

# Supply Chain Risk Management

Presented by:  
Cisco Systems Inc., and Deloitte & Touche LLP



## Introduction

We are from Deloitte Advisory, part of Deloitte & Touche LLP. We will discuss two aspects of supply chain security, of interest to the power industry.

First, **Tom Alrich** will provide an update on the status of the upcoming NERC CIP standard for supply chain security.

Second, **Larry Kivett** will review common third party risks, including those best addressed via advanced due diligence techniques.

## FERC's Order 829

- In July, FERC issued Order 829, requiring NERC to develop a new CIP standard for supply chain security. They required that the standard be developed and approved by NERC and delivered to FERC by next September.
- As with any new or revised standard, NERC constituted a Standards Drafting Team (SDT) composed of SMEs from NERC member entities.
- The team decided FERC's Order could be addressed with a single new standard, which will be CIP-013.
- The first draft of CIP-013 will most likely be posted for comment and ballot in December.

## FERC's Order 829

- CIP-013 will apply to NERC entities that own High, Medium or Low impact BES Cyber Systems.
- The standard requires these entities to develop and implement a supply chain risk management plan.
- FERC ordered that the new standard address four specific goals. Each entity's plan will need to address these four goals.
- Note that CIP-013 will be a non-prescriptive standard. The entity will need to effectively address each of the four goals, but the means used to address each one will be up to the entity.
- The SDT will provide extensive guidance, discussing different approaches to achieving each of the four goals.
- The standard will be risk-based. You will have to focus on vendors, assets, etc. that pose the biggest BES risk.

## The Four Goals of CIP-013

- The first goal is verifying both the *identity* and *integrity* of any software or firmware that is installed on BCS, PACS and PCAs. This includes the original software as well as any patches or upgrades.
- This will apply not just to OS's and main applications, but device drivers, utilities, etc.
- Remember, the standard is risk based. You will not have to make the same effort for software running on a fairly unimportant system as for a critical one.

## The Four Goals of CIP-013

- The second goal is remote access controls for vendors. You may ask, how does this differ from CIP-005 R2?
- First, machine-to-machine access will be covered, not just interactive (by a person).
- Second, you will have to monitor remote access sessions (both types).
- Last, you will have to be able to “detect and respond” to unauthorized activity.
- Implementing this may require a significant effort. However, keep in mind that the requirement is risk-based and non-prescriptive.

## The Four Goals of CIP-013

- The third goal is having security planning controls to address risks in information system deployment (and presumably development).
- You will have to assess risks that a third party might introduce, then evaluate methods to address these risks. These include risks of errors your organization may make in deploying the new systems.
- Network security will be a big part of this. FERC used the example of the Ukraine cyber attacks, where some systems were deployed in an insecure fashion, allowing the attack to succeed.

## The Four Goals of CIP-013

The fourth goal is “procurement controls” to verify vendors follow particular security controls. This could include using contract language, but is not limited to it.

FERC specified four areas to address:

1. Notification of vendor security “events”
2. Notification of applicable personnel changes
3. Disclosure of known vulnerabilities
4. Coordination of response to “vendor-related security incidents”

# The Supply Chain Risk Execution Gap

While most companies have experienced supply chain risk events and aspire to better manage these risks, few have confidence in their ability to effectively do so



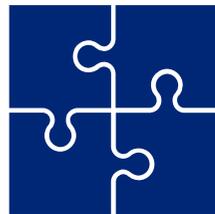
**87%** of respondents *have faced a disruptive incident with third parties* in the last 2-3 years...



**28%** faced *major disruption...*



**11%** experienced a *complete third party failure*



**55.1%** of respondents *aspire to have integrated third party risk management systems in a year or more*, with 16.5% aspiring to be “best-in-class”



**94.3%** of respondents *have only low to moderate confidence in the tools and technology* used to manage third party risk and **88.6%** *have a similar level of confidence in the underlying risk management processes*, despite significantly higher levels of confidence in organizational commitment and governance frameworks – *creating the execution gap*

Source: Deloitte 2016 global survey on Third Party Governance and Risk Management of 170 organizations

© 2016. For Information, contact Deloitte Touche Tohmatsu Limited.

