CAPCO

REAL RESPONSES TO REPEL CYBERATTACKS ON UTILITIES

Cybersecurity risks have become a major headache for utilities. Attacks have been escalating in intensity, as well as frequency. Independent studies show utilities' management teams are not as prepared as they need to be. In this whitepaper, Capco highlights key areas those leaders must prioritize if they are to mitigate the risks of cyberattacks that will surely keep coming.

It shouldn't have been a surprise. But when the cyberattack hit Colonial Pipeline in May, the distributor of almost half of the vehicle fuel used on the U.S. East Coast, it caught everyone off guard.[1]

Fortunately, the attack did not impede the flow of fuel for long: the company shut down its pipelines for a few days as a precautionary measure. However, Colonial had to pay a $5 million ransom just to get back its stolen data. Coming after other cyberattacks in recent years – including the shutdown of Johannesburg's electrical utility and earlier, two hits in a year on Ukrainian utilities – it was another clear sign that utilities worldwide are being actively targeted by bad actors, some of them likely to be state-sponsored.[2]

The power sector has become a top target for cyber-criminals over the last decade, according to the French Institute of International Relations, a think-tank. In the U.S., there were 150 successful attacks between 2010 and 2014 that targeted systems that hold electrical grid information, reported the Department of Energy.[3]

Utility leaders are clearly worried. Nearly two-thirds of respondents to a recent large-scale study say sophisticated cyber-attacks are a top challenge.[4] More than half, 56%, say they experience at least one shutdown or operational data loss per year, resulting in outages, equipment damage, injury, and sometimes even environmental disaster[5]. Nearly 55% of survey respondents anticipate an attack on their critical infrastructure in the next 12 months[6].

It's noteworthy that cyber-criminals are targeting utilities' operational technology (OT) infrastructure – including ICS (industrial control systems), such as SCADA (supervisory control and data acquisition), smart substations, and distribution management systems. In fact, the 2020 study of cybersecurity threats by Honeywell revealed the number of cybersecurity threats specifically targeting OT systems grew from 16% of all cyber threats against industrial systems in 2019 to 28% in 2020. Over the same time, the number of threats capable of causing major disruption to OT systems more than doubled, from 26% to 59%.[4] In years gone by, OT systems were often air-gapped, or isolated, and thus more difficult to attack, but that doesn't mean utilities can ease up on securing their OT systems. Today, the lines between IT and OT are blurring fast as OT systems become more digitized.[7]

In general, the vulnerabilities are heightened by the growing digitization of the grid, the shift to renewables, by utilities' greater reliance on suppliers and third parties, and more remote operation of assets. And, all the while, utilities are up against more and more stringent requirements from regulators and rising expectations from customers.

What are utilities' business leaders doing to combat the rising threats? The short answer: nowhere near enough. In the study cited above, just 42% of respondents rated their cyber readiness as high, and only 31% gave high ratings to their readiness to respond to or contain a breach.[8] The complexities of the challenge are formidable.

3 BEST-PRACTICE INITIATIVES TO MITIGATE RISKS OF CYBER ATTACKS

Our longtime work across the power sector reveals several best-practice initiatives that we urge industry executives to focus on if they are to have any chance of mitigating the risks of cyber-attacks. Importantly, the initiatives span both IT and OT, and increasingly, they must be launched and managed in integrated ways. For simplicity, though, and because many utilities still approach OT and IT separately, here are three initiatives that are of most concern to the OT side:

Better management of supplier risks

If ever there was a demonstration of vulnerability to supplier risk, it is the notorious SolarWinds hack. In late 2020, cyber-criminals – believed to be Russian operatives – infiltrated the highest levels of the U.S. government by packaging their malware inside a trusted piece of software used by SolarWinds, a top-tier government contractor.[9]

As electric utilities have grown in size and complexity, their reliance on increasingly specialized technology has grown too. Installing, maintaining, and updating that technology often involves outside contractors, opening up many more vulnerabilities. Reliance on third parties is no small thing; some sources indicate that at many utilities, contract labor can make up more than half of total labor hours. Expanding supply chains widen the attack surface that utilities need to monitor and secure.

Utilities must, as a first priority, align with their nations' best-practice supplier-risk standards. In the U.S., those standards are promulgated by the North American Electric Reliability Corp. (NERC). In 2017, the NERC board signed off on a supply chain risk mitigation program in the form of proposed Reliability Standards CIP-005-6 and CIP-010-3(Supply Chain Standards), and then in October 2020, CIP-013-1, addressing cyber security supply chain risk management issues.[8] NERC has also approved the associated implementation plans[10].

In our work with electricity utilities, we have found an array of supply chain challenges, from multiple software vulnerabilities in suppliers' systems to suppliers' sub-standard cybersecurity practices or processes. Often, we've found that utilities lack detailed visibility into a supplier's cybersecurity practices; and it's not uncommon to find unauthorized storage of data within third-party systems. Any of those, left undetected and unremedied, could prove to be catastrophic.

