Utility Cybersecurity: Culture Comes First

It's a date those in the energy sector know well: August 14, 2003. On that day, more than 50 million people in eight states and portions of Canada lost power when a high-voltage line in Ohio softened, sagged, and brushed against some trees. The fault, combined with a cascading series of technical issues, caused the largest blackout in North American history.

In just a little over an hour, more than 508 generating units at 265 power plants shut down.[1] Telephone and cellular systems became overloaded. Traffic was reduced to gridlock because signals weren't operating. Hundreds of thousands of commuters were stranded in subway tunnels and train stations. Airports were forced to close. Hospitals and critical patients were left vulnerable due to overtaxed backup generators. Hundreds of millions of gallons of untreated sewage flowed into recreational waterways. Neighborhood stores and restaurants suffered wholesale financial losses.

The lessons learned from the Northeast blackout were many. At the most basic level, it was an education in the obvious: nothing works without a reliable electric grid. For the U.S.'s network of decentralized utility operators, that fundamental takeaway emphasized the need for greater coordination, cooperation, and collaboration, leading to initiatives and exercises such as GridEx.

What is receiving heightened attention today isn't a future blackout caused by human error, aging equipment, or load imbalances. A cyberattack could create a similar power disruption in the future. Whether in the form of a rogue internal agent such as a disgruntled employee or via an outside state-sponsored agent with the skill and resources to exploit complex networks, a cyberattack capable of causing a cascading failure like the blackout of 2003 is a real-world challenge that power companies must deal with.

To reinforce the importance of protecting the bulk power system, the North American Electric Reliability Corporation, an international regulatory authority, has imposed civil penalties of up to $1 million per day, per violation for non-compliance to NERC rules, regulations, and orders.[2] The $25 million civil penalty levied on Florida Power & Light, Co. in 2009 is an example of the high priority placed today on grid reliability.[3] Beyond the monetary price tag, reliability failure can damage a utility's brand, public perception, shareholder value, and more.

[1] U.S.-Canada Power System Outage Task Force. (2004). Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. https://energy.gov/oe/downloads/blackout-2003-final-report-august-14-2003-blackout-united-states-and-canada-causes-and

[2] Energy Policy Act of 2005, Pub. L. No. 109-58, 119 Stat. 594 (2005).

[3] Federal Energy Regulatory Commission. "FERC Approves Settlement $25 Million Fine for FPL's 2008 Blackout." October 8, 2009. http://www.nerc.com/FilingsOrders/us/FERCOrdersRules/FERC%20Press%20Release.pdf

AVTEC

Phone: 1-833-308-5155 • avtecinc.com/utilities
100 Innovation Place • Lexington SC 29072 USA

Today's Cyberlandscape

Cybersecurity is an issue all businesses and governmental agencies face. Recent, well-publicized breaches, such as those launched against Equifax, the Internal Revenue Service, Chipotle, Target, Blue Cross Blue Shield/Anthem, Verizon, and many others, underscore the far-reaching implications. According to BTB Security, a cybersecurity and digital forensics company headquartered in Philadelphia, the number of consumers compromised by data hacks grew from 44.2 million in 2005 to 190 million just ten years later. BTB Security estimates the cost of cybercrime to the average U.S. business grew from $24,000 in 2005 to $1.5 million in 2015.[4]

In the energy sector, a 2017 survey conducted by the Ponemon Institute found that 68% of U.S. oil and gas cybersecurity risk managers said their operations have had at least one security compromise in the last year. In addition, only one-third rated their organization's operational cyberreadiness as high.[5] The FBI and Department of Homeland Security have issued joint reports in recent years to U.S. energy companies regarding hacking activity—placing special emphasis not only on cyberattacks designed to compromise energy and other critical infrastructure sectors (known as "intended targets"), but also on malicious attempts to target trusted, third-party suppliers with less secure networks and equipment (known as "staging targets").[6] The recent highly customized strikes on the power grid in Ukraine—breaches that took control of switches and breakers—serve as an example of the potential damage that a sophisticated cyberattack can inflict.

