NERC Compliance Update

vermont electric power company

VELCO

Operating Committee

April 18, 2019

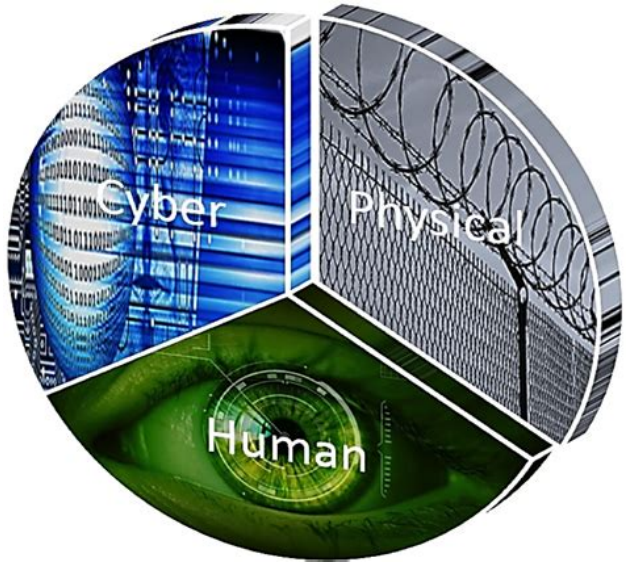
Outline

- Key NERC identified risks
- 2018 cyber attacks on utilities
- California's new rules for Distribution Utilities
- Recent $10M NERC fine
- How can you help us all maintain a safe, reliable and secure electric grid within the State of Vermont

NERC identified industry risks in 2019

The biggest industry risks facing the North American Electric grid today are due to:

- Human error
- Access control management
- Insider access
- Insufficient training
- Lack of vigilance by all stakeholders



The human element of security plays a major role in reducing and eliminating that risk. That is why the information contained within this training is so critical.

I believe a major cyber attack is on its way, appearing as early as 2019. It would cause unimaginable disruption and devastation. The only limitation aside from the attacker's imagination is our preparedness. We must keep our fingers on the pulse! During 2019, we must understand the value and importance of our assets, as well as the potential threats should a cyber attack take place.

Source: Forbes.com Jan.2, 2019 by Rajinder Tumber

NERC expected future attack trends to be launched against the national infrastructure

Credential harvesting: Tactics to acquire legitimate user credentials to gain initial access to targeted networks and establish persistence mechanisms will continue to be popular, because it helps evade detection. Sophisticated spear phishing activity to harvest credentials is the most common technique observed by members.

Use of native tools: Adversaries will likely continue to use tools and capabilities already present on a compromised network – such as PowerShell or Windows Management Infrastructure (WMI) – to conduct reconnaissance, lateral movement, and privilege escalation. The presence or use of these tools on a targeted network is unlikely to raise alarm, so their inappropriate use helps evade detection.

NERC

Exploitation of the trust relationship between targeted organizations and their business partners: Nation-state adversaries are targeting the electric sector by compromising the networks of third parties with which the intended targets have established business relationships. This tactic is a type of supply chain attack, and increases the success rate of tactics used to initially compromise the intended target.

Network device targeting: Switches and routes located on the edge of networks are a prime target for threat actors capable of intercepting and processing a large amount of information. Because these devices are placed at the boundary between internal networks and the internet, and exist to allow controlled access to the internal network, they will most likely continue to be a target of reconnaissance.

Ten 2018 cyber attacks on utilities

1. Toll number charged customers for calling customer service
2. Fake tax returns filed after W-2 forms hacked
3. Unknown connection to Russia through a new HVAC system
4. Compromised interactive voice response system
5. Attack against advanced metering infrastructure server
6. Unsecured meter reading system cost municipality over $2M
7. Rural electric cooperative knocked off-line due to cyberattack on cable TV company
8. Joint action agency hit with malware
9. Ransomware re-building system
10. Ransomware costing $20M impact to date

California's new laws for Distribution Utilities and Physical security:

January 22, 2019 PUC of California Ordered all state DU's to do the following:

- Within 18 months – preliminary assessment of priority facilities for their distribution assets and control centers
- Within 30 months – submit their final security plan report
- Plans must consist of: Assessment, independent review and utility response to recommendations; safety and enforcement division review, local plan review, maintenance and plan overhaul/new review.
- Once reviewed the subsequent changes should be applied to the plan
- Any future changes to the plan must be shared with the Safety and Enforcement Division for approval.
- All new or renovated distribution substations must be designed to incorporate reasonable security features
- Plan must describe how:
  - Detailed narrative explaining how the utility is taking steps to implement an asset management program to promote optimization, and quality assurance for tracking and locating spare parts stock, ensuring availability, and the rapid dispatch of available spare parts.
  - They are planning to implement a robust workforce training and retention program to employ a full roster of highly-qualified service technicians able to respond to make repairs in short order throughout the utilities service territory using spare parts stockpiles and inventory.
  - Implementation of a preventative maintenance plan for security equipment
  - Implement a description of Distribution Control Center and Security Control Center roles and actions related to distribution system physical security.
- Plan must be reviewed every 5 years by the state of California PUC
- For major physical security events that impact public safety or results in major sustained outages, utilities will preserve records and evidence associated with the event and provide to Commission
- Any DU OE-417 reports must be submitted to the State within two weeks of filing
- Must submit an annual report on physical incidents that resulted in any insurance claims.

Recent $10M NERC Utility fine

- 127 violations including failures to:
  - Protect critical cyber assets,
  - Protect BCSI information
  - Maintain required annual cybersecurity training
  - Implement physical access controls to limit unescorted access within a physical security perimeter
  - Revoke former employees and contractors access rights within 24 hours.
- The company was seen as giving “lip service”, lacked implementation and oversight, and there was a disassociation of compliance and security.

- In addition, on Jan 29th the US government reported:
  - Russian hackers have the capability to disrupt or damage electrical service in the US
  - The intended targets include small and medium organizations within the Energy Sector, specifically **power generation, transmission, and distribution**.

How can you help?

- Review the following key excerpts from our training with your teams to verify they understand the risks involved and mitigations taken to prevent events from occurring
- When assigned training please ask everyone to take it prior to the due date – this is a requirement by NERC
- If you or anyone on your team has questions on the goals and responsibilities – please reach out and ask us
- Report anything that does not seem right – no matter how small
- If **ANYONE** of your staff that has unescorted access to a VELCO facility leaves your company, for ANY reason, we must be notified **ASAP**. We are required to remove all access within **24 hours** of their last date of employment.
- **Lets work to protect all of our information and systems together!**

VELCO training excerpt

The following slides identify the key roles and responsibilities your teams play in helping us maintain a reliable, robust, secure and safe electric grid for the State of Vermont.

If you or anyone on your team would like a full copy of the cyber security training deck please reach out to VELCO and we would be more than happy to provide it to you!

Your Physical Access Protocol

Do…

- Wear your identification badge or FOB visibly at waist level or above at all times
- Scan your own badge or FOB every time you access a controlled area *(this automatically logs your access)*
- Ensure access doors to controlled areas close securely behind you
- Immediately report lost or stolen ID Badges to VELCO Security at 802-772-6670

Do not…

- Tailgate or let others tailgate
- Lend your badge or FOB to anyone else
- Allow unauthorized visitors onto the premises
- Tamper with any physical access control

Your Visitors Access Protocol

- All visitors must be issued a visitor badge and escorted by an authorized badged associate.

  To acquire a visitor badge:

  – Substations: Visitor badges are just inside the control building. Contact Security to confirm the badge number assigned to each visitor, then swipe once issued.

  – Pinnacle Facility: Check in with the Security Officer to be issued a visitor badge

- Visitors must:

  – Wear their badge at all times

  – Swipe their badge when entering and exiting

  – Be continuously escorted within your line of site at all times while in ‘Restricted Areas’

  – Return their visitor badge when their visit ends

Your role in maintaining security in our substations:

Do…

- Monitor who is accessing equipment inside the substation
- Assign badges and follow escorting rules at all times
- Access equipment using a qualified TCA laptop
- Notify Security of any suspicious activity within the facility

Do Not…

- Access any equipment within a VELCO substation with your personal electronic devices
- Share your secured laptops with others

Remember that some of our most critical cyber assets are located within our substations.
Please remember - When in doubt, ask!

