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.

AVTEC

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

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.

AVTEC

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

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.

AVTEC

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

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/

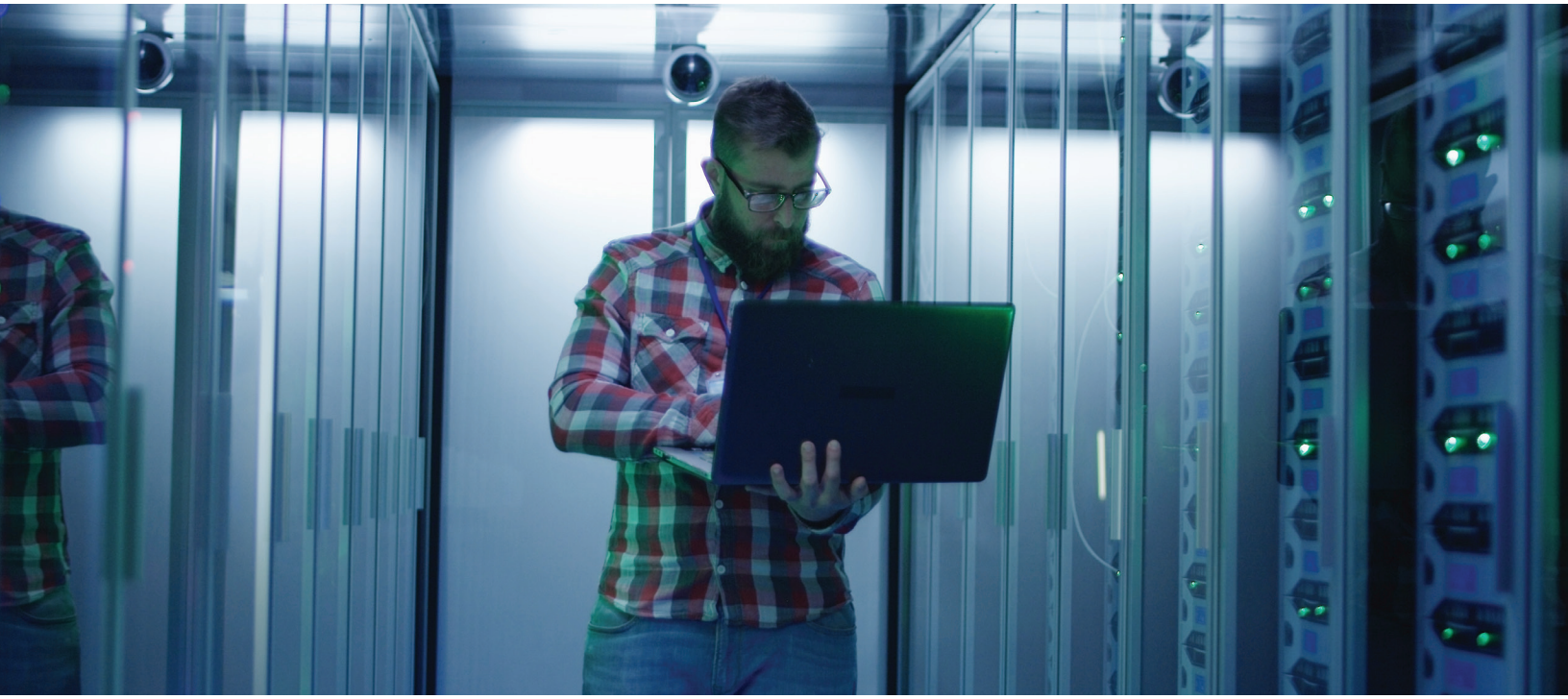
AVTEC

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

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.



AVTEC

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

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."

Avtec and the Avtec logo are trademarks or registered trademarks of Avtec. Scout™ is a trademark of Avtec. Inc.

Third party trademarks mentioned are the property of their respective owners.
The use of the word partner does not imply a contractual relationship.

AVTEC

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