Cyber Vulnerabilities and Mitigation Strategies for Electric Co-ops

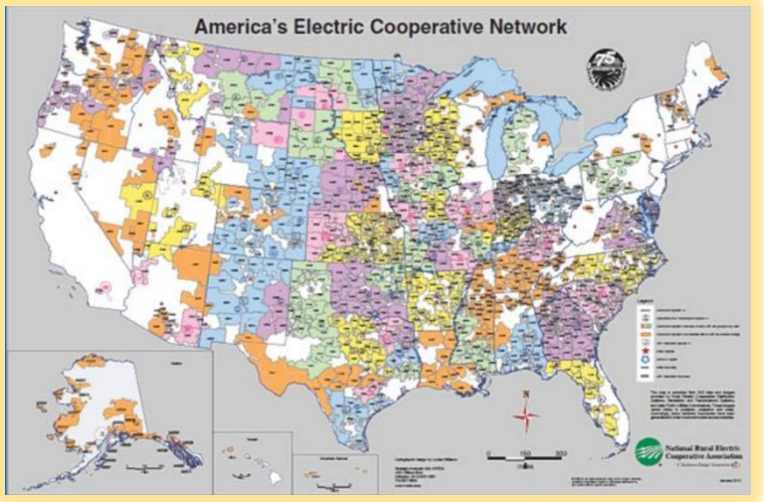
December 2021

Introduction

The Department of Homeland Security has designated the energy sector as one of sixteen critical infrastructure sectors. The energy sector includes electricity, natural gas, oil, and refined oil products. This white paper is focused on electric cooperatives (co-ops), which comprise an important component of the U.S. electric grid and the energy sector. Cyber criminals often gain access to large enterprises by compromising smaller organizations in the sector that lack the funding to maintain the systems and expertise needed to combat cyber-attacks. For the electric grid, electric co-ops present this potential point of entry. A cyber incident that shuts down part or all an electric co-op utility's operation may have serious, far-reaching, and life-threatening ramifications and, because of the ubiquitous requirement for electric power, will also impact each of the other critical infrastructure sectors reliant on that co-op.

The Nature of Electric Cooperatives

Electric cooperatives are a vital component of the electric utility ecosystem. They provide affordable electric power to residents and businesses in sparsely populated areas across the country. The concept was implemented beginning with the 1937 Electric Cooperative Corporation Act, a model law for states to adopt, authorize and regulate the formation and operation of not-for-profit, consumer-owned electric cooperatives.



The NRECA map at the right shows the location of the nearly 900 co-ops spread across the country. Individual co-ops generally have one administrative headquarters and, depending on the size of co-op and coverage area, may have additional satellite offices and distributor locations. There is a wide variation in size, geographic area, and budget among electric co-ops. The electric co-op value chain can be broken down into four parts: power generation, power distribution, power transmission, and Information Technology/Operational technology (IT/OT) networks.

Co-op Mission

In reading the mission statements of electric co-ops, two common mission themes are apparent across all, despite location and size:

nuariinfo@norwich.edu
nuari.net
P.O. Box 30
Northfield, VT 05663
+802.485.2213

- Provide reliable and sustainable electric power to their communities, often over considerable distances and in remote locations.
- Keep costs low. The not-for-profit business structure seems well suited to this objective.

The means to achieve the first mission objective are easily understood by managers, operators, and customers. The equipment required for power generation, distribution, and transmission must be purchased, maintained, and eventually replaced. Business decisions can be reached by combining considerations of cost-effectiveness and available budgets. While there may be some controversy, usually in the end the decisions are accepted if the co-op mission of providing reliable and sustainable electric power is being served. Achieving the second mission objective is difficult, especially when supporting a customer base that must manage their own businesses and homes in a very cost-constrained environment. There is a natural tendency to interpret not-for-profit as meaning that the operating income derived from ratepayers should not exceed the operating costs needed to meet the first mission, and to deliver the power with a minimum of excess capacity or redundancy.

In the case of a for-profit business, any excess of income over expenses can either be used for investments in growth and resiliency or else returned to shareholders as dividends. The situation of a not-for-profit business is similar, except that there are no dividends to be paid, so costs should be lower than a competing for-profit business. The not-for-profit electric co-op has operating income from ratepayers, and likely also records non-operating income from depreciation and income from investment of reserve funds. In addition to direct operating expenses for staff salaries and the equipment used to deliver electric power, there are also indirect expenses for staff and IT/OT equipment and networks to manage and administer the business. Like a for-profit business, a not-for-profit electric co-op must set rates that allow it to maintain a margin of income over expenses sufficient to respond to unplanned emergencies and to make prudent investments for future growth and to respond to opportunities and threats that emerge in the business environment.

