From Worms to Phishing

THE COMPLETE GUIDE TO UTILITY CYBERSECURITY

AVTEC

Table of Contents

From Worms to Phishing: The Complete Guide to Utility Cybersecurity

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: 1.803.358.3600 • avtecinc.com
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/

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

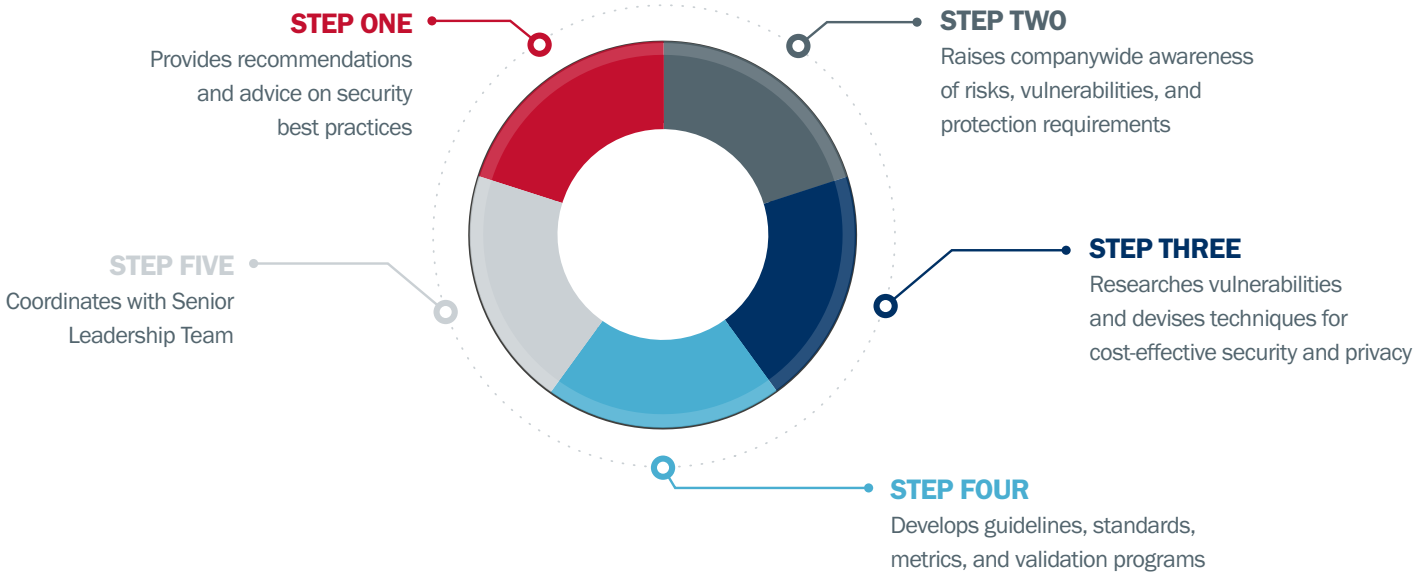
[10] NERC. Quarterly Workplan Update. (2017) http://www.nerc.com/comm/CIPC/Agendas%20Highlights%20and%20Minutes%202013/CIPC%20Presentations.pdf

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.



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

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: 1.803.358.3600 • avtecinc.com
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. Related, 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

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

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.

Part I: Conclusion

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.

Utility Cybersecurity: Shut Back Doors to Critical Operational Systems

Cyberattacks on utilities are becoming more frequent, more successful, and more dangerous. While utilities have some of the most sophisticated and effective cybersecurity measures and protocols in place and update them frequently, they also face significant and proven vulnerabilities posed by third-party vendors.

Early in 2018, the Department of Homeland Security (DHS) and FBI issued a Technical Alert (TA18-074A)[1] warning that the Russian government is targeting the energy and other industrial sectors. Attacks were comprised of strategic, multi-stage campaigns, using techniques such as spear-phishing and staging of malware, all designed to conduct network reconnaissance and collect information pertaining to industrial control systems (ICS). The ultimate goal for these threat agents: reach a point where they can throw switches.

Before this alert was released, Symantec issued its own report on these campaigns, detailing what it referred to as the re-emergence of a cyberespionage group known as "Dragonfly," which had been targeting the energy sector since at least 2011.[2] After a period of relative quiet, the Dragonfly group re-appeared in 2015, continuing its efforts to carry out campaigns aimed at learning how utility facilities operate and maneuvering its way towards gaining access to the ICS themselves. Of note, Symantec had previously described Dragonfly as "technically adept and able to think strategically."[3] It continued with: "given the size of some of its targets, the group found a 'soft underbelly' by compromising [utility] suppliers, which are invariably smaller, less protected companies."

[1] United States Computer Emergency Readiness Team, Alert (TA18-074A), "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors (2018). https://www.us-cert.gov/ncas/alerts/TA18-074A

[2] "Dragonfly: Western energy sector targeted by sophisticated attack group," Symantec blog, October 20, 2017. https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks

[3] "Dragonfly: Western Energy Companies Under Sabotage Threat," Symantec blog, June 30, 2014. https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat-energetic-bear

AVTEC

Phone: 1.803.358.3600 • avtecinc.com
100 Innovation Place • Lexington SC 29072 USA

As detailed by the DHS and FBI, these threat actors target two distinct categories of victims—staging and intended targets. Hackers begin by exploiting the systems and applications provided by trusted third-party suppliers—staging targets—using any opening as a pivot point to gain direct access to utility systems, the intended target. Utilities use many applications, components, and systems that are developed, installed, and upgraded by third-party vendors, including mission-critical communications technology. These communication systems often share a common network that is necessary not only for day-to-day operations, but also for resiliency and restoration processes. Protecting these third-party, mission-critical communications systems must be a consideration when assessing and managing a utility's overall cybersecurity posture.

Systems Security

While the task is daunting and there are many areas for concern, there are multiple, achievable ways to provide systems with secure operating environments. This paper identifies some of the energy-focused ones for consideration.

Security Awareness Training

The best defense against any cybersecurity attack starts with the front line of an organization and extends to business partners. Employees, contractors, and third-party suppliers must be trained to be vigilant regarding system and application use, maintenance, and physical access. These individuals are the ones most likely to be targeted and are also the people who, when properly trained, will be first to notice an attempted intrusion. Training should be performed systematically and tailored to align with business roles to ensure best practices for cybersecurity are always top of mind. The objective for training should be to instill a culture of cybersecurity, one where individuals are vigilant about recognizing potential threats and equipped with processes and procedures to fend them off.