[4] BTB Security. Cyber Crime: Then and Now. https://www.btbsecurity.com/images/PDFs/BTBAnniversaryInfographic.pdf

[5] Ponemon Institute. The State of Cybersecurity in the Oil & Gas Industry: United States (2017). http://news.usa.siemens.biz/sites/siemensusa.newshq.businesswire.com/files/press_release/additional/Cyber_readiness_in_Oil__Gas_Final_4.pdf

[6] Forrest, C. "DHS, FBI Warn of Cyberattacks Targeting Energy Infrastructure, Government Entities." TechRepublic. October 23, 2017. https://www.techrepublic.com/article/dhs-fbi-warn-of-cyberattacks-targeting-energy-infrastructure-government-entities/

AVTEC

Phone: 1-833-308-5155 • avtecinc.com/utilities
100 Innovation Place • Lexington SC 29072 USA

Buttoning Down Mission-Critical Communications

To address this complex, multi-faceted threat, utility companies and regulatory entities have been aggressively assessing and reworking standards, procedures, and protocols to confront the changing cybersecurity ecosystem. Boundaries are being drawn for protecting critical infrastructure within an electronic security perimeter necessary to sustain operations.[7] NERC's Jan. 2, 2018 glossary of terms used in reliability standards defines a bulk electric system cyberasset as one that if rendered unavailable, degraded, or misused would—within 15 minutes—adversely impact one or more facilities or systems, potentially affecting reliability of the BES.[8] For purposes of this glossary, NERC describes a BES cybersystem as one or more cyberassets logically grouped together to perform a reliability task for a functional entity. Of note, redundancy of potentially affected equipment is not a consideration when determining adverse impact. With this structure in place, many utilities are now treating mission-critical electric control center communications systems as a BES cybersystem. In fact, the Western Electricity Coordinating Council, which promotes BES reliability in the Western Interconnection, notes that a Voice over Internet Protocol system connected to a system operator's communication console may be considered a BES cyberasset.[9] Related, during NERC's Critical Infrastructure Protection Committee Meeting on Dec. 12-13, 2017, the CIPC outlined a 2018 task of providing guidance for the use and protection of cyberassets used for voice communications, particularly within control center environments.[10]

[7] NERC. Security Guideline for the electricity Sector: Identifying Critical Cyber Assets (2010). http://www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf

[8] NERC. Glossary of Terms Used in NERC Reliability Standards. (2018) http://www.nerc.com/files/glossary_of_Terms.pdf

[9] WECC. CIP-002-5.1 FAQ from WECC Entities: What can I do to...? (2016) https://www.wecc.biz/_layouts/15/WopiFrame.aspx?sourcedoc=/Administrative/14%20CIP%20v5%20FAQ%20from%20WECC%20Entities%2003%2022%2016%20Baugh.pdf&action=default&DefaultItemOpen=1

