

Risk Practice

The energy-sector threat: How to address cybersecurity vulnerabilities

Electric-power and gas companies are especially vulnerable to cyberattacks, but a structured approach that applies communication, organizational, and process frameworks can significantly reduce cyber-related risks.

by Tucker Bailey, Adam Maruyama, and Daniel Wallance



© Monty Rakusen/Getty Images

In our experience working with utility companies, we have observed three characteristics that make the sector especially vulnerable to contemporary cyberthreats. First is an increased number of threats and actors targeting utilities: nation-state actors seeking to cause security and economic dislocation, cybercriminals who understand the economic value represented by this sector, and hacktivists out to publicly register their opposition to utilities' projects or broad agendas. The second vulnerability is utilities' expansive and increasing attack surface, arising from their geographic and organizational complexity, including the decentralized nature of many organizations' cybersecurity leadership. Finally the electric-power and gas sector's unique interdependencies between physical and cyber infrastructure make companies vulnerable to exploitation, including billing fraud with wireless "smart meters," the commandeering of operational-technology (OT) systems to stop multiple wind turbines, and even physical destruction.

To answer these challenges, we apply our work in more cyber-sophisticated industries (e.g., banking, national security) and our on-the-ground international experience with utilities at various stages of technological sophistication to propose a three-pronged approach:

- *Strategic intelligence on threats and actors before attacks on the network.* Companies must move beyond reactive measures and take
- *Programs to reduce geographic and operational gaps in awareness and communication, creating a culture of security.* A high-functioning utility security apparatus should be aligned to ensure that the best minds across the enterprise—not just in security—are aware of threats and have robust processes to report potential vulnerabilities and emerging incidents. Furthermore, technical systems should provide security with a common operating picture of sites across geographies and business units to detect coordinated attack and reconnaissance campaigns.
- *Industry-wide collaboration to address the increasing convergence of physical and virtual threats.* Industry partnerships, as the eyes on the ground for leading-edge technologies (and corresponding vulnerabilities), should engage in regular dialogue on how to secure the delicate ties between physical and virtual infrastructure, as well as IT and OT networks.

Several characteristics of the energy sector heighten the risk and impact of cyberthreats against utilities.

Why the industry is vulnerable

The cyberthreats facing electric-power and gas companies include the typical threats that plague other industries: data theft, billing fraud, and ransomware. However, several characteristics of the energy sector heighten the risk and impact of cyberthreats against utilities (Exhibit 1).

Expanding number of threats and threat actors

The threat landscape for utilities has expanded to include more threats from more actors. Nation-state actors and other sophisticated players have demonstrated greater willingness to target infrastructure providers as part of their broader campaigns. A January 2020 alert from one government source indicated that critical infrastructure providers should beware of nation-states “capable, at a minimum, of carrying out

attacks with temporary disruptive effects against critical infrastructure” as a deterrent or retaliatory measure for other geopolitical developments.¹

In addition, cybercriminals target utilities and other critical infrastructure players for profit. One of the most public examples of this willingness to disrupt daily life occurred in May 2019, when a ransomware attack disabled Baltimore city computers for weeks, incurring an estimated \$18.2 million in damages—more than the demanded ransom.² The focus of such attacks is no longer limited to IT networks alone; a government agency recently warned that ransomware had been deployed to disrupt a gas company’s visibility into pipeline operations, leading to a loss of productivity and revenue until the ransomware was removed.³

Exhibit 1

Electric utilities can be affected by cyberattacks across the whole value chain.

Potential threat impacts



Generation

Disruption of service and ransomware attacks against power plants and clean-energy generators

Root cause: Legacy generation systems and clean-energy infrastructure designed without security in mind



Transmission

Large-scale disruption of power to customers through remotely disconnecting services

Root cause: Physical security weaknesses allow access to grid control systems



Distribution

Disruption of substations that leads to regional loss of service and disruption of service to customers

Root cause: Distributed power systems and limited security built into SCADA¹ systems



Network

Theft of customer information, fraud, and disruption of services

Root cause: Large attack surface of IoT devices, including smart meters and electric vehicles

¹Supervisory control and data acquisition.