All content protected under nondisclosure and may not be used or reproduced without the express permission of Deloitte

Confidential

# Supply Chain Risk Examples

**For a large complex company, no one knows when a crisis will demand the best your organization can deliver. These are moments of truth that test your readiness, resilience, and character. Advance planning, ongoing vigilance and persistent risk monitoring are critical elements of mitigating reputational risks.**

## Supply Chain Risk Examples



**Disruption to supply chain** by economic turmoil, political unrest, or product safety/recall issues.



**Compliance with and changes in environmental laws**, such as climate change legislation and regulations



**Interruption to transportation logistics** due to weather events, accidents, derailment, collision, fire, explosion, government regulations, or vendor actions



**Corruption or Bribery** risk exposure arising from vendors, use of third-party agents and increased enforcement focus by authorities



A **significant interruption** of business operations due to a major accident, mechanical failure, severe weather event or terrorism



**Information Technology (IT) interruptions** to include unauthorized access or cyber attacks



**Work stoppages, strikes, or slowdowns and new labor legislation** issued by regulators



**Compliance with changes to existing tax laws and regulations**

# Supply Chain Risk Mitigation – Persistent Monitoring

## Example Risks to Monitor



# Contact Us



Steve Livingston  
Principal, Cyber Risk  
Services  
Deloitte & Touche LLP  
+1 206 716 7539  
[slivingston@deloitte.com](mailto:slivingston@deloitte.com)



Tom Alrich  
Manager, Cyber Risk  
Services  
Deloitte & Touche LLP  
+1 312 515 8996  
[talrich@deloitte.com](mailto:talrich@deloitte.com)



Larry Kivett  
Partner, Forensics &  
Investigations  
Deloitte Financial Advisory  
Services LLP  
+1 713 982 4690  
[lkivett@deloitte.com](mailto:lkivett@deloitte.com)



This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

#### **About Deloitte**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of DTTL and its member firms. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.