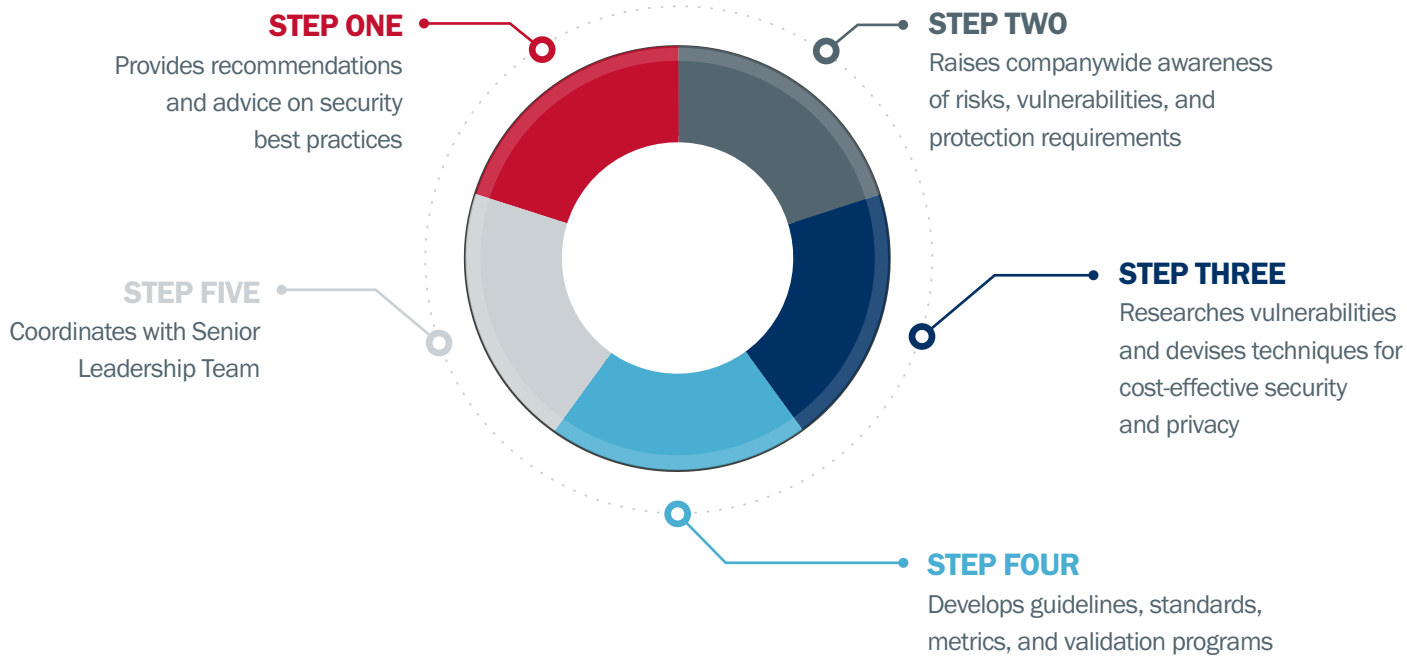
[10] NERC. Quarterly Workplan Update. (2017) http://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/CIPC%20Presentations.pdf

A Review of Best Practices

Robust cybersecurity requires a methodical and strategic approach. Documentation is invariably part of this effort, but documentation alone is not a sufficient strategy. The best practices of utilities that are leading the way in cybersecurity are both top-down and enterprisewide. Senior management is ultimately responsible for the protection of a utility's assets and cybersecurity policies. Executives must understand, support, and direct cybersecurity affairs, while simultaneously ensuring that corporate objectives are aligned with best practices to address deficiencies.

Establishing a Cross-Functional Security Council

The multi-layered, complex nature of cybersecurity requires an experienced, expert team at the helm for both utilities and their suppliers. Because cybersecurity is so very broad in scope, a cybersecurity council should include a cross-section of managers and subject matter experts, including engineering and information technology, sales and marketing, and legal, depending on the organization. Senior leadership should appoint cybersecurity council members, as well as review, approve, and support the group's efforts. The purpose of the council is to deliver and maintain a security program that safeguards information and assets against unauthorized use, disclosure, modification, damage, or loss. The council should meet on a regular schedule to define and communicate the overall corporate cybersecurity posture, and to identify and prioritize opportunities for improvement using a continuously repeatable process. In doing so, members should also require ongoing employee training and certification, so that those on the front lines are prepared to recognize and address emerging threats.



AVTEC
Phone: 1-833-308-5155 • avtecinc.com/utilities
100 Innovation Place • Lexington SC 29072 USA

Forming a Security Incident Response Team

Logically functioning as subset of the corporate cybersecurity council, a utility's security incident response team takes ownership of:

- Guidelines and procedures for effective incident response.
- The communication process upstream to senior leadership with respect to detection, containment, and response efforts to any incident.
- Returning systems to "ready" status and holding after-action reviews.
- Execution of the business continuity plan and periodic training scenarios.