Providing Power in a Cost Constrained Environment Versus Cyber Security
The inherent conflict between the two mission themes is exposed when considering prudent investment for growth, for changes in the operating technology, and for providing the ability to maintain delivery of electric power while responding to hazards from extreme weather and from malicious behaviors.

Unfortunately, the natural understanding of the business decision to invest in physical infrastructure does not carry over into investing in cyber security. In a cost-constrained environment, the costs needed to protect IT/OT assets against hazards and threats are difficult to defend. This is especially true for IT/OT because, unlike the equipment used to deliver electric power, the networks and their vulnerabilities are not concrete and visible.

Significant IT/OT Considerations

Equipment

Unsurprisingly, small rural electric co-ops have similar IT/OT infrastructure because their mission and business processes are the same, and they operate in similar rural environments. Like most businesses, co-ops conduct IT functions by using a variety of software, databases, and custom applications, most of

nuariinfo@norwich.edu
nuari.net
P.O. Box 30
Northfield, VT 05663
+802.485.2213

which are routinely connected to the internet for ease of internal communications and management. They also rely heavily on OT networks, connecting through the internet SCADA and PCL devices to a control center for monitoring and control of electric power generation, transmission, and distribution resources. Although the number of systems used and the degree of specialization of the equipment differ greatly between small co-ops and those that serve a large base in geographic area, number of customers, or both, the vulnerability to cyber-attacks arising from internet dependence is common to all.

Personnel Support

All but the smallest electric co-ops will have an IT staff to configure and maintain the network and equipment, and to provide user support when something is not working. In most cases, the IT staff will be diligent in making software upgrades that (among other things) respond to identified network weaknesses that expose the system to cyber-attack. The IT staff is less likely to be aware of vulnerabilities that come through operational firmware or hardware.

By its nature, the OT equipment operates for months and years at a time without requiring any attention. Failures are more likely to arise from animal activities than from any network or software issues. This means that the co-op has little need for in-house OT staff and is almost entirely reliant equipment vendors to communicate emergent vulnerabilities that expose the system to cyber-attack. The co-op will likely rely on consultants and vendors to respond to equipment failures and periodic upgrades.

The cybersecurity field faces a serious talent shortage, so that there is tremendous competition for the talent needed to respond to cyber threats. Overwhelmingly rural and with tightly controlled budgets, many co-ops find themselves at a severe disadvantage in competing against other organizations offering higher pay and more desirable locations. This often leaves co-ops relying upon consultants or forgoing specialized cybersecurity support.

IT/OT Vulnerability to Cyber Attack

Like many businesses, the IT systems of electric co-ops maintain customer data such as contact, billing, and payment methods. These systems are vulnerable to the same cyber-attacks as any other organization. The OT systems are vulnerable to both unauthorized data access and to an adversary taking control of specific equipment and grid elements. This vulnerability is increased when customers with their own generation capability through solar panels or other equipment must be allowed bidirectional power flows with the grid, while remaining outside the control of the electric co-op. As the state of practice moves to smart meters that use wireless access to meter readings (to reduce the cost of tracking usage) and the Internet of Things that gives customers control through the internet over many household electric devices, there will be increased opportunity for malicious cyber-physical access.

It is not uncommon to find smaller co-ops utilizing outdated software and network hardware within their IT networks. Because this equipment is familiar and may operate for years without any failures or need for retraining, the co-op is not made aware that the product is no longer being sold or maintained, and perhaps that the original provider is no longer even in business. This is very important for cyber security, because once a vulnerability is known in the hacker community, it can be exploited in many ways against users unaware of their risk. These small users are also vulnerable to changes in system settings meant to

nuariinfo@norwich.edu
nuari.net
P.O. Box 30
Northfield, VT 05663
+802.485.2213

maintain system and network security. These changes reduce network security for a valid one-time purpose, but through carelessness may not be restored to the original configuration. Upgrading the IT/OT network must compete for limited funds against the claims of the physical power distribution infrastructure, which may also face obsolescence. The need to replace the generators, transformers, and the poles and distribution wires is apparent to managers who began their careers operating and maintaining the power grid, while they have no experience with or understanding of computer networks

The OT software and network devices present unique additional risks. Obsolete, vulnerable Supervisory Control and Data Acquisition (SCADA) devices and protocols may remain in service for decades. These devices continue to function so that co-ops have little incentive to make operational upgrades, and the threat of cyber-attack seems remote and hypothetical. The lack of in-house staff with the necessary skillset to install, configure, and test upgraded equipment means that the cost of upgrades is further increased by the cost of network consultants, while the only people available to explain the benefits are vendor sales personnel, not trusted in-house experts.