Supply Chain Risk Management

On Oct. 18, 2018, the Federal Energy Regulatory Commission (FERC) approved the supply chain risk management reliability standards, CIP-013-1, submitted by the North American Electric Reliability Corporation (NERC) in response to the commission's directives from Order No. 829.[4] The purpose of CIP-013-1 is to mitigate cybersecurity risks in a utility's supply chain, including communications technology and ICS. Compliance with CIP-013-1 requires the development of one or more plans to address four objectives for high- and medium-impact Bulk Electric System (BES) cybersystems:[5]

1. Software integrity and authenticity.
2. Vendor remote access.
3. Information system planning.
4. Vendor risk management and procurement controls.

Before procuring any mission-critical system, including a communications technology, energy companies should closely examine their vendors' security protocols, including how often measures are updated to counter evolving threats. Vendors must be held accountable to ensure that software, hardware, and other components have not been tampered with or maliciously infected before arrival onsite. Specific security requirements, expectations, and controls should be included in a Statement of Work (SOW), contracts, and Requests for Proposals (RFPs). Another alternative is to tie payments to the validation of implemented security controls and features. This linkage will motivate vendors to be vigorous in their compliance, tightening their own security and achieving higher standards through creative, enhanced solutions.

For hardware and software designed and manufactured overseas, vendors should be required to utilize tamper tapes to secure boxes and track all shipments end-to-end using a certified signature method. The goal is to create an audit trail and ensure the shipment never deviates from its safe route to its destination. Even with strict controls, it is a challenge for the average vendor to accomplish the objectives because of inadequate processes or controls. Unfortunately, non-compliant vendors may be the only option available. Nonetheless, utilities should push back and demand vendors do more to reduce the likelihood of breaches and exploitations.

Before granting system access to a vendor, complete a thorough screening and contract process. Ensure vendor employees have gone through background checks. Also, use only secure connections from the vendor's network. The vendor must be able to adhere to the utility's corporate security policy. A review of the vendor's security policy and controls may be necessary to find out how well the vendor is going to be able to secure the utility's data and the interconnections between both systems. Only vetted and authorized personnel should be allowed onto the utility's network.

This vendor-focused activity leads to Vendor Risk Management and Supply Chain Risk Management efforts at a corporate level, which is now recommended by the National Institute of Standards and Technology (NIST) through its published guidance document, SP 800-161 "Supply Chain Risk Management Practices."[6]

[4] U.S. Federal Energy Regulatory Commission, Order No. 850, Supply Chain Risk Management Reliability Standards (2018). https://www.ferc.gov/whats-new/comm-meet/2018/101818/E-1.pdf?csrt=15773227531081670129

[5] North American Electric Reliability Corporation, CIP-013-1, Cyber Security – Supply Chain Risk Management (2017). https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf

[6] National Institute of Standards and Technology, Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, (2015). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

Testing of Systems and Applications

After a successful implementation of security awareness training and supply chain risk management, the next step is to test the mission-critical systems and applications in a controlled environment before deploying into the production network. Mission-critical communication systems should be set up and tested using various automated and manual tools to validate that security requirements, expectations, and controls are met. Scenarios such as misuse testing—acting like a user—are employed to provide some confidence that the application will behave correctly under stress-based conditions. These tests are sometimes performed by external organizations under the term, "red team." Vulnerability testing, looking for common security weaknesses, penetration testing, and acting like a hacker should be considered at this phase. Any discovered vulnerabilities should be noted and communicated to the appropriate vendor. If the vendor cannot immediately resolve the issue, then request the vendor create a Plan of Action and Milestones (POA&M) item, including a secure workaround until the vulnerabilities are fixed. The ultimate objective is to introduce "clean" systems and applications to the production environment to establish a clean baseline.

Ports, Services, and Protocols Management

Utilities should require vendors to provide architecture and networking design of a mission-critical communications system. It should include all hardware and software connections and state the necessary source and destination ports, including port ranges, and services and processes tied to each port required for business operations. Only the required logical network ports and services deemed necessary should be utilized. It is essential to identify approved ports and services to help network defenders manage network traffic through firewalls and intrusion-detection and prevention systems. The best practice is to logically disable/uninstall unnecessary ports and services on all devices within the production environment to mitigate unauthorized access.
In addition, a packet-filtering firewall should be leveraged to look at destination and source addresses, ports, and services requested. At the network layer, only the approved whitelisted ports and services should be accepted. All unauthorized incoming and outgoing traffic should be disabled or blocked.

Security Patch Management

Every applicable major and minor release of security patches and firmware updates from third-party vendors should be tracked and evaluated expeditiously. Test security patches and firmware updates in a controlled environment prior to full production deployment. Confirm that each new device is fully patched before deploying to the production environment. Utilize an application and system scanning tool to validate that security patches and firmware updates are up-to-date.

There is an intricate balance with patch management—security verses availability. There are times when a security patch could impair the behavior of the system or cause downtime. A secured system that is not fully functioning or offline is useless. Meanwhile, an available system with security holes may be subject to various threats. Utilities and their suppliers should be able to assess risk versus reward as well as potential compensating measures. Not all vulnerabilities have related patches, so system administrators must not only be aware of applicable vulnerabilities and available patches, but also of other methods of remediation (e.g., device or network configuration changes, employee training) that limit the exposure of systems to vulnerabilities.

Malicious Software Management

Malware attacks come in many insidious forms, from viruses, worms, and Trojan horses, to hybrids and exotic programs. There are various malware solutions on the market. Choosing the right solution for the appropriate environment can be an overwhelming task. The right solution should at least provide standard and embedded system and application protection and must be updated to receive and distribute the latest definitions. Additionally, the solution should have the option of either agent or agentless deployment. For embedded devices that do not support malware solutions, it is essential to have a layered approach—firewall and intrusion detection and prevention systems. These compensating controls will help cover and reduce potential exposure. Some mission-critical communication systems may not be able to run a malware solution due to an adverse impact on the system and application. In this case, the best option is to exclude the identified and approved directories and executables to maintain a host-based malware solution.

Configuration and Baseline Profile Management

Configuration management should be instituted to reduce unauthorized changes and record implemented changes. Utilities should establish a Configuration Control Board (CCB), which is typically comprised of business unit and information technology managers. The CCB is the organizational group responsible for overseeing all configuration changes to active systems, including approving, disapproving, or deferring a request, managing costs, and minimizing downtime. When a change is presented to the CCB for approval, the system and application owners should be notified before authorization. This allows for review and evaluation of the proposed change to be conducted. After deployment, all parties involved in any update—including vendors, users, and application owners—should be notified to allow time to provide information and training to the operators and support staff affected by the change. Whenever unscheduled changes must be implemented, and time does not allow for a prescribed protocol to be followed, those changes should still be managed and controlled. A solid change-management process that includes proper vetting will help minimize changes that could have an adverse impact on the production environment.

