Methods for Reducing Cybersecurity Vulnerabilities of Power Substations Using Multi-Vendor Smart Devices in a Smart Grid Environment

Date: October 24, 2017

Authors/Presenters:

J. Matt Cole, PE (Presenter) – *Sargent & Lundy, LLC*

Atilla Aksoy, PE (Presenter) – *Sargent & Lundy, LLC*

Jordan Bridges (Presenter) – *Sargent & Lundy, LLC*

F. Lee Napier – *Sargent & Lundy, LLC*

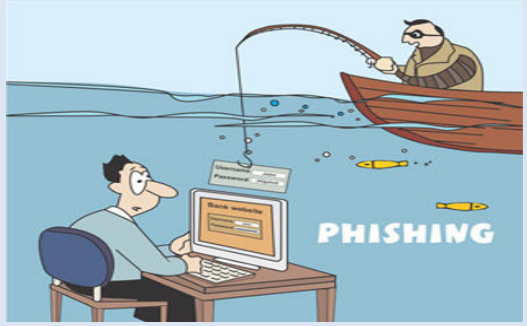
Paper Focus

- Target's Cybersecurity Breach
  - **Via a 3rd Party HVAC Vendor (Fazio Mechanical Services)**
  - **40 million accounts affected, $400+ million in damages**
- Utilities rely heavily on several vendors/suppliers
  - **Multi-vendor devices (IEDs) installed in substations**
- NERC CIP V5 & V6 do not govern vendors
  - **A critical substation's weakest link is a vendor device**
- Vendor's cybersecurity policies
  - **Does the policy match the utility's policy?**

This paper focuses on cybersecurity vulnerabilities utilities face with using multi-vendor smart devices in substations. Critical steps are recommended to minimize security risks when using multiple suppliers.

Increased Attack Vector for Utilities

- Deficiencies in personnel security awareness & training program **(no routine, regular or required security training conducted)**
- Appropriate staff not identified as security personnel **(for incident reporting or first responders)**
- No security assessments or audits performed **(both internal or external)**
- Maintaining legacy devices that vendors no longer support **(no more security or firmware patch updates)**
- Allowing vendors remote access capabilities to devices **(no management access controls or oversight)**



Increased Attack Vector for Utilities (cont.)

- No firewalls, demilitarized zones (DMZs) or data gateways implemented on networks **(no access controls)**
- Lack of password management **(infrequent password changes or weak passwords)**
- No network segregation/separation **(all critical and non-critical devices are on the same network)**
- No intrusion prevention / intrusion detection systems **(IPS/IDS)**
- No physical security installed **(no record of who is entering or leaving a substation)**
- No data encryption or VPNs utilized **(3rd party leased comm path)**
- Lack of virus / malware protection or no routine signature updates

Tools & Techniques Used by Hackers

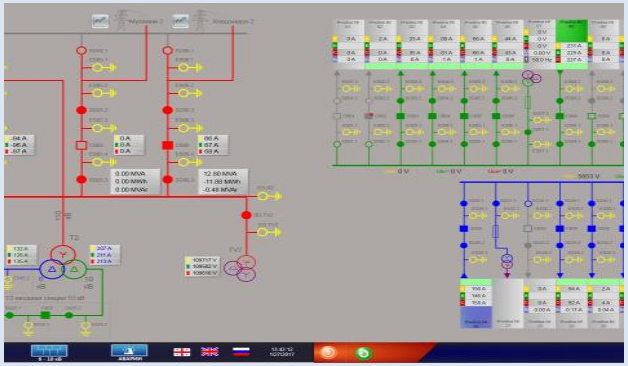
- Social Engineering and Spear Phishing Emails
  - **Spear Phishing emails used in both Ukraine cyber attacks**
- Sniffing/Spoofing/Jamming Critical Data
  - **How do you know the data is good/accurate?**
- Spyware/Malware/Ransomware/Malicious Code
  - **WannaCry Ransomware Virus (Worst Attack in 2017)**
- Viruses/Worms/Trojan Horses
- Distributed Denial of Service (DDoS) Attacks
  - **Ukraine's phone network shutdown (no calls coming/going)**
- Man-in-the-Middle (MITM) Attacks
- Network Breaches/Cyber Intrusions
- Data Logger/Theft of Credentials
- Penetration to Data Encryption of VPNs
- Hijacking SCADA/HMI/IEDs/other critical functions
- KillDisk - **Wiping all code and traces that hackers were there**

