BRADFORD NETWORKS

» WHITE PAPER

Always On. Always Up.

How Network Security Enhances Cybersecurity Initiatives in the Energy and Utilities Sector

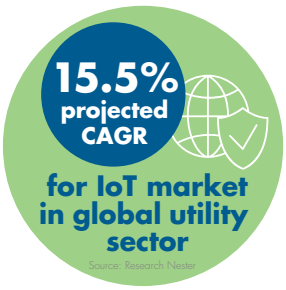
www.bradfordnetworks.com

Cybersecurity is Front and Center for the Energy and Utilities Industry

Breaches in this industry have been widely documented and understood. The multiple mega trends that are converging for this industry – primarily digitalization, increasingly diverse infrastructure, and aging technology – is being met head-on as the complex network of companies unite to address the growing issue of cybersecurity.

By 2018 the oil and gas industries could be spending $1.87 billion USD each year on cybersecurity.[i]

In Utility Dive's fourth annual State of the Electric Utility Survey, more than 600 utility professionals named cyber and physical security the most pressing concern for their companies, with 72% saying it is either "important" or "very important" today.[ii]



According to the consulting firm Research Nester, the IoT market in the global utility se tor is projected to register a compound annual growth rate of 15.5% during the forecast period of 2016-2023.[iii]

The MIT Energy Initiative's recent Cybersecurity white paper cited "The increasing interconnectedness of electricity grids and other critical infrastructure along with higher penetrations of distributed energy resources will increase digital complexity and attack surfaces, and therefore require more intensive cybersecurity protection."[iv]

Rising to Meet the Security Challenges in the Energy and Utilities Sector

Managing the security of dispersed facilities and systems is a challenge of unique scale and complexity for energy providers and other utilities. Operational technology networks weave a complex web of industrial control systems (ICS) that can include Supervisory Control and Data Acquisition (SCADA) systems and programmable logic controllers, or distributed control systems, all of which must be maintained for efficiency and reliability while also being secured from attacks as they become increasingly internet-facing. Opening these systems up to the internet can offer great benefits for managing delivery processes, auditing maintenance tasks and understanding system performance in real-time, but they also introduce a new set of risks to highly distributed systems that may only rarely be seen by IT personnel, if ever.

The Energy and Utilities Operations Sword of Damocles

Given the criticality of what the ICS may provide, it's not an easy ask to merely take one offline to deploy a new patch, so often these systems will sit without updates for months, if not years. This may ensure no interruption in service in the short-term, but it can introduce bigger problems in the long-term if these machines remain increasingly vulnerable yet interconnected to the OT network at large. The internet-enabled systems and devices used in utilities, with all their benefits and innovations, can be a sword of Damocles: They've created a massive attack surface, but it's one that's not yet as mature as other more established components of the infrastructure, leaving the organizations that use them potentially significantly exposed. As we saw with the massive disruptions after WannaCry and NotPetya emerged this year, threats today move very quickly. They also have a rich environment to attack in unpatched or out-of-date endpoints that serve as an entryway to vulnerable — and valuable — networks.

Breaches have global implications

Indeed, these attacks are finding fertile ground in the systems that power our critical infrastructure. NotPetya specifically targeted oil and gas production systems and worked to gain administrator access on vulnerable systems. It then pivoted to take down networks, stealing credentials and encrypting data for ransom. When the Stuxnet worm made the rounds in 2010, its primary goal was to infect and take down SCADA systems. Though the worm is commonly thought to be a targeted attack at a nation-state, once the worm was unleashed it caused a lot of collateral damage to industrial control systems across the world, far beyond its conjectured initial target. Hardening these systems against attack is a race against time despite the high stakes and urgency — for example, the very first ICS village at DEF CON started in 2014, a full four years after Stuxnet.

That's why improving the defensive capabilities in the energy and utilities sector is of increasing concern for providers and for government regulators. Attackers also know the stakes are high for key infrastructure and utilities, which is why these systems can prove such a tempting target. Keeping grids online is not a matter of mere inconvenience for customers. The potential for disruption and impact can't be overstated.