A mission-critical communications system should not only go through change control, but a baseline profile should be established for each device and application. It is important to utilize an automated tool to have an established baseline structure. If any change deviates from the baseline without an approved change control, then the tool should flag such incidents and a specialized team should carefully investigate. If it's a false positive, accept those changes as the new baseline. If not, remove the change and perform testing to ensure the system and application have not been adversely altered or compromised. Validate that both the system and application are in a secure state and working appropriately.

System Access and Alert Notification

Access control begins and ends with an organization's internal policy. The appropriate policy should support local domain or Active Directory authentication. The appropriate data and asset owners should identify approved users and determine access, permission, and restrictions for user roles assigned to a given asset. User access should be restricted based on roles and responsibilities. Role-based access helps prevent unauthorized access to critical and important applications and systems. Further, implementing strong password complexity settings, secure connection, and two-factor authentication will help safeguard the confidentiality and integrity of system and application access. An important aspect of system and application access that is often overlooked is the removal or adjustment of access rights and default credentials. When an employee has been transferred or terminated, or the status of a vendor has changed, the access to electronic systems, applications, and physical facilities should be reviewed, adjusted, and disabled/removed in a timely manner. Also, remove or change default usernames and passwords tied to systems and applications to eliminate the possibility of exploitation.

A Simple Network Management Protocol (SNMP) Manager and SNMP Agent should be installed in the appropriate environment to query, collect, and send system and application information. Whenever a notification trap is triggered (disk capacity, hardware failure, system offline, successful and unsuccessful authentications, password threshold, error messages, etc.), an alert should be sent to the appropriate groups and/or personnel. The alert notification allows system and application custodians to be proactive and help defend the physical and logical security boundaries.

Application Security

Applications, especially web applications, are vulnerable to cyberattacks. The primary problem with an insecure application usually lies in the roots of the software development foundation and process. That's why utilities should expect their mission-critical communication system vendors to participate in an ongoing audit and compliance process for their systems. A vendor that has participated in vulnerability testing, penetration testing, black-box testing, or white-box testing has a proven level of due diligence.

Before procuring an application, energy companies should request NERC-CIP, NIST 800-53, and other relevant security compliance or certification accreditation. Without knowing the status of the application source code and pre-existing vulnerabilities, software defects, and logical flaws, the organization opens their network infrastructure for potential exploitation.

Additionally, utilities should review and use standards that are accepted and instituted for application security such as the Open Web Application Security Project (OWASP). This project is an open, worldwide security community dedicated to enabling organizations to develop, purchase, and maintain applications and application programming interfaces (APIs) that can be trusted. The following page provides an overview of OWASP's Top 10 Application Security Risks, as produced in December 2017, with the general causes for each risk.[7]

[7] "Category: OWASP Top Ten Project," Open Web Application Security Project (2017). https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
The OWASP Top 10 is free to use and licensed under the Creative Commons Attribution-ShareAlike 4.0 license: https://creativecommons.org/licenses/by-sa/4.0/

OWASP's Top 10 Application Security Risks

A1 Injection

Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2 Broken Authentication Exposure

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

A3 Sensitive Data

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged using a browser.

A4 XML External Entities (XXE)

Attackers can exploit vulnerable XML processors if they can upload XML or include hostile content in an XML document, exploiting vulnerable code, dependencies, or integrations. These flaws can be used to extract data, execute a remote request from the server, scan internal systems, perform a denial-of-service attack, as well as execute other attacks.

A5 Broken Access Control

Exploitation of access control is a core skill of attackers. Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) tools can detect the absence of access control, but cannot verify if it is functional when present. Access control is detectable using manual means, or possibly through automation for the absence of access controls in certain frameworks. When they gain access control, attackers can act as users or administrators with the ability to use privileged functions and create, access, update, or delete every record.

A6 Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up-to-date

A7 Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser that can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A8 Insecure Deserialization

Exploitation of deserialization is somewhat difficult, as off-the-shelf exploits rarely work without changes or tweaks to the underlying exploit code. The impact of deserialization flaws cannot be overstated. These flaws can lead to remote code execution attacks, one of the most serious attacks possible.

A9 Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

A10 Insufficient Logging and Monitoring

Exploitation of insufficient logging and monitoring has caused nearly every major incident. Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected. Most successful attacks start with vulnerability probing. Allowing such probes to continue can raise the likelihood of successful exploitation to nearly 100 percent. In 2016, identifying a breach took an average of 191 days — plenty of time for damage to be inflicted.

OWASP developed this list to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. This guidance and these basic techniques will help protect against high-risk problem areas.

To this extent, application development frameworks, such as the OWASP-developed Software Application Maturity Model (SAMM), have been developed, instituted, and implemented by many software and systems companies over the past few years, providing a guide for software security strategy, evaluation, and measurement. System and application security, however, must be an ongoing process, not a destination. There is no bulletproof solution to completely protect or isolate systems and applications from being compromised by threat actors. To better manage and protect systems and applications, it is essential to examine governance and administrative policies, operational and technical risks, and implemented controls. With a good foundation and understanding of risk and control management, organizations can better protect, mitigate, and manage cybersecurity risks.

Above all, the implementation of a comprehensive security ecosystem starts with a paradigm shift throughout the organization, from senior officers to end users. Without proper management support and a culture of continuous improvement that includes ongoing security awareness training, organizations will struggle and likely fail to defend their systems and applications.

The internal and regulatory pressure to protect systems and applications is already enormous. As the public learns more about emerging threats and vulnerabilities, they put on more pressure for an urgent response. Businesses and organizations then push vendors and manufacturers to quickly develop security patches and hotfixes to protect or mitigate system and application holes and exploitations. While the urgency is real, it's easy to overreact in such an environment, resulting in quickly developed solutions that can cause adverse impacts on hardware and software. Software repairs require testing and review of the patches themselves. Installing these software components quickly can, and often does, lead to other software, hardware, and system deficiencies and weaknesses that are open to unforeseen compromise. Therefore, it's important for utilities to follow a methodical development, testing, and implementation process, such as the OWASP-based SAMM, to mitigate the introduction of any other potential vulnerabilities.

