EEI Supply Chain Security Conference
Panelist Slides
Special Pre-Event Discussion:
EEI Fireside Chat - Electric Company Response to COVID-19

- Chris Eisenbrey, Edison Electric Institute
- Pat Hart, Edison Electric Institute
- Wally Mealiea, Edison Electric Institute
- Laura Schepis, Edison Electric Institute
The Electricity Subsector Coordinating Council

ESCC Mission

The ESCC serves as the principal liaison between the federal government and the electric power industry, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure.

ESCC Members

The ESCC includes CEOs and executives from electric companies, public power utilities, and rural electric cooperatives, as well as their trade association leaders, who represent all segments of the electric power industry. Canadian electric company executives also are represented on the ESCC due to the international make-up of the North American energy grid.
The ESCC created eight “tiger teams” to identify and help address major issues and challenges during the pandemic response. The teams are comprised of representatives from all segments of the electric power industry, and include participation from the natural gas industry and independent power producers.
ESCC COVID-19 Resource Guide

- The “tiger teams” develop tools, resources, and planning considerations that can be used to make localized decisions.

- These tools are included in a resource guide that is updated regularly and publicly available on the ESCC website: www.ElectricitySubsector.org
EEI Member Company Mutual Assistance

- Voluntary partnership of investor-owned electric companies across the country committed to providing resources to help restore power.
  - Some municipal and cooperative utilities participate in Regional Mutual Assistance Groups (RMAGs), but they also have their own mutual aid programs

- Mutual assistance is a force-multiplier.
A Regional Approach to Mutual Assistance

Regional Mutual Assistance Groups
Industrywide Approach to Safely Restore Power

- Pre-pandemic planning through EEI mutual assistance leaders
- Pandemic Mutual Assistance Checklist
- Mutual Assistance ESCC Mutual Assistance Tiger Teams
- COVID-19 Resource Guide
COVID-19 Mutual Assistance Considerations

- Work Practices
- COVID-19 Safety Protocols
- Staging Sites
- Lodging and Meals
- Health Issues
- Contact Tracing
Mutual Assistance Lessons Learned

- Spring and Summer storms
  - COVID-19 protocols followed
  - Decentralized/remote processes are effective and efficient
  - Appropriate distancing in work, lodging, meals
  - PPE
  - Good management and supervision is critical

- Opportunities – vehicles, support services, crew movement, contact tracing
COVID-19 Reentry Planning

- The ESCC will continue to support companies/utilities/co-ops as they shift from remote operations back to the workplace.

- Strategic principles for reentry planning:
  - Focus on the health and safety of our workforce and our customers.
  - Phased reentry coordinated with state/local governments.
  - Anticipate technology-related challenges and cyber threats.
  - Clear and consistent internal and external messaging.

- Contract tracing programs are a key part of any reentry plan.
ESCC COVID-19 Interim Action Report

- The ESCC has begun a process to assess how it responded to the pandemic.

- The goal is to identify opportunities to enhance and strengthen how it continues to respond to this pandemic and any future health emergencies.

- The process began with a series of “hotwash” calls that will inform the development of an Interim Action Report to be released in early August.
Panel: State of Supply Chain Threats: Industry Perspective

- Matthew Harvey, CrowdStrike Services
- Steve Herrin, E-ISAC
- Shawn Wallace, IronNet Cybersecurity
State of Supply Chain Threats: Industry Perspective

The Border is Gone

Indiscriminate vs. Electric Sector Specific

Nation State Adversaries

Targeting

Current Approach:
T’s & C’s, Requirements = Compliance

Where We Need to Get:
Partnership, Collaboration = Resiliency
VARIETIES OF SUPPLY CHAIN ATTACKS

- Hardware supply chain
- Software supply chain
- Services supply chain
SOFTWARE SUPPLY CHAIN

