RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: GRC-W03

Integrating Cybersecurity Into Supply Chain Risk Management

Jon Boyens

Program Manager, Cyber SCRM
National Institute for Standards and Technology

#RSAC

What does Cybersecurity Have to Do with Supply Chains Anyway?

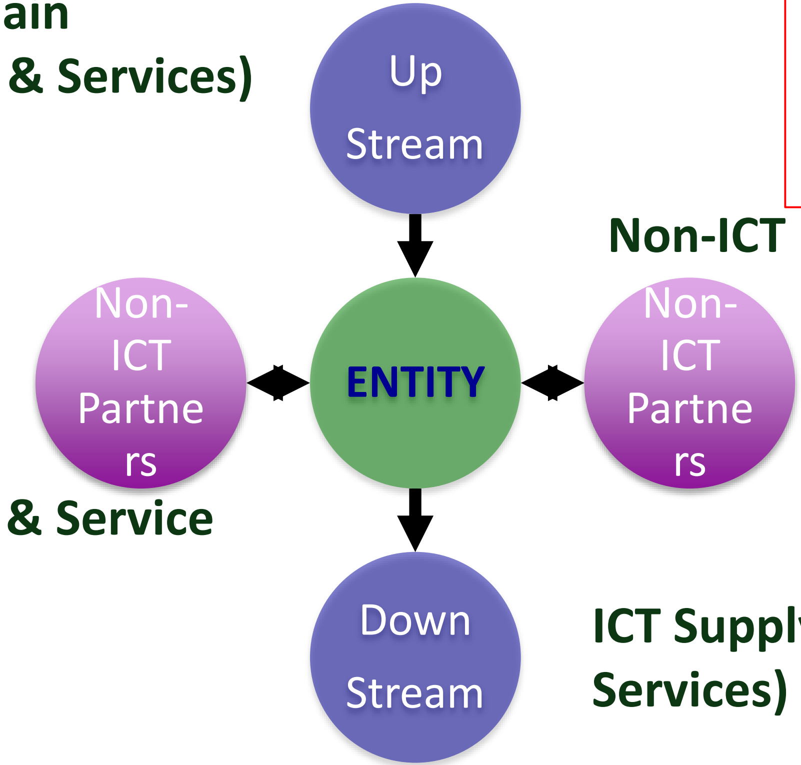
ICT and Non-ICT External Dependencies

ICT Supply Chain
(ICT Products & Services)

<u>TRUST</u>
-Organization
-Process
-Products/Service

<u>But Verify</u>
-Due Diligence
-Standards/Audits
-Testing

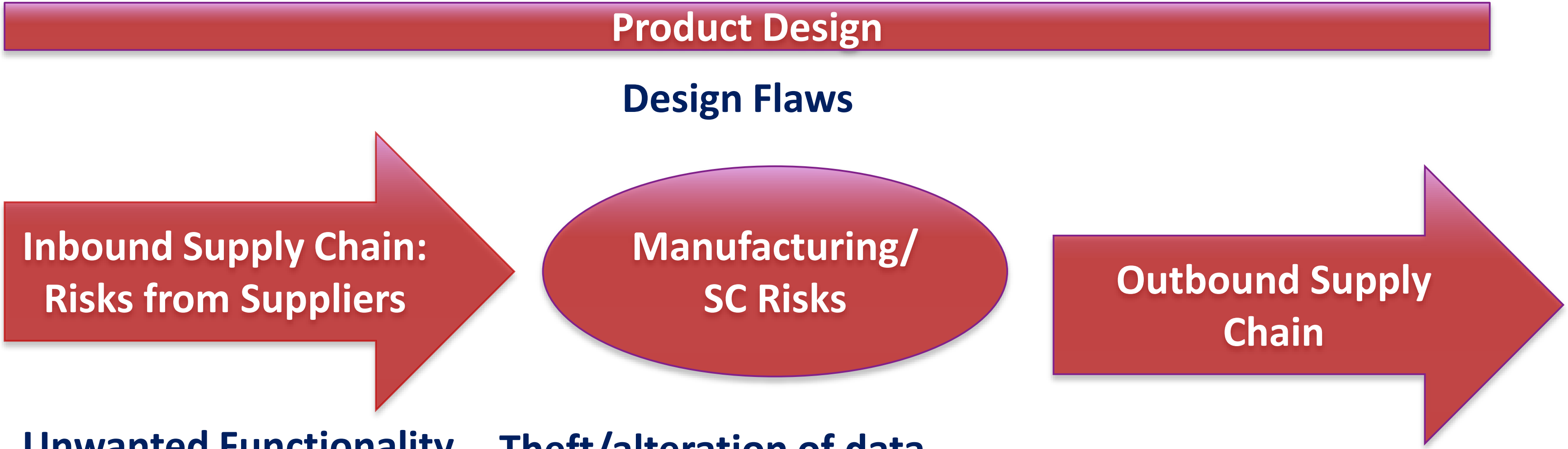
Non-ICT Products & Service



Non-ICT Products & Service

ICT Supply Chain (ICT Products & Services)

Anatomy of Cyber Supply Chain Risk



Product Design

Design Flaws

Inbound Supply Chain: Risks from Suppliers

Manufacturing/ SC Risks

Outbound Supply Chain

Unwanted Functionality
Info/Network Breaches
Supplier Insider Threats

Theft/alteration of data
Compromise of SC business SW
Compromise of control systems, test or other equipment.
Disruptions in vetted suppliers

Theft/Tampering
Counterfeits

How Did We Get Here?

