Deloitte.
Insights

FEATURE

Managing cyber risk in the electric power sector

Emerging threats to supply chain and industrial control systems

Steve Livingston, Suzanna Sanborn, Andrew Slaughter, and Paul Zonneveld

The power sector is one of the most frequently targeted and first to respond to cyberthreats with mandatory controls. But threats continue to evolve, reaching into industrial control systems and supply chains, and requiring even greater efforts to manage risk.

THE NETWORK OF power plants and lines connecting to homes and businesses is widely considered to be among the most critical infrastructure in the world, especially in advanced economies. It's also one of the most frequently attacked, with consequences that could potentially reach far beyond the power sector.[1]

Many countries across the globe have classified electrical infrastructure as critical to a functioning society. The US government labels energy as one of 16 critical infrastructure sectors considered so vital that "their incapacitation or destruction would have a debilitating effect on security, national economic security, (and) national public health or safety."[2] In particular, the power sector is seen as uniquely critical for the "enabling function" it provides across all critical infrastructure sectors.[3] If the power went out across a large region for an extended period, highly dependent systems—such as financial, communications, transportation, water, and sewer networks—would be severely impacted, leaving the population immobile, incommunicado, and in the dark. In a word, vulnerable.

Many countries across the globe have classified electrical infrastructure as critical to a functioning society.

In this article, we assess the growing sources of cyber risk in the power sector, track evolving threats, threat actors, and vulnerabilities, and explore one of the sector's most challenging vulnerabilities—cyber risk to the electric power supply chain. We then examine the nature of cyber supply chain risk, delve into recent supply chain attacks and their impact on the power sector, and discuss challenges in addressing these risks. Finally, we explore the steps that power companies can take to manage cyber risk across the enterprise and up the supply chain.

Much ado about something: Growing cyber risk in the power sector

Energy is one of the top three sectors targeted for attack in the United States. In 2016 alone, the sector reported 59 incidents, 20 percent of the 290 total incidents reported in that year.[4] Only two other sectors reported more incidents—critical manufacturing and communications. This, however, is not specific to the United States alone—the sector has been a prime target in Europe and Japan; in Australia, it was identified as the sector with the highest number of reported incidents or near-incidents related to critical infrastructure.[5] What's more, electric power companies report a continuous barrage of attempted intrusions, and though most fail, activity is accelerating. US Energy Secretary Rick Perry commented that such intrusions are "happening hundreds of thousands of times a day."[6] And in early 2018, there was "an extreme uptick" in cyberattacks targeting the electric grid in North America.[7]

Not only are attacks rising, but cybersecurity experts and intelligence sources report that the number of threat actors is increasing and their capabilities expanding.[8] Internal threats due to human error, disgruntled employees, or contractors have typically been one of the most common

threats. But nation-states and organized crime are becoming more active, and most disturbingly, could be intersecting.[9] Nation-state actors are believed by some to be contracting with organized crime groups, possibly to ensure deniability.[10] The problem can be compounded as hackers with little institutional or technical knowledge can increasingly access sophisticated tools on the dark web, which operates outside of the traditional internet. Figure 1 illustrates the variety of adversaries that may threaten electric grids, and the perceived severity of the threat and impact in the United States. This threat profile typically changes over time and from country to country.

One of the most common attack vectors in the power sector is phishing, or attacks launched via email asking users to click on a link that then injects malware into their systems, or via email asking for personal data to enable unauthorized network access. In 2017, out of 226 cyber bulletins posted by the US Electricity Information Sharing and Analysis Center (E-ISAC) on its portal, over 30 percent involved phishing.[11] Other common attack vectors include "watering hole," credential theft, denial of service, and remote access trojans.

Attackers set sights on ICS and third parties

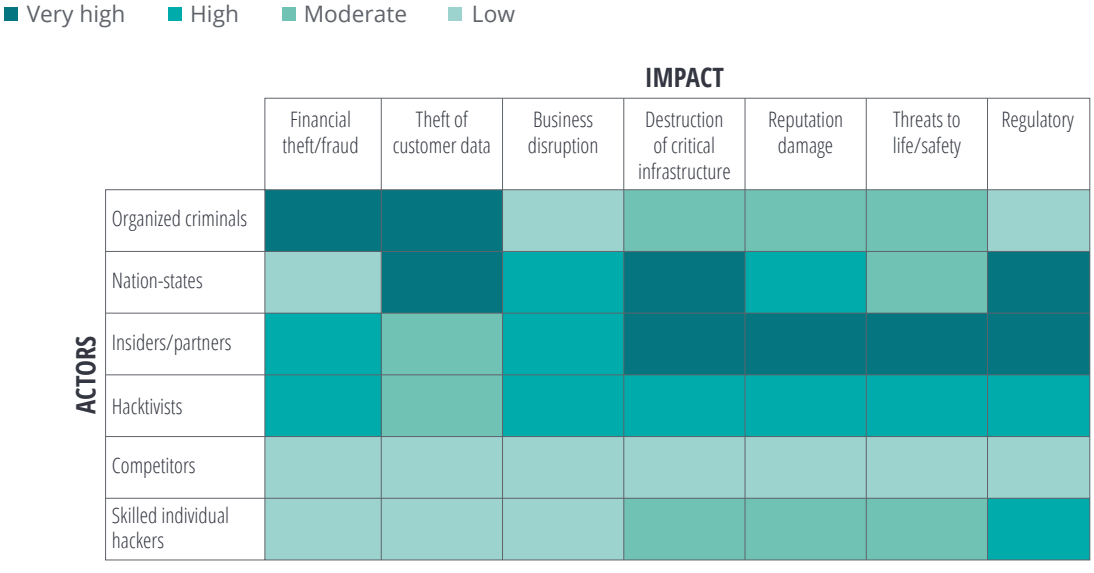
Power companies have long been aware of growing cyber risk, and were one of the first industries to respond, with requirements to implement cybersecurity controls through the North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC-CIP) standards, initiated in 2007. Nonetheless, the threat continues to evolve, as attackers home in on industrial control systems (ICS) and attempt to access them through third parties in the power sector supply chain.