- Common apps
- Open-source components
- In-house software
SERVICES SUPPLY CHAIN

- 3rd Party Web Components
  - Web components incorporated by reference
- 3rd Party Service Providers with various levels of system access
- 3rd Party IT Service Providers
  - MSP
  - MSSP
E-ISAC Supply Chain

Steve Herrin, Director Operations and Strategic Partnerships
July 15, 2020
Panel: Cloud Services Supply Chain Considerations
12:50 PM ET
Cloud Services Supply Chain Considerations

Samara Moore, Sr. Manager Security Assurance
Amazon Web Services

Sam Icasiano, Senior Manager, Strategy & Governance
Deloitte Cyber
Mission
Secure critical infrastructure by implementing controls-based automation at economies of scale

About Fortress
- Approximately 100 employees
- Rated in Orlando’s “Top 10 Places to Work”
- Clients have a direct line to Fortress executives
Making success reliable

Fortress Knows Utilities
- Securing 15% of US power grid
- Managing 300k+ assets
- Managing 40k+ vendors
- Managing CIP-002 to 014 and other frameworks

Flexible Solutions
- Fortress Platform comes preconfigured or customized
- Dedicated developer resources ensure perfect fit
- Existing tools are integrated for complete visibility
- Bridge vendor and asset (IT/OT/IoT/IIoT) risk management
Asset & Vendor Management – “A2V”

**Preparation**
- Document Process
- Define Asset Scope
- Define Asset Security
- Requirement Taxonomy
- Identify Stakeholder Groups
- Identify Sites and Networks

**Asset & Vendor Identification**
- List of Assets including CIP Labels
- Network Placement / Resilience
  - Active Scanning
  - Passive Monitoring
  - Manual / Physical Inspection
- Secondary Data Integration (CMDB, Procurement)

**Asset & Vendor Classification**
- CIP Applicable Asset Terms
- Software, OS, Applications,
- Firmware
- Locations
- Line of Business (LOB)
- Owners (Business, Technical)
- Threat Exposure
- Controls

**Asset & Vendor Mgmt & Monitoring**
- Collaboration
- Change Monitoring
- Vulnerability Lifecycle
- Network & Device Configuration
- Reporting and Metrics
- Automation
Four Components of Supply Chain Risk Mgmt

**Managed Services**
Fortress provides vendor and product assessments, resolution and program management. Services can be interchanged throughout the contract.

**Exchange**
Asset to Vendor Network is the only exchange that is utility focused, offers royalties, provides both product and vendor assessments.

**Software**
Fortress Platform integrates with leading security platforms and procurement systems. It features risk management orchestration through workflow, approvals, dashboarding, customized reports, and vendor portal.

**Data**
Fortress subscribes to dozens of data sources and has a team of 30 research analysts that enable data-driven solutions and comprehensive monitoring. These solutions cover financial, legal, regulatory, safety, compliance, cybersecurity, country, fourth party and reputation risks.
Data-Driven Risk Ranking - Process

When you need instant visibility

DDRR was developed to overcome the challenge experienced by many third-party risk management programs – “Where do I even start?”

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Manual Risk Rank</th>
<th>Data-Driven Risk Rank</th>
<th>Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cycle Time</td>
<td>30-Day industry-average</td>
<td>Days to process</td>
<td>20x faster delivery</td>
</tr>
<tr>
<td>Frequency</td>
<td>Annually</td>
<td>Quarterly</td>
<td>4x more up-to-date</td>
</tr>
<tr>
<td>Accuracy</td>
<td>90% assumed*</td>
<td>83%</td>
<td>Trade-off</td>
</tr>
<tr>
<td>Projected Coverage</td>
<td>50%</td>
<td>100%</td>
<td>2x more coverage</td>
</tr>
</tbody>
</table>

*Even the manual risk ranks are subject to some error

Validation
- Company’s primary business
- Revenue
- Employees
- Domain names

Deep Insights
- Keyword scan vendor website
- Identify cyber global footprint
- Match against public and private databases

