BCG

The Boston Consulting Group

ENSURING CYBERSECURITY IN THE ELECTRIC UTILITY INDUSTRY

By Nadya Bartol, Michael Coden, David Gee, and Craig Lawton

Today's electric utilities are far more vulnerable to cyberattack than in the past. Their highly interconnected digital infrastructure enables real-time visibility into power outages, lets customers manage electricity consumption from their smartphones, and deploys sophisticated tools for energy management. All this means that utilities are more and more exposed, because offering these features over the internet requires connectivity between utilities' formerly standalone operational systems and their IT networks.

Utilities must act definitively to minimize this risk, yet a number of challenges affect their ability to do so. These challenges include continually evolving business and technology requirements, a widespread shortage of qualified personnel, additional risks associated with third-party relationships, and the need to enable participation of the entire workforce in managing cybersecurity risks. The magnitude of these challenges is only amplified for small utilities, which lack the scale and resources of their larger peers.

The electric utility industry and governments worldwide have taken steps to address the challenges. Still, they need to do much more. Utilities should make better use of government resources, share lessons learned, train and mentor more cybersecurity practitioners, and make cybersecurity a business—not just a technical—imperative. Building a culture that supports and sustains cybersecurity is a top priority.

Where Are We Heading?

Electric utilities are making a dramatic transition to intelligent digital networks. Today's business, regulatory, and consumer requirements—for such needs as renewable and distributed energy generation, smart cities, and electric vehicles—demand it. As utilities introduce increasingly sophisticated technologies to their legacy systems, however, they find themselves progressively more exposed on the internet and vulnerable to cyberattack.

Increasing Exposure

To make the transition, electric utilities are being compelled to connect—and allow data to flow between—their existing IT and operational-technology (OT) networks. While IT systems are thought of as office systems, OT systems control the equipment that performs the utility's mission, generating and distributing power over vast areas. These OT systems were once standalone, and their obscure proprietary protocols made it difficult to access or control them from the outside world. Over the past two decades, however, the growing demand for OT-generated data to provide planning, forecasting, billing, customer service, and other business-critical information to various parts of the business and to customers has necessitated greater connectivity between OT and IT systems.

To facilitate data interchange and increase standardization, utilities are phasing out OT systems' older proprietary technologies in favor of standard hardware, such as Intel and ARM processors, and operating systems, such as Windows and Linux, used in IT systems. These technologies include control systems and smart meters with many more capabilities—such as remote access and management—than devices had in the past. As a result, modern OT systems are built on software and hardware platforms that malicious actors know and understand. In addition, these formerly standalone systems are now connected to the enterprise IT systems and, consequently, exposed to risks originating from the internet.

With so many devices linked to the network, its attack surface is exponentially greater as well: more devices mean more vulnerabilities—and more possible points of entry. Moreover, cyberwarfare is asymmetrical: attackers can succeed if they find even a single exploitable weakness, whereas defenders must protect all points of access from every possible attack.

The human factor only compounds these vulnerabilities. Technology is advancing rapidly, and cybersecurity awareness and education have not kept up. With intelligent digital networks and more extensive features comes greater connectivity for all utility employees and the ability for them to inadvertently create a situation that threatens the cybersecurity of the enterprise. According to Verizon's *Data Breach Digest,* attackers use phishing 92% of the time to obtain credentials, to manipulate victims into letting attackers into their network, or to do both. Once people click a link in a phishing email—as happened in the December 2015 cyberattack in Ukraine—malicious code is downloaded onto their computers and propagates throughout the network to which their computers are connected.

An Evolving Threat

Today's would-be attackers are quite familiar with the industrial control systems (ICSs), Internet of Things devices, and specialized communications devices that are part of many OT systems. According to publicly available government and industry reports, hostile actors have been exploring and mapping OT networks throughout the world, including in the US and Europe, for a number of years. In recent reports, the US Department of Homeland Security (DHS) and the US Federal Bureau of Investigation have described Russian actors' network reconnaissance of US nuclear power plants and other critical infrastructure targets.

Moreover, attackers have created malware that specifically targets ICSs and other critical infrastructure systems. These hostile actors have become more sophisticated and knowledgeable as utility systems and networks have become more visible and accessible.