TARGETING ICS BLURS LINE BETWEEN CYBER- AND PHYSICAL ATTACKS

In another unsettling but growing trend, cyberattackers are increasingly targeting industrial control systems (ICS), sometimes potentially laying

FIGURE 1

The cyberthreat profile for the US electric power sector is highest from three key actors



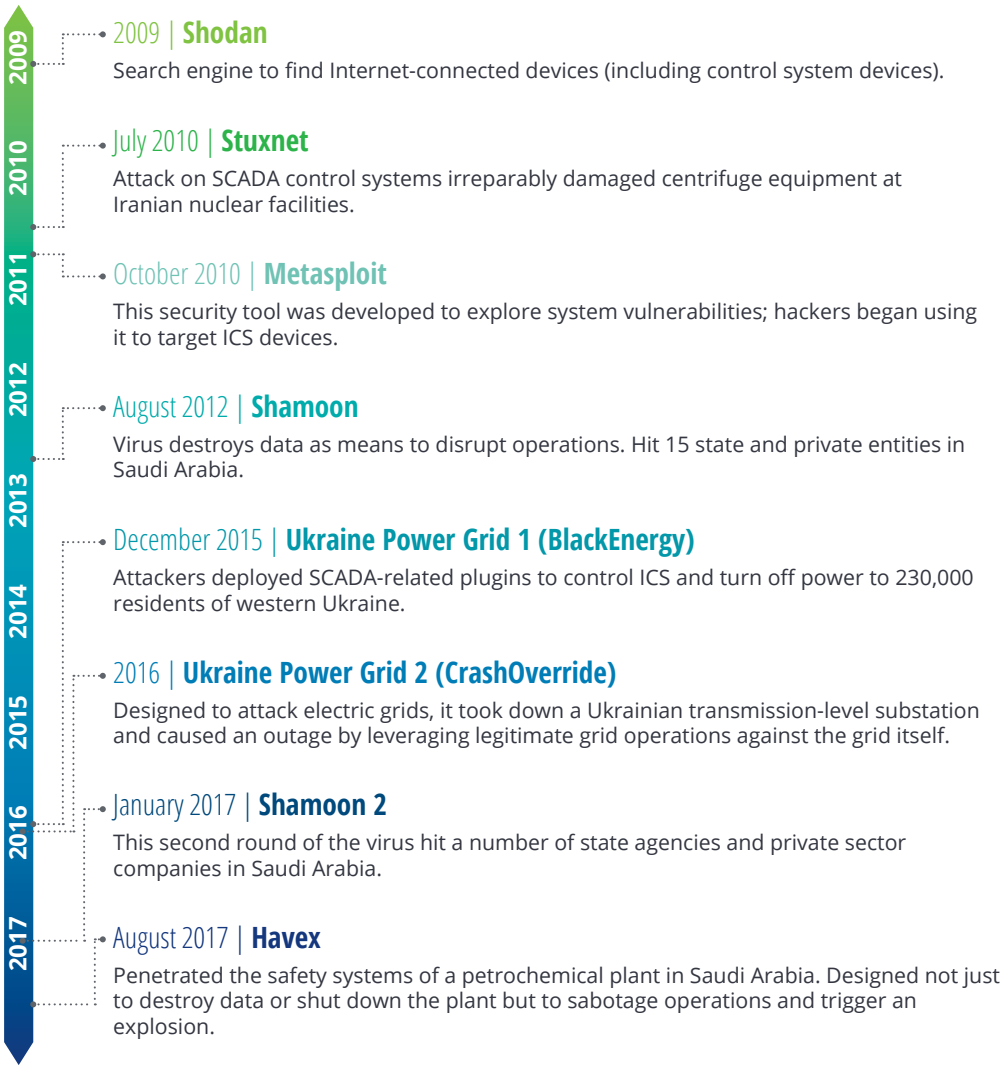
Source: Deloitte analysis.

the groundwork to do physical damage to the grid. Previously, attackers primarily targeted utilities' information technology (IT) systems to steal data or launch ransomware for financial gain. The threat is now becoming even more insidious, with reports of hackers tied to nation-states and organized crime trying to burrow their way into utility ICS, seeking to learn how systems operate, and positioning themselves to control critical physical assets, such as power plants, substations, transmission, and distribution networks, and to potentially disrupt or destroy them.