The most common method for updating software and firmware to the latest version within co-op OT networks involves a process known as patching. A patch is an immediate solution to an identified problem that is downloaded from the vendor's website as a part of normal product service. Installing a software or firmware patch is a complex task which must be analyzed carefully to identify second order effects on equipment outside the purview of the vendor supplying the patch. Detailed change management process and accurate asset inventory are critical to accurately identifying downtime during maintenance windows. While the latest technology is vastly simpler to maintain than that of the past, many organizations are bound to legacy equipment. Maintaining security for these networks is difficult and can exceed the technical capability of small electric co-ops.

Eventually, older software/firmware is no longer supported by the manufacturer, so that vulnerabilities are no longer recognized and remediated. Any electric co-op using outdated software is at risk of compromise by malicious code that is in the hands even of common criminals.

While it is vitally important to upgrade obsolete OT network equipment, the costs can be substantial for several reasons. Often it is not possible to spread out the expense over a longer period by using a phased upgrade path. Because electric power is an essential service, upgrades must be installed and tested with no disruption or service.

Cyber Vulnerability and Mitigation

Vulnerability

In any business, the IT system is vulnerable to attack because it must be accessible to employees, and often even to the public on a limited basis. Cyber criminals exploit human error and even deliberate insider sabotage to gain access. Once inside the network, a persistent threat monitors operations to gain additional and deeper access in the network to exploit data and to gain control of assets on the network. Access can also be gained through peripheral devices with wireless access, such as printers and cameras, or by seemingly innocent physical access given to individuals with incidental functions, such as janitors or technicians for ventilation or lighting systems.

nuariinfo@norwich.edu
nuari.net
P.O. Box 30
Northfield, VT 05663
+802.485.2213

We frequently read of the business impact of a variety of cyber-attacks conducted for financial gains or simply to cause disruption:

- Ransomware attacks, where the attacker freezes computer systems and threatens to also destroy all data on the systems unless a ransom is paid.
- Denial of Service attacks where the attacker overloads the network servers so that websites and internal email are unavailable.
- Compromise and theft of customer and employee data, which can be sold to criminal groups that are engaged in credit card sales and identity theft.

Malicious access to OT systems is a different problem. Most SCADA and PCL systems transmit much more data than is received, and the received data comes from only a very small number of network sources and can be limited to those sources. The most likely paths for unauthorized access result from carelessness by technicians accessing the system for routine maintenance or through malicious code inserted into software patches or new software, firmware, or hardware. The difficulty of gaining access and the limited potential for financial gain means that attacks on the OT system are more likely to come from a state actor or a business adversary attempting to damage the co-op as a business. While these attacks can cause significant damage, an attack that penetrates to the OT network is certain to cause major damage, and to leave lingering doubt that the malware has been completely removed so that normal operations can safely resume.

Mitigation

There are several actions that an electric co-op can pursue to reduce vulnerability to counterattacks. First, and most important, is to isolate the operational (OT) network from the administrative (IT) network. The nature of the IT network requires allowing many sorts of access that introduce vulnerability to compromise.

- Second, hire an individual with cybersecurity expertise. It may be necessary to hire two individuals to properly address both IT and the very specialized needs of the OT network supporting an electric grid. For all but the largest electric co-ops, this will mean hiring consultants rather than giving additional tasking to the in-house network administrator. However, if outside consultants are employed, then it is essential to have an experienced and trusted in-house staff member assigned to learn the basics of network security and work with the consultant. This will ensure that the needs and constraints of the co-op are effectively communicated to the consultant, and that, when the consultant departs, the in-house team will have the knowledge and training to properly operate and maintain the networks.
- Third, work with vendors and appropriate sector associations to identify hardware upgrades for the electric grid equipment used for generation, transmission, and distribution, and for the SCADA and PCL equipment for monitoring and control, to remove obsolete equipment with known vulnerabilities.
- Fourth, carefully review all IT and OT software in use to identify any software packages that are no longer supported by the manufacturer. Replace those packages with secure modern software.
- Fifth, provide training to all staff members to raise awareness of the many ways that malicious actors will attempt to gain access through a careless action by an employee. Also, provide training

nuariinfo@norwich.edu
nuari.net
P.O. Box 30
Northfield, VT 05663
+802.485.2213

on how to identify internal threats. Conduct periodic tests by sending messages like common phishing attempts to help employees recognize the ease with which they can be lured into a mistake, and to develop habits to resist these efforts.

- And finally, review all maintenance requirements that give outside persons legitimate access to spaces housing network equipment, and then develop and enforce processes that will prevent a malicious actor from exploiting this sort of access to sensitive equipment.