¹ “Summary of terrorism threat to the U.S. homeland,” *National Terrorism Advisory System Bulletin* (US Department of Homeland Security), January 4, 2020, dhs.gov.

² Ian Duncan, “Baltimore estimates cost of ransomware attack at \$18.2 million as government begins to restore email accounts,” *Baltimore Sun*, August 28, 2019, baltimoresun.com.

³ “Ransomware impacting pipeline operations,” Cybersecurity and Infrastructure Security Agency (CISA) Alert AA20-049A, February 18, 2020, us-cert.gov.

Finally, hacktivists may pose threats that tend to be less sophisticated but still have potential to disrupt electric-power and gas operations. As noted in a 2017 law-enforcement assessment, hacktivists are more likely to target utilities using publicly available attacks such as a distributed denial of service (DDOS). The effects of these attacks, if not properly mitigated, can be as great as the impact of cybercrime.⁴ In addition, hacktivists have stolen personal data from climate leaders.⁵ Such data could be used to carry out cybersecurity attacks against individual industry leaders.

While most utilities have become aware of the risks associated with cybersecurity, inconsistencies still exist in their ability to secure funding to invest in OT and IT cybersecurity controls. In many states, regulators lack the dedicated talent needed to review cybersecurity program budgets, which factor into a utility's billing rates to customers. This results in, at best, a good-faith approach to approving incremental investment in cyber capabilities and, at worst, skepticism from regulators in approving larger rate increases associated with strategic security overhauls. Additionally, certain municipalities offer energy services independent of a major utility. This may alleviate customer concerns with existing energy players in the market, but many of these municipalities remain underprepared or understaffed to ensure the deployment of enough cybersecurity controls to decrease risk.

Besides the difficulties of securing funding, regulatory inconsistencies also may result in a less strategic, more piecemeal approach to utility cybersecurity. To comply with North American Electric Reliability Corporation (NERC) critical-infrastructure protection standards and other industry requirements, many security functions face continual stress from addressing gaps identified in ongoing site-specific or regional-level security assessments. While an ongoing assessment and

improvement program is essential to maintaining a high-performing security function, continual tactical-level assessments can tax a security team's resources and attention at the expense of a more holistic, strategic-level approach to the evolving threat landscape and expanding attack surface.

Expansive footprint

By their very nature, utilities must operate a geographically distributed infrastructure across many sites—121 plants over 94,000 miles of distribution for an average top 25 US power company.⁶ That makes it difficult to maintain the necessary visibility across IT and OT systems, much less correlate network activity against physical security systems, such as badge access logs and server room surveillance feeds. This challenge is heightened in developing regions of the world and in large-footprint, low-energy-return production sites such as solar farms, where our colleagues have found that the cost of robustly securing a site and powering additional cyber and surveillance infrastructure could exceed any revenue realized from site operations.

In addition to utility-controlled sites, utilities have geographic vulnerabilities in consumer-facing devices (either utility owned or simply grid connected) that may contain cyber vulnerabilities that could compromise either a company's revenue or the overall security of the grid. These vulnerabilities first came to light as early as 2010, when a Puerto Rican utility estimated that tampering with wireless smart meters could result in revenue losses as high as \$400 million per year.⁷ New technologies, such as electric-vehicle charging stations, have further increased the stakes, as one security research report indicated that a coordinated attack against charging stations could take down an entire power grid if proper measures are not in place.⁸

⁴ Eduard Kovacs, "DDOS attacks more likely to hit critical infrastructure than APTs: Europol," *Security Week*, September 27, 2017, securityweek.com.

⁵ Francis Churchill, "Anonymous hacked the data of more than 1,000 climate change officials," *Mother Jones*, December 4, 2015, motherjones.com.

⁶ ABB Energy Velocity, data accessed 16 April 2020.

⁷ Brian Krebs, "FBI: Smart meter hacks likely to spread," *Krebs on Security*, April 21, 2012, krebsonsecurity.com.

⁸ Kenneth Rohde, "Electric vehicle cyber research," slide presentation for SANS Automotive Security Workshop, May 2017, sans.org.

Both geographic distance and organizational complexity make the industry vulnerable to cyberattacks.

But geographic distance is not the only—and perhaps not the most important—separation that makes the industry vulnerable to cyberattacks. The other is organizational complexity.