This targeting of ICS, which has developed over a decade, is blurring the lines between cyber- and physical attacks, prompting national security concerns in many countries. ICS attacks have evolved in scope and purpose across the globe (figure 2). Attackers began by exploiting software developed for

FIGURE 2

Software and malware attacks on ICS have been evolving since 2009



Source: Deloitte analysis; Hank Kenchington, *DOE strategy for energy sector cybersecurity*, US Department of Energy, September 14, 2018, p. 7; news reports.

legitimate purposes, such as Shodan and Metasploit, to find components and devices connected to the internet, and to target supervisory control and data acquisition (SCADA) and other ICS software. A common thread is that all of these attacks are either known or suspected to have been carried out or supported by nation-states to further political goals, and such activity appears to be on the rise. In a particularly disturbing ICS-targeted attack in 2017, a revised version of the Havex virus penetrated the safety systems of a Saudi petrochemical plant. Investigation revealed that the attack, which was foiled only by a bug in the computer code, was likely intended to cause an explosion that could have killed and injured people.[12]

Against this backdrop of increasing threats to power grids across the globe is a growing source of potential cyber vulnerability—grid modernization. Despite almost limitless advantages to be gained from digitizing and modernizing the grid, modernization can also increase a utility's "attack surface," or the number of routes hackers can exploit to enter utility systems. As grids become increasingly "smart," with information and communications technologies and devices embedded throughout, networks are being linked, the system is gaining complexity, and the number of access points is rising. In addition, as utilities introduce more commonly used software and information technologies into their operations, their systems may become more accessible to adversaries. And, as they increasingly automate functions, the impact of an attack is potentially magnified. Taken together, all of these factors spell increased vulnerability.

ONLY AS STRONG AS ITS WEAKEST LINK: CYBER SUPPLY CHAIN RISK

Power companies used to consider cyber risk in terms of the vulnerability of either *IT systems*, meaning software, hardware, and technologies that process data and other information, or *operational technology* (OT) systems, meaning software, hardware, and technologies that help monitor and control physical devices, assets, and processes, including the ICS. In recent years, however, the two systems have been converging as companies digitize and build the power sector's version of the industrial internet of things, including the "smart grid." And, as challenging as it may be for power companies to identify their own critical assets and protect them, the challenge seems to be expanding exponentially, since today's interconnected world also requires them to secure vast, far-flung, and increasingly complex global supply chains.

Power companies purchase information, hardware, software, services, and more from third parties across the globe. And threat actors can introduce compromised components into a system or network, unintentionally or by design, at any point in the system's life cycle. This may be through software updates or "patches," which are downloaded frequently, or through firmware that can be manipulated to include malicious codes for exploitation at a later date. Adversaries may also compromise the hardware that utilities install in their operating systems.[13]

Threat actors can introduce compromised components into a system, unintentionally or by design, at any point in the system's life cycle.

In the attack that nearly triggered an explosion and casualties at a Saudi petrochemical plant in 2017 (figure 2), a newly engineered version of the Havex virus was introduced remotely through a brand of controllers used in about 18,000 industrial plants globally.[14] These controllers perform safety functions such as regulating voltage, pressure, and temperatures in nuclear and water treatment facilities, refineries, and chemical plants. The virus was meant to disrupt those functions in the plant.

Investigators suggest that although this malware is not highly scalable, the method of attack provides a blueprint for those seeking to corrupt similar equipment elsewhere in the world.[15]

To further explore this threat, figure 3 examines three recent cyberattacks that originated in the supply chain and impacted the power sector. Two of them targeted ICS specifically, and the third targeted IT systems. Alarmingly, all three appeared bent on immediate or potential future disruption rather than financial gain.

FIGURE 3

Three cyberattacks demonstrate threat to power sector through supply chain

ATTACK
Hackers breached utility ICS in United States and other countries through multiple supply chain partners (2016–17)

PERPETRATOR
Dragonfly, aka Energetic Bear[16]

VECTOR
- Attackers altered commonly visited industry websites (watering holes) to spread malicious content, harvest visitor credentials (i.e., passwords), and use them to launch attacks on trusted partners.
- Eventually gained access to IT service providers and utilities' corporate IT networks and sought documentation to help breach ICS firewalls.[17]

IMPACT
- Accessed hundreds of utilities' and other industrial facilities' ICS in the United States, Turkey, and Switzerland.[18]
- Conducted reconnaissance; assessed control system design, capabilities, and vulnerabilities.[19]
- Copied configuration information and interface screens.

IMPLICATIONS
- Investigators believe Dragonfly is an advanced persistent threat actor backed by a nation-state that was gathering information and potentially laying the groundwork for future attacks.
- National security experts are deeply concerned about these breaches and their repercussions.[20]

ATTACK
Attack on small cloud services provider impacted US natural gas, oil, and electric power sectors (April 2018)[21]

PERPETRATOR
Unknown or undisclosed

VECTOR
- Vector undisclosed, but analysts suggest it could have been ransomware, with attackers freezing the company's computers and demanding payment in exchange for the key to unencrypt the files.[22]

IMPACT
- At least five natural gas pipeline companies shut down electronic communications, slowing the tracking and scheduling of gas flows.[23]
- Some large power providers cut links with the platform that provides them with pricing and demand models for electricity transactions and issued estimated bills.
- Some providers issued bills late, and some risked under- or overestimating the amount of power to purchase for customers.

IMPLICATIONS
- Did not disrupt gas or electricity flows but underscored interdependence between the two sectors and their vulnerability to widespread disruption through an attack in the supply chain.
- Highlighted importance of planning and preparing for supply chain disruptions from cyberattacks.
- Such electronic data interchange (EDI) systems could enable intruders to jump from IT systems to ICS[24]

ATTACK	PERPETRATOR
NotPetya attack crippled company operations across multiple sectors, costing at least US$10 billion in damages globally (spring 2017)[25]	**State-sponsored actor**

VECTOR

- Attackers hacked into the servers of a Ukrainian accounting software provider and sent corrupted software updates to its clients globally. The infected malware mimicked ransomware by encrypting files but did not demand ransom.

