New York Law Journal

A NEW YORK LAW JOURNAL SPECIAL SECTION

An ALM Publication

Cybersecurity and Privacy

WWW.NYLJ.COM

MONDAY, MARCH 7, 2016

Ensuring Cybersecurity Of **Critical Infrastructure**

BY BORIS SEGALIS AND KATHRYN LINSKY

It should come as no surprise to anyone who has used a mobile phone to pay for coffee or start a car that the world's infrastructure is computerized and connected through the Internet and private networks. The connected world is in many ways more reliable and more efficient. For example, the use of "smart," networked electricity meters that monitor home energy usage in real time has allowed utilities to reduce the need for additional power plants to meet energy demand. This technology also allows utilities to quickly pinpoint and resolve outages. At the same time, the increasingly connected electric grid is vulnerable to cyber threats, such as the recent attacks that disabled electric grids in Ukraine and Israel. These and other incidents demonstrate a key concern with cyber attacks on critical infrastructure—that virtual attacks perpetrated from across the planet using nothing more than a laptop keyboard can result in loss of life, and damage to property and economy.

BIGSTOCK

From power plants to stock and commodity exchanges, from water treatment plants to aircrafts, the systems that make the world tick have been computerized and Internet-connected. Connectivity is what drives efficiency, and as connectivity increases—as it surely will—so too will cyber risks that threaten this critical infrastructure. The true potential for damage resulting from the exploitation of such cyber risks has

BORIS SEGALIS *is a partner of Norton Rose Fulbright in New York, where he is U.S. co-chair of the data protection, privacy and cybersecurity group.* KATHRYN LINSKY *is an associate in the group.*

catapulted the cybersecurity of critical infrastructure out of the virtual realm and into the minds of the public, Congress, regulators, trade groups and other stakeholders. While the United States has not yet experienced a large scale cyber attack resulting in massive loss of life or economic damage, a string of small incidents has helped all stakeholders to understand the devastating potential of an attack on critical infrastructure.

An early example of a cyber attack that garnered significant attention from the public was the Stuxnet malware. Stuxnet is speculated to have been developed by the United States and Israel to attack industrial controls infrastructure that operated Iran's uranium enrichment centrifuges.[1] Stuxnet commandeered industrial controls and inflicted physical harm on Iranian nuclear facilities. The malware also made itself nearly impossible to detect, and offered virtually no clues as to its origin. It is no consolation that the Stuxnet attack was perpetrated by the West because it's only a matter of time before state actors that are not friendly to the United States achieve the level of technical expertise to turn the tables. In fact, this may have already happened, as a string of recent attacks suggests.

A December 2015 attack on Ukraine's power grid—allegedly perpetrated with the support of the Russian government—cut off power to hundreds of thousands of Ukrainian residents in the middle of a cold winter. U.S. investigators from the Department of Energy and Department of Homeland Security (DOH)and the FBI concluded that hackers used malware to destroy computers and wipe out critical control systems, including systems for restoring power and call centers used to report outages.[2] The malware that was used in this attack has also been found in U.S. industrial systems, which raises difficult questions about the cyber preparedness of the U.S. power grid.

Just a month later, in January 2016, Israel's electric grid was also the target of a cyber attack. Israel's Energy Minister released a statement that the Israeli Electric Authority suffered a malicious attack, which paralyzed computers and caused parts of Israel's power grid to be shut down.[3]

> Even technology that seems innocuous, but is ubiquitous, **can wreak havoc in the physical world.** In January 2016, Nest smart thermostats, which operate via the Internet, experienced a software glitch that drained the batteries of thermostats installed in homes across the country.

To put the Ukraine and Israel attacks in context, a cyber attack on the U.S. power grid could potentially replicate the damage that the country already experienced when a blackout in 2003 blanketed the Northeast United States. The blackout affected 50 million people across eight states and Canada, including 14.3 million people in New York City and the surrounding areas. The blackout was a chaotic event, causing concerns over potential contamination of water supply, among other things. According to some reports, the blackout also caused at least 11 deaths and resulted in an estimated $6 billion dollars in total loss.[4]

Indeed, smaller scale cyber attacks have already targeted the United States. Though disclosed only recently, a cyber attack by Iranian hackers in 2013 breached the control systems of a dam in Rye, N.Y. Hackers were able to take control of the dam's flood gates, which would have allowed them to cause flooding and other complications for the area's water infrastructure.[5]

Even technology that seems innocuous, but is ubiquitous, can wreak havoc in the physical world. In January 2016, Nest smart thermostats, which operate via the Internet, experienced a software glitch that drained the batteries of thermostats installed in homes across the country. When consumers expect thermostats to operate autonomously and remotely, and the system fails, results can include freezing homes, bursting pipes, or health problems for people whose conditions may be aggravated by extreme temperature.

Cyber vulnerabilities also affect transportation. In 2015, two researchers demonstrated that they could remotely control a Jeep Cherokee through the vehicle's entertainment control panel. They employed the hack to stop the vehicle by remotely disengaging its transmission.[6] It was eventually discovered that the method the researchers used to simulate the attack could be used to hack hundreds of thousands of vehicles on the road.

While these incidents are not numerous, they have received significant publicity. The White House, Congress, regulators, trade associations and other stakeholders began connecting the dots to understand the significance of this cyber threat, and have begun to move swiftly to fill the legislative and regulatory vacuum in this space. Indeed there has been a staggering number of legislative, regulatory and self-regulatory initiatives to bolster critical infrastructure cybersecurity.

The effort to meaningfully address cybersecurity began in the early part of this decade. When partisan gridlock prevented Congress from enacting cybersecurity legislation, the Obama Administration stepped in with an Executive Order in February 2013. The order, entitled "Improving Critical Infrastructure Cybersecurity," sought to address the shortcomings in the nation's approach to cybersecurity in critical infrastructure.[7] In a companion Presidential Policy Directive: Critical Infrastructure Security and Resilience,[8] the Administration also designated as "critical infrastructure" the physical and virtual systems and assets relating to chemical plants, communications providers, water supply facilities, defense industrial base, emergency services, energy and utilities (including nuclear), financial services, food and agriculture, government facilities, health care industry, information technology, waste management and transportation systems, and water and waste-water systems. By extension, the Framework would extend to the service providers of critical infrastructure owners and operators.

The Executive Order also directed the development of a cybersecurity framework, designed to reduce cyber risks to critical infrastructure. A year later, in 2014, the National Institute of Standards and Technology (NIST) released the Framework for Improving Critical Infrastructure Cybersecurity (the Framework).[9] Though intended to be voluntary, the Framework has already been incorporated into mandatory regulations and industry guidance. The Framework is also being viewed as a best practice benchmark for developing a cybersecurity program.

At a high level, the Framework establishes a common language for owners and operators of critical infrastructure, and their service providers, to use for (1) describing the current cybersecurity posture of their organizations, (2) setting their target state of cybersecurity, (3) identifying and prioritizing opportunities to improve cybersecurity safeguards, (4) assessing progress towards the target state of cybersecurity; and (5) fostering communication between internal and external stakeholders.

The Framework applies this common language to five core principles of (1) *Identify* (identification of cybersecurity risks faced by an entity), (2) *Protect* (implementation of safeguards to mitigate the identified cybersecurity risks, (3) *Detect* (implementation of activities to detect cyber incidents), (4) *Respond* (implementation of procedures to respond to cyber incidents), and (5) *Recover* (implementation of procedures to restore systems affected by cyber incidents and improve safeguards). The Framework itself is based on a broad swath of regulatory and industry cybersecurity experience, cross-referencing a variety of cybersecurity standards and guidance.[10]

The Framework is incorporated into a number of key cybersecurity requirements and initiatives. For example, the Department of Homeland Security (DHS) relies on the central tenets of the Framework in conducting cyber resilience and cybersecurity reviews under several programs—such as the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)—designed to assist critical infrastructure industries in assessing and strengthening their cyber preparedness.

Certain sectors of the financial industry have also begun to rely on the Framework to inform their expanding cyber preparedness regulation efforts. For example, the National Futures Association (NFA) has promulgated rules that will require its members to develop Information Systems Security Programs (ISSPs) starting March 1, 2016.[11] The rules will require NFA members and member firms, including futures commission merchants, introducing brokers, and retail foreign exchange dealers, to adopt and implement policies and procedures to prevent and mitigate unauthorized access to information technology systems that may expose markets and customer data to cyber attack. ISSPs must include an analysis of security and risk, the identification of threats and vulnerabilities, the deployment of corresponding protective measures, the implementation of procedures for response and recovery in the event of an incident, and employee training. The NFA suggests that its members look to the Framework to develop their ISSPs (among other resources).

In the self-regulatory space, the Framework underpins the cybersecurity guidelines developed by the shipping industry. In January 2016, five leading shipping organizations—lead by the Baltic and International Maritime Council (BIMCO)—released a set of guidelines to help the global shipping industry prevent and mitigate the safety, environmental and commercial consequences of a cyber attack onboard a ship.[12] The guidelines, which are not mandatory by authority, focus on cybersecurity awareness, suggest concrete actions ship owners and operators can take to improve cybersecurity, and encourage companies to take a risk-based approach to cybersecurity that may vary based on the business and types of ships involved.

While the Framework is authoritative, regulators have also developed their own, more tailored approaches to addressing cyber risk. For example, the Federal Energy Regulatory Commission (FERC) has approved Critical Infrastructure Protection (CIP) cybersecurity standards for the U.S. power grid. The standards are a set of mandatory controls designed to ensure the security and reliability of the electric grid.[13] Among other issues, the CIP standards address critical cyber asset identification, security management controls, electronic security perimeters, and physical security of cyber assets. To address evolving cyber threats, on Jan. 21, 2016, FERC approved revisions to seven of the CIP reliability standards, such as those related to training and physical security.[14] The CIP standards are mandatory—a failure to comply with these standards may subject relevant regulated entities to potential enforcement actions and penalty assessments. The North American Energy Standards Board (NAESB) has also developed cybersecurity standards that are mandatory for various segments of the energy industry.[15] In the case of natural gas companies, for example, NAESB's cybersecurity standards mandate the use of digital signatures and self-certification to support mutual entity authentication. In contrast, NAESB's Smart Grid standards have only been adopted by FERC as non-mandatory guidance.

These examples of regulations and guidance suggest that while the efforts to regulate cybersecurity of critical infrastructure are only now gaining steam, there is already a rich library of guidance that companies can rely on to develop their cyber resilience programs. Were an attack to occur and result in loss of life, property damage, business interruption or other liability, regulators and plaintiffs are likely to attempt to use this existing and rich guidance to establish that the affected critical infrastructure businesses lacked adequate cybersecurity safeguard, regardless of whether such safeguards were legally required. Regulators and plaintiffs may argue that the relevant cybersecurity controls were not "commercially reasonable" under the circumstances, as benchmarked by legal requirements, industry practices and other relevant guidance. This is the strategy that plaintiffs have already pursued—at times successfully—in data breach litigation.[16] For these reasons, critical infrastructure owners and operators and service providers should be actively assessing and enhancing their cybersecurity programs in anticipation of cyber attacks.

To mitigate potential liability for cybersecurity breaches, critical infrastructure owners, operators and their service providers should first and foremost understand which regulators might come looking for answers in the event of an cyber incident, and how those regulators view cyber risk. Companies should then perform an assessment of their cyber assets to prioritize and quantify associated risk. This assessment must be informed by applicable legal and contractual requirements, industry guidance and other best practices, including the NIST Framework. This assessment should be leveraged into a cybersecurity compliance program that would assist companies in demonstrating, in the event of an investigation or litigation, that they had reasonable cybersecurity measures in place to protect critical infrastructure.

[1] Ellen Nakashima and Joby Warrick, "Stuxnet Was Work of U.S. and Israeli Experts, Officials Say," THE WASHINGTON POST (June 2, 2012), https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

[2] Evan Perez, "U.S. Investigators Find Proof of Cyberattack on Ukraine Power Grid," CNN.COM (Feb. 3, 2016, 8:00 PM), http://www.cnn.com/2016/02/03/politics/cyberattack-ukraine-power-grid/index.html.

[3] Gil Ronen, "Israel Electric Grid Under Severe Cyberattack," ISR. NAT'L NEWS (Jan. 26, 2016, 7:27 PM), http://www.israelnationalnews.com/News/News.aspx/207075.

[4] JR Minkel, "The 2003 Northeast Blackout—Five Years Later," SCIENTIFIC AMERICAN (Aug. 13, 2008), http://www.scientificamerican.com/article/2003-blackout-five-years-later/.

[5] Shimon Prokupecz, Tal Kopan, and Sonia Moghe, "Former Official: Iranians Hacked Into New York Dam," CNN.COM (Dec. 22, 2015, 6:17 PM), http://www.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/.

[6] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With me in it," WIRED (July 21, 2015, 6:00 AM), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[7] THE WHITE HOUSE, EXEC. ORD.—IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (2013), available at https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[8] https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[9] Nat'l Inst. of Standards and Tech., "Framework for Improving Critical Infrastructure Cybersecurity," (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[10] The Framework is mapped to, among other requirements, ISO/IEC 27001/27002, NIST Special Publication 800-53, ISA 99.02.01, ISACA Control Objectives for Information and Related Technology, and Council on Cybersecurity Top 20 Critical Security Controls.

[11] National Futures Association Rule Submission Letter: Information Systems Security Programs—Proposed Adoption of the Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (Aug. 28, 2015), https://www.nfa.futures.org/news/PDF/CFTC/InterpNotc_CR2-9_2-36_2-49_InfoSystemsSecurityPrograms_Aug_2015.pdf.

[12] BIMCO, "The Guidelines on Cyber Security Onboard Ships" (January 2016), http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=10.

[13] North Am. Electric Reliability, "CIP Standards," http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

[14] 154 FERC ¶ 61,037 (2016), available at https://www.ferc.gov/whats-new/comm-meet/2016/012116/E-2.pdf.

[15] 148 FERC ¶ 61,205 (2014), available at: http://www.ferc.gov/whats-new/comm-meet/2014/091814/E-5.pdf.

[16] See, e.g., *Shames-Yeakel v. Citizens Fin. Bank*, 677 F. Supp. 2d 994 (N.D. Ill. 2009).