: Although the process of bringing a product from design through production, service and end-of-life often looks seamless to a customer, a number of different organizations in a company actually "own" different parts of that process – and their attendant risks**.** R&D and engineering, product development, sourcing, procurement, traditional supply chain risk management, quality assurance, security, legal, and IT all have a piece of cyber supply chain risk management. The challenge for silo'ed organizations is that cyber risks in particular cut across every major function and business line. When these functions don't communicate and collaborate, gaps in risk management can emerge. An overarching cyber supply chain risk management program is necessary.

Moreover, the best practices and tools needed to manage cyber supply chain risks often have applicability to other areas as well – and may already be in use in those areas. Supply chain mapping capability should identify all involved suppliers through the sub-tiers – a fundamental capability for supply chain continuity, quality and cybersecurity. Track and trace tools are part of quality assurance, but they also create a forensic capability to distinguish between design flaws, manufacturing flaws and malware. When risk management goals are not aligned, opportunities to leverage tools for multiple risk management objectives and eliminate redundant capabilities can be lost.

Supply Chain Risk Management lies at the intersection of security, integrity, resilience, and quality[1] :



- **Security** provides the confidentiality, integrity, and availability of information that (a) describes the supply chain (e.g., information about the paths of products and services, both logical and physical); or (b) traverses the supply chain (e.g., intellectual property contained in products and services), as well as information about the parties participating in the supply chain (anyone who touches an product or service throughout its life cycle).
- **Integrity** is focused on ensuring that the products or services in the supply chain are genuine, unaltered, and that the products and services will perform according to acquirer specifications and without additional unwanted functionality.

[1] NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

- **Resilience** is focused on ensuring that the supply chain will provide the required products and services under stress or failure.
- **Quality** is focused on reducing vulnerabilities that may limit the intended function of a component, lead to component failure, or provide opportunities for exploitation.

Best Practices in Managing Cyber Supply Chain Risks Holistically: An overarching cyber supply chain risk management program is necessary. Some organizational best practices include:

- **Executive-level visibility**: Executives are aware of and involved in cyber supply chain risk decisions. In some cases, functional leaders sit on a management committee made up of the senior leadership that drives both strategic and operational oversight of the business. This leadership model puts cyber supply chain risk management at the core of business decision-making.
- **Cross-Functional Leadership Structures**: There are several different ways to create cross-functional coordination which breaks down the siloes between R&D and engineering, product development, sourcing, procurement, supply chain risk management, quality assurance, security, legal, and IT. Methods include:
    - **Supply Chain Risk Council:** A number of companies create Supply Chain Risk Councils, in which representatives from multiple functions meet regularly to review the risk environment, exposures and cyber vulnerabilities and prioritize mitigation efforts.
    - **Enterprise-level Security Groups:** A centralized security group which integrates physical and cybersecurity, sets security standards across the organization, has primary responsibility for assuring a holistic view of supply chain risk management and is responsible not only preventing, detecting and responding to incidents, but also identifying emerging threats and vulnerabilities.
    - **Centers of Excellence (COE):** Supply chain centers of excellence create formal and standardized processes to improve operations and foster collaboration between the business units and the COE to identify and manage best practices.
    - **Cross-functional reporting pyramid:** A number of companies create an executive position, typically SVP level, to which the key supply chain functions report. This creates a de facto integration of different risk elements, but IT and cyber supply chain risk is often left out in this structure.