Web Application Development

Applications running with web enablement make up most of the development in today's rapidly advancing technology market. Multiple lessons have been learned since the World Wide Web was invented in 1989 with respect to conducting secure transactions and communications. Some of these lessons include such things the deployment of web-application firewalls (WAFs) between web servers and the internet, and validating inputs and testing by ensuring inputs are within the expected range.

Other advancements include handling errors and exceptions with invisibility to the user so motivated attackers cannot get additional information about potential weaknesses in the application, and creating self-monitoring software that monitors the user's activity to flag unusual events and actions.

Development Life Cycle

Mission-critical communication technology vendors may have different software development life cycles (SDLC), but the goal of any energy organization is to understand pre-existing software weaknesses and mitigation steps. Applications are usually compromised because of poor programming practices. Utilities should implore vendors to use secure software best practices like DevOps and other secure techniques to decrease the chances of repeating known software bugs, defects, logical flaws, and vulnerabilities. Establishing application security requirements, designing application security architecture, implementing standard security controls, continuously monitoring and improving the secure development life cycle, and enforcing application security education will create a more secure software ecosystem.

Find out which programming language each software vendor or development organization uses. There are many different software languages and code development techniques, each with known strengths and weaknesses. Ensure that all software developers receive training in writing secure code for their specific development environment and language.

Application Testing

Utilities and their suppliers should use these four recommended application testing methods to ensure the safety of the software used in especially critical energy sector applications:

1. **Static Testing of Software (SAST)**, which involves software code reviews, line-of-code logic reviews, and automated software exams that search for errors in the logical structures and flaws in the implementation of routines.

2. **Dynamic Testing of Software (DAST)**, which checks the software in action to see if it actually works and how well it produces the expected outcomes.

3. **Testing the application while connected to other software**, which will reveal how the application performs when connected to and communicating with other applications and output devices. All components and applications need to be reviewed and evaluated to show operational status, expected behaviors, and expected outputs.

4. **Production level testing of the application** must occur before going live. Regulators usually require operational testing of applications and systems to show both risk management and due diligence in employing new components. This type of testing is conducted as the last step prior to the application being deployed in the production environment. This level of testing often uncovers communication errors or deficiencies in design or development of software that supports equipment deployed in the field.

Part II: Conclusion

The DHS and FBI have reminded the energy industry that it continues to be a prime target for cyberattacks. Hackers have proven that, under the right circumstances, they can find a path into staging targets, gather info, and move on to intended targets. And they're relentless in their efforts to break through any barriers erected to keep them out.

With this as the backdrop, it's fair to say a utility's cybersecurity posture is only as strong as its weakest link. With third-party suppliers and vendors increasingly being used as staging targets, they have the potential to become this weak link unless they are fully vetted and can demonstrate they are able to meet cybersecurity requirements for systems and applications. Consider this: All it takes for a serious breach is for a hacker to learn the password of a vendor's employee who has access to the system. And there are, unfortunately, many other opportunities.

All energy organizations and vendors must protect and defend their technologies, systems, applications, and communications with even more vigor, imagination, intelligence, and resources than the hackers who are attempting to break in. From the smallest suppliers to industry leaders, all systems and applications must be protected and secured starting with how they are built, transported, and installed through how they are used, maintained, and updated. The focus must be on all mission-critical systems and applications, including those used for communications.

Transforming Your Utility's Tech Partners into Cybersecurity Allies

Utilities rely on numerous third-party vendors to support core business functions, including command center and dispatching communications. What this means in practical terms is that effective cybersecurity management is no longer the responsibility of a single organization.

Ronald Keen, senior energy adviser at the Department of Homeland Security's National Risk Management Center, believes the days of companies independently defending themselves "are pretty much gone. We need to begin looking at cohesive defense: defense where we're working together. We need to be able to start working together to design multilayered defenses that work with each other."[1]

A guide from the National Institute of Standards and Technology (NIST) echoes Keens sentiments and points to the vulnerabilities and challenges presented by what are often complex, interconnected systems and networks: "Energy companies rely on operational technology to control the generation, transmission, and distribution of power. While there are a number of useful products on the market for monitoring enterprise networks for possible security events, these products tend to be imperfect fits for the unusual requirements of industrial control system (ICS) networks...A network monitoring solution that is tailored to the needs of control systems would reduce security blind spots and provide real-time situational awareness. To improve overall situational awareness, energy companies need mechanisms to capture, transmit, view, analyze, and store real-time or near real-time data from across ICS and related networking equipment."[2]

[1] Brooks, Michael, "Experts Urge Utilities to Train, Collaborate on Cybersecurity," *RTO Insider*, December 10, 2018. https://www.rtoinsider.com/federal-energy-policy-summit-cybersecurity-107607/

[2] National Cybersecurity Center of Excellence, National Institute of Standards and Technology (NIST) Special Publication 1800-7, *Situational Awareness for Electric Utilities*, (2017). https://www.nccoe.nist.gov/projects/use-cases/situational-awareness

AVTEC

Phone: 1.803.358.3600 • avtecinc.com
100 Innovation Place • Lexington SC 29072 USA

Both of these viewpoints (DHS and NIST) highlight the need for utilities to evaluate and connect the communications of their systems with each other as well as the various third-party systems found throughout control rooms and operational facilities that generate and deliver energy products and services. Utilities have many components and systems installed and used in today's production environment, but how do they know if these systems are secure in light of the current cyberthreat environment in which we live and operate? With the current state of a "breach a week" and consistent reminders of another cyber compromise just around the corner, what can utility managers do to ensure the best possible security?

Communications and Systems Security

Utilities can start with mission-critical communications and systems security postures and understand the requirements needed to create and deploy good and practical security for equipment, components, and operational activities. Connection paths and exchanges of information all require a focus on identifying and protecting critical information that can become compromised or altered.

Defining Cybersecurity

The standard definition of cybersecurity is the protection of information assets by addressing the threats to how it is processed, stored, and transported by internetworked systems. This definition provides the key to communications and systems security—at the core, those responsible for cybersecurity must thoroughly understand the internetworked connections and the paths information flows over in order for the utility to be able to buy, sell, and conduct the normal business activities each day.

Protecting Communication Structures

Communications structures on the network are vital to the operations of any networked activity. These structures require many components to interchange information to other parts and equipment on the network as well as externally to outside devices and connections. The traffic that flows on these structures connects all of the various equipment, servers, workstations, and laptops and requires internetworked data exchange to work properly. Data exchange points are often where cybercriminals will steal data and user passwords from unsuspecting users. Using various forms of encryption on the links between these devices will stall or stop these malicious efforts and is highly recommended in today's networking environments.

