CYBERSECURITY

THE NEW PROFESSIONAL RISK

PART 3 OF 4: WILL A CYBERATTACK ON THE ENERGY AND TRANSPORTATION INDUSTRIES BECOME THE NEXT GLOBAL CRISIS?

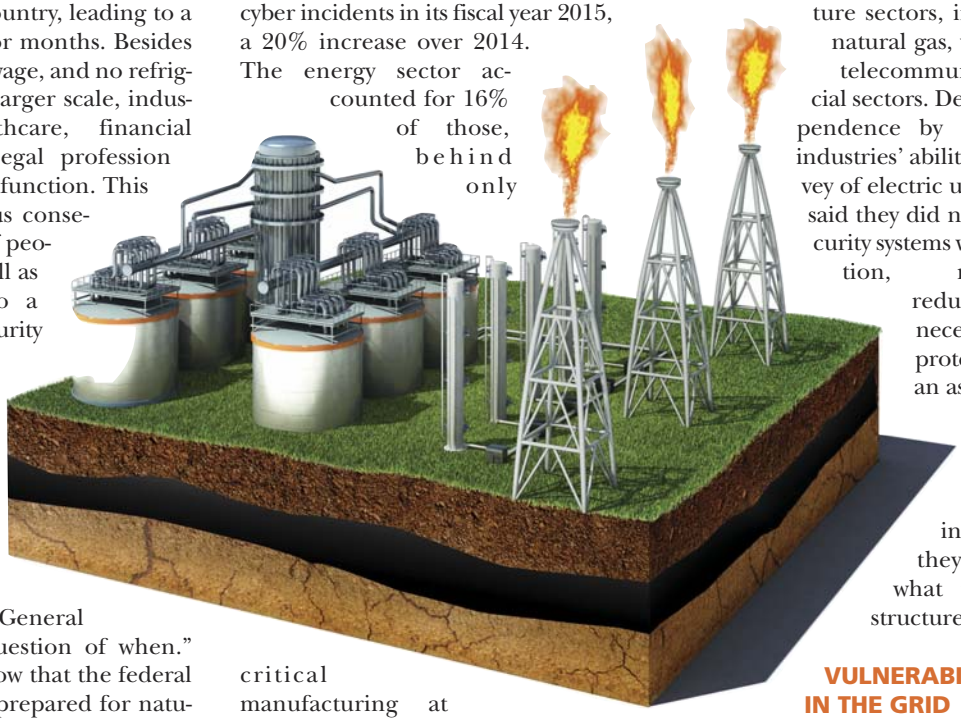
Karen Painter Randall and Steven A. Kroll Connell Foley LLP

According to a report in 2014 by a division of the Department of Homeland Security, there were 79 hacking incidents investigated at energy companies. In connection with same, it has been reported that an attack on just one of the nation's three electric power grids could cripple much of the United States' infrastructure. Should this occur, such a cyberattack could have a catastrophic effect on our country, leading to a blackout lasting weeks or months. Besides no running water, no sewage, and no refrigeration and light, on a larger scale, industries such as healthcare, financial institutions, and the legal profession would also be unable to function. This could lead to dangerous consequences for the safety of people in this country as well as bring our economy to a grinding halt. A cybersecurity advisor to President Obama believes that independent actors – from "hacktivists" to terrorists – have the capability as well to attempt such an attack, thus, "It's not a question of if," says Centcom Commander General Lloyd Austin, "it's a question of when." Nevertheless, reports show that the federal government, while well-prepared for natural disasters, has no plan for the aftermath of an attack on the power grid. Thus, Homeland Security has recommended that the best way to prepare is to keep a battery-operated radio nearby.

In addition to the energy industry, the transportation industry has faced similar threats this past year. In the third of a four-part series touching on various professional, business and insurance sectors, this article will discuss the cybersecurity risks facing the energy and transportation industries.

THE ENERGY INDUSTRY

According to national security experts, cyberattacks on America's electric grid top the target list for terrorists and rogue states, yet remain highly vulnerable to same. It was reported that the U.S. Department of Homeland Security Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT) responded to 295 cyber incidents in its fiscal year 2015, a 20% increase over 2014. The energy sector accounted for 16% of those, behind only critical manufacturing at 33%. Although many companies admit to being the targets of these attacks, most have said that they complied only with mandatory cybersecurity standards set by the North American Electric Reliability Corporation (NERC). Other countries face similar threats; a cyberattack against a Ukrainian utility company in December 2015 caused a blackout. The incident, believed to have been perpetrated by Russian cyber criminals using sophisticated malware, demonstrated the vulnerability of the power and utility sector to cyberattacks.



Every critical infrastructure in the United States, from banking to agriculture, is connected to the electrical grid. The electrical grid consists of approximately 6,000 power stations and other small generation facilities, as well as 45,000 substations connected by approximately 200,000 miles of transmission lines. The electrical grid is considered "uniquely critical" because it enables and supports other critical infrastructure sectors, including the oil and natural gas, water, transportation, telecommunications, and financial sectors. Despite such a heavy dependence by the aforementioned industries' ability to function, in a survey of electric utility companies, 48% said they did not have integrated security systems with proper segmentation, monitoring and redundancies, which are necessary for cybersecurity protection. Moreover, only an astonishing 32% of the electric utility companies surveyed stated that they have such protections in place, while 20% said they do not even know what their security infrastructure included.

VULNERABILITIES IN THE GRID

One of the features of the electrical grid that makes it so susceptible to a cyberattack is due to the control systems used. Specifically, the grid uses Supervisory Control and Data Acquisition (SCADA), which is operated with programmable logic controllers (PLCs) making it vulnerable to a cyberattack. Another area of vulnerability relates to the decentralized network owned by numerous local operators. In particular, the deregulation of the electric power industry has resulted in a network of more than 3,000 companies, some of which are well-protected, many of which are not.

However, all the companies are interconnected and, as such, hacking into the most vulnerable could lead to a "domino-like" penetration of even the most secure companies.

Furthermore, a break in one of these transmission lines – accidental or intentional – can cause widespread power outages like the 2003 event that blacked out portions of northeastern United States and southern Canada. The 2003 blackout affected 50 million people, including 14.3 million in New York City and the surrounding areas. Beyond loss of power, the 2003 blackout caused concerns over potential contamination of water supply. It also disrupted transportation systems, mobile communications, cable television systems, and even some radio systems. Moreover, factories came to a halt, or were forced to shut down to conserve energy. According to some reports, at least 11 deaths were attributed to the blackout, and the total cost of the event topped an estimated $6 billion.

PROPOSED SOLUTIONS TO IMPROVE GRID SECURITY

There have been several recommendations made to enhance the grid's reliability, which include upgrading power plant and transmission line infrastructure, incorporating more grid-level storage (batteries, compressed air, pumped hydro, and supercapacitors), adding capacitor banks to handle variations in reactive power, installing advanced circuit protection and communication equipment, and designing fault-tolerant computer hardware and software for use in grid control centers. Furthermore, in the event of a cyberattack, it is likely that multiple systems would be affected; thus, new strategies and protocols are needed to ensure that the automated systems that deal with single-mode failures do not adversely affect each other.

The government's awareness of these risks also appears to be on the rise, which has resulted in an effort to standardize the energy sector's cybersecurity compliance obligations, and will eventually lead to new regulatory activity. Moreover, the U.S. Senate has introduced a wide-ranging energy reform bill, which includes a number of cybersecurity provisions. Specifically, the bill includes a section dedicated to cyber threats, which would empower the Department of Energy (DOE) to take swifter action in the event of a major hack. It authorizes additional cybersecurity research and directs the DOE to work more closely with countries such as Canada and Mexico that are also connected to the North American electrical grid on fighting cyberattacks.

THE TRANSPORTATION INDUSTRY

Similar to the energy industry, the transportation industry also faces cyber threats. In particular, today's vehicles are loaded with electronics, making them an increasingly enticing option for hackers. The cyber threat facing the transportation industry can range anywhere from stealing data, such as credit card numbers stored in iPhones, to a mass-scale cyberattack that could result in hundreds of accidents at the same time. Although the current threat is "more consumer-related," in that car thieves are using wireless software to unlock doors and gain access to vehicles, many believe that these threats could become more safety-related in the future. In fact, researchers have already found ways to hack into a vehicle and compromise safety-critical systems, including features such as the brakes and turning the engine on and off.

Most recently, it was revealed that there was security vulnerability in the Uconnect Internet-enabled software that allows remote control, which could allow hackers to take control of the Jeep Cherokee. Specifically, a hacker could remotely apply the brakes, steer the car, turn the windshield wipers on, and take control of the engine. Unlike other cyberattacks that only target the entertainment system, a Uconnect hack affects the Jeep's driving systems such as GPS, brakes, steering and engine management, enabling remote control of the drive via the Internet. Accordingly, owners of Fiat Chrysler automobiles vehicles were advised by security experts to update their on-board software to prevent a potential cyberattack.

Although automobile manufacturers are well aware of these problems, most have not discussed the specifics of their deterrent systems, because it is such a sensitive issue. The National Highway Traffic Safety Administration (NHTSA) recently established a task force to combat the threat that hackers could pose to automobiles. However, the current complexity of vehicles, not to mention cutting-edge work being done in the field of self-driving cars, only makes the task of keeping cars immune to cyber-terrorism that much harder.

Besides motor vehicles, the U.S.'s air traffic control systems are also vulnerable to cyberattacks. It has been reported that support systems have been breached, which allowed hackers access to personnel records and network servers. According to an audit done by the Department of Transportation's inspector general, it was concluded that although most of the attacks disrupted only support systems, they could spread to the operational systems that control communications, surveillance and flight information used to separate aircraft. This is especially worrisome at a time when the nation is facing increased threats from sophisticated nation state-sponsored cyberattacks.

CONCLUSION

Unlike other industries, the stakes are much higher in the transportation and energy industries. While victims of a cyberattack in the healthcare and retail industries are subjected to costly fines and civil lawsuits, an attack in the transportation and energy industry can have much more serious ramifications, including physical harm to its consumers and ultimately a global crisis. As a result, it is imperative that these sectors implement sufficient policies and procedures to not only prevent an attack, but have a rapid response plan in place in the event such an attack were to occur. Proactively developing a targeted, comprehensive cybersecurity plan is vital to placing a company in the best position possible to withstand government and public scrutiny in the event of a catastrophic cyber incident, an occurrence that according to experts is a foregone conclusion.

Karen Painter Randall is a Complex Litigation Partner with Connell Foley LLP in Roseland, N.J., and co-chair of the firm's Cyber Security and Data Privacy and Professional Liability Practice Groups. She provides representation and advocacy services to professionals and businesses in a wide variety of complex litigation matters and is a veteran trial attorney in state and federal courts. Ms. Randall, vice chair of USLAW's Data Privacy & Security Practice Group and a former chair of USLAW's Professional Liability Group, is designated a Certified Civil Trial Attorney by the Supreme Court of New Jersey.

Steven A. Kroll is an Associate with Connell Foley LLP in Roseland, NJ. In addition to representing professionals in various areas, Mr. Kroll concentrates his practice in the areas of professional liability, general insurance litigation and employment law matters in both New Jersey and New York. Mr. Kroll received his J.D. from Rutgers-Newark School of Law in 2009, cum laude, and received the distinguished award of Order of the Coif.