This whitepaper is meant only to provide a brief overview of the aspects of cybersecurity that need ongoing attention. It should go without saying that every supplier's data should be traceable and visible to the customer. Concurrently, utility business leaders must partner with their HR teams to create and continuously improve workshops that train all workers about the nature of cyber risks. Just one snapshot: flash drives used by non-employee workers are one of the most common vulnerabilities.

Fundamentally, utilities must reset expectations with their suppliers, developing and implementing new security protocols and writing new, strict language into contracts. It is essential to set up and enforce incentives for "good practice" along with clear penalties for violations of the new protocols. Higher insurance levels will need to be included in supplier contracts. Above all, the management of the supply chain has to be highly proactive, fully engaged, and continuous.

Improved vulnerability management

A rapidly shifting threat landscape and multiplying points of exposure mean utilities must, as a matter of urgency, rethink their vulnerability management strategies. That means moving away from reactive strategies toward a proactive, comprehensive, risk-based approach that continuously identifies, evaluates, and maps potential threats using data analytics and, in response, proposes remediation and mitigation techniques.

Vulnerability management is defined by the U.S. National Institute of Standards and Technology (NIST) as "a capability that identifies vulnerabilities on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network."[11] It provides continuous centralized reports and visualizations to better assess an organization's cyber health.

An effective vulnerability management system can help protect against SQL injection and cross-site scripting (XSS) attacks, where code is input by an attacker that processes an action not intended for the original prompt's purpose. It can guard against faulty authentication systems that allow an attacker to gain unauthorized access or privileges. And it can help identify insecure configurations and standards that do not meet the organization's security policies.

The key to the success of a vulnerability management program is transitioning to a risk-based model that identifies and addresses the greatest threats. Organizations can begin building a program by taking these four steps:

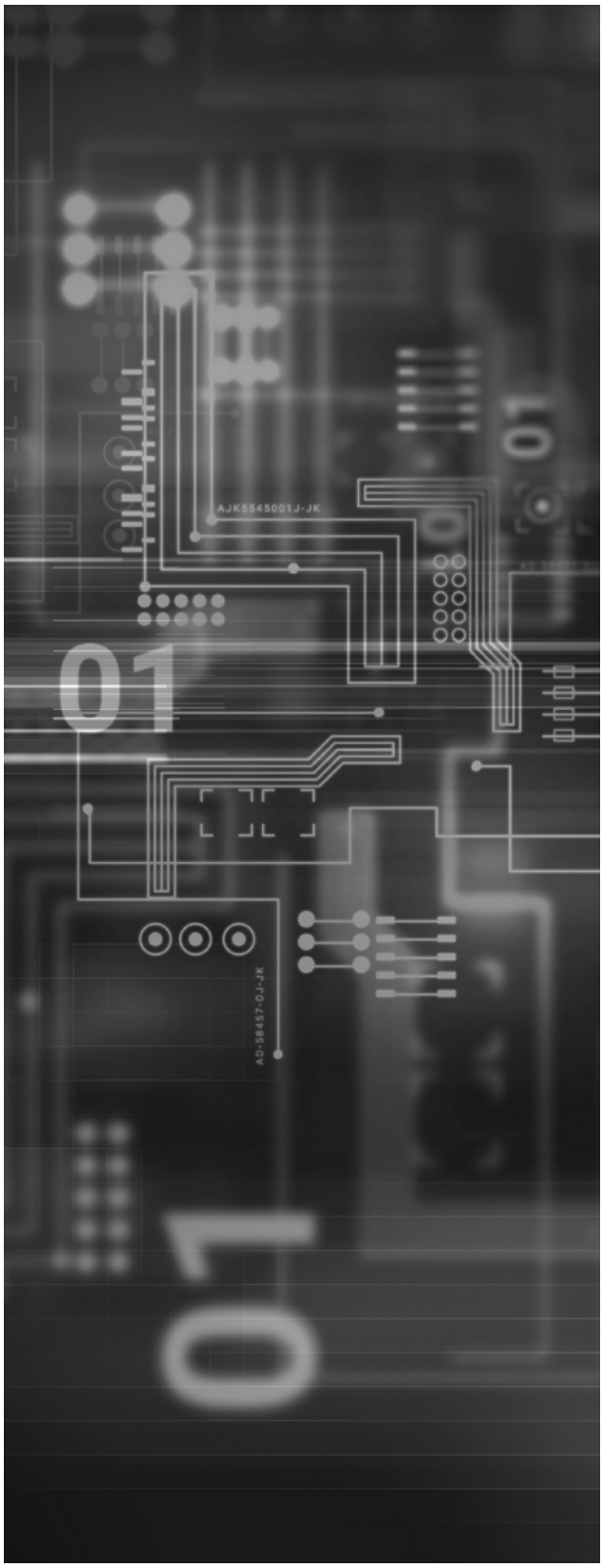
1. Identify and classify the organization's assets. This will ensure the ability to accurately measure and communicate risk to key stakeholders.