IMPACT

- Attack infected at least six local electric utilities and jumped to Ukrainian branches of several large global companies.
- Sprinted across the globe, disrupting operations in shipping, pharmaceuticals, construction, consumer goods, and other sectors.
- Trucks backed up at ports, goods piled up in warehouses, key vaccine supplies dwindled.
- Damages reached at least US$10 billion.[26]

IMPLICATIONS

- This was the first high-impact global supply chain attack, demonstrating the destructive power of such an assault. Similar attacks could be as bad or worse.
- Demonstrated a new diplomatic norm; perpetrator unconcerned with collateral damage across globe. Any company could become an unintended target.
- Attack unleashed hypervirulent cyberwarfare weaponry developed by nation-states.[27] Utilities and others should assess their vulnerabilities to such attacks and consider addressing them.

Source: Deloitte analysis.

When it comes to reducing cyber risk in the supply chain, companies in the power sector face many challenges. First, cyber supply chain accountability and ownership typically do not fall into well-defined, specific groups within a company. They may touch diverse departments, including supply and procurement, corporate information security, cloud and infrastructure, legal, IT, and OT. Most CISOs have no control over the enterprise's supply chain, and may have little access to supply chain cyber risk intelligence. To mitigate cyber supply chain risk, ownership and accountability should be clearly established.

Second, the business may be pressuring managers to increasingly move operations out to the cloud before they can determine whether the provider is secure. However, companies often have scant visibility into suppliers' risk management processes and what those processes imply for their own operations.[28] Given sufficient time, they can analyze the potential impact of a cyberattack and map, plan, and build resilient solutions. This should be done before moving operations to the cloud, especially data and energy management systems that could impact reliability if hacked.

Another frequent challenge is the lack of manpower, especially given the overwhelming number of suppliers that should be assessed. A study of 20 electric and gas utilities in North America revealed that the utilities had on average 3,647 total active suppliers, 39 strategic relationships, and 140 suppliers that accounted for 80 percent of their total external spend.[29] Companies may be unable to get access to some suppliers, and some suppliers may be unable or unwilling to adopt secure practices. In addition, certain types of potential cyberthreats can "walk past" controls, such as supply chain firmware updates. Today, most power companies have little control over what suppliers are doing; they're just beginning to make suppliers more aware and accountable, and to demand supplier integrity.

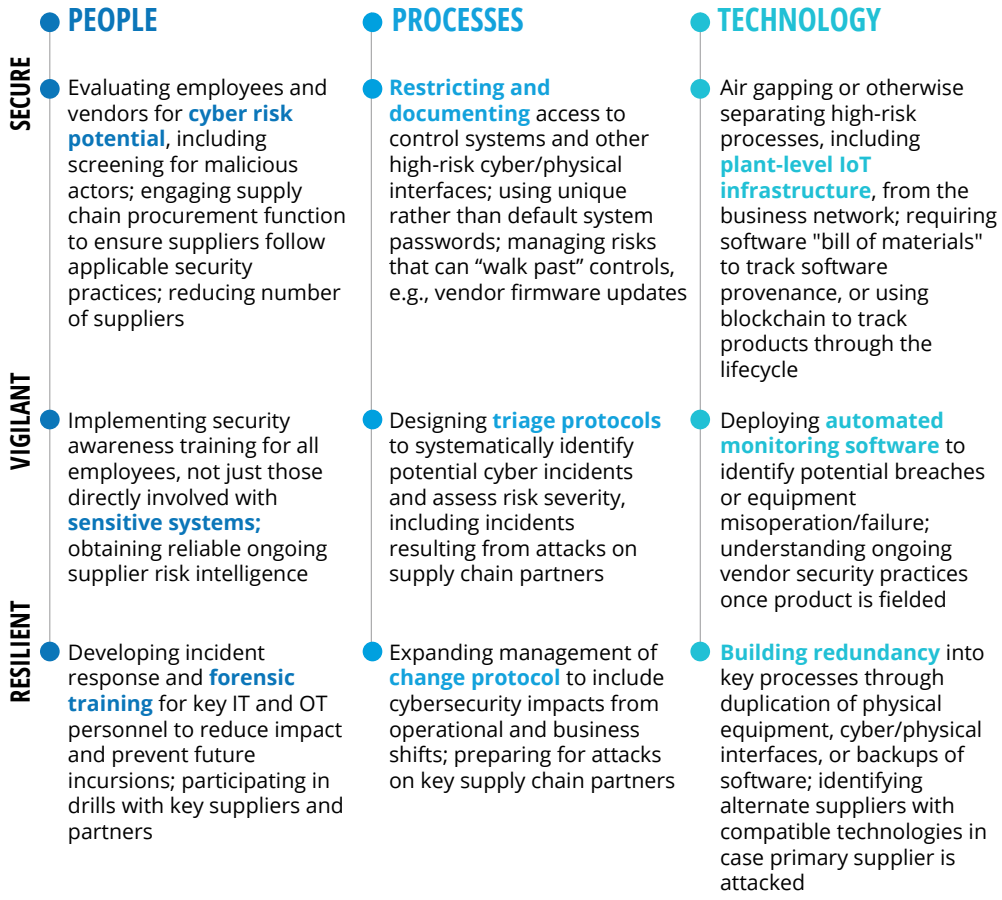
Nonetheless, there's hope. There are several steps that companies can take to address cyber risk, particularly in the supply chain.

Managing cyber risk across the enterprise and up the supply chain: Next steps

The first step to consider in reducing cyber risk across the enterprise is to identify and map assets and their connections, and prioritize them by criticality. The next is to determine if critical assets and networks have well-known and exploitable vulnerabilities. An example would be a control systems network with a default hardcoded password that's available through an internet search. The third step is assessing the maturity of the controls environment for proactively managing threats. To do this, it's often helpful to use an established model, such as the Deloitte cybersecurity maturity model.[30] The final step would be to build a framework to protect critical assets that uses people, processes, and technology to become secure, vigilant, and resilient (figure 4).

