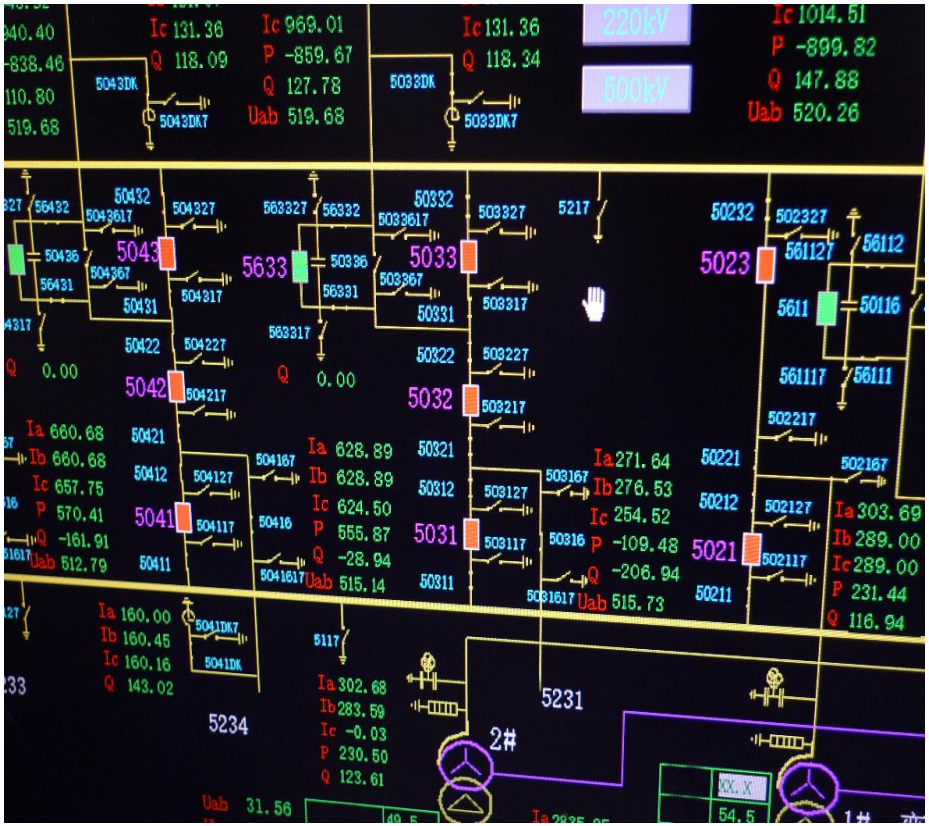
Supply Chain Risk Management

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

Utilities Technology Council™

utc.org

Deloitte.



Supply Chain Security and Regulation

Tom Alrich and Larry Kivett
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

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.

- **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

Tom Alrich

Manager, Cyber Risk Services

Deloitte & Touche LLP

+1 312 515 8996

talrich@deloitte.com

Larry Kivett

Partner, Forensics & Investigations

Deloitte Financial Advisory Services LLP

+1 713 982 4690

lkivett@deloitte.com

Deloitte.

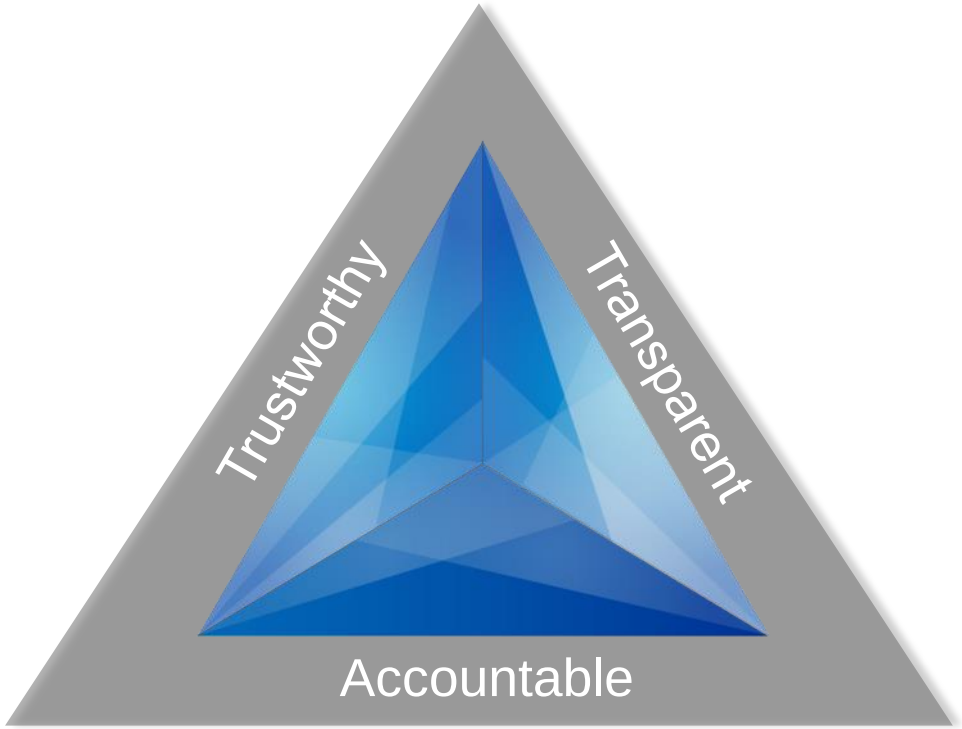
Value Chain Risk:
Pervasive Security and the 3rd Party Ecosystem