Many, if not most, utilities rely on several different business units to refine, generate, transmit, and distribute energy and resources. In our experience, with this diversity often come separate OT and even IT policy regimes—a structure that makes it difficult to assure the overall security of the network. For example, some OT policy regimes may allow the use of untested IoT technology and even makeshift technical solutions to monitor operations without considering larger-scale cyber vulnerabilities. One regional utility we visited relied on smartphones running a videoconferencing app to monitor the pilot flame in an oil refinery. Combined with the large number of employees, contractors, and vendors who require access to utility company sites and systems, these organizational gaps make IT security policies, including identity and access management (IAM), especially difficult.

Complicating this issue is the fact that many OT systems run on legacy technology that is serviceable only by one or two vendors. These vendors frequently do not prioritize security and may introduce attack vectors by using unpatched laptops and improvised solutions such as USB-based file transfers across separate utility companies. In some cases, utilities that want vendors to use “clean,” patched laptops for OT maintenance are required to provide this equipment to vendors at their own expense. When breaches

in legacy OT hardware occur, response time is frequently lengthened by a dependency on vendor timetables, an inability to leverage crowdsourced solutions such as cloud detection, and the need to create new solutions for hacks targeted against specific OT systems and configurations.

Even with these inherent weaknesses in the upgrade and maintenance process, the costs of upgrading an OT network are high; a recent rate case for a major US regional utility quoted an overall programmatic upgrade at over \$100 million.⁹ These costly network redesigns that can begin to allow for remote monitoring, upgrades, and other capabilities can at least partly mitigate some of the inherent technological weaknesses of OT systems. Still, they remain difficult to justify to regulators and shareholders, as they provide no immediate benefit to either the business or its customers.

In some cases, risk also increases with greater use of start-up-developed specialized connected devices across the value chain for innovative capabilities, given the resource limitations of smaller companies. While these start-ups typically offer connected devices with built-in security, the companies themselves may lack sufficient resources to respond to a large-scale incident, given the number of affected devices deployed. The presence of these specialized devices in a larger ecosystem further complicates the multivendor, multigenerational technology environment of utility IT and OT networks. Additionally, by collecting vast amounts of customer information, including billing data with itemized energy-usage information,

⁹ Dwight L. Jacobs, Duke Energy, “Accounting request related to cybersecurity informational technology—operational technology program,” letter to Kimberly D. Bose, US Federal Energy Regulatory Commission, referencing Docket No. AC19-75-000, March 13, 2019.

such devices may add incremental privacy risk, necessitating increased data-protection requirements. A data breach could result in regulatory response and reputational risk, such as fines and customer dissatisfaction with privacy controls. In addition, an unauthorized access of the data could reveal sensitive behavioral patterns to adversaries. In the hands of criminals, data based on power usage may provide clues about when a family is home or away, paving the way for break-ins and theft.

Physical–cyber convergence

The unique interdependencies between virtual systems and physical infrastructure in the electric-power and gas industry create high stakes for security officers. A disruption of one portion of this interdependency could very well affect the other. At worst, consequences could include loss of power, destruction of equipment, and damage to devices throughout the grid. For example, a cyberattack targeting smart inverters that control home solar systems' "sell back" of power to the grid could overload parts of the grid, damaging critical equipment of the utility and causing power outages.¹⁰

Other concerns involve critical equipment in the OT sphere and the telecommunications networks being used to communicate between OT sites and even across providers. For example, operators may trust data from safety and transport monitoring systems used to regulate the flow of electricity or gas without further manual validation or strong data integrity regimes. Data tampering could cause dangerous overages (potentially damaging equipment) or outages without tripping the built-in fail-safes designed to mitigate such impacts. Because these systems do not directly contribute to utility value streams, they may become targets of cost cutting (e.g., consolidating safety and control systems onto one platform, increasing the risk of compromise to both) and are not high priorities for upgrading beyond required standards.