Network managers should begin with the basic network data component, the packet, and from there start to build the parts of the data exchanges that travel the network. Each device adds to and subtracts from these data exchanges as they traverse the network, which is moving the data from one location to another all the time. Since this data is always moving, at each point where it touches another device, managers should ensure there is a record of that activity in logs for further review. This gives the engineers data to monitor the health of the network for checks and balances on the components and parts of the network. The network administrators then review these logs for proper actions and activities to ensure all data is safe and secure as it is processed throughout the network path and traffic flow.

As the Department of Energy's 2018 energy cybersecurity plan states: "Energy control systems are specially designed digital systems that operate real-time physical processes by dispatching commands to millions of nodes and devices dispersed across the energy delivery infrastructure. These systems exchange massive amounts of data at high speeds over cyber networks to monitor and control physical devices such as transformers, switches, compressors, pumps, and valves. This makes data availability and integrity of paramount importance to energy operations."[3]

[3] U.S. Department of Energy, Office of Electricity Delivery & Energy Reliability, *Multiyear Plan for Energy Sector Cybersecurity*, (2018). https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf

System-Level Security Evaluations

It's important for utilities to know that third-party vendors have evaluation criteria for all applications in both a developmental and operational environment to ensure systems, network functions, and computing machines operate optimally.

Security Evaluation Best Practices

It's also a best practice to evaluate software and system-level defects and bugs prior to final operational approval, and the processes needed for this management review effort should be both detailed and well as high level in their implementations. Utilities should ask third-party vendors if they are compliant with reliability standards developed by the North American Electric Reliability Corporation (NERC) and NIST's Cybersecurity Framework, as well as other industry standards that have been developed over the past 30 years.

Testing of Systems and Applications

In the application development environment, utilities should expect vendors to conduct testing and review of the actual software code components as they are developed to make sure the code is designed and written correctly, as well as when components are placed together with related pieces of code to ensure proper and correct functioning. Once the vendor tests a module and combines it with other developed portions of code, the resulting unit that is created should be evaluated for proper logic flows, functioning, and completeness, all to ensure there are no bugs in the software or activity. Often units are assembled together to provide the full system software, which is also tested to prove it provides the intended functions, logic, actions, and results the programmers intended it to produce. This is a vital step in the development process, since it shows the requirements for the development are being met by the software as well as showing the code is operating as intended. Finally, the system-level examination should be performed, and this process is often conducted by outside reviewers. This step gives utilities an external view into the operation of the application and its software to provide proof the application is functioning properly and proficiently with respect to its intended purpose. This review often results in the discovery of software defects in the code—typically referred to as "bugs"—and identifies possible weaknesses in the logical flow of the processing. These defects and weaknesses are then assigned to the vendor's programmers for repair and redesign. All of these evaluation efforts are designed to provide the software developer, systems integrators, and end users with the evidence needed for compliance to user requirements, development standards, and regulatory mandates.

Once of this effort is completed, utilities should expect the vendor to conduct operational testing of the full application to show that it will work properly in its intended operating environment with all of the other applications, systems, and devices the application will be operating with under normal circumstances. Upon successful completion, the utility should conduct a formal user acceptance test, which provides all stakeholders with the required reviews, tests, and formal acceptance of the application.

Rigorous operational testing provides utility management assurance that the system under review is meeting the operational requirements, that the user interactions with the system will not impede operations or security of the system, and that the security of the system meets or exceeds mandated requirements for confidentiality, integrity, and availability.

Security Testing

Vulnerability management is critical to the security and operations for all cyber-based systems and starts by understanding the cybersecurity assets and where they reside—both physically and logically.

Vulnerability Management

Therefore, the first step in the operational testing previously mentioned is for the utility to conduct vulnerability scan testing of the applications and systems on its network during operations. This step is critical to determining the health of the systems while they are running and producing the expected results. There are many vulnerability scan tools available today, and it is important to test scanners to ensure they are both functional and safe in the operating environment and will not interrupt the operations of the utility's other applications and systems. Each of these scan tools will need network connectivity to the outside environment as they are often connected to the National Vulnerability Database maintained by the U.S. Government, which defines and lists all of the known vulnerabilities for operating systems, applications, databases, and platforms currently in use around the world. Some of the best practices with use of these scan tools include a scheduled scan time and sequencing after systems and applications are patched, results tracking reporting, and rescans after repair to confirm proper configurations of systems to minimize cyberexposures to internal and external risks.

Another area utilities should look for with third-party vendors is their security use case/abuse case testing of systems and applications. This type of testing centers around trying the "break" the system by testing the potential areas of deficiency on the system and flooding the system with deviations of inputs from the user perspective. Overloading the input fields with extra data, sending incorrect inputs into the system, and sending thousands of possible inputs in rapid sequences (called "fuzz" testing) are all ways to conduct this type of abuse case testing. The intent is to determine the error handling capabilities of the application or system and to ensure the application design accounts for these types of situations successfully and does not fail under duress.

Third-Party Vendor Testing

Utilities should also expect third-party vendors to test applications and systems from the outside through penetration testing. In today's cyberclimate, the ability of the hackers to identify exposures and vulnerabilities of the system through external testing is a very common practice. Penetration testing emulates these actions by the "bad guys" by utilizing the same tools and techniques that they use. Penetration testing allows a utility to identify potential deficiencies and weaknesses in the system and application security posture before the negative effects are realized and a breach happens. There are typically two types of these testing efforts. One is called "white-box" testing and is typically conducted by a known group call the "blue team." This testing focuses on evaluating the applications and systems from an understanding of the applications and systems themselves. The other type of penetration testing is called "black-box" testing and is often conducted by a "red team," which attacks the system from outside without knowing any of the internal network or particulars of the applications at all. This effort completely emulates what outside hackers and criminals do when they attack a system. This process often produces results that identify deficiencies in the security posture, the security control implementations, and the security actions taken by the utility's cyberdefenders. Test results are then used to update and provide inputs to security remediation efforts of the software vendor to improve the security of the applications and systems.

Security Baselines

Once a new system is implemented, utilities need a reference for the system operations, maintenance, and security staff to compare the current status and operation to; this reference is typically known as the security baseline.

Minimum Security Baselines

Utilities should use this security baseline to manage and evaluate any change or particular event on a third-party system or application to gauge any differences in operations, maintenance, and security. The process for setting baselines requires a utility to identify the inventory of their IT assets, determine the current state of each inventoried item, then set the minimum security and configuration of that asset. Once that process is accomplished, the system or application settings, configurations, patch level, and minimum user settings are all recorded, and a master list is created with all pertinent data. This result is then called the Minimum Security Baseline (MSB) for that system or application, and the utility can use this MSB in a variety of tests during operation of that system or application to ensure continued security and operation criteria are met.

