McKinsey & Company

Risk Practice

The Latin American energy sector: How to address cybersecurity

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

by Kevin Eiden, Elias Goraieb, Kevin Nobels, and Daniel Wallance

January 2021

The risk of a cyberattack against electric-power and gas services in Latin America is significant. According to a security studies 2016 paper, "in Latin America and the Caribbean, cyberattacks on energy power plants could become the most serious threat to any country for the impact on the population and the physical destruction of structures in an extremely wide area." In addition, electric-power and gas companies in Latin America face a formidable challenge because of mixed ownership across public and private entities for energy generation, transmission, and distribution.[1]

We have observed three characteristics that make the sector especially vulnerable to cyberthreats. First is an increased number of threats facing utilities, from nation-state actors seeking to cause security and economic dislocation to cybercriminals who understand the economic value represented by this sector. Second is utilities' expansive and increasing footprint, arising from geographic and organizational complexity, including the decentralized nature of cybersecurity leadership. Third, the electric-power and gas sector's unique interdependencies between physical and cyber infrastructure make companies vulnerable to exploitation, including physical destruction.

The below examples illustrate the threat of cyberattacks to critical-infrastructure firms in Latin America:

— In June 2020, a Brazil-based electric company was targeted by hackers with ransomware. The firm has not disclosed details about the attack, but attackers demanded a $14 million ransom.[2]

— In late April 2020, a Brazilian electric company was hit with a cyberattack that took many services offline for several days. Customers were only able to access customer-support services via a call center and through the WhatsApp platform.

— In 2017, a Latin American oil company was presumed to be affected by the WannaCry ransomware attack. The firm reportedly disconnected systems from the internet to prevent spread of ransomware.[3]

To answer these challenges, we apply our work in more cyber-advanced industries (for example, 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 implement a forward-looking approach to security that integrates the security function into critical decisions about corporate expansion and the accompanying increase in infrastructure and geographic complexity.

— *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.

— *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 continue to engage in regular dialogue on how to secure the delicate ties between physical and virtual infrastructure, as well as IT and

[1] Boris Saavedra, *Critical infrastructure in Latin America: Connected, dependent, and vulnerable*, William J. Perry Center for Hemispheric Defense Studies, April 2016, williamjperrycenter.org.
[2] Ionut Arghire, "Ransomware operators demand $14 million from power company," SecurityWeek, July 2, 2020, securityweek.com.
[3] Peter A. Manos, "Utility companies among those impacted by ransomware attack," *T&D World*, May 25, 2017, tdworld.com.

operational-technology (OT) networks. In Latin America, there are multiple stakeholders that participate in the energy industry (for example, private organizations, governments/regulators) that should continue to collaborate on cybersecurity.

Utilities should consider the following actions:

— Start with a holistic assessment to evaluate current cybersecurity maturity, benchmark capabilities against industry peers, and identify opportunities to build incremental capabilities.

— 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.

— Ensure that the cybersecurity program has a strong underlying operating model, including a cybersecurity service catalog and accompanying process flows, key roles and touchpoints across stakeholders, and measures of success for the program.

Why is the industry vulnerable?

Several characteristics of the energy sector heighten the risk and impact of cyberthreats against utilities (Exhibit 1).

Expanding number of threats and threat actors

Nation-state actors and other sophisticated players have demonstrated greater willingness to target infrastructure providers as part of their broader campaigns.[4]

In addition, cybercriminals target utilities and other critical-infrastructure players for profit. One compelling example occurred in Puerto Rico. Cyberattacks on smart meters owned by a Puerto Rican electric-power utility cost the company up to $400 million in revenue.[5] As Latin American energy

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 SCADA[1] systems

Network

Theft of customer information, fraud, and disruption of service

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

[1]Supervisory control and data acquisition.

[4]"National Terrorism Advisory System Bulletin: Summary of terrorism threat to the US homeland," US Department of Homeland Security, January 4, 2020, dhs.gov.
[5]Brian Krebs, "FBI: Smart meter hacks likely to spread," Krebs on Security, April 12, 2012, krebsonsecurity.com.