Physical security also is a critical element of maintaining the integrity of power grids and their connected networks, including both IT and OT. Good physical security is essential for maintaining the integrity of sensitive locations such as data centers and transmission and distribution sites. Without close controls on access to critical systems, cyber response becomes significantly more difficult. Additional risk accompanies the expansion of new technologies, especially those associated with large-footprint green-energy sources (e.g., wind and solar farms). Access panels for wind turbines are sometimes left unsecured, allowing attackers physical access to both internal device controls and a segment of the broader OT network. Recent security research at a wind-turbine farm indicated that physical vulnerabilities (an easily picked lock) and a lack of network security allowed researchers to traverse the entire wind farm's network within minutes—with access privileges that would have enabled them to cause anywhere from \$10,000 to \$30,000 of revenue losses per hour or even destroy the turbines entirely.¹¹

Weaving a web of protection

The cyber and corresponding physical threats to electric-power and gas security are not insurmountable. A structured approach that applies communication, organizational, and process frameworks along with technical improvements in a few areas can significantly reduce cyber-related risks for utilities.

Strategic threat intelligence

Utilities must take a proactive, preemptive view of the varied and advanced threat landscape facing their companies and networks. It isn't enough to rely on tactical threat intelligence—especially not the threat intelligence supplied off the shelf by vendors (e.g., CTI script and signature-based detection models). Instead, organizations should consider employing analytic teams that can provide

¹⁰ Kelsey Misbrener, "Cyberattacks threaten smart inverters, but scientists have solutions," *Solar Power World*, April 30, 2019, solarpowerworldonline.com.

¹¹ Jason Staggs, "Adventures in attacking windfarm control networks," slide presentation, Black Hat USA 2017, Las Vegas, NV, August 2017, blackhat.com.

a holistic, proactive view of threats by monitoring threats across the industry and region, including intelligence about technical vulnerabilities and the various factors (e.g., geopolitical, economic, legal) that shape the threat environment (Exhibit 2).











In the electric-power and gas sector, it is also critical that this strategic intelligence not only provide awareness but also inform strategic decision making and response plans, thus a rethinking of technology, policies, and operating models (Exhibit 3). Effectively, this calls for strategic intelligence written in a bottom-line, up-front style that highlights the potential impact of threats to the company, its operations, and its customers. Intelligence analysts should be prepared to present their understanding of threats and their impact

on the company. They also must be prepared to participate actively in dialogues to find solutions.

Especially important for a robust strategic intelligence function, as threats from advanced actors such as nation-states are on the rise, is the ability to prepare the organization for instances in which it must address a known unknown, such as an emergent ransomware tool or a coordinated multiphase attack. In addition to utilizing a security information and event management (SIEM) solution and other tactical solutions that monitor and help organizations contain, mitigate, and eradicate attacks, organizations should have well-designed and well-tested incident response plans and enough institutional muscle memory from plan exercises to minimize the impact of a large-scale attack quickly and decisively.

Exhibit 2

Historically ‘air-gapped’ operational-technology (OT) systems are now online, but myths persist about how these systems are operated and secured.

 <p>Myth: Air-gapping is the only way to assure security of OT systems</p>	 <p>Myth: A firewall will protect my OT network from attacks originating from the connected IT network</p>	 <p>Myth: No external connections exist besides the connection to the corporate network</p>	 <p>Myth: Employees operate OT equipment to manage production day-to-day</p>	 <p>Myth: OEM vendors (SCADA¹ providers) adequately secure their equipment</p>
 <p>Fact: Even in the unlikely case that an air gap existed today, attackers can enter the OT network through other pathways, such as laptops and USB</p>	 <p>Fact: A firewall alone is not sufficient to protect the network perimeter; in case of intruders, anomaly detection and monitoring need to be implemented</p>	 <p>Fact: More and more, vendors require backdoors built into the equipment for remote access and/or control; these are sometimes required in their service-level agreement</p>	 <p>Fact: Operations are increasingly outsourced to vendors—some of which sit in remote locations—increasing risk of insider threat and expanding the attack surface</p>	 <p>Fact: Contracts often lack requirements for the vendor to ensure that security features and processes are implemented and kept current</p>

¹Supervisory control and data acquisition.

An integrated approach to security

To address the vast geographic, organizational, and technical gaps in their networks and visibility, utilities must take an integrated approach to security (see sidebar “A cybersecurity vision for Dominion Energy”). The pace and breadth of today’s threats make it unwise to allow organizational stovepipes to decrease the speed of detection, reaction, and response.