Compliance Regulations and Standards: Where to Start?

Compliance regulations add additional difficulty to catching what can feel like a moving target, but they are crucial in keeping up with the ever-changing landscape that energy and utility providers face. There are a number of security standards that apply to these providers in North America.

- The International Organization for Standardization (ISO) maintains a number of standards known across industries, such as the 9000 series for quality control, and more recently, the ISO/IEC 27000 series specifically for information security management systems (ISMS). This broad set of guidelines relates to controls that fall under an ISMS purview, including potential metrics, baseline requirements, and various tactics relating to building and maintaining an information security practice.
- The National Institute of Standards and Technology (NIST) Cybersecurity Framework outlines controls that any infrastructure or utility organization should have in place to address all stages of the security lifecycle, but largely leaves implementation details to the organization's discretion. Still, the scope of NIST's Framework is very broad — it does make strategic prioritization easier with built-in parameters to determine what controls to address first. NIST compliance became a requirement of all federal agencies as of 2017. It should be noted that the American Petroleum Institute standards support adoption of NIST's Cybersecurity Framework, and the Pipeline and Hazardous Materials Safety Administration (PHMSA) and ICS-CERT reference the NIST Framework as well.
- The North American Electric Reliability Corporation (NERC) critical infrastructure protection requirements are only for electrical providers, and their compliance mandates cover both cybersecurity controls and response as well as physical security and employee security training. The Federal Energy Regulatory Commission works in conjunction with NERC on cybersecurity standards, and its mandate in overseeing reliability of the bulk power grid includes ensuring reliability and security in the IT systems that operate the grid.
- The Federal Information Security Modernization Act (FISMA) specifically applies to the stewardship of government data, and any entity, public or private, that interfaces with or provides data to the U.S. federal government must be in FISMA compliance.
- Energy Expert Cyber Security Platform Expert Group has identified 39 gaps not covered by existing legislations. These gaps must be closed in order to achieve a sufficient level of assurance of cybersecurity in the energy sector.

Outside of compliance regulations mandated by industry or government associations, many standards (like ISO/IEC 27K or the NIST Framework) are optional to adopt, but highly recommended as a goal for energy and utility providers to work towards.

Energy & Utilities: Adopt Best Practices From Enterprise Brethren

Keeping up with market disruptions, securing resource delivery and complying with multiple stringent compliance standards is no small order. Security automation and orchestration solutions like Network Sentry from Bradford Networks help utilities and energy delivery organizations rise to meet and surpass these challenges.

Widely deployed across industries with similar cybersecurity challenges and needs, Network Sentry can especially help utilities secure highly distributed endpoints and their networks from SCADA-seeking malware by detecting endpoints with unpatched vulnerabilities. Network Sentry then instantly and automatically removes them from the network until they are sufficiently patched. Administrators can easily set controls to exclude unsafe endpoints automatically or send users to a self-remediation page if appropriate. Once the endpoint is up-to-date, Network Sentry will automatically bring that endpoint back into the network from a central dashboard, all without needing additional overhead or visiting remote sites.

Network Sentry provides visibility, control, and response to any issues or changes in endpoints on the network, regardless of location, while reducing overhead and increasing efficiency with automated threat response.

"In our highly regulated industry, network security is not only critical from a vulnerability exposure perspective, but also from a regulatory standpoint," says Michael Seymour, vice president of information technology of Pike Electric. "As one of the world's largest energy solutions providers, [Network Sentry provides] an enhanced security posture across our locations with singular control of each and every endpoint, regardless of location. Now we have full capability to control access and permissions, and automate our ability to respond to threats."

Utilities can ensure they're getting the best out of internet-enabled ICS technology without inviting risk with Network Sentry's proven capabilities to provide:

Visibility

End-to-end visibility into all devices and endpoints on the network is crucial, especially when these assets are widely dispersed. Network Sentry gives a continuous view of endpoint devices on network, no matter where they are. This also includes what applications are on that endpoint, device ownership, and the endpoint's connectivity. By knowing exactly what you have on your network, no matter where it is, you can exert better security measures. You also have a real-time, accurate status of your entire network and its security posture.