Recent Attacks from Vendor Vulnerabilities

Victim	Year	Technique Used
RSA	2011	Phishing Email
Target and Home Depot	2013	Theft of Credentials
Boston Medical	2014	Security Breach
CVS and Wal-Mart	2015	Security Breach
Ukraine Cyber Attacks	2015/2016	Phishing Emails
Bizmatic	2016	Theft of Credentials
Kroger and Wendy's	2016	Theft of Credentials
ADP and Seagate	2016	Theft of Credentials
DHS and Verizon	2016	Security Breach
Multiple Companies (WannaCry)	2017	Security Breach
Multiple Companies (Petya)	2017	Security Breach

Multi-Vendor Remote Access (Critical Devices)

Critical substation devices communicating via internet protocol (IP):
Remote Terminal Units (RTUs)
SCADA I/O Controllers
Human Machine Interfaces (HMIs)
IEDs and Programmable Logic Controllers (PLCs)
Phasor Measurement Units (PMUs)/Synchrophasors
Digital Fault Recorders (DFRs)
Communication Processors
Smart Meters



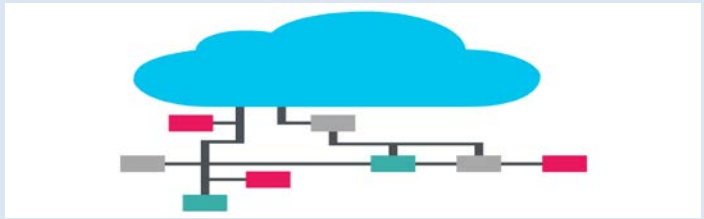
Proposed Regulation for Utility's 3rd Party Suppliers

- FERC released order # 829 on July 21, 2016 to direct NERC to create a new reliability standard **(for transmission utilities):**

- Address supply chain risks for control system devices affecting BES
- To mitigate cybersecurity risks affected by 3rd Party Vendors

  - **Main objectives:**
    1) **Software Integrity & Authenticity**
    2) **Vendor Remote Access to BES Cyber Systems**
    3) **Information System Planning and Procurement**
    4) **Vendor Risk Management & Procurement Controls**

NERC CIP



NERC released draft standard CIP-013-1 on November 2, 2016

Recommended Critical Steps for Utilities

- **This paper recommends 15 Critical Steps to perform for decreasing security vulnerabilities caused by vendors/suppliers**

1) **Develop a vendor risk management program**
   - **Perform a risk-based approach on the roles vendors will play within the supply chain.**
2) **Evaluate the vendors**
   - **Interview the vendors with a thorough list of questions. Evaluate the reliability and security of their products and services.**
3) **Review the vendor's security policies**
   - **Ensure the vendors have the same or similar security policies.**
4) **Mitigation strategies**
   - **Review the vendor's mitigation strategies for when a cyber breach or incident occurs.**

Recommended Critical Steps for Utilities (Cont.)

5) **Has the vendor had a cyber incident?**
   - **Clarify whether the vendor has had a cyber breach or incident. Evaluate how the vendor responded to the incident.**
6) **Clarify the vendor's third party suppliers**
   - **Evaluate the vendor's third party suppliers and review their cybersecurity policies.**
7) **Establish a trust relationship with vendors**
   - **Ensure you have a good working relationship with your vendors and suppliers and they have a proven track record of cybersecurity protection / awareness. Have a backup vendor on hand in case primary vendor relationship deteriorates.**
8) **Ensure vendors and their suppliers check their employees**
   - **Ensure that thorough background checks are being performed on vendor employees / contractors and their suppliers.**

Recommended Critical Steps for Utilities (Cont.)

9) **Ensure vendors and their suppliers are training their employees**
   - **Make sure vendors and their suppliers are training their employees and contractors on cybersecurity annually or on a regular basis.**

10) **Patch Management**
   - **Ensure vendors provide firmware updates and security patches on a regular basis to mitigate potential or known security threats.**

11) **Testing**
   - **Test and validate all updates and security patches in a lab or testing environment before rolling out to the live system.**

12) **Monitor vendors/suppliers by performing annual audits**
   - **Audit the vendors cybersecurity policies on an annual basis.**

Recommended Critical Steps for Utilities (Cont.)

13) Restrict remote access

- Restrict all remote access to the utility's networks, if possible.

14) Perform network segregation

- Isolate networks by only allowing vendors access to the networks required.