Utilities should think critically, from both an organization and people standpoint, about how to address organizational silos that may, for valid

business reasons, have very different requirements and indicators. In terms of strategic leadership, this means setting an agenda and standards for the cybersecurity program, to be utilized and implemented across even the most disparate business units. To support this increasingly centralized approach, leaders of each business unit or geographic area with cyber decision making should participate in meetings to ensure alignment across all stakeholders, thereby preventing situations in which one business unit implements cutting-edge protections while another remains underprepared because it lacks resources or a sense of urgency.

A cybersecurity vision for Dominion Energy

by Adam Lee

When I left the FBI to take over as Dominion Energy’s chief security officer, I knew I would be leading a team with responsibility for protecting Dominion Energy’s business of supplying the gas and electrical-energy needs of more than five million household and business customers across 18 states. To serve these needs, we would need to secure over 29 gigawatts of production capacity leveraging wind, solar, hydro, gas, coal, and nuclear plants across the United States. In addition, Dominion Energy is a critical national asset as a large-scale liquid-natural-gas (LNG) energy exporter and the energy supplier to the Pentagon, massive Loudon County data centers, and the Norfolk Naval Base and Shipyard, among other critical customers. We face several threats from nation-state actors, violent domestic activists, and ever-evolving cybercrime. As Dominion’s operations embrace new opportunities related to digitization and the smart grid, I also knew that we had to defend an expanding attack surface.

To confront these challenges, I developed the vision of the Threat Response and Analysis Center (TRAC) in partnership with

Dominion’s business units and McKinsey. The TRAC is an integrated security organization that provides Dominion’s leadership with the insight to make strategic decisions that mitigate risks and provide a timely, coordinated response to the tactical threats that arise. McKinsey’s team of intelligence, cyber, and organization experts partnered seamlessly with our leadership on a three-pronged approach to establish the TRAC, focusing on the organization, processes, and reporting and products that would help us succeed.

Organizationally, we broke down many of the traditional stovepipes between cyber and physical security in our organization, ensuring that my desk as the chief security officer wasn’t the first place where these two critical threat streams converged. By pushing awareness of the converged threat picture further into the organization, we empowered our analysts and Security Operation Center (SOC) to identify strategic gaps and more quickly remedy incidents that spanned both spheres.

Building on this new organization, we created processes within the TRAC and across the business units at Dominion that

increased corporate awareness of security. The new processes focused on threats to the entire organization, including vendor risk and insider threats. This ensured that security leaders, business leaders, and security personnel on the front line are aware of relevant strategic and operational concerns and are well positioned to protect Dominion’s operations.

Finally, we developed a suite of strategic intelligence products to create a security culture at Dominion that underscores the impact of security threats to the business operations of the company. We evolved our threat reporting from local-newspaper, police-blatter-style reports to strategic intelligence modeled on executive products such as the President’s Daily Brief. By putting the business impact of intelligence up front in a digestible format, this new product suite ensures that my peers across Dominion’s business units will be able to make strategic decisions about Dominion with security risks in mind.

Adam Lee is the chief security officer of Dominion Energy.

At the tactical and operational level, we have found that the organizational design works best when teams within the security organization have visibility into—if not decision authority over—all IT and OT networks and architecture (Exhibit 3), allowing them to detect and communicate trends that may indicate a coordinated attack. To allow for a robust two-way communication conduit, it is also desirable to create a formal program that designates “security champions” within each business unit to serve as the eyes and ears of the security organization and to advocate for good security practices in technical and process designs.