The nature of cyberthreats has also changed substantially over the past ten years. The frequency of incidents in which nation-states have targeted various critical industries, including the utility industry, has steadily increased. Industry reports indicate reconnaissance activities by nation-state actors going as far back as 2013. The first confirmed cyberattack power outage was the December 2015 attack in Ukraine. More than 250,000 customers lost power for more than six hours. Although its impact was not

as widespread, a second power outage, in December 2016, was more dangerous and disquieting: it represented the first use of a modular, automated cyberweapon capable of inflicting multiple types of damage to a much larger number of power grids. These events have made the contours of the threat far more tangible.

Distressingly, cybercrime has become a full-fledged industry: hostile actors can buy malware that comes complete with warranty, service contract, and access to a 24-7 help desk. Cybercriminals monetize their skills by selling to the highest bidder, and nation-states—armed with sophisticated expertise and effectively unlimited time and resources—can hire the best in the business.

Numerous nation-states are building cyberarmies and investing in the capabilities of their own specialized staff. As a result, perhaps for the first time in history, private enterprises must protect themselves against attacks by nation-states. If a foreign nation-state were to make a land, air, or sea attack against a US utility, the US Army, Air Force, or Navy would protect that utility. However, in the case of a nation-state-sponsored cyberattack, the utility needs to respond on its own.

Security that may not have been required in the past has therefore become essential. Utilities need to address new and emerging security threats, even while designing, implementing, and maintaining smart networked systems.

What's Holding the Industry Back?

As the industry attempts to respond to potential cyberthreats, it faces several important challenges. For one, business and technology requirements continually evolve. For another, there is a serious shortage of qualified workers who understand how to secure the converged—IT-plus-OT—utility enterprise. In addition, managing risk associated with third parties adds a significant layer of difficulty to the implementation of good cybersecurity. Small utilities in particular struggle with these issues, because they lack the resources and scale to cope with cyberthreats as their larger peers do. Last, the challenges are broader than mere technical issues and need to be dealt with holistically.

Constant Change

Electric utilities must continually ensure their reliability and safety in a fast-changing environment. Not only are cybersecurity threats evolving, but so are regulatory and compliance requirements, consumer demands, and business needs—all necessitating deployment of ever-advancing technologies. Although some of these technologies are not yet mature, utilities must plan for future networked systems that will provide new capabilities reliably, safely, and securely.

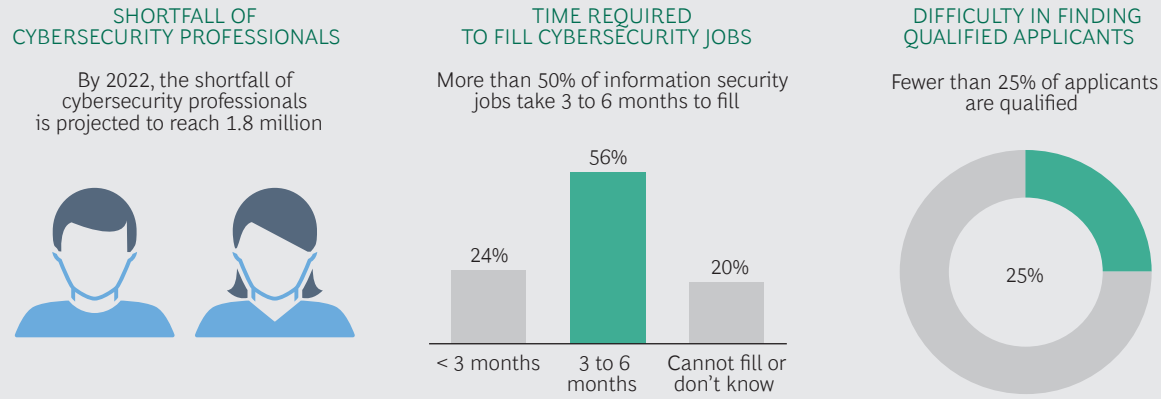
It will, therefore, be important for utilities to make anticipated security requirements for future power generation and distribution an integral part of their business planning. They can begin by answering some critical questions: Will the system have to support and protect electric vehicles, renewable energy, and smart cities? What specific kinds of cybersecurity measures will be required?