This MSB of operations, metrics, controls, and configuration settings is often controlled through a utility's formal configuration management system. This process allows for performance and measurements against security standards and risk frameworks, which produce results for compliance and legal attestation purposes with additional proof of security of the system or application being assured to a measurable level for the utility and its third-party vendor. This MSB promotes the development, implementation, and operation of more secure information systems by establishing minimum levels of due diligence for information security and facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems that meet minimum security requirements.

The concept of the MSB is also adjustable for the operation of systems and applications. Utilities should review security controls at least annually and, if necessary, revised and extended to reflect:

- Experience gained from using the controls.
- Any changing security requirements.
- New security technologies that may be available.

Operations and Maintenance for Applications

Once utilities deploy systems and applications, they should continue efforts to maintain the security status while in operation. The first and primary focus for a utility should be on system and application patch management.

Patch Management

Patch management is the process of receiving, evaluating, and then applying vendor patches to systems and applications during operational activities. Patches are issued by the vendor to repair identified deficiencies or weaknesses in their software or applications. Vendors typically issue patches on a predetermined schedule to help maintain the security and performance of their product. Once the patch is received by the utility, system managers should evaluate the applicability of the patch within their operating environment, test the patch in a non-production environment to assure the patch does not break any feature or required process, then install it as soon as possible in accordance with the utility's configuration management process and the criticality of the patch.

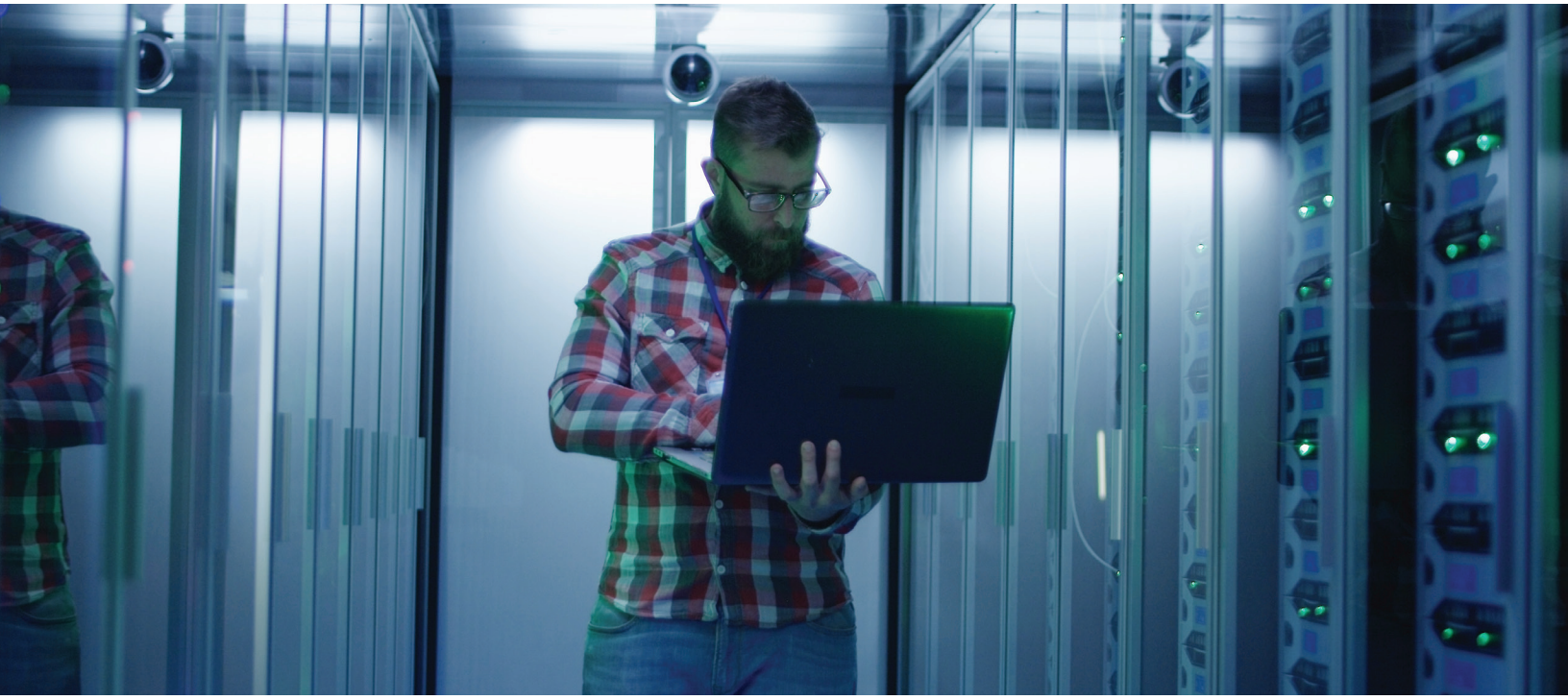
A utility's third-party vendors should always test patches before release, but that testing is typically somewhat generic in nature, so it is vital that the utility test the patch itself before deployment. The Equifax data breach in 2017, which affected the personal data of 143 million people, was a high-profile yet all-too-common situation that can be avoided by comprehensive, timely patch management. As news reports portrayed: "Equifax...confirmed that attackers entered its system in mid-May through a web-application vulnerability that had a patch available in March."[4] Clearly, patching is a critical activity for any organization—utilities especially—in today's cybersecurity environment.

[4] Hay Newman, Lily, "Equifax Officially Has No Excuse," *WIRED*, September 14, 2017. https://www.wired.com/story/equifax-breach-no-excuse/

Status Reporting

Reporting on the status and the operation of each system and application is another typical cybersecurity effort utilities should conduct during the operations and maintenance phase for any system. Current activities, patches applied, remediation efforts completed, new vulnerabilities identified, and changes in configurations are all among the typical reportable events that are often included. These reports are focused on the systems and applications critical to the utility and its business objectives for successful accomplishment of the system or application's job. How the users are interacting with the system or application and the current status of the system or application are also often included in the reporting efforts.

Since each application or system has a unique operating environment and user base, utilities must identify and track this information system by system in order to properly understand the security profile and needs of the utility in relation to this profile. As the systems and applications evolve through changes in inputs, configurations, outputs, uses, and environment, the utility should track any variables in the system or application to help support long-term IT health and security. This also allows the utility to gather historical data of the system for trend analysis and long-term strategic reviews needed for future growth and operational needs analysis.