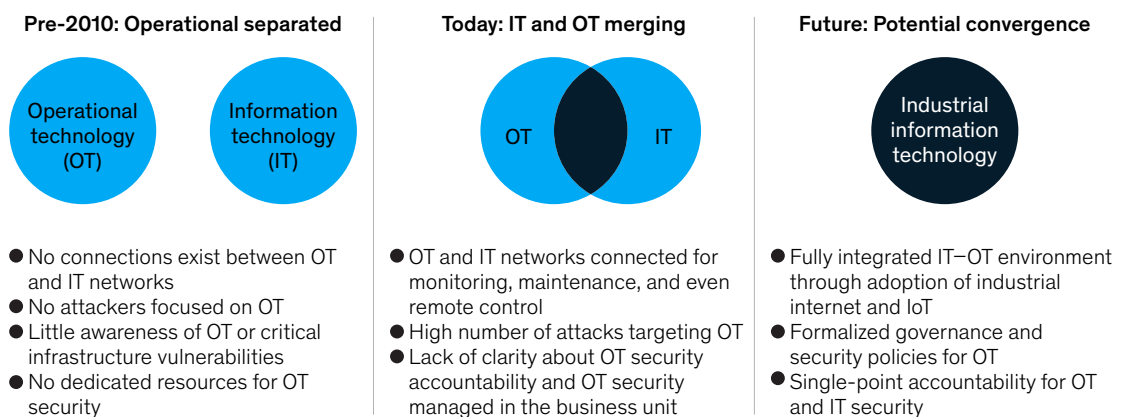
From a process standpoint, even organizations with firm distinctions between security team members need a defined and structured process to enable clear, rapid communication of security information. Integration and clear internal processes across teams are especially critical in the electric-power and gas sector, where different methods of production and parts of the generation, transmission, and distribution chain can use

significantly different technology. The security champions can serve as the linchpins of these capabilities and processes, ensuring the sharing of critical information and marshaling the response to individual incidents.

Throughout the entire organization, utility companies must integrate cyber and physical security into their already-robust safety cultures. From the CEO on down, employees must hear consistent, aligned messages underscoring the theme that security is everyone’s responsibility and emphasizing specific tactical actions that will be needed as individual threats arise. Utilities should leverage their best practices to ensure that all employees are aware of the specific threats facing the organization and the specific indicators they, as employees, should be looking for in order to contribute to the overall security of the company and its customers. While the creation of a security champion may create a point of responsibility for security, companies must be clear that it is a shared responsibility (Exhibit 4).

Exhibit 3

As data analytics drives convergence of OT and IT, organizations will need to rethink technology, policies, and operating model.



Source: Bengt Gregory-Brown and Derek Harp, *Security in a converging IT/OT world*, SANS Institute white paper, November 2016, ge.com

Exhibit 4

Defined security zones help to keep threats in one part of the operation segregated.

Illustrative architecture for a power-generation plant

○ Conduit

Location	Level						
Headquarters/ office	Level 4: IT corporate network	Corporate network domain controller		Corporate network computer		Enterprise resource planning (ERP)	
Plant office	Level 4: IT plant business network	Business network domain controller		Business network computer			
Data center	Level 3.5: DMZ	IT firewall	OT firewall	Web server	Asset- management system	Log location and forwarding	DMZ
Central control room	Level 3: Process-control network	Turbine-management system Performance-management system			Emergency shutdown Emergency shutdown system		
Local control room/plant proceses area	Level 2: Supervisory control	Workstation	Local human– machine interface		Workstation	Local human– machine interface	
Plant process area	Level 1: Process control	Field controller			Field controller		
Plant process area	Level 0: Field process devices	Turbines			Emergency-shutdown- system sensors and actuators		

From a technical standpoint, we do not support the conventional wisdom advocating complete air gaps between IT and OT networks. Critical infrastructure elements such as turbine-control systems and monitoring equipment throughout the network require internet connectivity to vendors and other third parties; developing a policy by exception to allow individual devices to circumvent air gaps introduces points of vulnerability into the system. Further, OT systems are never truly air-gapped, as they have unintentional pathways that result in connections between OT networks, systems and devices, and the IT network. Instead, we recommend that utilities take a security-minded standpoint in designing clear DMZs between IT and OT networks. IT and OT

organizations should maintain their own firewalls at the edge, but firewall policies should be coordinated to ensure that both organizations have access to requisite functions and data on the other's networks.

Furthermore, additional security zones on the IT network should be established to ensure the protection of IT systems that can have a significant impact on operations. For example, placing maintenance systems and trouble ticketing for OT systems—both of which are IT functions—into a separate security zone will ensure that these critical functions have extra protection in case of a compromise of the broader IT network (see sidebar “Key recommendations in utility cybersecurity”).