Manual Enrichment
- Review validation and insights
- Machine learning for continuous improvement

Business Rules (Client Customized)
- Use pre-configured business rules or bring your own

Further Enhancement
- Cyber risk
- Breach data
- AI applied to proprietary data sources
New features available to industry:

- Provenance Assessments
- 50 total are available for purchase
- 50% discount on Provenance Assessments for new and active A2V members
- assettovendor.com/marketplace

<table>
<thead>
<tr>
<th>Company</th>
<th>Watchlist</th>
<th>Cyber Presence</th>
<th>Physical Presence</th>
<th>Corporate Families</th>
<th>Foreign Ownership</th>
<th>Merger &amp; Acquisition</th>
<th>Manufacturing locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor 1</td>
<td>N</td>
<td>China</td>
<td>China/Russia</td>
<td>China</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Vendor 2</td>
<td>N</td>
<td>N</td>
<td>China</td>
<td>China</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Vendor 3</td>
<td>N</td>
<td>N</td>
<td>China/Russia</td>
<td>China/Russia</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Vendor 4</td>
<td>N</td>
<td>N</td>
<td>China/Russia</td>
<td>China/Russia</td>
<td>N</td>
<td>N</td>
<td>China</td>
</tr>
<tr>
<td>Vendor 5</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Vendor 6</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Vendor 7</td>
<td>N</td>
<td>China</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Vendor 8</td>
<td>N</td>
<td>China</td>
<td>China/Russia</td>
<td>China/Russia</td>
<td>N</td>
<td>N</td>
<td>China/Russia</td>
</tr>
<tr>
<td>Vendor 9</td>
<td>N</td>
<td>N</td>
<td>China</td>
<td>China/Russia</td>
<td>N</td>
<td>N</td>
<td>China</td>
</tr>
<tr>
<td>Vendor 10</td>
<td>N</td>
<td>N</td>
<td>China</td>
<td>China/Russia</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Vendor 11</td>
<td>N</td>
<td>China</td>
<td>China/Russia</td>
<td>China</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>
Workflow & Automation

- Security nomenclature based on electric sector terms
- Compliance Workflows – based on NERC CIP Standards and the NERC Evidence Request Tool
- Custom workflow integration based on internal policy and procedure language and controls structure
Built to manage CIP requirements