FIGURE 4

Advancing cybersecurity maturity by becoming more secure, vigilant, and resilient



Note: Learn more about the secure, vigilant, and resilient framework in Andrew Slaughter and Paul Zonneveld, *An integrated approach to combat cyber risk: Securing industrial operations in oil and gas*, Deloitte, May 2017, p. 8.

Source: Deloitte analysis.

MANAGE CYBER RISK IN THE SUPPLY CHAIN

To manage cyber risk in the electric power supply chain, consider starting by engaging the supply chain procurement function. It's often helpful to get everyone in the same room and focus on good governance. Address procurement language and obtain reliable supplier assessments and cyber risk intelligence. Focus on the larger vendors first and drop those you aren't using. Understand risks that can "walk past" controls, such as supply chain firmware updates. Perform business analyses and business planning for resilience in case an attack succeeds.

Enhance procurement practices

When it comes to evaluating potential suppliers, a key goal should be to understand the supplier's maturity and security processes for connected products and services. Companies can conduct vendor risk assessments and gather ongoing intelligence themselves or through specialized cybersecurity firms and consultants.

At the program level, focus on whether the supplier's processes adhere to leading security practices and keep the product or service secure once fielded or sold. Such practices tend to include threat intelligence, and patch and vulnerability management. At the product level, focus on whether the vendor's corporate processes ultimately include security safeguards in the product or service design. To accomplish this, ask the supplier to provide a summary of its security features. Companies can also require that the supplier respond to a cybersecurity questionnaire and provide evidence of having completed a security risk assessment.

When it comes to evaluating potential suppliers, a key goal should be to understand the supplier's maturity and security processes for connected products and services.

Power companies can also consider the following practices when seeking to integrate cybersecurity into the procurement process:

- **Establish the criteria to determine product prioritization.** Companies might consider attributes such as widescale dependence where reliability is critical or when large quantities of the product are used.
- **Create and socialize information to be collected in advance of procurement.** Assessments can range from simple attribute-based checklists to comprehensive control-based assessments based on unique needs and security initiatives.
- **Use procurement and sales to open dialogue with service providers.** Product manufacturers and service providers are more likely to fully engage when procurement initiates the conversation.
- **Ensure that the right people are engaged and have ownership of the process.** The relevant product manufacturer and service provider subject matter specialists (such as engineers) should be engaged to provide insights.
- **Process integration, automation, tooling, and scale can increase efficiency.** Organizational buy-in, cross-functional collaboration, tooling, and learning efficiencies can dramatically reduce the cost and time needed to integrate cybersecurity and procurement.

There are many other measures that power companies can implement to enhance procurement practices. An increasingly common practice is to require a software bill of materials, or composition analysis, which tracks the software components in a system across the supply chain to reveal any potential issues. Such procurement language generally mandates disclosure of commercial and open-source, third-party software

components as well as any defects listed in public reference databases.[31]

ENGAGE WITH INDUSTRY PEERS AND GOVERNMENT AGENCIES

To further manage both supply chain and enterprise cyber risk, consider going beyond individual enterprise efforts. This could mean helping to develop industry standards and certification programs, exchanging threat intelligence with peers and government agencies, and testing new technologies and innovative processes.

Help develop standards and certification programs

Consider engaging with industry peers and government agencies working to reduce cyber risk in the power sector locally, nationally, regionally, and globally. Get involved with national and international standards-setting efforts or join initiatives to establish common frameworks for reducing cyber risk globally. Collaborate with peers and government agencies to exchange intelligence on threats and vulnerabilities. Participate in local, national, and global cybersecurity drills, such as the North American Electric Reliability Corporation's (NERC's) GridEx or the EIS Council's transnational EarthEx exercise.[32] Finally, keep abreast of innovative technologies and processes being developed to manage cyber risk.

To get involved in global standards-setting, reach out to organizations such as the International Society for Automation and the International Electrotechnical Commission, which has established the IEC-62443 series of multi-industry cybersecurity standards for industrial automation and control systems (IACS).[33] A set of commonly accepted OT standards is being developed because while most IT systems allow the user to deploy a wide variety of software, OT devices and systems may not be compatible with other software systems. These standards will apply to hardware and software systems such as SCADA, networked electronic sensing, and monitoring and diagnostic systems, as well as associated internal human, network, or machine interfaces.[34]

POWER SECTOR LEADS WITH MANDATES TO REDUCE CYBER RISK, INCLUDING SUPPLY CHAIN

The North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC-CIP) reliability standards have put the power sector at the forefront in establishing regulations to reduce cyber risk. NERC-CIP standards became a legal requirement for bulk electric system (BES) owners, operators, and users in 2007. In 2018, NERC added a new standard (NERC-CIP 013) and modified two existing standards to address cyber supply chain risk. However, NERC-CIP standards apply only to high- and medium-impact BES entities and power companies, and not their suppliers and vendors, or low-impact entities—which leaves additional systems and assets potentially at risk if not addressed.[35]

Another option is to join efforts to build comprehensive frameworks to help protect critical hardware, software, and networks from cyberthreats. For example, Siemens has joined hands with the Munich Security Conference and other governmental and business partners (including global power companies AES Corporation and Enel SpA) to launch the Charter of Trust initiative.[36] The initiative calls for binding rules and standards to ensure cybersecurity and advance digitalization. It urges business and trade partners to deploy more robust identification procedures for network access, increase the use of encryption and firewalls, engage in constant monitoring and anti-virus protection, and use international standards, such as IEC 62443.[37]

