Combating Cyber Risk in the Supply Chain

ALABAMA GLOBAL SUPPLY CHAIN & LOGISTICS SUMMIT

Intro

Brent Hutfless is the Director of IT Operations at Austal USA, the US division of the global commercial and defense shipbuilder Austal. Brent's technology and security experiences cover aviation, training, healthcare, manufacturing and intelligence-related fields, in roles at Austal, AT&T, Raytheon, and several US Navy commands. He holds graduate and undergraduate degrees in computer science and software engineering, a CISSP certification, and plays an active role in several professional organizations along the Gulf Coast.

Agenda

- Risks by the Numbers
- Intellectual Property Theft
- Material Threats & Risks
- Supplier & Vendor Access
- Mitigating the Threats

What are the risks?

80% of all information breaches originate in the supply chain

72% of companies do NOT have full visibility into their supply chains

59% of companies do NOT have a process for assessing cyber security of third party providers with which they share data or networks

45% of all cyber breaches were attributed to past partners

40% of attack campaigns targeted manufacturing and service sectors (20% each)

Source – National Institute of Standard and Technology (NIST) – 2016 RSA Conference

Intellectual Property Theft

- Adherence to non disclosure agreement (NDA)
- Subcontractor flow-down agreements
- Incidental exposure of technical specifications
- Compromise of supplier systems
- Vendor personnel

A Tale of Dueling Compressors – Death and Mayhem in the Industrial Refrigeration Industry

IP Theft Risks

- Loss of market share
- Loss of research and development investment
- Exploitation of product vulnerabilities

Material Threats & Risks

- Counterfeit and/or substandard parts or subassemblies
- False flag operations (Easter eggs)
- Brand dilution and reputational damage
- Increased warranty claims or service cost

GSA and the Gray Market Switches

Samsung Phones Violate FAA No-Smoking Policy

Supplier/vendor access risk

- Third party access to proprietary information
- Third party access to network resources
- Failure to remove access after need expires

Target Payment System Network and Fazio Mechanical Services

Mitigating the threats

- Communication
- Flow-down language in NDA and contracts
- Understanding of vendor personnel, business practices and partners
- Information rights management
- Cyber security awareness of network and data access
- Quality assurance and sample testing

FIN!

Thank you!