<table>
<thead>
<tr>
<th>Foundations</th>
<th>CIP 002 — BES Cyber System Categorization</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Identify and Certify BES Assets</td>
</tr>
<tr>
<td></td>
<td>Impact Ratings</td>
</tr>
<tr>
<td>Cyber Security Protection</td>
<td>CIP 003 — Security Management Controls</td>
</tr>
<tr>
<td></td>
<td>Security Awareness</td>
</tr>
<tr>
<td></td>
<td>Physical</td>
</tr>
<tr>
<td></td>
<td>Electronic Access</td>
</tr>
<tr>
<td></td>
<td>CSIRT</td>
</tr>
<tr>
<td></td>
<td>CIP 004 — Personnel &amp; Training</td>
</tr>
<tr>
<td></td>
<td>Security Awareness</td>
</tr>
<tr>
<td></td>
<td>Identity Confirmation</td>
</tr>
<tr>
<td></td>
<td>Min. Access</td>
</tr>
<tr>
<td>CIP 005 — Electronic Security Perimeter</td>
<td>CIP 007 — System Security Management</td>
</tr>
<tr>
<td></td>
<td>Perimeter Isolation</td>
</tr>
<tr>
<td></td>
<td>Remote Access</td>
</tr>
<tr>
<td></td>
<td>Monitoring</td>
</tr>
<tr>
<td></td>
<td>Network Access</td>
</tr>
<tr>
<td></td>
<td>Patch Management</td>
</tr>
<tr>
<td></td>
<td>Malware Prevention</td>
</tr>
<tr>
<td></td>
<td>Event Monitoring</td>
</tr>
<tr>
<td></td>
<td>Access Control</td>
</tr>
<tr>
<td>Incident Response</td>
<td>CIP 008 — Incident Reporting &amp; Response Planning</td>
</tr>
<tr>
<td></td>
<td>Processes to Identify, Classify &amp; Respond</td>
</tr>
<tr>
<td></td>
<td>Incident Response Group Roles</td>
</tr>
<tr>
<td>Physical and Supply Chain</td>
<td>CIP 009 — Recovery Plans for BES Cyber Systems</td>
</tr>
<tr>
<td></td>
<td>Conditions for Activation of Recovery Plans</td>
</tr>
<tr>
<td></td>
<td>Responder Responsibilities</td>
</tr>
<tr>
<td></td>
<td>CIP 009 — Information Protection</td>
</tr>
<tr>
<td></td>
<td>Identify BES Cyber System</td>
</tr>
<tr>
<td></td>
<td>Cyber System Information</td>
</tr>
<tr>
<td></td>
<td>Procedures to Protect</td>
</tr>
<tr>
<td></td>
<td>Information Storage, Transit &amp; Use</td>
</tr>
<tr>
<td></td>
<td>CIP 013 — Supply Chain Risk Management</td>
</tr>
<tr>
<td></td>
<td>Vendor Risk</td>
</tr>
<tr>
<td></td>
<td>Mgmt Plans</td>
</tr>
<tr>
<td></td>
<td>Remote Access</td>
</tr>
<tr>
<td></td>
<td>Software Integrity</td>
</tr>
<tr>
<td></td>
<td>Known Vulns</td>
</tr>
<tr>
<td></td>
<td>Security Incidents</td>
</tr>
<tr>
<td></td>
<td>S Exposures</td>
</tr>
<tr>
<td></td>
<td>CIP 014 — Physical Security</td>
</tr>
<tr>
<td></td>
<td>Risk</td>
</tr>
<tr>
<td></td>
<td>Assessments of Transmission Stations</td>
</tr>
<tr>
<td></td>
<td>Third Party Verification</td>
</tr>
<tr>
<td></td>
<td>Threats &amp; Vuln Analysis</td>
</tr>
</tbody>
</table>
**Threat Monitoring & Mitigation**

- Fortress-tailorable workflow allows you to integrate your existing threat mitigation into the tool, enabling you fine-grain control over your identification, reporting and resolution cycles.

- Respond to threats by assessing inventory to see if the threat is applicable and perform remediation.

- Known vulnerabilities and threats analyzed against the inventory to determine susceptibility based on CVE/CWE/ICS vulnerability vs asset in inventory and presenting action to be performed.

---

**Identification (Threat Source)**

**Solution (vulnerability identification with CVE/CWE/ICS)**

**Disposition applicability analysis (tie asset to vulnerability to asset owner)**

**Action plan model**

Tracking of actions to completion of patches with governance 30/60/90

**Resolution and Archival**
Patch & Vulnerability Management

ICS/OT Patch Management & File Integrity Assurance
- Baseline configuration for each in scope asset stored in AM Module
- Ports and Services Inventories tied to the AM Module
- Known vulnerabilities linked with each asset within AM Module
- Using the A2V model, patch testing and validation services can be leveraged against other utilities using the same technology footprint for lower costs

Using scanning or OT management software to determine versions and susceptibility

Patented “Block-Chain” technology used for authentication and non-repudiation of patch and software sources

Evaluation of Vulnerabilities & Patches per Vendor

Mitigation, Remediation & Tracking

Validation of Sources & Remedies

Archival & Reporting
Contact Information
Name: Tobias Whitney
Title: Vice President - Energy Solutions
Cell: (314) 422-7050
Web: assettovendor.com/marketplace
Email: twhitney@fortressinfosec.com