Part III: Conclusion

The DOE's energy cybersecurity plan succinctly outlines three overarching areas of concern, which underscores the need for utilities to work collaboratively with government agencies, third-party vendors, and industry associations to mount a comprehensive defense for systems and applications implemented by utilities to support core business functions:

- "Energy owners and operators have integrated advanced digital technologies to automate and control physical functions to improve performance and adjust to a rapidly changing generation mix. This has created a larger cyber attack surface and new opportunities for malicious cyber threats.
- The frequency, scale, and sophistication of cyber threats have increased, and attacks have become easier to launch. Nation-states, criminals, and terrorists regularly probe energy systems to actively exploit cyber vulnerabilities in order to compromise, disrupt, or destroy energy systems. Growing interdependence among the nation's energy systems increases the risk that disruptions might cascade across organizational and geographic boundaries.
- In response, the government and private sector continue to increase their spending on cybersecurity operations and maintenance. Despite improving defenses, it has become increasingly difficult for energy companies to keep up with growing and aggressive cyber attacks."[5]

The cyberbasics of system and application patching, managing communication and system-level connections, and testing everything that can be evaluated is without doubt more important than ever for those charged with overseeing a utility's internetworked systems.

[5] U.S. Department of Energy, "Multiyear Plan for Energy Sector Cybersecurity."

Glossary of Terms

Active Directory authentication
Microsoft® based access control application that facilitates user acceptance onto the system or computer.

Application programming interfaces (APIs)
Application software designed to allow for the interexchanging of data and commands between applications and programs.

"Black box" testing
The process of evaluating the performance of a system or application without knowing the underlying operating characteristics of the system being tested.

Blue team
An organizational component designed to assist the operations staff in determining the best approaches to cybersecurity by evaluating the components in operation.

Bulk Electric System (BES)
As defined by the North American Electric Reliability Corporation (NERC), this is comprised of all transmission elements operated at 100 kV or higher, as well as real power and reactive power sources connected at 100 kV or higher.

BES cybersystem
One or more cyberassets logically grouped together to perform a reliability task for a functional entity.

Checksum
A digital number representation of the sum of the stored or transmitted data used for the purposes of ensuring the data has not been altered.

CIP-013-1
The NERC standard designed to mitigate cybersecurity risks to the reliable operation of the BES by implementing security controls for supply chain risk management of BES cybersystems.

Clustering
The process of connecting different computers together in a unique method so these devices will work together as a single system.

Configuration control board (CCB)
The organizational entity that oversees and manages changes to network components, devices and applications when a system is in an operational environment.

Corporate cybersecurity council
Typically, the oversight board in an organization or corporation tasked with management and governance of the cybersecurity activities in the organization.

Cross-site scripting (XSS)
A type of computer security vulnerability typically found in web applications.

Cyberasset
Programmable electronic devices, including the hardware, software and data in those devices.

Cybersecurity
The protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems.

Cybersecurity ecosystem
The full spectrum of organizational activities, manpower, applications and networks within the cybersecurity area.

Cybersystem
Internetwork information system, including all hardware and software.

Device access control
A security technique that regulates who or what can view or use resources in a computing environment.

DevOps
A methodology of software and application development by which developers and operations staff work together during the development lifecycle.

DOE Multiyear Plan for Energy Sector Cybersecurity
Department of Energy guide produced in March 2018, designed to improve the cybersecurity of the U.S. energy system.

Dragonfly
Nickname of a cyberespionage group focused on electrical providers and management organizations.

Dynamic application security testing (DAST)
A method of testing application software while it is running by, typically, applying a wide range of inputs and evaluating the results.

Encryption
The process of converting plain text data into unknown and unreadable data to ensure confidentiality.

Energy Independence and Security Act of 2007
Signed into law on Dec. 19, 2017, with an aim to move the U.S. toward greater energy independence and security.

Equifax data breach of 2017
A data breach, suffered by the credit reporting organization, which released 146 million credit reports to an undisclosed group through an unpatched web application.

Federal Energy Regulatory Commission (FERC)
A U.S. government independent agency that regulates the interstate transmission of electricity, natural gas and oil.

FERC Order No. 829
Outlines reliability standards concerning supply chain risk management for industrial control system hardware, software and computing and networking services associated with BES operations.

Firewall
A network flow component that manages data traffic and delivery, and provides edge protection, based upon specific requirements and specifications.

Firmware
Specialized software developed to run the CPU of a computer.

Generation, transmission and distribution of power
The full scope of the delivery of electrical power for consumer consumption.

Hashing algorithm
A mathematical formula designed to convert variable length input files or data streams into fixed length output as a means of ensuring data integrity.

Identity assurance
The concept of the trustworthiness of a user's identity when signing into a computing device.

Industrial control system (ICS)
Computing systems designed to monitor and control physical processes in many different industries and sectors.

Information security operations center (ISOC)
An entity focused exclusively on information assets and their security.

Injection flaws
Vulnerabilities that allow cyberattackers to insert malicious code in another system using an application.

Insecure deserialization
A vulnerability that occurs when untrusted data is used to abuse the logic of an application, inflict a denial of service (DoS) attack, or even execute arbitrary code upon its deserialization.

Intended targets
The final devices or machines that contain information desired by cyberattackers.

Intrusion detection and prevention
The process by which network devices monitor and identify malicious or suspect actions taking place on the network.

Local domain
The closest management of connected devices and computers to each other with similar activities or roles.

Logical control
Software safeguards to protect an organization's systems, including user identification and passwords, authentication, and access/authority levels.

Malware
Malicious software often designed to corrupt or steal user data.

MD5
A hashing algorithm used for integrity verification and protection of data.

Minimum security baselines (MSB)
Standards for all systems on your network, ensuring that they meet a set of minimum requirements in order to avoid putting your entire network at risk.

Mission-critical communications system
The most important system for accomplishment of data and/or voice activities during operational activities.

National Institute of Standards and Technology (NIST)
U.S. government agency responsible for developing and providing the recommended standards and guidelines for computer security, cybersecurity and privacy for all agencies and departments.

National Vulnerability Database (NVD)
A listing maintained by the U.S. government of all known deficiencies, flaws or identified weaknesses in software, hardware, applications, operating systems software and databases in a public forum.

Network monitoring solution
A tool or system that constantly monitors a computer network for slow or failing components and notifies the network administrator in case of outages or other trouble.