Cyber

- Growing sophistication of ICT
- Number and scale of information systems
- Increasing reliance on COTS

Supply Chain

- Speed and scale of globalization
- Complex supply chain (logically long and geographically diverse)

Risk

- Significant increase in the number of entities who ‘touch’ products and services
- Natural disasters, poor product/service quality and poor security practices

Management

- Lack of *visibility* and *understanding*: how technology is developed, integrated and deployed and practices to assure security.
- A lack of *control* of the decisions impacting the inherited risks and ability to effectively mitigate those risks.

No End in Sight for Supply Chain Cyber Risks

Three trends are exacerbating cyber risks to supply chains:

- **Internet of Things**: everything is smart and interconnected
- **IT-enabled Supply Chain Management:** product and supply chain data run on top of business software that connects supply chains – and weak links abound globally
- **3-D Printing**: production is going viral and digital.

Cyber Supply Chain Risks Emerge At Every Stage

What Can Happen?

- Delivery of poor quality, compromised or counterfeit products that diminish brand reputation
- Loss of intellectual property shared with supply chain partners
- Access to company IT networks, customer information or operational control systems through supplier access
- Impact on revenues, brand reputation and shareholder value

What Does Supply Chain Have to Do with Cyber Risks?

80% of all info breaches originate in the supply chain

45% of all cyber breaches were attributed to past partners

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

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

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

Supply Chain Disruptions are Costly!

98% of manufacturers will experience a supply chain disruption in the next 2 years (80% for all firms)

55% of disruptions cost over $25 million

53% of disruptions caused from *unplanned IT/Comms outage*

24% of disruptions caused from *cyber attacks*

22% of disruptions caused from *data breaches*

Need More?

What’s the Risk? For Example….

- **Supplier-provided keyboard software** gave hackers access to owner data on 600 million Samsung Galaxy phones
- **Supplier-provided advertising SW** tampered with computer security so that attackers could snoop on browser traffic on Lenovo computers.
- **Poor information security** by service suppliers led to data breaches at Target, Home Depot, Goodwill….and many others.

Match the Supplier with the Compromised Customer

Suppliers

- Data breach of Tech Certification firm exposed personnel data on employees of client company
- Hack of credit check database exposed new customer PPI.
- Supplier entertainment system enabled remote take-over of controls in a car.
- Uncancelled credentials of former contractor enabled unauthorized sewage release from water treatment plant.

Customers

- Maroochy
- Cisco
- Fiat/Jeep
- T-Mobile

Ask Yourself the Following

- Can you identify the sub-tier suppliers for critical IT components or software embedded in your products and systems?
- Is cyber risk part of vendor selection, management and audit?
- Do you know what information or IT systems your vendors can access?
- Do you scrutinize vendor personnel practices?

And Most Importantly….

- Does the IT Security Group participate in the procurement process, vendor assessments and vendor management?
- What other groups should you be working with to assure end-to-end cybersecurity?

What are best practices and tools to manage supply chain cyber risks?

NIST Case Studies

- Cisco
- Boeing & Exostar
- Schweitzer Engineering Laboratories
- Exelon Corporation
- John Deere
- Intel Corporation
- Smart Manufacturing Leadership Coalition
- Northrop Grumman Corporation
- Fujitsu
- FireEye
- Dupont Crop Protection
- Resilinc
- Procter & Gamble
- NetApp
- Juniper Networks
- Great River Energy
- *Utility Company*
- *Communications Company*

Findings from NIST Case Studies

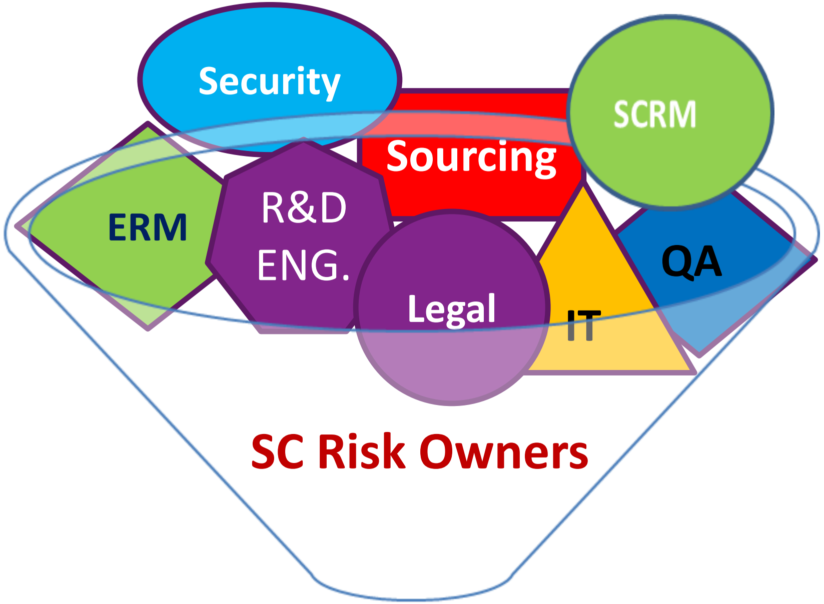
Key Findings:

- Existing tools to mitigate supply chain for quality, integrity, security and continuity risks are also relevant for cyber risks
- Best practices and tools to mitigate cyber risks in the supply chain are hiding in plain sight – often in other parts of the company.

Synergies of solution are not well exploited.

Organizational Strategies to Manage Supply Chain Cyber Risks

- Many hands and different functions affect cyber risks in the supply chain.
- Lack of communication and cooperation creates **risk blind spots.**



Best SCRM Practice: Supply Chain Risk Council

Supply Chain Risk Councils bring together key players for a holistic and end-to-end supply chain risk management strategy

Vendor Risk Assessment Tools

What? Risk ratings to assess and mitigate vendor performance financial, security risks as well as corporate social responsibility risks.

Synergies with Cyber Risks:

- Baseline security requirements for contracts
- Integrates security risks with other business risks in the up-front selection process and ongoing audits.

Supply Chain Resiliency Tools

What? Databases identifying and mapping key suppliers at all levels, components and critical chokepoints as well as prequalified backup sources of supply and vendors

Synergies with Cyber Supply Chain Risk Management

- Identifies lower tier suppliers
- Validated sources of backup supply in the event of disruption, reducing risk that poor quality or counterfeit goods enter SC.

Track and Trace Tools

What? Detailed information on parts and materials to ensure quality, integrity and backstop warranties. Where it was built? Who built it? What assembly line? What test station?

Cybersecurity Benefits

- Visibility by part, supplier, production process down supply chain
- Anti-counterfeiting tools
- Capability to distinguish between design flaws and deliberate defects

Master Security Specification Framework

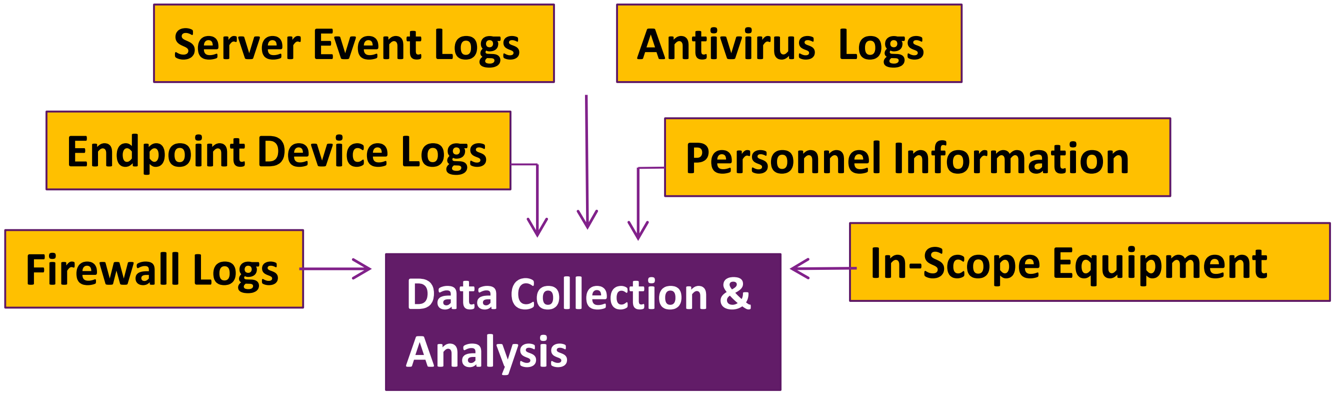
What? Master security specification customizes security requirements to product, service or site.

Cybersecurity Benefits

- Gives business units a full roadmap of security requirements
- Eliminates inconsistencies across business units
- Enables flexibility to deal with multiple supplier roles

Enterprise Risk Intelligence

What? Data collection center reviewing all sources, not just those traditionally associated with information security



Server Event Logs

Antivirus Logs

Endpoint Device Logs

Personnel Information

Firewall Logs

Data Collection & Analysis

In-Scope Equipment

Resources: NIST Best Practice Case Studies

http://www.nist.gov/itl/csd/best-practices-in-cyber-supply-chain-risk-management-october-1-2-2015.cfm

Disclaimer: "*The identification of any commercial product or trade name is included solely for the purpose of providing examples of publicly-disclosed events, and does not imply any particular position by the National Institute of Standards and Technology.*"

Questions?

Jon Boyens
Program Manager, Cyber SCRM
National Institute for Standards and Technology

Jon.Boyens@nist.gov

Http://scrm.nist.gov