2. Select software that fits the needs of the organization's IT and OT footprint.

3. Determine frequency of scanning.

4. Remediate and fix vulnerabilities. The hard work begins once the vulnerabilities have been identified and assigned risk-based scores.

It's worth noting that not all vulnerabilities discovered will require an all-hands-on-deck mitigation approach. Some may be queued for future efforts and recorded in mitigation service level agreements. Most mature software offerings integrate with existing change management tools to easily track vulnerability mitigation efforts.



Continuous threat detection

Utilities are in no position to rely on one-off security scans; the stakes are far too high. Cybersecurity teams have to be able to track adverse events as they are happening, not later. They must ensure threat detection is a continuous and rigorous business discipline.

Continuous threat detection (CTD) is a broad term for advanced threat detection that provides an additional level of security against advanced malware and zero-day attacks. It uses advanced tools and analysis, such as source reputation, executable analysis, and threat-level protocols, in order to analyze network traffic in ways that heighten security. The idea starts with continuous visibility into the organization's systems. The underlying principle: to protect what you have, you need to know what you have – and know what it's doing.

Most CTD programs use "sandboxing" to separate communications and commands from programs on the network so those communications and commands can be assessed for malevolent intent without affecting the broader networks. By running in a virtual environment in the sandbox, a suspicious communication or command's behavior can be assessed and, if warranted, excluded from the broader network.

Unfortunately, CTD is not a strength for many utilities. Industry leaders give low ratings to their organizations' ability to achieve comprehensive and continuous visibility of digital assets. Many concede a lack of visibility with regard to OT security in particular.[12] Worldwide, only 18% report using analysis of big data or AI monitoring to track operations and recognize threats.[13]

Yet those are exactly the kinds of tools and techniques needed to help utilities find and neutralize "sleeping" malware, for instance, and detect other unknown threats. Cybersecurity teams can use advanced analytics to spot anomalies in the behavior of their assets; they can trace activity from the OT network to the IT network and vice-versa, and pinpoint gaps and unpatched systems that allowed an enemy to possibly take control long after penetrating the system and then lying dormant.

Such advanced tools can also help build the foundations of proactive mitigation and predictive attack analysis – essentially anticipating the most likely adverse events and building in protections against them.

The points made above are, we hope, a sharp reminder of what needs to happen now. Cyber threats against utilities are not going away and the severity and impact of attacks aren't about to ease off. In a newly volatile world, well-equipped, tech-savvy nation-state actors will almost certainly intensify their assaults, and the dark web will continue to be a ready marketplace for new and low-cost ways to pinpoint and penetrate weak entry points.

This whitepaper has focused more on traditional OT themes, and a companion piece, to be published soon, will address specifics on the conventional IT side. However, we urge utilities managers to view OT and IT security not as distinct activities but as interwoven elements of an active enterprise-wide risk management initiative. At a minimum, managers must recognize that there are more and more IT capabilities in the OT hardware that they are upgrading. OT-IT convergence is not going to stop.

REFERENCES

1. https://www.securityweek.com/cyberattack-forces-shutdown-major-us-pipeline
2. https://www.securityweek.com/ransomware-causes-disruptions-johannesburg-power-company
3. https://www.power-technology.com/features/the-five-worst-cyberattacks-against-the-power-industry-since2014/
4. https://assets.siemens-energy.com/siemens/assets/api/uuid:38ab2dff-3ee6-48ee-a2a9-29df5e24bfbd/siemens-energy-cybersecurity.pdf
5. https://dailyenergyinsider.com/infrastructure/22281-survey-56-percent-of-utilities-have-faced-a-cyberattack-in-the-last-year/
6. https://assets.siemens-energy.com/siemens/assets/api/uuid:38ab2dff-3ee6-48ee-a2a9-29df5e24bfbd/siemens-energy-cybersecurity.pdf
7. https://www.power-technology.com/comment/cybersecurity-power-utilities-agenda-covid-19-globaldata/
8. https://www.siemens-energy.com/global/en/news/magazine/2019/cyber-security-ponemon-study.html
9. https://www.cnet.com/tech/services-and-software/solarwinds-hackers-accessed-dhs-acting-secretarys-emails-what-you-need-to-know/
10. https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx
11. https://csrc.nist.gov/glossary/term/Vulnerability_Management#:~:text=Definition(s)%3A,extend%20compromise%20to%20
12. https://assets.siemens-energy.com/siemens/assets/api/uuid:38ab2dff-3ee6-48ee-a2a9-29df5e24bfbd/siemens-energy-cybersecurity.pdf
13. https://www.siemens-energy.com/global/en/news/magazine/2021/artificial-intelligence-for-a-secure-energy-ecosystem.html

AUTHOR

Robert Furr
Managing Principal
Robert.Furr@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com**, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO