The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 9 May 3, 2017

ENERGY

Infrastructure Cybersecurity Challenges: A View Through the Oil and Gas Pipeline Lens

By Andrew R. Lee
Jones Walker

In 1997, the ad hoc Presidential Commission on Critical Infrastructure Protection issued an ominous warning that "the capability to do harm" by "cyberattack" to America's critical infrastructures "is growing at an alarming rate, and we have little defense against it."

Since then, we have accepted the reality that the threat of critical infrastructure terror attacks is now pervasive, and has also grown increasingly complex and diffuse. Terrorist actors are employing more sophisticated tools and vectors and have succeeded at targeting public utilities and private companies by permeating the computer-control systems that monitor and manage their assets. State actors have stepped up their targeting of critical U.S. energy infrastructure in particular. Within this energy infrastructure, oil and gas pipelines present a significant area of concern.

See "*WilmerHale Attorneys Explain the Evolving Cybersecurity Environment of the Energy Sector*" (Nov. 16, 2016).

Interdependencies and Lack of Standardization Create Exposures

Energy infrastructures have multiple connection points, or interdependencies, at which assets of different agents combine to create an intricate system. As a result, isolating a calamity (terrorist-initiated or accidental) to one component of the network is exceedingly difficult.

Further, because of the pervasive computerization and automation of infrastructures over the last several decades, interdependencies are increasingly "cyber" in nature – their operation depends on the transfer of digital data and commands. As a result, any discussion of threats against critical infrastructure must begin with the threats posed to cyber assets.

A cyberattack against a pipeline system in the U.S. could cause significant damage, including loss of life and deep shocks to the economy. Despite widespread acceptance of this premise, the federal government has exercised minimal regulatory authority aimed at protecting against external cyber threats to pipeline infrastructure. This is in part due to the primarily private ownership of the nation's oil and gas industry.

In the United States, private companies own the vast majority of pipeline infrastructure, including 2.5 million miles of pipelines transporting natural gas, refined petroleum products, ethanol, chemicals, and other liquids. They are, as a result, responsible for all aspects of pipeline safety, subject to federal and state regulations. Owners generally rely on automated monitoring and control systems, otherwise known as supervisory control and data acquisition (SCADA) industrial control systems (ICS) to manage unmanned facilities. Given the lack of standardization of SCADA systems, however, private owner-operators that have sub-par cybersecurity defense systems present attractive opportunities for hackers to launch large-scale attacks.

In addition to the fact that no mandatory industry- or government-led SCADA system safety guidelines exist to promote system security and to protect against cyber vulnerabilities, historical efforts to formally regulate and standardize cybersecurity measures for pipeline SCADA systems have largely been unsuccessful. Instead, public-private partnership initiatives have long been endorsed as the road to any real security and the path of least resistance.

See "*Energy Industry Demonstrates Public-Private Cybersecurity Coordination*" (Oct. 14, 2015).

Recent Cyberattacks on U.S. Pipeline SCADA Systems

The prospect of cyberattacks on U.S. pipelines reached the public consciousness in March 2012, when DHS revealed that an active "spear-phishing" campaign had targeted the natural gas pipeline industry. (Spear-phishing is a specific type of "phishing" in which an email that appears to be from a known acquaintance or colleague, but it is in fact from a criminal hacker, attempts to entice the recipient to click a link that will deploy malware designed to steal data and hijack computers.)

An investigation conducted by the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) confirmed that targeted attempts and intrusions into multiple natural gas pipeline owners' SCADA systems had begun several months earlier. Analysis of the malware and artifacts of the successful breaches indicated that the cyber threats all related to a single campaign that targeted personnel with emails designed to appear as though they were sent from another trusted member of organization. The study confirmed that the campaign targeted 23 gas pipeline companies and that the cyber-thief stole sensitive operational and technical data sufficient to give the recipient sufficient insider knowledge to cause multiple simultaneous pipeline compressor station explosions.

A separate report by the cybersecurity-consulting firm Mandiant fingered a unit of the Chinese People's Liberation Army as the most likely culprit.