Several certification efforts are also underway. One is the Cyber Product International Certification Commission initiative, which seeks to create a centralized, industry-driven mechanism to certify hardware and software products and provide a sus-

tained validation process.[38] Another is the European Union Agency for Network and Information Security's program to create a certification framework for information and communication technology security.[39] Groups such as the International Organization for Standardization (ISO) and the IEC currently provide standards and certification for IT and IACS products and processes globally, and have been developing cybersecurity-related standards. Among the many other initiatives, Eaton is collaborating with global safety consulting and certification company Underwriters Laboratories to help establish measurable cybersecurity criteria for connected power management products and systems.[40]

Regardless of which cybersecurity framework and certification schemes are adopted, businesses are seeking widespread, or even mandatory, participation among peers globally to avoid any incentives to gain competitive advantage through noncompliance. Ultimately, for these efforts to work, customers would need to understand the value of cybersecurity and be willing to pay for it. After all, the cost of not securing the grid is likely to be far higher.

A successful industrywide cybersecurity framework requires widespread business participation and customers that are willing to pay for it.

Exchange threat intelligence with peers and government agencies

Collaboration for threat intelligence and incident response involves exchanging information about cyber- and physical threats and vulnerabilities on the grid. Many countries have launched information sharing and analysis centers (ISACs), such as the E-ISAC managed by the NERC. The E-ISAC seeks to boost the industry's response capabilities by gathering, analyzing, and sharing data, coordinating incident management, and communicating mitigation strategies. The group also manages a public–private partnership, called the Cybersecurity Risk Information Sharing Program, which collaborates with energy sector partners to share threat information and develop tools to help protect critical infrastructure.

Some countries also have computer security incident response teams and computer emergency response teams for the power sector. The US Department of Homeland Security, Department of Energy (DOE), and intelligence agencies are seeking to enhance coordination and accelerate sharing of actionable intelligence on cyberthreats and vulnerabilities with the industry.[41]

Beyond government intelligence sources, private cybersecurity consulting firms, often staffed by former intelligence analysts, can provide real-time cyberthreat and vulnerability monitoring to power companies. Some also conduct supplier risk assessments and provide ongoing third-party threat intelligence.

INNOVATE AND DEPLOY NEW TECHNOLOGIES TO MANAGE CYBER RISK

Innovation is at the forefront of power companies' and their suppliers' quest to reduce cyber supply chain risk. Research labs across governments, universities, and the private sector are developing new tools and technologies to help them do so. Initiatives may involve redesigning devices, components, and processes. For example, some suppliers are automating manufacturing to reduce risk associated with human intervention. Or they're implementing new track-and-trace programs to establish provenance by capturing the component's "as built" identity and linking it to sourcing information. Many devices now contain computer chips that can be tracked through scanning and auditing throughout their life cycle. This can help companies explore ways to reduce cyber risk, process data

more efficiently, and safely archive this data by using blockchain (see sidebar).

BLOCKCHAIN CAN TRACK COMPONENTS THROUGHOUT THE SUPPLY CHAIN

Often described as an automated, distributed ledger, blockchain technology can be used to track a transaction or follow the physical journey of a component through every stage of its life cycle, translating it into a code that provides an accurate and immutable digital record of where it's been and who may have had access to it. To circumvent nearly constant cyberattacks, Estonia has digitized most government operations and put them on a blockchain.[42] The technology's encryption protocols allow data to be re-encrypted faster than hackers can intercept it, thereby providing a virtual safety net that has not so far been hacked. Blockchain can make cloud computing more secure as it creates decentralized nodes that contain copies of all data in the ecosystem. It becomes more difficult to alter any one record, because each exists in multiple locations.

In the United States, the DOE, its labs, and research partners are developing tools and technologies to help identify malicious functionality in hardware, firmware, or software of components as they traverse the supply chain.[43] Researchers have already developed ways to monitor and detect suspicious traffic, intrusions, and anomalies on networks; spot insider attacks, spoofed data, and malicious commands; and recognize emerging threats and develop real-time responses. One useful tool to deploy against supply chain threats examines how an executable file will operate without running the file, allowing operators to examine new software and detect tampering before deployment.[44]

Researchers are also working on technologies to help prevent cyber incidents, such as those that can decrease the cyberattack surface by enabling secure exchange of cryptographic keys to prevent compromise of critical energy sector data.[45] They are also working on tools that could potentially deny any unexpected cyber activity from taking place on an energy delivery system—preventing it from doing anything off-spec—and then changing the control system configuration dynamically, creating a moving target to help prevent reconnaissance and impede attack planning.[46] Such tools could be useful to counter threats such as the 2017 Dragonfly or Energetic Bear attacks.

USE ANALYTICS AND VISUALIZATION TO AUDIT REAL-TIME CYBER RISK PROFILE

The role of internal audit is important in reducing cyber risk. To help gain real-time visibility into a company's cyber risk profile, analysts can collect relevant data, pull it into an analytical model, and build a customized real-time dashboard to track cyber risk in real time.

Conclusion

The power sector cyberthreat landscape is rapidly evolving and expanding, with more frequent attacks, more numerous and varied threat actors, and increasingly sophisticated malware and tools that are more widely available and sometimes indiscriminately deployed. Power companies are among the most frequently attacked targets, increasingly by nation-state actors aiming for disruption and even destruction through ICS. One of the most challenging vulnerabilities to address is cyber supply chain risk, given the increasingly far-flung and complex nature of the supply chain. Cyber supply chain accountability and ownership are not well-defined within companies, most CISOs have no control over their enterprises' supply chain, and they may have little access to supply chain cyber risk intelligence or visibility into suppliers' risk management processes. Add to that a lack of manpower and the sheer number of suppliers and transactions, and you begin to appreciate the scope of the challenge. Most companies are just beginning to make suppliers more aware and accountable, and to demand supplier integrity.