Fortress Information Security
189 S. Orange Ave., Suite 1950
Orlando, FL 32801
fortressinfosec.com
Panel: Comprehensive Vendor Risk Assessments
3:30 PM ET
EEI Virtual Supply Chain Security Conference
Session: Comprehensive Vendor Risk Assessments
Wednesday, July 15 3:30-4:05 pm

Registration

Featuring Industry Experts:

Jeffrey Sweet
Director of Security Assessments,
American Electric Power

Tony Turner
VP Security Solutions,
Fortress Information Security
AEP

Third Party
Risk Governance
Where We Were

- 10’s of thousands of vendors
  - Contracts created by a variety of groups
  - No central view of who, what, when, where, or why

- New view of risk
  - Vendors engaged without consideration of the risk they introduced
  - Did not have any insight into whether they have had a security practice

- Started requiring security language in contracts
  - The first step was to get accountability
Where We Are

- Robust Risk Assessment Process
  - Risk Determination
  - Risk Rank
  - Controls questionnaire
  - Security language
  - On-site Assessment
  - Continuous monitoring
Where We Are Going

Building a solution to assist the industry

- **A2V**
  - Platform to exchange controls assessment data with other utilities (CIP-013)

- **FIA**
  - Ability to validate the source and integrity of software, firmware and patch downloads (CIP-010 – R1.6.1 and R1.6.2)
  - Ability to perform malware analysis of files retrieved
  - Deposited into a central repository for all person needing code to gain access

- **VulNEXT**
  - Ability to identify vulnerability, determine availability of patch and process the patch for deployment
Fortress Overview
Assessing Vendor Risk can be challenging

• Resource intensive
• Time consuming
• Some vendors are uncooperative
• Vendors provide answers that do not match the evidence
  o Not having the evidence to validate vendor responses
  o Answers reflect a single point in time
• Vendor answers aren’t always useful
  o Reusing old questionnaires
  o Sending you their certifications
• Vendor assessment programs are difficult to scale
• Without context, cyber scores have low value, since they are a small component of overall risk
9 “Lessons Learned” from Vendor Risk Management for Utilities

1. Boil the ocean to get to a manageable number of vendors to evaluate.
2. Partner with an organization that has the conveyor belt. Scalable and repeatable.
3. Vendor Cooperation is preferred. But don’t rely solely on the vendor.
4. OSINT & 3rd party data sources are POWERFUL.
5. Utilize a framework that automatically maps vendor responses to how you manage risk.
6. Utilize standardized assessments and participate in collaborative efforts.
7. Monitor your vendors. Ensure they are telling you everything (vulns, breaches, M&A, etc.).
8. Use alternate approaches to assess your vendors.
9. Utilize capital treatment. Don’t focus on the bodies, focus on the generated value.
Assessment Solutions

• **Traditional Approach** – Questionnaire-driven Security / Controls Risk Assessment
• **Collaborative Approach** – Purchase from a data exchange such as Asset to Vendor
• **Data-Driven Approach** – Use of OSINT and data source automation to produce quick results
• **Continuous Monitoring** – Trust but verify what the vendors are telling you
• **Product Assessments** – CIP-013 asks for more than just vendor assessments

One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).

• **Provenance Assessments** – The EO is coming. This topic is multi-dimensional
Thank you!

AssetToVendor.com    (407) 573-6800    Sales@AssetToVendor.com
Panel: Supply Chain Regulations: Current State & On the Horizon

• Howard Gugel, North American Electric Reliability Corporation
• Joseph McClelland, Federal Energy Regulatory Commission
Supply Chain

Howard Gugel, Vice President of Engineering and Standards
EEI Meeting
July 15, 2020
- Standard development
  - EACMS and PACS
  - Low impact BES Cyber Assets
- NERC Alerts
  - 2019 – specific manufacturers of telecom and drones
  - 2020 – Generation and transmission assets
- Industry partnerships
  - NATF work on certifications
  - Vendor work with DoE
• DERs – the great unknown
• System planning with cyber in mind
• Threat vs visibility
• Virtualization/cloud
Questions and Answers
Vendor Lightning Round: Silver Sponsor
Deloitte
4:50 PM ET
Introduction

