
CONFI

The Fourth Dimension of Today's Supply Chains

New technologies are empowering supply chains as never before, but they are also exposing them to new risks. To bolster confidence in their supply chains, manufacturers must undertake a comprehensive approach to supply chain security.

By Edna Conway and Robert Dean

Bob Dean *is Executive Director, Americas Customer Value Acceleration, at Cisco. Dean has a bachelor's degree in business administration from the University of North Texas. He is also a member of the Manufacturing Leadership Council.*

ADVANCEMENTS IN MOBILITY, CLOUD, AND COLLABORATION technologies are opening up new possibilities as well as challenges in the management of manufacturing supply chains. These technologies, delivered by the Internet of Everything (IoE), which is the connection of people, processes, data, and things, provide a unique opportunity for greater supply chain productivity. While supply chains will remain acutely focused on their traditional dimensions of cost, quality, and delivery, these technologies and the pervasiveness of the IoE have also created a new challenge that manufacturers must face and address—confidence in the security of their supply chains.

Today, supply chains are being redefined as they embrace this fourth dimension—confidence.

Defining Supply Chain Confidence

Simply put, confidence in the supply chain means being security-aware. As manufacturers and supply chain practitioners continue to rely on information and communications technology to enhance their operations, they are exposing their operations to malicious or inadvertent activity. These kinds of attacks require constant vigilance and monitoring. They require being security-aware. Creating confidence requires a plan to address and mitigate this risk across complex supply chains.

By deploying mature security capabilities, overall supply chain resiliency will strengthen, but it is security that delivers the enhanced value of confidence. Confidence means a product will have impeccable quality; it will not have been tampered with; and it is, in fact, authentic and exactly what the customer expects to receive.

Mature security capabilities serve to enhance key supply chain competencies. For example, new product introduction, manufacturing line efficiency, and merger and acquisition integration can be positively influenced with secure development, design, production, and sustainment practices.

The Security Challenge

The security challenge, created by the complexity of the supply chain network, is two-fold: first, the heavy reliance on information and communications; and, second, the ever-growing set of geographically diverse regulatory requirements. These requirements address,

"Addressing security comprehensively means being prepared for forensic analysis of the inevitable security breach."

Figure 1

among other things, privacy, counterfeiting, and indigenous innovation.

Ubiquitous reliance on information technology renders the very core of supply chain operations subject to manipulation, observation, or attack. As a result, a comprehensive approach to supply chain security is essential.

The Cisco Approach

A prerequisite for confidence is defining the scope of your supply chain. Specific elements of a comprehensive supply chain will vary by industry sector. One end-to-end view of supply chain is shown in Figure 1 above.

Cisco has identified four key focus areas that should be addressed to deliver confidence:

1. Malicious Modification/Substitution of Technology
2. Counterfeit Products (raw materials and finished goods)
3. Embedding Security into Supply Chain Resiliency
4. Misuse of Intellectual Property

If these four focus areas are considered across the end-to-end supply chain, they will allow the delivery of products that are genuine and have not been altered in a way that would cause them to operate in a fashion other than intended.

As we all know, 100 percent security can never be achieved. Addressing security comprehensively means being prepared for forensic analysis of the inevitable security breach. For Cisco, Printed Circuit Board Assemblies (PCBAs) are critical to our solutions; there-

Figure 2

1. Secure development

2. Information exchange and access controls

3. Physical plant security

4. Talent security and integrity

5. Supplier resiliency and crisis management

6. Protection of high-value/IP-containing components and finished goods

7. Logistics security

8. Fabrication security

9. Scrap management

10. Service and end-of-life security management

fore, preparedness for forensic analysis requires key information about PCBAs. To gather that information, we deploy a proprietary methodology for PCBA traceability at the component level. Capturing key data such as date code, lot code, and material content creates a rich repository of information gathered in real-time during PCBA testing. Furthermore, by embracing the four focus areas, we simultaneously embed electronic identity "handshakes" during this testing process. This combination of security technology and process effectiveness enhances our supply chain's fourth dimension: confidence.

Areas of Discipline

Effectively tackling the four key focus areas across the entire supply chain requires establishing certain foundational process areas. At Cisco, we have identified 10 disciplines which, when deployed in the right supply chain node in the right way, establish a comprehensive framework. The 10 areas are shown in Figure 2.

Making it all work

Once your organization knows what it is focusing on and has its own set of disciplines, consider a three-pronged deployment approach. While not all security activities in every node of your supply chain need to be utilized, consider the applicability of:

- Physical Security Practices
- Logical (rule-based) Security Processes, and
- Security Technology.

Physical security practice examples include: component-to-finished good traceability, real-time transport tracking, security checkpoints, segregation of high-value materials, and role-based access control.

Some logical security processes are: encrypting transmitted data, material reconciliation, and data destruction and scrap-handling processes. Finally, available security technologies might incorporate anti-counterfeiting chips, data extracting test beds, and tamper-resistant labeling and packaging.

As with all process improvement, supply chain security must be relentlessly adhered to and validated. Validation across your supply chain can be implemented in multiple ways. Foundational validation practices include both physical audits and information security assessments. Embedding security into supplier ratings can inspire suppliers to embark on the security journey with you. This layered set of validation and measurement processes will ensure the continuous feedback, remediation, and enhancement essential to a successful supply chain security capability.

Communication and information are crucial to an efficient supply chain. Securely extending access and visibility throughout the supply chain can create an integrated workflow that promotes innovation, improves efficiency, facilitates collaboration and decreases business risk. M

Edna Conway *is Chief Security Officer, Global Supply Chain, at Cisco. Conway also leads Cisco's supply chain cyber-protection plan, serving on the company's Cyber-security Board and Risk and Resiliency Operating Committee. She holds a degree in Bio-mechanical Engineering and Medieval and Renaissance Literature from Columbia University, and earned her law degree at the University of Virginia.*

"As with all process improvement, supply chain security must be relentlessly adhered to and validated."