Network path and traffic flow
The connections and directions taken by data packets as they traverse the network to get to their destination.

NIST 800-53
The NIST Special Publication (SP) that lists all available security and privacy controls for implementation in computing systems and applications.

NIST 1800-7A
The NIST SP that focuses on the situational awareness activities for electrical utilities.

NIST Cybersecurity Framework (CSF)
A policy framework of computer security guidance for how U.S.-based private sector organizations can assess and improve their ability to prevent, detect and respond to cyberattacks.

NIST National Cybersecurity Center of Excellence (NCCoE)
A U.S. government organization that helps coordinate public and private resources for risk mitigation strategies.

North American Electric Reliability Corporation (NERC)
A not-for-profit international regulatory authority overseeing the bulk electricity risk posture for most of North America.

North American Electric Reliability Corporation Critical Infrastructure Protection standards (NERC-CIP)
A set of requirements designed to secure the assets required for operating North America's bulk electric system.

Open Web Application Security Project (OWASP)
A non-profit organization focused on improving software security.

Parallel processing
The practice of simultaneously breaking up and running program tasks on multiple microprocessors to expedite processing.

Patch management
The process used for identifying, evaluating and applying security patches to operating systems and applications in a structured and systematic manner.

Penetration testing
The practice of emulating malicious outside attacks as a means of evaluating potential ways to breach a network.

Phishing
A technique used by hackers where an email is sent that appears to be from a legitimate organization in order to obtain sensitive information such as passwords or account numbers.

Physical access control
The management of people entering and exiting a room, building or facility.

Plan of Action and Milestones (POA&M)
U.S. government process for fixing and repairing identified deficiencies in systems and operations that place an organization at risk.

Ponemon Institute
A security research institution, founded in 2002, that primarily focuses on data protection and emerging information technologies.

Ports
The network address of a transmission connection through which data is transported.

Protocols
A set of rules for network communications based on the criteria of the data to be sent or received.

Red Team
An organizational component designed to test operational security by attempting to penetrate the system from outside.

Requests for proposals (RFPs)
A contract document that delineates the methodology and process to meet the requirements of a proposed project.

Risk Management Framework
A guide developed by NIST to manage risks to organizations and agencies in an ongoing and continuous manner.

RJ-45 ports
The connection ports used to provide connections between customer devices and telephone company wiring.

Role-based access control (RBAC)
A method of access control whereby all access is managed via standard roles rather than by individual identities.

Secure data exchange
The process by which data flows between users and computers in a confidential manner.

Secure intrasystem communication
The activity of ensuring the confidentiality of data flowing within a system while being transmitted and received.

Security baselines
Refers to the current security structure of the system or application as designed and implemented.

Security Incident Response Team (SIRT)
The corporate organization with the responsibility to respond to and fix incidents that can have an adverse impact upon the organization and its operations.

Security Operations Center (SOC)
The corporate department tasked with monitoring and responding to cybersecurity events, incidents and response efforts.

Security patch
Software code developed to fix deficiencies and weaknesses in deployed software applications and programs.

Services
The various types of activities delivered by computing devices.

Simple Network Management Protocol (SNMP) Manager
The SNMP-based application that monitors a group of SNMP-capable devices on a computer network.

SNMP Agent
An application/interface that can be enabled or installed to provide SNMP connectivity from an SNMP manager. Data is sent via the SNMP protocol back to the SNMP manager, providing health of the device such as resource utilization, issuing SNMP traps as alarms identifying anomalies in operation, and allowing for polling of a device if maintained communication isn't available.

Software Application Maturity Model (SAMM)
An OWASP-developed open framework used to implement strategies for software security around organizational risks.

Software development life cycle (SDLC)
The organizational program used to manage and direct the development of systems, applications and components as they are implemented with the organization, covering all areas from conception to system retirement and disposal.

Source code control management
The process of managing and controlling modifications or alterations to basic software code.

SP 800-161
The NIST Special Publication that focuses on supply chain risk management practices for agencies and organizations.

Staging targets
The intermediate devices or machines compromised during a cyberattack as a means to access the intended target.

Statement of work (SOW)
A contract document that specifies the exact requirements and deliverables to be developed in support of the project.

Static application security testing (SAST)
A method of source code analysis that looks for logic or coding flaws in software prior to compiling the code into a program.

Supplier business continuity plan
The organizational plan for handling interruption of business activities of service providers and suppliers.

Survivability
The concept of maintaining operations in a hostile or corrupt operating environment.

System data encryption
The process of using cryptography on data to maintain its confidentiality during use.

Threat agent protection
The concept of preventing and interrupting the actions and activities of potential malicious perpetrators – also known as threat agents.

Trojan horse
A type of software that carries a malicious payload inside other software that appears normal.

Universal Serial Bus (USB)
A connection-based communications protocol used on hardware, computers and devices.

User acceptance testing
The final gauge of a new application or system, used to ensure that it meets the needs and requirements of the intended user.

Utility sector control systems
Operational technology systems used to monitor and control physical devices, assets, and processes, including ICS.

Virus
A malicious program that infects machines and computers as a means of attack on the data held on the machine.

VMware
A publicly traded software company that originated the computer process of virtualization.

Vulnerability management
The organizational program for identifying, managing and repairing the various weaknesses and flaws identified in software and hardware in an organization.

VxWorks
A real-time operating system used in embedded systems.

Web-application firewalls (WAFs)
Application-based software components used to manage and control incoming data that uses internet-based protocols of delivery.

"White box" testing
The process of evaluating the performance and design of a system or application using known and understood processes.

Worm
A type of virus which is self-propagating and needs no user action once a computer is infected.

XML External Entities (XXE)
An application that accepts XML directly or XML uploads, especially from untrusted sources, or inserts untrusted data into XML documents, which is then parsed by an XML processor – making a system vulnerable to attacks.

Additional Resources

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

OWASP Top 10 (2017)
https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

NISTIR 7298, rev. 3 – Glossary of Key Information Security Terms (2019)
https://csrc.nist.gov/publications/detail/nistir/7298/rev-3/final

CNSSI-4009 CNSS Glossary – Committee on National Security Systems Glossary (2015)
https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

NIST Special Publication 800-37, rev. 2 Risk Management Framework for Information Systems and Organizations (2018)
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Framework for Improving Infrastructure Cybersecurity v. 1.1 (2018)
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

1.800.310.7045
1.803.358.3620
www.avtecinc.com

sales@avtecinc.com
100 Innovation Place
Lexington, SC 29072 USA

11.2019