All these actions will be expensive, and because the threat seems abstract and remote the expense will be difficult to justify in the cost-constrained culture of an electric co-op. Structured wargame decision-making exercises are an excellent tool to help educate management on the very real (and urgent) risks electric co-ops must face. Exercises can also test incident response and identify gaps in recovery plans. These types of exercises allow co-op staff to fully explore the specific damage from an attack and the actions required to recover. Exercises are important in each phase - from identification of problems and developing an Incident Response Plan to conducting training to ensure that the co-op staff will be able to recognize an attack when it occurs and be confident in executing the planned response.

Conclusion

Despite regional differences in geography and systems of governance, electric co-ops face common difficulties in preparing for and preventing cyber-attacks. Electric co-ops, especially small ones, deploy a small staff to operate and maintain an electric grid over a large area, while serving a customer base that demands costs be maintained at the lowest practical level. The difficulties will only increase as technology changes introduced by customers require that utilities allow reverse flow of power from solar panels, and the Internet of Things is used to give remote control of many electric appliances in the home.

To maintain reliable and sustainable service in this environment, electric co-ops must make substantial investment in their IT and OT networks. Wargame and decision-making exercises that examine the operational consequences of common cyber-attacks are a valuable tool in conducting these upgrades and educating management on the justification for these expenses.

"The NUARI exercise helped us identify communication gaps and other issues that must be addressed before we face an actual cyber incident."
A Florida Co-op

References

About our cooperative. (2021). Alaska Village Electric Cooperative (AVEC). Retrieved from https://avec.org/about/our-cooperative/

nuariinfo@norwich.edu
nuari.net
P.O. Box 30
Northfield, VT 05663
+802.485.2213

About us. (ca. 2020). Cape Hatteras Electric Cooperative (CHEC). Retrieved from https://www.chec.coop/touchstone-energy-cooperatives

About us. (2020). Salem Electric Cooperative. Retrieved from https://www.salemelectric.com/about-salem-electric

A summary of terrorism threat to the U.S. homeland. (2020). *National terrorism advisory system bulletin.* Retrieved from www.DHS.gov.

Bailey, T. (2020). The energy sector threat: how to address cybersecurity vulnerabilities. Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities#

Critical infrastructure sectors: energy sector. (ca.2020). Retrieved from https://www.cisa.gov/energy-sector

Electric utility industry. (2017). Retrieved from https://www.publicpower.org/system/files/documents/final-electricutilityindustryoverviewappa2017fallinstitute_0.pdf

Freestate believes in transparency. (2021). Freestate Electric Cooperative. Retrieved from https://www.freestate.coop/transparency

Karaim, R. (2019). Co-op tech: DIY GIS. Retrieved from https://www.cooperative.com/remagazine/articles/Pages/co-op-tech-diy-geographic-information-system.aspx

Krebs, B. (2012). FBI: Smart meter hacks likely to spread. *Krebs on Security*. Retrieved from www.krebsonsecurity.com.

Misbrener, K. (2019). Cyberattacks threaten smart inverters, but scientists have solutions. *Solar Power World*. Retrieved from www.solarpowerworldonline.com.

NRECA: The Electric cooperative story. (ca. 2019). Retrieved from https://www.youtube.com/watch?v=tenKnIx4ouY

NIST. (2021). Retrieved from: https://csrc.nist.gov/glossary/term/patch

Sayegh, E. (2020). As The End Of 2020 Approaches, The Cybersecurity Talent Drought Gets Worse. *Forbes.* Retrieved from: https://www.forbes.com/sites/emilsayegh/2020/09/22/as-the-end-of-2020-approaches-the-cybersecurity-talent-drought-gets-worse/?sh=460615f15f86

SCADA. (2021). Retrieved from www.vermontelectric.coop/SCADA

Sunshine, W. (2021). How electric co-ops and commercial utilities differ. Retrieved from https://www.thebalance.com/electric-cooperatives-vs-utilities-1182700

The PI system unlocks operational insights and new possibilities (2021). Retrieved from https://www.osisoft.com/pi-system

Welcome to Magnolia Electric Power. (2021). Magnolia Electric Cooperative. Retrieved from https://www.mepcoop.com/

nuariinfo@norwich.edu
nuari.net
P.O. Box 30
Northfield, VT 05663
+802.485.2213

What are electric coops? Retrieved from https://www.anzaelectric.org/content/what-electric-cooperative

Whitman, M.E., Mattord, H.J. (2016). *Principles of information security*. Boston, MA: Cengage.

Wintch, T. (2021). PERSPECTIVE: cyber and physical threats to the U.S. power grid and keeping the lights on. Retrieved from https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/

Zurcher, S. (2020). The Current State of Wildfire Liability in California. *LegalPlanet.* Retrieved from https://legal-planet.org/2020/10/05/guest-contributor-samantha-zurcher-the-current-state-of-wildfire-liability-in-california/

nuariinfo@norwich.edu
nuari.net
P.O. Box 30
Northfield, VT 05663
+802.485.2213