Developing a Cybersecurity Policy

A comprehensive corporate policy for a utility should cover all facets and phases of cybersecurity, including:

- Identification of information assets and how they are to be managed.
- High-level directional guidelines and standards to be followed by all business units.
- Roles and responsibilities of system and data owners, custodians, managers, and users, including acceptable use of information and data.
- Procedures and processes for team transitions that affect owners, managers, and users.
- A process for exceptions, as well as periodic guideline review and evaluation.
- A comprehensive set of guidelines related to outside business partners and their access and use of physical and information systems, including security requirements for different asset classification levels.
- Development of a business continuity plan, including training criteria.
- A well-defined process for policy review, updates, approvals, and change communication as conditions dictate

AVTEC

Phone: 1-833-308-5155 • avtecinc.com/utilities
100 Innovation Place • Lexington SC 29072 USA

Benchmarking of Lessons Learned

In developing and maintaining a forward-looking corporate cybersecurity policy, utilities should evaluate the causes of and solutions for cyberattacks across all industry segments. Individuals charged with cybersecurity systems should continuously evaluate the latest breaches and emerging threats, assessing them as they relate to the utility's physical assets and information systems.

Developing a Plan of Action and Milestones

The Plan of Action and Milestones functions as the security roadmap for utilities and business partners. The POA&M provides a corrective plan to track, resolve, and mitigate security weaknesses, including defining implementation steps. No company, including an energy provider, is ever 100% prepared to fend off all security threats, but the goal for any business is to get as close to 100% as possible, with a clear method to document and track countermeasures and compensating controls that will address problem areas efficiently and effectively. Using a POA&M process gives all involved a clear procedure for ongoing security improvement efforts.

Updating Software

Utilities that are the most effective of staying ahead of the cyber vulnerability curve review and evaluate security updates every 35 calendar days. Compensating measures and/or mitigation plans must be implemented to address security gaps when updates cannot be deployed. These updates should include firmware and security patches, rolled in together to strengthen the enterprise's defense against current security threats, thereby reducing the chance for data and system compromise.

Building Intrusion Prevention & Detection Systems

In the past, cyberattackers focused on easy targets. Today, their attacks are not only far more sophisticated, but also, once unleashed, are progressively becoming more automated. The recent cyberattacks on Ukraine's power grid illustrates this fact. Beyond external threats, leading cybersecurity professionals realize that damaging attacks may also originate from internal operatives such as a disgruntled employee. To combat both internal and external threats, intrusion prevention and detection systems should be in place to minimize risks and quickly detect and address security breaches. Solid protect-and-defend IPS and IDS systems should include such elements as traffic and packet monitoring, well-defined firewalls, port scanning, and, ultimately, system logs/alerts. A separate, expertly staffed information security operations center, or ISOC, should be in place to monitor, assess, and defend systems and assets.

AVTEC

Phone: 1-833-308-5155 • avtecinc.com/utilities
100 Innovation Place • Lexington SC 29072 USA

Pursuing System Certification

Electric and gas utility companies, along with businesses in related essential services, use communication networks that have come under increasing scrutiny due to their importance with respect to public health and welfare, economic stability, and national security. Bulk power system operators must comply with North American Electric Reliability Corporation Critical Infrastructure Protection standards, which are derived from the more comprehensive federal National Institute of Standards and Technology requirements. In addition, since the Energy Independence and Security Act of 2007, NIST was charged with the task of developing a framework for interoperability and cybersecurity for smart grid applications.[11] The path of cybersecurity strength for any utility lies in mapping of NIST to NERC-CIP standards in order to eliminate potential security gaps. Utility companies should exercise due diligence when partnering with outside vendors, particularly those providing control center communication systems. NERC-CIP compliance of deployed products should be an expected goal for these external system suppliers.

Hiring a Third-Party Security Auditor

A utility's day-to-day cybersecurity practices should include both vulnerability scanning to detect weaknesses as well as penetration testing to assess whether corrective actions taken to thwart identified vulnerabilities have done their job in adequately protecting essential systems. Beyond these internal practices, however, it is equally important for utilities to conduct an annual third-party audit to identify weaknesses and continually strengthen their cybersecurity position. Experienced internal security experts can miss critical vulnerabilities that can jeopardize efforts to protect a utility and its customers, so having an unbiased third-party auditor is as critical as the maintenance of a utility's physical infrastructure. As with NERC-CIP compliance, outside vendors and business partners should, likewise, employ third-party auditing as a standard business practice to help identify and mitigate any cybersecurity risks to the utility.