In Latin America, most countries have laws and standards for cybersecurity, but many are in the early stages of maturity.

firms expand their deployment of smart meters, threats such as these will need to be mitigated. 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.[6]

Hacktivists may pose threats that tend to be less sophisticated but still have potential to disrupt electric-power and gas operations such as through distributed denial-of-service (DDoS) attacks.[7]

While most utilities have become aware of the risks associated with cybersecurity, there are still inconsistencies in investments in OT and IT cybersecurity controls and in developing coordinated strategies. In Latin America, most countries have laws and standards for cybersecurity, but many are in the early stages of maturity.[8]

Accelerated digital transformation

Latin American energy firms are rapidly digitizing to meet the scale and complexity of energy demands for more distributed and less predictable sources of energy (wind, solar). While these new systems allow energy firms to more efficiently and effectively match supply and demand, they also increase the exposure to different types of cyberthreats. The following are two examples of high-profile digital transformations in Latin American energy firms:

— A major global electricity-generation company operating in Chile has digital transformation at the heart of its strategy. Owners of electric vehicles can link their car batteries to the energy grid and act as energy suppliers.[9]

— A Latin American oil and gas company has also put digital transformation as a core pillar in its corporate strategy. The transformation seeks to capture value from a wide array of digital technologies, including automation, cloud, machine learning, and blockchain.[10]

Expansive footprint

By their very nature, utilities must operate a geographically distributed infrastructure across many sites. For example, Brazil is home to the longest high-voltage direct-current transmission line in the world.[11] Large geographic footprints

[6] "Alert (AA20-049A): Ransomware impacting pipeline operations," Cybersecurity and Infrastructure Security Agency, February 18, 2020, us-cert.cisa.gov.
[7] Eduard Kovacs, "DDOS attacks more likely to hit critical infrastructure than APTs: Europol," SecurityWeek, September 27, 2017, securityweek.com.
[8] *Critical infrastructure in Latin America*, 2016.
[9] "Enel, the digital transformation," Enel, November 28, 2017, enel.com.
[10] "Petrobras puts people at the heart of its digital transformation," DNV GL, January 7, 2019, dnvgl.com.
[11] "Brazil has the third-largest electricity sector in the Americas," US Energy Information Administration, March 23, 2017, eia.gov.

make it difficult to maintain the necessary visibility across IT and OT systems. This challenge is heightened in developing regions of the world and in large-footprint, low-energy-return production sites such as solar farms, where the cost of robustly securing a site could exceed any revenue realized from site operations.

Many utilities rely on several different business units to refine, generate, transmit, and distribute energy and resources. For example, some OT-policy regimes may allow the use of untested Internet of Things technology and even makeshift technical solutions to monitor operations without considering larger-scale cyber vulnerabilities. Combined with the large number of employees, contractors, and vendors who require access to utility-company sites and systems, these organizational constraints make IT security policies, including identity and access management, especially difficult.

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.

For example, a cyberattack targeting the complex network of regional authorities in charge of distributing and monitoring distribution of electricity across transmission lines could lead to swift physical damage.[12] An attacker could disrupt routine monitoring processes so that monitoring authorities cannot detect overloaded transport systems.

Additional risk accompanies the expansion of new technologies, especially those associated with large-footprint green-energy sources (for example, 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.[13]

Weaving a web of protection

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 continue to take a proactive, preemptive view of the varied and advanced threat landscape. Organizations should employ analytic teams that can provide a holistic, proactive view by monitoring threats across the industry and region, including intelligence about technical vulnerabilities and the various factors, such as geopolitical, economic, and legal, that shape the threat environment.

It is critical that this strategic intelligence not only provide awareness but also inform strategic decision making and response plans. 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. 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 for emergent ransomware or a coordinated multiphase attack.

An integrated approach to security

To address the vast geographic, organizational, and technical gaps in their networks and visibility, utilities must continue to take an integrated approach to security (see sidebar "A cybersecurity vision for a Latin American critical-infrastructure firm"). 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 continue to think critically, from both an organization and people standpoint, about how to address organizational siloes that may, for valid

[12] *Critical infrastructure in Latin America*, 2016.
[13] Jason Staggs, "Adventures in attacking wind farm control networks," Black Hat, July 2017, blackhat.com.

business reasons, have very different requirements and indicators. This includes setting an agenda and standards for the cybersecurity program that can be utilized and implemented across even the most disparate business units, 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.