Key recommendations in utility cybersecurity

Develop strategic threat intelligence that is relevant to the C-suite:

- Lead intelligence reporting with the potential business impact of threats.
- Integrate intelligence reporting into strategic planning and war-gaming.
- Exercise incident response plans to build institutional muscle memory and process clarity.

Integrate security across regions and organizations:

- Centralize all regions and business units under a single set of cybersecurity standards with input from across the enterprise.

- Create a common operating picture across physical security, cybersecurity, and IT.

- Integrate security into business units' culture through security champions.

- Create structured processes for security-related information sharing and decision making across organizations.

- Design clear and safe DMZs between IT and OT network according to a defined set of rules. Do not depend on air-gapping.

- Identify and create security zones to protect critical functions across both IT and OT networks.

Partner across the industry:

- Create common standards, and use industry organizations to push for security by design in IT and OT technologies, especially smart-grid devices that may lie outside utilities' direct control.
- Participate in regional consortiums to discuss security across shared power grids and ensure secure implementations of OT protocols (e.g., IEC 101, IEC 104) from utility to utility.
- Organize future-facing industry-wide exercises to predict and preemptively address threats to broader grid security.

A whole-of-industry approach to converged threats

Utilities are well aware of the cybersecurity threats against critical infrastructure, have security programs in place, and are taking active cross-utility steps, including through industry working groups, to protect their organizations. One such group is the Electricity Subsector Coordinating Council (ESCC), a CEO-led organization that coordinates and cooperates between the electric utility industry and government organizations to prepare for, respond to, and recover from threats to critical infrastructure. A part of ESCC is the Cyber Mutual Assistance Program that provides for shared cyber, IT, and other resources and expertise in the event of a cyberattack. The structure allows for participating organizations to cross-leverage services, people,

and tools, which is an effective method to both gain scale and share knowledge.

Another such organization is the Electricity Information Sharing and Analysis Center (E-ISAC) that is operated by NERC and was established at the request of the US Department of Energy in 1999. E-ISAC, organizationally separated from NERC's enforcement processes, serves as a collaborative organization across the United States, Canada, and Mexico for the sharing of cybersecurity-threat information including alerts across both cybersecurity and physical security. There are also other collaborative efforts across the energy sector and between the private sector and government agencies including at the national, state, and regional levels.

Together, these organizations are channels for the utility industry and government organizations to coordinate on, prepare for, and respond to cybersecurity threats, vulnerabilities, and incidents.

Getting started: How utilities can adopt a best-practice approach

To inform an integrated approach to security and establish a whole-of-industry approach to converged threats, utilities should begin with a holistic cybersecurity maturity assessment to evaluate current cybersecurity maturity, benchmark capabilities against industry peers, and identify opportunities to build incremental capabilities. In addition, they should map key business functions into a value chain, allowing business units to prioritize and protect the most critical information assets and systems that drive business value. By examining the protections for those systems, companies can ensure that the cybersecurity program is robust and systems are protected against emerging threats.

Utilities looking to develop a strategic threat intelligence program should perform the following actions:

- Identify gaps and opportunities based on the company's existing threat intelligence program, with a view toward increasing situational awareness across teams and identifying areas

where information sharing can be improved internally as well as externally with other utilities, vendors, and service providers.

- Define a robust threat intelligence program, including identification of tactical, operational, and strategic threat intelligence topics, products, and artifacts and a corresponding cadence for release of each product.
- Conduct detailed review of enablers to the strategic threat intelligence program, including the threat intelligence team's operating model and knowledge-sharing capabilities.
- Train key threat intelligence stakeholders on product-development and information-sharing best practices.

In addition, best-in-class companies ensure that the cybersecurity program has a strong underlying operating model. Critical to success is the design of a cybersecurity service catalog and accompanying operating model and process flows, identifying key roles and touchpoints across stakeholders, and creating measures of success for the program. Success measures include metrics for technical, operational, and process-related activities, including information sharing and feedback on shared strategic or cyberthreat intelligence products.

Tucker Bailey is a partner in McKinsey's Washington, DC, office, of which **Adam Maruyama** is an alumnus; and **Daniel Wallance** is an expert in the New York office.

Designed by McKinsey Global Publishing
Copyright © 2020 McKinsey & Company. All rights reserved.