15) Cybersecurity insurance

- Obtain insurance (if possible) to cover direct damages caused by security breaches to vendors or suppliers.

Conclusions

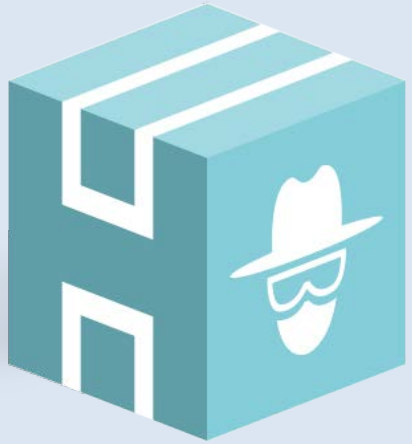
- As more multi-vendor substation devices are connected to IP networks – **attack surface will continue to increase**
- One solution is to disconnect all devices – **not feasible due to necessity of increasing Smart Grid applications**
- **Exercise caution and test thoroughly** - before selecting a vendor to supply smart substation devices
- **Perform security risk assessments** of all networked devices within the substation
- **Ensure vendors or suppliers are providing timely updates** if there is a potential vulnerability or threat

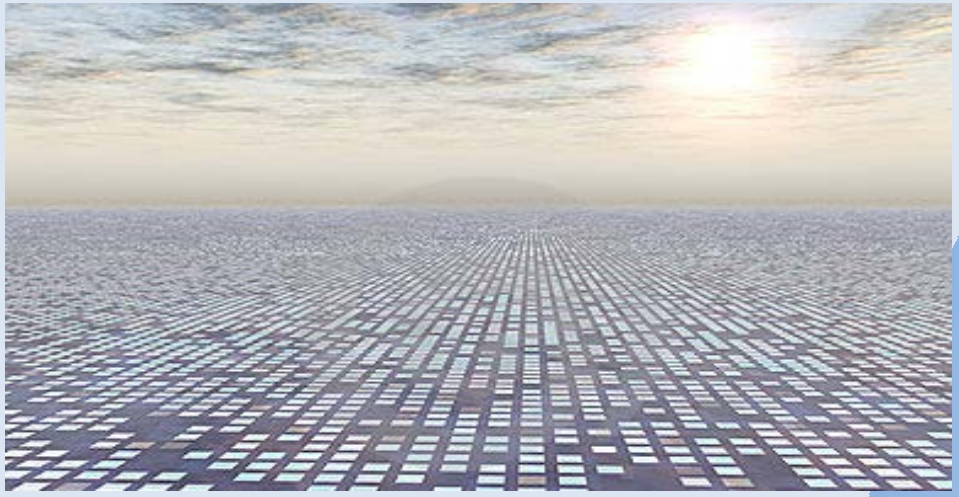
Conclusions (cont.)

- **Test all updates and patches** – within a lab or testing environment before pushing onto the live system
- **Make sure vendors are properly trained and match your cybersecurity policies**
- **Utilities should proof and fortify their networks** - against external attacks should vendors or their suppliers' equipment become compromised

Future Research/Discussions

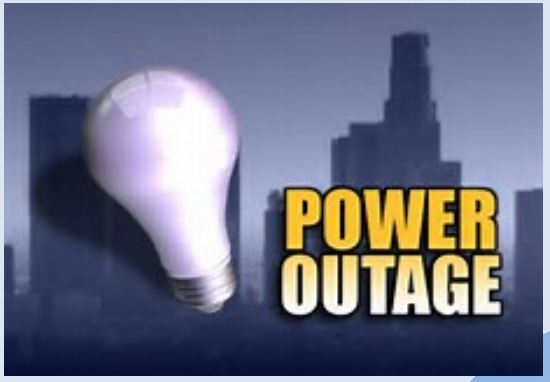
- ***Vendors need to align together to push security patches simultaneously.***
- ***Additional security should be applied to vendors and their suppliers' manufacturing facilities.***





Questions?

"There are three power grids that generate and distribute electricity throughout the United States, and taking down all or any part of a grid would scatter millions of Americans in a desperate search for light, while those unable to travel would tumble back into something approximating the mid-nineteenth century."
Ted Koppel, Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath



J. Matt Cole, PE (Presenter) – *Sargent & Lundy, LLC*
Atilla Aksoy, PE (Presenter) – *Sargent & Lundy, LLC*
Jordan Bridges (Presenter) – *Sargent & Lundy, LLC*
F. Lee Napier – *Sargent & Lundy, LLC*