[11] NIST. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. (2014) https://www.nist.gov/sites/default/files/documents/smartgrid/NIST-SP-1108r3.pdf

AVTEC

Phone: 1-833-308-5155 • avtecinc.com/utilities
100 Innovation Place • Lexington SC 29072 USA

A Run-Through of Security and Access Management

Utilities treating their control center communication systems as protected cyberassets are requiring their mission-critical communication system providers to be fixed and focused on three pillars—confidentiality, integrity, and availability. Just as these pillars should define and guide a utility's day-to-day approach to policies, operational processes, and reliability standards, they should be required of any business partner that supplies mission-critical communication systems and technology.

1

PILLAR ONE

Confidentiality

- Logical control
- Physical access control
- Secure data exchange
- System data encryption
- Identity assurance
- Secure intra-system communication

2

PILLAR TWO

Integrity

- Source code control management
- System change management
- Hashing algorithm
- Data assurance
- Malware management
- Device access control

3

PILLAR THREE

Availability

- Survivability
- Threat agent protection
- Parallel processing
- System backup and restore
- Platform support
- Quality assurance testing
- Supplier business continuity plan

AVTEC

Phone: 1-833-308-5155 • avtecinc.com/utilities
100 Innovation Place • Lexington SC 29072 USA

1

PILLAR ONE

Confidentiality

A mission-critical communications system supplier must have controls and policies in place at both the corporate and product level that vigorously protect intellectual property and product data. Within the communication system itself, internal data must be secured, whether stored locally or when exchanged between two or more distributed devices within a network. Confidentiality safeguards for a mission-critical communication system provider should include:

- **Logical control**—enforcing authentication and identification policies that restrict unauthorized access, including stringent password policies, well-defined role-based access, and network segregation/isolation where required.
- **Physical access control**—preventing unauthorized access to secure development facilities and critical equipment necessary for core business operations, including two-factor building access controls and datacenter authentication, visitor log management, video surveillance, and secure/locked equipment cabinets.
- **Secure data exchange**—utilizing secure transfer protocols and controlled credentials during utility/supplier data exchanges, including secure remote access to customer networks, software/patch releases via Secure File Transfer Protocol sites, and login credentials with link expiration.
- **System data encryption**—preventing unauthorized penetration of critical communication systems via secure access and data transport, including encryption during password transmit/store, external interface encryption (Advanced Encryption Standard, Data Encryption Standard, and enhanced privacy), and key management.
- **Identity assurance**—granting permission access only to authorized administrators and users, including assignment of unique user credentials, secure Windows Active Directory, and central distributor user management.
- **Secure intra-system communication**—using secure protocols (Secure Shell/Secure File Transfer Protocol, Hypertext Transfer Protocol Secure/Secure Sockets Layer) to strengthen against packet snooping and potential hacking.

2

PILLAR TWO

Integrity

Beyond confidentiality controls, a utility's mission-critical communications system must safeguard against the unauthorized access or alteration of hardware and software at the system, device, network and/or data communication level. Integrity safeguards for a mission-critical communication system business partner should include:

- **Source code control management**—utilizing source code control management to ensure software integrity, quality, and consistency throughout the development and delivery process, including source code and regression testing, quality control validation, and software revision control.
- **System change management**—restriction of system access and change auditing to mitigate unauthorized modification and to enable forensic reconstruction of events, including tiered permission control and deployment status.
- **Hashing algorithm**—ensuring data integrity between source and destination, whether downloading software from a secure site or validating packet origination between components, including software integrity MD5 Checksum and message source verification.
- **Data assurance**—insisting on software deployment and revision validation to ensure components maintain compatibility and latest code build, including agile development methodology, component version validation, software deployment confirmation, and data normalization.
- **Malware management**—requiring malware policy flexibility that allows for use of the utility's standards, provides streamlined deployment, and simplifies corporate management, including support of utility malware/antivirus policies and directories whitelist baselines.
- **Device access control**—disabling of unused ports and services to reduce unauthorized access, modification, or harmful code introduction to system components, including block/disable of USB and RJ-45 ports.