Cyber risk is challenging to address, but companies can start by identifying and mapping critical assets across the extended enterprise; using a cybersecurity maturity model to assess the maturity of the control environment; and building a framework that is secure, vigilant, and resilient.

After reducing their own cyber risk profiles, power companies can collaborate with peers, governments, suppliers, and other industrial sectors to share intelligence, participate in practice exercises, develop new standards and frameworks, and pilot new technologies. New tools are increasingly available, and the capability to monitor networks in real time, discover threats, and address them is also advancing rapidly. If electric power companies seize these opportunities, they can reduce risk significantly for themselves, the power sector, and, given the critical nature of the service they provide, society as a whole.

Endnotes

1. National Cybersecurity and Communications Integration Center, *FY 2016 incidents by sector*, U.S. Department of Homeland Security, accessed October 28, 2018, p. 1.
2. U.S. Department of Homeland Security, "Critical infrastructure sectors," accessed October 28, 2018.
3. U.S. Department of Homeland Security, "Energy Sector," accessed October 28, 2018.
4. National Cybersecurity and Communications Integration Center, *FY 2016 incidents by sector*.
5. Australia Cyber Security Centre, *2016 threat report*, accessed October 2018, p. 15.
6. Jeff St. John, "U.S. government accused Russia of hacking into energy infrastructure," Greentechmedia, March 19, 2018.
7. Rich Heidorn, Jr., "Expert sees 'extreme uptick' in cyberattacks on utilities," *RTO Insider*, February 19, 2018.
8. Ibid.
9. Matthew J. Schwartz, "Cybercrime groups and nation-state attackers blur together," Bankinfosecurity.com, June 28, 2018.
10. Lillian Ablon, "Data thieves: The motivations of cyber threat actors and their use and monetization of stolen data," The Rand Corporation, testimony presented before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance, March 15, 2018, p. 6.
11. E-ISAC serves as the primary security communications channel for the electricity industry. See: North American Electric Reliability Corporation, *State of reliability 2018*, June 2018, p. 40.
12. Nicole Perlroth and Clifford Krauss, "A cyberattack in Saudi Arabia had a deadly goal. Experts fear another try," New York Times, March 15, 2018.
13. Paul Stockton, *Securing critical supply chains*, Electric Infrastructure Security Council, June 19, 2018.
14. Ibid.
15. Robert M. Lee, *TRISIS: Analyzing safety system targeted malware*, Dragos Blog, December 14, 2017.
16. United States Computer Emergency Readiness Team, "Alert (TA18-074A): Russian government cyber activity targeting energy and other critical infrastructure sectors," U.S. Department of Homeland Security, March 15, 2018.
17. Ibid.
18. Security Response Attack Investigation Team, "Dragonfly: Western energy sector targeted by sophisticated attack group," Symantec Blogs, October 20, 2017.
19. United States Computer Emergency Readiness Team, "Alert (TA18-074A): Russian government cyber activity targeting energy and other critical infrastructure sectors."
20. Ibid.
21. Naureen S. Malik and Ryan Collins, "The cyberattack that crippled gas pipelines is now hitting another industry," Bloomberg, April 5, 2018.
22. Blake Sobczak, "Attack on natural gas network shows rising cyberthreat," *E&E News*, April 6, 2018.
23. Malik and Collins, "The cyberattack that crippled gas pipelines is now hitting another industry."
24. Sobczak, "Attack on natural gas network shows rising cyberthreat."

25. Andy Greenberg, "The untold story of NotPetya, the most devastating cyberattack in history," *Wired*, August 22, 2018.

26. Ibid.

27. Scott Shane, Nicole Perlroth and David E. Sanger, "Security breach and spilled secrets have shaken the N.S.A. to its core," *New York Times*, November 12, 2017.

28. Beau Woods and Andy Bochman, "Supply chain in the software era," The Atlantic Council, May 30, 2018, p. 4.

29. Tim Schmidt, "Three critical procurement best practices for electric utilities: Are you doing these?," Procureware.com, July 1, 2016.

30. Andrew Slaughter and Paul Zonneveld, *An integrated approach to combat cyber risk: Securing industrial operation in oil and gas,* Deloitte, May 2017, p. 6.

31. Woods and Bochman, "Supply chain in the software era."

32. North American Electric Reliability Corporation, "GridEx," accessed November 6, 2018; Electric Infrastructure Security Council, "EarthEx 2017," August 22, 2018.

33. The International Society of Automation, "ISA99, industrial automation and control systems security," accessed November 6, 2018.

34. Ibid.

35. North American Electric Reliability Corporation, *Reliability Standards for the Bulk Electric Systems of North America*, updated July 3, 2018.

36. Siemens, "Time for action: Building a consensus for cybersecurity," May 17, 2018.

37. Ibid.

38. Stockton, "*Securing critical supply chains*."

39. The European Commission, "The EU cybersecurity certification framework," August 22, 2018.

40. Eaton, "Eaton establishes cybersecurity collaboration with UL, announces industry's first lab approved for participation in UL program for cybersecurity testing of intelligent products," February 13, 2018.