# Value Chain Risk: Pervasive Security and the 3<sup>rd</sup> Party Ecosystem

Edna Conway

Chief Security Officer, Global Value Chain

# Security for a Digital World

Information  
Technology

Operations  
Technology

Business Models

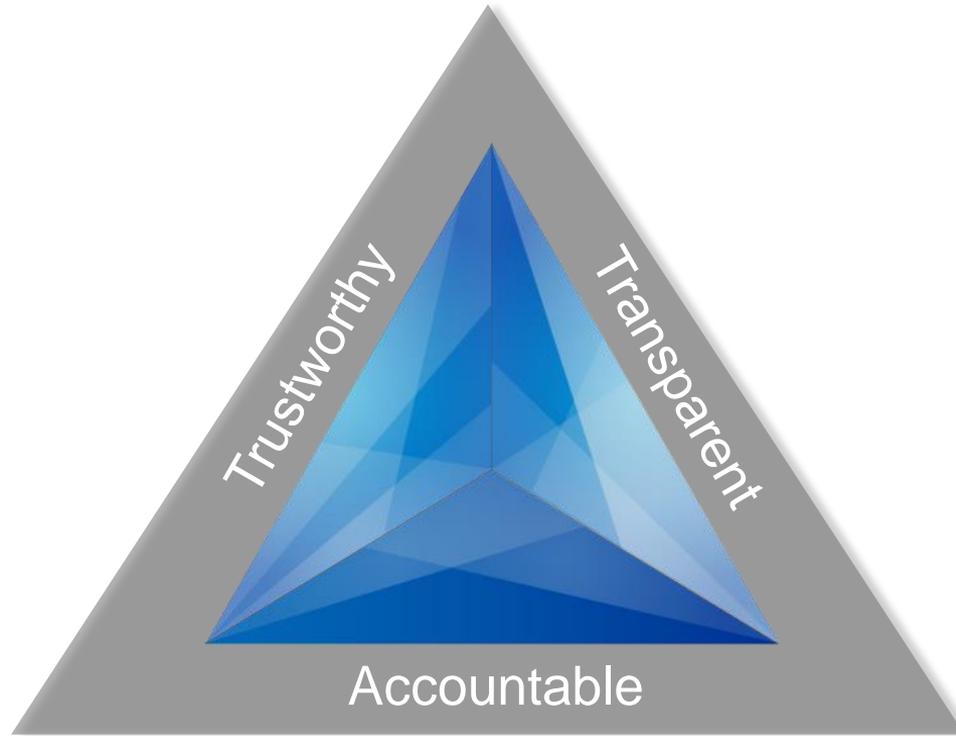


Offerings



Value Chains

# A New Approach to Security



# A New Approach to Security



# Value Chain Security

What is **My Value Chain**?

What are the **Threats** to my Value Chain?

How is **Security Embedded** into my Value Chain?

# Value Chain Security

## The Fundamentals

### Trusted Providers of Genuine Solutions

Uncompromised integrity throughout solutions lifecycle – cradle to grave



A Layered  
Approach



Logical  
Security



Security  
Technologies



Physical Security  
Practices

# Value Chain Security

---

## Threats

---



**Manipulation**  
Unauthorized Control



**Espionage**  
Unauthorized Visibility



**Disruption**  
Denial of Service

# Value Chain Security

---

## Exposures

---



### Taint

Alteration allowing unauthorized control or content visibility



### Counterfeit

Raw materials, finished goods or services which are not authentic



### IP Misuse

Unauthorized disclosure of intellectual property

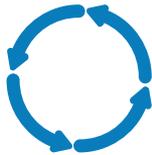


### Information Security Breach

Unauthorized access to confidential information

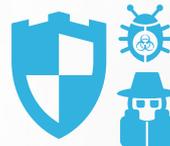
# A Layered Approach to Value Chain Security

## Product Lifecycle



Touch every stage of the product lifecycle, from design through end of life

## Multifaceted Security



Apply a combination of security technology, physical security, and logical (rules-based) security

## Industry Leadership



Work to develop key standards, policies, and tools across the industry

# Value Chain Security

## ICT Industry Alignment

### Join the Industry Discussion

#### Industry/Government Guidelines

A truly layered approach requires addressing security in the value chain across the industry and with governments worldwide



- ISO/IEC 27036 Part 3

- ISO/IEC 15408

- ISO/IEC 20243

Open Trusted Technology Provider Standard 



Common Criteria

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

- NIST Cyber Security Framework

- NIST SP 800-171

- NIST SP 800-161



NATO Directive:  
SC Security for COTS IT



**NERC**  
NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

Federal Energy Regulatory  
Commission (FERC) Order  
No. 829 – NERC Reliability  
Standard

# Value Chain Security

## ICT Industry Alignment

### Combating Crime and Terrorism Collaboratively

#### Certifications

International certifications obtained by Cisco and our value chain partners reflect our commitment to protect against terrorism, smuggling, and other criminal activities



Tier 3 Partner in US  
Customs and  
Border protection



Canada Border  
Services Agency

Canada's Border  
Services Agency's  
Partners in Protection  
Program



EU Authorized Economic  
Operator Program



Mexico's supply chain  
security program, the New  
Program of Certified  
Companies (NEEC)

# Cisco Value Chain Security Resources

- Value Chain Security Website
- Value Chain Security At-a-Glance
- Value Chain Security Infographic
- Videos & Webinars
- Blogs
- Media Articles
- Case Studies
- White Papers

## Trust and Transparency Center

Overview | Trust Principles | Built-in Security | Data Protection | Transparency and Validation

**Built-in Security**

Building Trustworthy Systems

**Value Chain Security**

**Counterfeit Detection and Mitigation**

Industry collaboration could make a big difference in stopping counterfeiters. (3:24 min)

Cisco Blogs

Security

Here, TH Harness Security

Edna Conway

Security threats are varied and often unpredictable. We Adversaries abound, spanning organized crime, nation-

It is against this backdrop that the IT solutions lifecycle best: the value chain. Many hypothesize that IT solution mythological unicorn. I propose quashing such a myth. And...the very place to do it is across the value chain.