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 allowing them to detect and communicate trends that may indicate a coordinated attack. A Latin American oil and gas firm recently deployed security champions across plants and facility locations with the mission of being the eyes and ears for security risk across the IT and OT environments.

From the CEO and down the line, employees must continue to hear consistent, aligned messages underscoring the theme that security is everyone's responsibility. 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.

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

A cybersecurity vision for a Latin American critical-infrastructure firm

In 2019 a critical-infrastructure company in Latin America built new cybersecurity capabilities as part of a longer-term cybersecurity transformation. The company suffered from cybersecurity incidents that resulted in financial losses.

An initial cybersecurity maturity assessment indicated maturity gaps below industry benchmarks resulting in risks that exceeded board risk appetite. The cybersecurity function needed the resources and capabilities to do the following:

1. conduct a comprehensive cybersecurity-maturity assessment
2. develop a strategy and road map of initiatives to fill critical cybersecurity gaps and improve maturity to meet board-mandated targets and risk appetite

The approach included a full cybersecurity-maturity assessment against each step of the value chain over eight weeks to understand the organization's current cybersecurity maturity and identify critical improvement opportunities. Using the output of the assessment, the company defined a vision and strategic road map comprising several initiatives to bring maturity in line with board-mandated targets.

To drive progress on the strategy, the company defined the strategic and tactical elements of the road map and several initiatives over six months to enable effective implementation and jump-start progress.

This effort showed the following significant impacts on the organization's cyber effectiveness:

1. transformed organizational culture to one that places cybersecurity on a level similar to safety
2. increased awareness of the board and executive leadership team, discussing security at each meeting to track risk reduction
3. implemented the cybersecurity road map and greater investment in cyber as a proportion of overall IT spend, growing the size of the security team

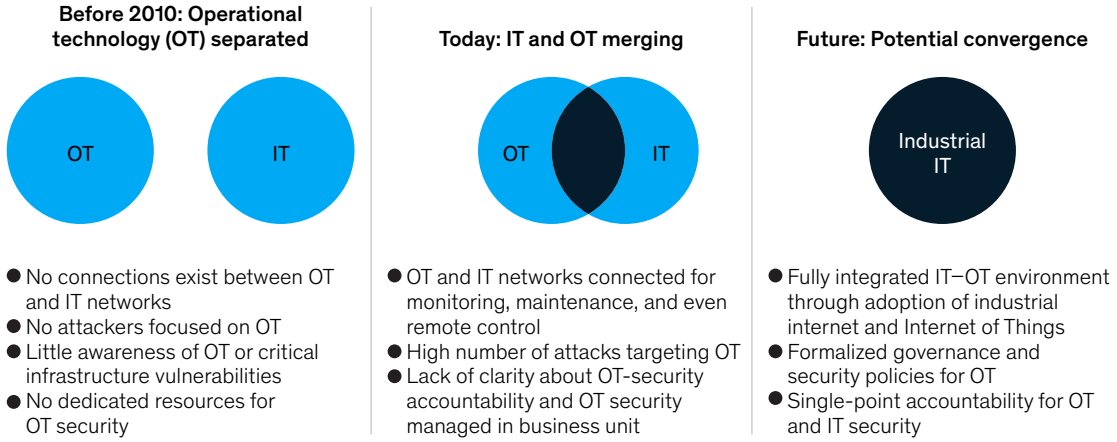
The company continued to design processes, including refining governance and crisis response as well as developing selection criteria for technology tools. Eventually the company achieved its target maturity and a path to continued cyberrisk reduction and rapidly transitioned to a work-from-home model after implementing priority controls, in response to the COVID-19 pandemic.

From the CEO and down the line, employees must continue to hear consistent, aligned messages underscoring the theme that security is everyone's responsibility.

systems and monitoring equipment throughout the network, require internet connectivity to vendors and other third parties. 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 segregation zones between IT and OT networks. 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 (Exhibit 2) (see sidebar "Key recommendations in utility cybersecurity").

Exhibit 2

As data analytics drive the convergence of operational technology and IT, organizations will need to rethink technology, policies, and operating models.