Physical Access Controls

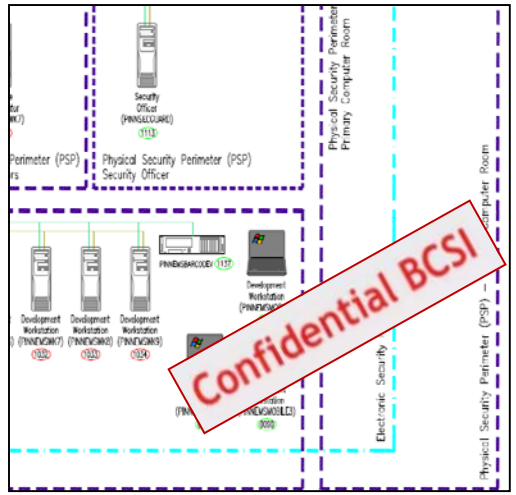
Work Exceptions / Emergencies

If you need to prop a door open:

- Contact Security so they know the reason for the ‘door open too long’ alarm. They can also help you monitor the access.
- EACH person that enters while the door is open must badge at least once on entering and during their final exit
- During other emergency situations exceptions to CIP Standard Requirements may be required.
  - Respond to the situation accordingly
  - Contact Security
  - During these ‘CIP Exceptional Circumstances’ compensating measures to minimize security risks should be used whenever possible.

Information security - Bulk Electric System (BES) Cyber System Information (BCSI)

VELCO uses the title: **"Confidential BCSI"** to identify its smallest subset of information that has the **highest cyber security sensitivity**; such information is unique to the BES asset(s) and provides direct knowledge for compromising the asset(s). This information is tightly controlled to ensure only those with a need to know can access this information.



DESCRIPTION

Could be used to gain unauthorized access or pose a security risk to BES Cyber Systems

- ❑ Network Topologies / diagrams
- ❑ Collections of network addresses
- ❑ Information identifying vulnerabilities
- ❑ Network boundary device info, ie. Firewall rules, access control lists, etc.
- ❑ Security plans

DOES NOT Include individual pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access

- ❑ **Device names**
- ❑ **Individual IP addresses**
- ❑ **Electronic Security Perimeter (ESP) names**
- ❑ **Policy statements**

BCSI Information Access Protocol

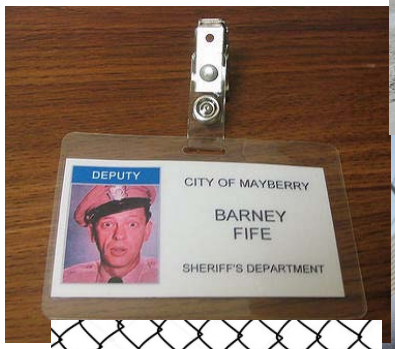
Do not…

- Provide access of BCSI to anyone that does not have a business need to know
- Leave BCSI unattended when not in use
- Throw away in a non-secured manner
- Remove BCSI information from a secured site unless authorized to do so

Recognizing physical threats and attacks

- When you access or are inside a VELCO facility be ALERT, look for the unusual.
- Examples include: a cut fence, copper theft, unauthorized person inside the facility, person(s) lingering outside the substation, person accessing a device who doesn't have the need, etc.
- These and any other questionable situation should be reported to Security, when in doubt CALL!!!

VELCO Security: 802.770.6260



Identification of a Cyber Security Incident

Remember: every asset/device with an internet connection is vulnerable to cyber attack.

Possible signs of a cyber attack

- Your computer is running slowly.
- Your hard disk usage light is solid on or CPU usage is high.
- Your computer says it is "installing new hardware" unexpectedly.
- Your internet browser changes homepage unexpectedly.
- Unrecognized applications or software on your device

What to do if you suspect a cyber attack

- Contact the SIRT (see box at right)
- If possible, don't use the computer
- Follow SIRT directions. Stay on the sidelines unless otherwise directed.
- The SIRT has been trained on the response to and recovery of the BES Cyber Systems due to cyber security incidents

If you suspect a cyber attack, contact the Security Incident Response Team (SIRT):

IT Help Desk
802-772-6555
during working hours

Security Officer
802-772-6670
after hours or weekends

Also, report a lost or stolen cyber device to the SIRT