Together, we cannot only harness the value chain best into our IT solutions.

I have the privilege of presenting on this critical challenge. I will clarify just what the IT value chain is and security in," architecturally and flexibly.

## Value Chain Security

What is a **Value Chain**?  
The end-to-end lifecycle for hardware, software or services that deliver value.

What is **Cisco's Value Chain**?  
The 3<sup>rd</sup> party ecosystem supporting the lifecycle of Cisco solutions.

38% Increase in Security breaches (2010 v. 2014)

80% Breaches originate with 3rd Parties

50% US Companies have no 3rd Party vendor assessment process

Value Chain Stages: Design, Plan, Source, Make, Quality, Deliver, Sustain, End of Life

Value Chain Threats	Value Chain Exposures
Manipulation	Counterfeit
Espionage	IP Misuse/Information Security Breach
Disruption	Taint

### The RIGHT SECURITY in the RIGHT PLACE at the RIGHT TIME

<b>Logical Security</b>	<ul style="list-style-type: none"> <li>Secure Developer Lifecycle</li> <li>Device-level protection</li> <li>Hardware-based access</li> </ul>
<b>Security Technologies</b>	<ul style="list-style-type: none"> <li>Chips</li> <li>Smart chips</li> <li>Customizing tool sets</li> </ul>
<b>Physical Security Practices</b>	<ul style="list-style-type: none"> <li>Camera monitoring</li> <li>Facility clean rooms</li> <li>Location of sensitive access center</li> </ul>

## Cisco Value Chain Security Program

Protecting Customers with Value Chain Security Throughout the Solutions Lifecycle

Cisco recognizes the important role of value chain security in a comprehensive Cisco cybersecurity strategy. Under that strategy, we deploy a capability that continually assesses, monitors, and improves the security of the Cisco value chain throughout the entire lifecycle of our solutions. Our commitment is to strive to meet our customers' integrity expectations.

**What You Can Expect from Cisco Value Chain Security**

- Our solutions are genuine (not counterfeit)
- Our solutions operate as our customers direct them to (not secretly controlled by or transferring data to unknown parties)

**Value Chain Security Process**

We manage a coordinated program across our engineering, manufacturing, and technical services teams, together with our global suppliers and channel partners to:

- Retain Cisco products and solutions in controlled development, manufacturing, logistics, and channel environments, using approved processes and tools together with software modules and hardware components
- Limit introduction of malware and/or rogue new materials that could compromise functionality
- Develop technology, build devices, and deploy processes that make it more difficult to produce undetectable counterfeit Cisco solutions

**Cisco Value Chain Security Focus Areas**

- Targeted Solutions
- Counterfeit Solutions
- Misuse of Intellectual Property

**Elements of Cisco Value Chain Security**

- Physical Security Practices:** Physical aspects of security such as camera monitoring, security checkpoints, locking devices, alarms, and electronic access control
- Logical Security Processes:** Systematic, repeatable, and auditable security processes designed to target areas of security risk and secure them
- Cisco Value Chain Security:** Cisco Value Chain Security helps ensure that data is transmitted via dedicated lines and/or uses encryption. This helps establish and validate adherence to strong handling processes and maintain configurations of production and distribution of key counterfeit protection labels
- Security Technology:** Applying technological innovation to enhance counterfeit detection, increase functionality, or identify non-audited components or users. Smart chips, data-etching test beds, and proprietary biographic or single security labels are a few of the innovations used in securing our value chain.

<http://www.cisco.com/c/en/us/about/trust-transparency-center/built-in-security/value-chain-security.html>



@Edna\_Conway