Clark Oeler
Principal, Cyber Risk Services
Deloitte & Touche LLP

Objectives

- Identify current state of evolving supply chain threat landscape
- Define the core focus areas on how to address the threat
- Understand how Deloitte can help
Why are we here?
Power producers and utilities face an evolving threat landscape

**Supply chain networks are complex and multidimension entities**

Cyber supply chain attacks are on the rise.

New Federal regulations in regards to Supply Chain will likely require utilities to invest in their cyber supply chain programs and re-think how they procure assets supporting the Bulk Power System (BPS).

The President’s Executive Order on the BPS, issued May 1, 2020, will impose limitations on utilities who contract with suppliers that have ties to foreign adversaries.

In the face of growing complexity and ambiguity, companies and government want to be confident that their supply chain is secure and their business is secure.

A compromised supply chain network can introduce a wide range of cyber, regulatory, legal, political and operational risk and can severely impact a business or programs’ integrity.

Deloitte.
Copyright ©2020 Deloitte Development LLC. All rights reserved.
What are power producers and utilities doing?

- Enhancing procurement processes to include vendor and product security risks
- Enforcing limited ways to procure critical equipment for the Bulk Power System
- Implementing third party and vulnerability risk management tools and exploring community models for assessing vendors
- Initiating conversation with their vendors to understand vendor practices around sourcing components from non-US entities

But is that enough?

In order to meet the intent of the executive order we need **insight** into the supplier ecosystem from who we procure products and services from.

We know our vendors and how we get equipment from them, but we **need visibility** into component and sub-component suppliers.

A software supplier for a manufacturer is breached and malware is introduced into their line of products. Not being promptly informed leaves us vulnerable. We **need correlation and integration** to understand how vendors are interconnected.
How do you address the risk?
Illuminate your asset and supplier network

Deloitte services and technology enablement helps clients address challenging problems when securing the supply chain.

01 Aggregate the scope of vendors, services and products to prepare for the illumination analysis

02 Illuminate the multi-tier supplier network to understand where the components are sourced

03 From your illuminated supplier network define the impact of the federal directives, regulatory requirements and cyber risks

04 Build your plan to prioritize and address the different impacts to your organization and how to respond

05 Engineer supply chain risk mitigations in the realms of regulatory, cyber, legal, financial and operational

06 Continuously monitor the supplier network and obtain alerts when there are new risks and vulnerabilities
Deloitte can help

Technology enablement to illuminate your environments, understand your vendor ecosystem, and provide better data for making business decisions in accordance with North American Electric Reliability Corporation (NERC) and anticipated federal requirements.

Environment illumination
- Asset discovery technologies
- One-time discovery and inventory
- Ongoing monitoring

Maintain vendor profile and ecosystem mapping
- Fourth-party and fifth-party identification
  - Identification of foreign-suppliers
- Sub-components library
- Integration with rating agencies
- Pro-active alerting and notification

Users of vendor information
- Third-party risk management
- Security risk assessments
- Approved vendor lists

IT/OT procurement planning
- Facility design
- Service provider selection
Let’s talk more about your Secure Supply Chain...

Sharon Chand
Secure Supply Chain Solution
Owner
Principal, Cyber Services
Deloitte & Touche LLP
+1 312 486 4878
shchand@deloitte.com

Sam Icasiano
Secure Supply Chain Solution
Architect
Senior Manager, Cyber Services
Deloitte & Touche LLP
+1 973 602 6091
saicasiano@deloitte.com

Clark Oeler
Secure Supply Chain Solution
Advisor
Principal, Cyber Services
Deloitte & Touche LLP
+1 412 338 7221
coeler@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.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.