Adding to the difficulty, the system and network architectures of electric utilities have accumulated new layers on top of older layers that were designed and implemented at a time before security was a priority. For many utilities, the OT refresh cycle is at least seven-years—and sometimes decades—long, whereas the refresh cycle of traditional IT-based industries is significantly shorter. Because replacing the installed base is expensive and consumes resources, utilities must protect their legacy infrastructure while building and securing the infrastructure of the future.

Workforce Shortage

The current shortage of qualified cybersecurity practitioners is well documented. (See the exhibit.) Given the complexity of securing both IT and OT systems, utilities in particular suffer from a shortage of pro-

Electric Utilities Must Compete for an Inadequate Number of Cybersecurity Professionals



Sources: (ICS)² Blog, 2017 Global Information Security Workforce Study; ISACA 2017 State of Cybersecurity; BCG Platinion analysis.

fessionals who can address cybersecurity needs. Although OT and IT now use the same hardware and operating systems, many OT systems' applications—and ways of applying cybersecurity techniques—are quite different. As a result, putting IT practitioners into the OT environment and expecting them to be effective immediately would be unrealistic and potentially dangerous. In addition, the goals of IT systems differ markedly from those of OT systems, as do the practices, culture, education, and mindsets of OT and IT operators. Perhaps the most important difficulty is that the available training and education programs aimed at this population are currently unable to meet the sheer weight of demand.

Third-Party Risk

Third parties, such as suppliers and systems integrators, have always been critical members of the utility ecosystem and—as a result of exponential growth in the deployment of smart software-enabled devices that need to be securely designed, implemented, and managed—the role of third parties has gained much greater importance than it had in the past.

Cybersecurity has therefore become a critical aspect of utilities' third-party risk management. Nonetheless, even as utilities work to educate third parties about various security methods and techniques, communicating security expectations to third parties—and then monitoring their adherence—remains a difficult work in progress. Some of the leading utilities have implemented sophisticated third-party and supply chain risk management programs, but these are not yet the norm.

Resource and Scale Disparities

Small utilities struggle to manage the same set of risks that face their larger peers, but they lack the same level of human and financial resources. Cybersecurity is a complex discipline covering many different areas, and larger utilities with access to more resources are better equipped to hire their own experts and run sophisticated cybersecurity programs. Small utilities are starting to outsource some of the services they require, but this approach has its own challenges, such as how to secure the necessary financial resources and negotiate contracts that include appropriate security provisions.

Nontechnical Issues

The issues associated with cybersecurity are not just technical. As discussed above, most data breaches are the result of human error. In addition, the solutions should not be limited to technical or systems responses. Utilities must establish clear organizational roles and decision rights for cybersecurity in IT, operations, and management. Core operational processes should be reviewed to identify and remedy exposure. And all members of the organization need

to be more aware and modify their behavior accordingly.

What's Been Done to Date?

Organizations worldwide are working to address these challenges and provide industry guidance. A number of organizations, including the US National Institute of Standards and Technology, the European Network and Information Security Agency, the Council on Large Electric Systems, the US Department of Energy and DHS, and the Electric Power Research Institute, have issued guidelines and research documents aimed at helping electric utilities conduct cybersecurity maturity assessments, articulate security requirements in procurement, develop security requirements for smart grids, and respond to incidents involving an ICS. Many of these resources are used globally—regardless of where and by whom they were developed.

Furthermore, utilities collaborate through a number of active cybersecurity working groups established for utility experts with different functional focuses, at different levels of the organization, and within utilities of different ownership types and sizes.

The US utility industry is one of the few subject to specific cybersecurity standards—in this case, the Critical Infrastructure Protection (CIP) standards developed by the North American Energy Reliability Corporation (NERC) and mandated by the Federal Energy Regulatory Commission. It should be noted that the NERC CIP standards are enforced by the regulatory commission, and failure to comply can result in substantial fines.

In addition to overseeing the development of NERC CIP standards, NERC is a powerhouse of cybersecurity resources for the industry. For example, it owns and operates the Electricity Information Sharing and Analysis Center, which provides essential cybersecurity services such as threat sharing, collaborative support, and monthly briefings on critical-infrastructure protection topics.

NERC also runs the industrywide all-hazards exercise known as GridEx. The exercise simulates industrywide cyberattacks and helps utilities test companywide and industrywide response-and-recovery processes. GridEx primarily involves the frontline operators who run the systems, but it also engages utility leadership, including CEOs and other senior executives. Utilities should conduct frequent simulated cyberattacks, known as tabletop exercises, at every level of the organization, including the board of directors and frontline operators. These exercises are as important as any fire or safety drill ever conducted.