3

PILLAR THREE

Availability

Utilities must ensure that their electric control center communications system, device, network, and data is maintained and kept operational. Loss of these systems can have a negative impact on load management, response, and restoration time, as well as field personnel safety. Availability safeguards for a mission-critical communication system business provider should include:

- **Survivability**—requiring network distributed and redundant components to eliminate single points of failure, enable location access flexibility, and improve system performance, including automatic failover, Simple Network Management Protocol alarm notification, geodiversity, global-free seating, and dynamic Session Initiation Protocol routing.
- **Threat agent protection**—implementing internal and external threat protection procedures that help identify, minimize, and eliminate exploitation of vulnerabilities, including security awareness training, system change auditing, access authentication, vulnerability scanning, security patch management, and ports and services management.
- **Parallel processing**—diversifying interfaces, applications, and services across multiple devices to improve scalability and performance through simultaneous processing, including load prioritization and balancing as well as Data Management System clustering.
- **System backup and restore**—adapting to the utility's changing internal and customer needs via system restoration and flexible revision management, including backup and restore of system configuration and data files, rollback to prior release, and multiple simultaneous revision support.
- **Platform support**—using standard utility operating environments, both hardware and software, to simplify development, deployment, maintenance, and security, including Microsoft Windows/server operating system, VMWare, VxWorks, commercial off-the-shelf personal computers and servers, and/or Cisco network compatibility.
- **Quality assurance testing**—improving product resilience through defect identification and resolution via end-to-end software validation throughout the development process, including installation/upgrade testing, functional testing, failover/recovery testing, load/stress testing, and regression testing.
- **Supplier business continuity plan**—maintaining source code survivability and accessibility, including off-site source code backup, redundant development, and QA platforms.

Looking Back, Looking Forward

It's evident to utility executives, operators, regulators, and related stakeholders that the Northeast blackout of 2003, or an event like it, could be repeated in history. The difference today is that such a cascading series of events could be set in motion not due to human error, extreme weather, aging equipment, or load/generation imbalances, but rather due to hackers inserting malware into a system and gaining operational access.

Accountability in the utility sector is high—NERC's 15-minute reliability standard in its 2018 glossary is a relatively short period of time to fully recover an electric control center communications system that has been degraded or otherwise rendered unavailable. What's more, NERC-CIP regulated utilities are required to report downtime that exceeds 15 minutes, including documentation explaining the reason for the interruption. Such reporting opens up the entity to auditing of its day-to-day operations and scrutiny of protocols in place to protect integrity and availability. Any lack of reliability can cause not only a major outage, but also imposes serious safety risks to personnel and the public. With safety as a top priority for utility companies, cybersecurity standards should be both comprehensive and robust.

For this reason, many utilities are now treating mission-critical electric control center communication systems as protected cyberassets, deploying the same reliability standards already in place for bulk power transmission equipment, systems, and facilities. As previously noted in the Ponemon Institute study, 68% of U.S. oil and gas security risk managers reported their operations had at least one security compromise within the last year. With this as the backdrop, a paradigm shift that incorporates communication systems within the electronic security perimeter is both prudent and strategic. By employing tighter operational standards, procedures, and protocols (as defined and required by NIST and NERC-CIP), and by requiring mission-critical communication system business partners to do the same, utility companies can build a future-looking strategy against cyberattacks, whether launched externally or internally. Such a strategy helps protect utilities from stiff NERC civil penalties, as well as difficult-to-measure tolls against a utility's brand and shareholder value.

AVTEC

Phone: 1-833-308-5155 • avtecinc.com/utilities
100 Innovation Place • Lexington SC 29072 USA