Edna Conway
Chief Security Officer, Global Value Chain

Security for a Digital World

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

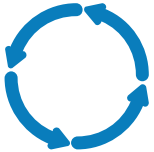
Unauthorized disclosure of intellectual property

Information Security Breach

Unauthorized access to confidential information

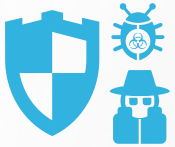
A Layered Approach to Value Chain Security

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 — Common Criteria
- ISO/IEC 20243 Open Trusted Technology Provider Standard — The Open Group

- NIST Cyber Security Framework
- NIST SP 800-171
- NIST SP 800-161

NATO Directive:
SC Security for COTS IT

Federal Energy Regulatory Commission (FERC) Oder 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

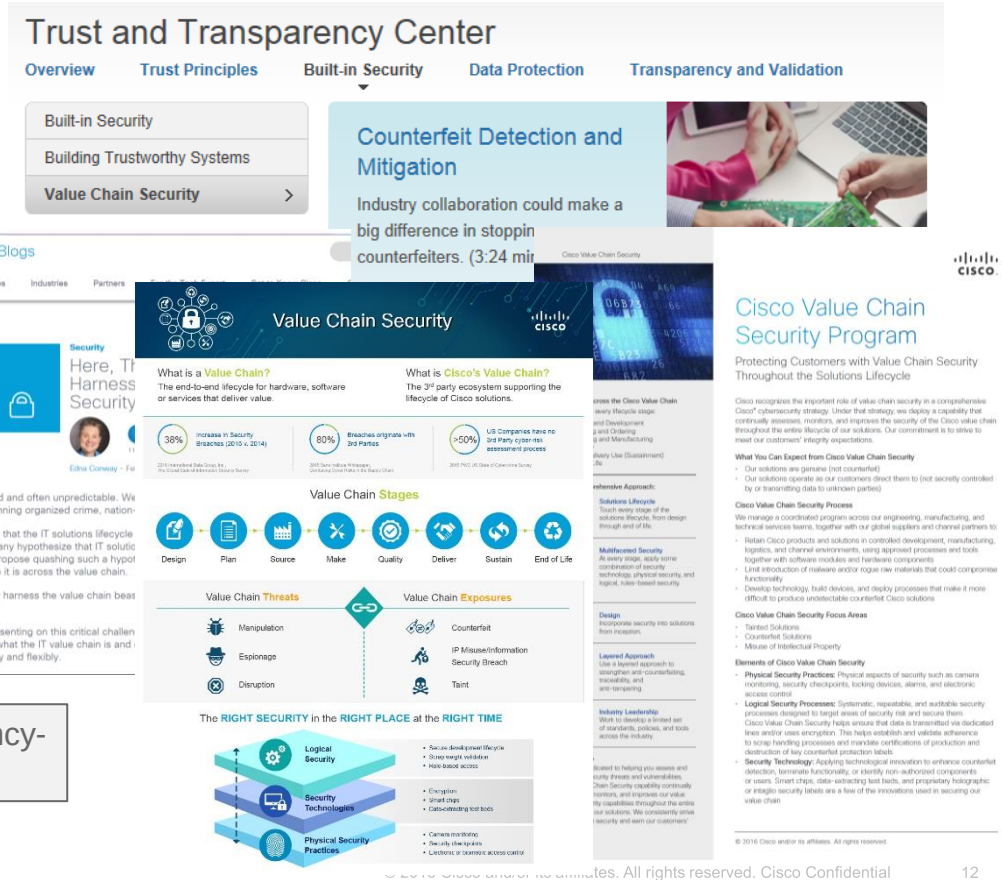
Canada's Border Services Agency's Partners in Protection Program

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



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

@Edna_Conway


Trustworthy
Transparent
Accountable