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

A whole-of-industry approach to converged threats

Only through a shared dialogue around emerging technologies and their integration with existing systems can utilities address the unique challenges posed by the convergence of cyber and physical infrastructure. This level of collaboration is extremely important when considering the national and regional power grids in place in many countries, where the responsibility for generating, transmitting, and distributing energy is shared across multiple publicly and privately owned entities and regulated by governments. Given the interconnected nature of the grid and grid systems, the industry must continue to collaborate to secure the data that drive national-level power grids and enhance the security of all players.

At a global level, we believe that multinational organizations—and organizations with international joint ventures—should continue to collaborate across national and regional boundaries to align on overarching organizational and governance standards (for example, NIST CSF or C2M2) and on more in-depth industrial technical standards (for example, IEC 62443). Specific additional controls as mandated by local regulations can supplement these standards. This balance, whether adopted at a corporate level or across a broader swath of the industry, will ensure continuous improvement of the cybersecurity program and address operational risks posed by more fragmented cybersecurity programs where business units in different countries often operate under vastly different models.

Key recommendations in utility cybersecurity

We recommend electric-power and gas companies implement three key recommendations focused on C-suite communications, integrations across regions and organizational units, and partnership across the industry.

1. 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.

2. 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 secure architecture that supports business goals and defines clear and safe demilitarized zones between IT and operational-technology (OT) networks according to a defined set of rules.
- Identify and create security zones to protect critical functions across both IT and OT networks.

3. 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.
- Continue to participate in regional consortiums to discuss security across shared power grids and ensure secure implementations of OT protocols.
- Organize future-facing, industry-wide exercises to predict and preemptively address threats to broader grid security.

Utilities 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.

Another such organization is the Electricity Information Sharing and Analysis Center (E-ISAC[14]) that is operated by the North American Electric Reliability Corporation (NERC) and was established at the request of the US Department of Energy in 1999.[15] The E-ISAC, organizationally separated from NERC's enforcement processes, serves as a collaborative organization across Canada, Mexico, and the United States for the sharing of information about cybersecurity threats, including alerts across both cybersecurity and physical security. There are also other collaboration efforts across the energy sector and between the private sector and government agencies.[16]

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.[17]

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.

McKinsey's Cyber 360 framework (Exhibit 3) integrates these approaches into a single comprehensive framework.

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

- Identify 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.

[14] E-ISAC, eisac.com.
[15] NERC, nerc.com.
[16] US Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, energy.gov.
[17] "Governance," E-ISAC, 2020, eisac.com.

Exhibit 3

An integrated cyberrisk framework provides a consistent point of reference for IT and operational-technology diagnostics.

Cybersecurity capabilities

User and developer awareness and practices	Asset identification and management	Threat intelligence	Technical protections	Security operations	Third-party controls	Incident and crisis response and recovery
Training for front line and executives	Value-chain mapping	Intelligence collection, analysis, and reporting (eg, for open source, dark web)	Identity and access management	Monitoring of and event detection for IT/OT networks and systems	Third-party risk assessment, inventory, and tiering of IT and OT	Incident classification and escalation
Training on secure software-development life cycle for developers	Critical-asset inventory	Modeling of IT and operational-technology (OT) vectors	Data protection and privacy	User-behavior analytics	Third-party technical testing	"Tabletop" technical simulations of IT and OT
Awareness communications	Mapping of information assets to systems	Insider-threat awareness	Encryption	Penetration and red-team testing	Automated onboarding and tracking	Response playbooks
Modeling by executives	Top-risk identification		Vulnerability management	Threat hunting		
			End-point protection of IT and OT networks	Cyberdeception awareness		
			App security	Digital forensics		
			Cloud security			
			SecDevOps			

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, which identify key roles and touchpoints across stakeholders and create measures of success for the program.

Kevin Eiden is a consultant in McKinsey's Chicago office, **Elias Goraieb** and **Kevin Nobels** are both partners in the São Paulo office, and **Daniel Wallance** is a consultant in the New York office.

The authors wish to thank Marcelo Aude, Tucker Bailey, and Pedro Menezes for their contributions to this article.

Designed by McKinsey Global Publishing