41. Cyber GRX, "CyberGRX is transforming third-party cyber risk management," accessed October 2018.

42. Nathan Heller, "Estonia, the digital republic," *New Yorker*, December 18 and 25, 2017.

43. Stockton, "*Securing critical supply chains*," p. 19.

44. Office of Electricity Delivery & Energy Reliability, *Multiyear plan for energy sector cybersecurity*, U.S. Department of Energy, March 2018.

45. Ibid, p. 34.

46. Ibid.

About the authors

STEVE LIVINGSTON, a principal with Deloitte & Touche LLP, has more than 24 years of information security and risk management experience. Livingston's diverse portfolio of cyber projects include: Identity and Access Management (IAM), Enterprise Resource Planning (ERP) security, Governance Risk and Compliance (GRC), and Security Event Management (SIEM) implementations. He is based in Seattle. Connect with him on LinkedIn at www.linkedin.com/in/stlivingston/.

SUZANNA SANBORN is a senior manager on Deloitte's Research & Insights team where she analyzes global energy trends with a focus on the power and utilities and renewable energy sectors. She has more than 20 years of experience in research, analysis, marketing, communications, and program management in the power and utilities, oil and gas, and renewable energy sectors. Sanborn is based in McLean, Virginia. Connect with her on LinkedIn at www.linkedin.com/in/suzanna-sanborn-510164/.

ANDREW SLAUGHTER is an executive director of the Deloitte Center for Energy Solutions, working closely with Deloitte's Energy & Resources leadership to define, implement, and manage the execution of the center's strategy; develop and drive energy research initiatives; and manage the development of the center's eminence and thought leadership. Slaughter specializes in strategy, market fundamental analysis, organizational design, and policy advice. He is based in Houston. Connect with him on LinkedIn at www.linkedin.com/in/slaughterandrew/.

PAUL ZONNEVELD is a partner in the Canadian firm with over 25 years of experience serving clients in oil and gas, mining, power, and utilities. He has in-depth knowledge of business issues facing ER&I clients including digital, innovation, cyber, sustainability, energy trading, and operational risk management. Zonneveld also serves as the global LCSP for Husky Energy, one of the largest accounts for the Canadian firm. He is based in Calgary, Canada. Connect with him on LinkedIn at www.linkedin.com/in/paul-zonneveld-917b7a3/.

Acknowledgments

The authors would like to thank the utility executives, association executives, and other industry experts who shared their perspectives with us for this article. We would also like to thank **Jaya Nagdeo** and **Deepak Vasantlal Shah** of Deloitte Support Services India Pvt. Ltd. for their research support; and **Sharon Chand**, **Michael Prokop**, **Brad Singletary**, **Nick Sikorski**, and **Steve Batson** of Deloitte US; Adam Crawford of Deloitte Canada; and **Charlie Hosner** and **Dave Clemente** of Deloitte UK for sharing their cybersecurity expertise.

Contacts

Scott Smith
Vice chairman
US Power & Utilities leader
Deloitte LLP
+1 619 237 6989
ssmith@deloitte.com

Sharon Chand
Risk Advisory principal
Cyber Risk Services leader
Energy, Resources & Industrials
Deloitte & Touche LLP
+1 312 486 4878
shchand@deloitte.com

Steve Livingston
Risk Advisory principal
Cyber Risk Services leader
Power & Utilities
Deloitte & Touche LLP
+1 206 716 7536
slivingston@deloitte.com

David Nowak
Risk Advisory principal
Cyber Risk Services
Deloitte & Touche LLP
+1 312 486 4126
danowak@deloitte.com

GLOBAL CONTACTS

Paul Zonneveld
Global Risk Advisory leader—Energy, Resources & Industrials
Deloitte Canada
+1 403 503 1356
pzonneveld@deloitte.ca

Brian Murrell
Global Risk Advisory leader—Power & Utilities
Deloitte US
+1 212 436 4805
bmurrell@deloitte.com

Felipe Requejo
Global Sector leader—Power & Utilities
Deloitte Touche Tohmatsu Limited
+34 914 381 655
frequejo@deloitte.es

Rajeev Chopra
Global leader—Energy, Resources & Industrials
Deloitte Touche Tohmatsu Limited
+44 20 7007 2933
rchopra@deloitte.co.uk

Jonathan Giliam
Risk Advisory leader—Power & Utilities
Deloitte Africa
+27 112 027 317
jgiliam@deloitte.co.za

Hendri Mentz
Risk Advisory leader—Power & Utilities
Deloitte Australia
+61 8 9365 7367
hmentz@deloitte.com.au

Anthony Hamer
Sector leader—Power & Utilities
Deloitte Canada
+1 416 643 8409
anhamer@deloitte.ca

Tsutomu Yamada
Risk Advisory leader—Power & Utilities
Deloitte Japan
+81 906 520 3928
tsutomu1.yamada@tohmatsu.co.jp

Andreas Langer
Risk Advisory leader—Power & Utilities
Deloitte Germany
+49 711 1655 47289
anlanger@deloitte.de

Charles Hosner
Risk Advisory leader—Power & Utilities
Deloitte North West Europe: UK
+44 20 7007 2827
chosner@deloitte.co.uk

Arup Sen
Risk Advisory leader—Power & Utilities
Deloitte India
+91 22 6185 6610
arupsen@deloitte.com

Richard Kuang
Risk Advisory leader—Power & Utilities
Deloitte China
+86 1085 207 401
rkuang@deloitte.com.cn

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Kavita Saini, Abrar Khan, Rupesh Bhat, and Preetha Devan

Creative: Kevin Weier and Molly Woodworth

Promotion: Nikita Garia

Cover artwork: Infomen

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

About Deloitte