Control

Network Sentry alerts you to any possible intrusion to your network by immediately detecting a rogue device that may be trying to cause device damage or a network outage, ensuring greater reliability and overall service stability. If a connected device is unwanted, or is behaving in an unexpected or undesirable way, Network Sentry will correlate all the information available so you can coordinate a real-time response with confidence.

Preventing unwanted device behavior and hardening your network from even an internal threat is made easier with Network Sentry's easy network segmentation capabilities. This means an unpatched PC or device can't and won't take down key ICS devices or clients.

Response

Should there be a risk introduced to your network, whether that risk is internal or external, a fast response can mean the difference between service uptime and downtime. Not every threat can or should require direct intervention, as that can place undue burden on security resources that are already stretched thin. That's why Network Sentry's automated threat response is a

crucial ally in addressing security events, automatically quarantining unauthorized or compromised devices, allowing your security controls to perform at scale without requiring additional resourcing. **Automated threat response also stops lateral movement of threats by removing the compromised device from the network at its connection point; this protects network data and other endpoints – something a firewall cannot do on its own.**

Kent Landrum from Opportune, an energy consulting firm, sums up the level of attention required by the industry. "Compliance is not an end game and utilities should consider cyber risk as a domain within their enterprise risk programs worthy of attention and oversight from the C-suite and Board." [vi]

The bottom line is that the utility industry is facing unprecedented cybersecurity threats. In 2017 the US government issued a rare pubic warning about hackers aggressively targeting critical nuclear, energy, aviation, water and manufacturing industries.[vii] With multiple targets already compromised, utility companies must improve their network security posture to avoid being the weak point in a nation's critical infrastructure.

If you are a utility or energy provider who would like to learn more about Network Sentry, get in touch with us for a free network scan and report to find out the state of your security posture, endpoints on your network, and any risks they may have. Call 603-228-5300 or visit **www.bradfordnetworks.com**

[i] https://www.worldenergy.org/wp-content/uploads/2016/09/20160906_Resilience_Cyber_Executive_Summary_infographic_WEB-1.pdf

[ii] http://content.industrydive.com/state-of-the-electric-utility-2017-survey-report/?utm_source=ud0328&utm_medium=webpost&utm_campaign=SEU2017

[iii] https://www.researchnester.com/reports/global-internet-of-things-iot-in-energy-sector-market-global-demand-analysis-opportunity-outlook-2023/256

[iv] https://energy.mit.edu/wp-content/uploads/2016/12/CybersecurityWhitePaper_MITUtilityofFuture_-2016-12-05_Draffin.pdf

[v] https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

[vi] http://opportune.com/content/uploads/2017/02/170207_bg_top-5-trends-utilities.pdf

[vii] http://fortune.com/2017/10/21/u-s-warns-public-about-attacks-on-energy-industrial-firms

BRADFORD NETWORKS

374 Congress Street, Suite 502, Boston, MA 02210, USA
Toll Free +1 866.990.3799 | Phone +1 603.228.5300
Email info@bradfordnetworks.com
Web www.bradfordnetworks.com

Bradford Networks is the leading provider of security automation and orchestration solutions that minimize the risk and impact of cyber threats by reducing containment time. The company's patented Network Sentry solution continuously assesses the risk of every user and endpoint, and automatically contains compromised devices that act as backdoors for cyber criminals. It is the first network security offering that can automatically identify and profile all devices and all users on a network, providing complete visibility and control. The company's award-winning Network Sentry is used by more than 1000 enterprise companies worldwide across many market sectors, including financial institutions, government & defense, healthcare, education, logistics & transportation, media and entertainment, retail & hospitality, technology, utilities and many others. For more information, please visit **www.bradfordnetworks.com**