What Should Be Done Next?

Additional approaches to improving cybersecurity in the utilities industry will require significant work and investment. We recommend that at the macrolevel, utilities put available government resources to good use and share lessons learned in implementing cybersecurity practices in their own environments. In addition, we recommend industrywide support for a number of initiatives.

Basic Practices

Utilities should make sure that they have implemented basic cybersecurity practices. Among an organization's most fundamental are the identification, inventory, and classification of all of its information and assets. Without full knowledge and understanding of its assets, a utility cannot protect and manage itself. Another fundamental security practice is to segregate IT systems from OT systems by partitioning the networks or, if possible, completely separating them.

Utilities should also consider security issues as they design new systems, networks, and applications. Where feasible, all utility systems, including the smart grid and advanced-metering infrastructure, should implement multifactor authentication, ensuring that users are granted system access only after confirming their identity through a combination of several disparate pieces of information. Furthermore, utilities should implement appropriate password

management, privilege management (access control), and other conceptually simple and cost-effective practices. To ensure that the implemented technology will be effective, utilities need to establish a culture of cybersecurity awareness and practices that emphasize the new technology.

Cybersecurity Maturity Assessment

Utilities should then assess the maturity of their organization's cybersecurity program. The assessment should include a review of the organization structure, management, operations, people, processes, and technologies. The results will help utilities prioritize cybersecurity investments and concentrate on the most potent and cost-effective initiatives.

Education

Teaching IT professionals about OT—and OT professionals about IT—is not always easy or effective. Education and training organizations should continue to focus on developing converged IT-OT cybersecurity practitioners. Furthermore, because there are so few formal educational opportunities, utilities must teach, train, and mentor their own personnel to facilitate knowledge transfer within the industry.

Third-Party and Supply Chain Security

Utilities should intensify their collaborative work with third parties to establish appropriate levels of security within the utility ecosystem. Leading utilities have implemented comprehensive third-party and supply chain risk management programs that include standardized security requirements for procurement, vendor assessment, and site visits, thus building security into the front end rather than adding it as an afterthought.

Culture

Most important, utilities should create a true culture of cybersecurity. Many organizations conduct, for example, phishing-awareness exercises. However, discerning the illegitimacy of a well-constructed phishing email can be difficult. Responding successfully therefore requires more than just a passing awareness of cybersecurity risk; it requires fundamental changes in behaviors. To be truly successful in any environment, including an electric utility, cybersecurity needs to become an integral part of the entire organization and how its individual members think and act.

One of the least expensive and most effective actions a utility can take is a survey of the cybersecurity culture of its organization. The results can inform a focused set of training and awareness initiatives aimed at changing the mindsets and behaviors of its employees. The utility can then retake the measure of its culture, gauging where improvements have occurred and where additional awareness training is needed.

No technology can protect an organization from attack if an employee clicks a dangerous phishing link. Awareness of cybersecurity must therefore be raised to at least the same level of awareness as that of safety, compliance, ethics, and quality. And it must be fully embedded within the organizational psyche—from the boardroom and senior executives to the most recently hired employee.

Much of the material for this article was adapted from BCG's response to the Presidential Commission on Enhancing National Cybersecurity, September 9, 2016, and "Our critical infrastructure is more vulnerable than ever. It doesn't have to be that way," February 24, 2017, an article published by the World Economic Forum.

About the Authors

Nadya Bartol is a senior manager in the Washington, DC, office of The Boston Consulting Group and associate head of cybersecurity at BCG Platinion, a subsidiary of the firm. You may contact her by email at bartol.nadya@bcgplatinion.com.

Michael Coden is an associate director in BCG's New York office and head of the Cybersecurity practice at BCG Platinion. You may contact him by email at coden.michael@bcgplatinion.com.

David Gee is a senior partner and managing director in the firm's Washington, DC, office and a core member and former leader of the Energy practice in North America. You may contact him by email at gee.david@bcg.com.

Craig Lawton is a senior partner and managing director in BCG's Atlanta office and the CEO of BCG Platinion. He is responsible for cybersecurity topics in North America. You may contact him by email at lawton.craig@bcg.com.

The Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with more than 90 offices in 50 countries. For more information, please visit bcg.com.