A year later, ICS-CERT confirmed that a number of pipeline gas compressor stations were the targets of "brute force" attempts to compromise their networks. A widely-reported Iranian campaign later in 2013 resulted in the hackers' successfully penetrating SCADA systems before they were detected and the system was salvaged. It was determined that, in both of the 2013 events, the victims' SCADA systems were connected to the public internet, despite the prevalence of expert recommendations that SCADA systems not be internet-facing or at least not have entry-point devices with only default credentials or weak passwords to protect their systems. (As an important aside, a subsequent 2014 DHS survey revealed that 82,000 known ICS hardware or software systems, including SCADA systems, were directly accessible from the public internet, making those systems particularly vulnerable to cyberattacks.)

Around the same time, Infosecurity Magazine reported that a Russian hacker group going by the name "Energetic Bear" caused significant disruption by hacking U.S. energy companies, including petroleum pipeline operators. The group used malware to break into the targets' SCADA systems and relayed sensitive company data and information back to the hackers.

Attacks on industrial control systems have increased exponentially in subsequent years, with 2016 seeing the most ICS attacks to date and, according to IBM Managed Security Services, a 110 percent increase over the previous year. IBM points out that the threat actors are not merely foreign; in fact, the majority of the 2016 attacks originated in the U.S.

Much Ado Government-Led Initiatives, but Few Results

Regulatory efforts to strengthen pipeline-related cybersecurity have had poor results. Months after the 2012 Chinese PLA attack described above, Congress attempted to pass legislation mandating cybersecurity regulations for privately owned critical infrastructures, including pipelines. The bill, however, failed in the Senate, prompting one of its sponsors, Senator Joe Lieberman (D-CT), to remark: "This is one of those days when I fear for our country … we've got a crisis, and it's one that we all acknowledge. It's not just that there's a theoretical or speculative threat of cyberattack against our country — it's real."

Months later, Chairman of the House Committee on Homeland Security, Rep. Michael McCaul (R-TX), shared similar concerns over the lack of statutory and regulatory mandates, specifically highlighting the threat posed by

China, which a 2014 Internet Security Association report had indicated was targeting more than 60 percent of oil and gas pipelines in North America using remote-access technologies.

While the Transportation Security Agency (TSA) has been assigned a key role in pipeline cybersecurity management, it has been criticized repeatedly for failing to do enough. A 2012 report by the Congressional Research Service pointed out that TSA has long had the statutory authority to promulgate cybersecurity regulations that would apply to pipelines, but it has not done so. More recently, a 2015 report from the U.S. Senate Committee on Homeland Security and Governmental Affairs concluded that DHS's cybersecurity programs and practices were unlikely to provide meaningful protection.

The report asserted that DHS is "lousy" at cybersecurity and operates a "dysfunctional culture" managed by incompetent outside contractors. The report also charged that DHS is rife with cybersecurity disasters and widespread wasted resources, and that DHS has failed to comply with its own rules and policies for cybersecurity – hardly serving as a model for private industry.

Finally, the GAO reviewed DHS's programs for overseeing critical infrastructure over a three-year period and found uneven application across critical infrastructure sectors, calling into question DHS's ability to properly assess and prioritize vulnerabilities.

In its defense, TSA has established the National Cybersecurity and Communications Integration Center (NCCIC), with the stated mission to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the nation's critical information technology and communications networks. The NCCIC is DHS's cybersecurity clearinghouse, operating as a physical space where cybersecurity communications monitoring is coordinated. NCCIC is separated into four branches, including the ICS-CERT, which coordinates control systems (including SCADA-related) security incidents and information sharing among federal agencies, state, local, and tribal governments, and control systems owners, operators, and vendors.

Since then, TSA has worked with industry stakeholders to support their adoption of the public-private NIST Framework and the DHS C3 Program (both described below) and has coordinated a voluntary cyber-assessment program with the Federal Energy Regulatory Commission to examine pipeline operators' cybersecurity programs. TSA has also begun to work closely with the pipeline industry to identify and reduce cybersecurity vulnerabilities, including facilitating classified briefings to increase industry's awareness of cyber threats.

In addition to DHS, government initiatives to secure pipeline SCADA systems are overseen by two other government departments – Transportation and Energy. The DOT's Pipelines and Hazardous Materials Safety Administration (PHMSA) oversees the regulatory environment that governs pipelines and also is staffed with dozens of pipeline inspectors. The agency establishes national policy and standards for hazmat transportation and regulates the nation's pipeline companies and their millions of miles of pipelines. PHMSA also has empowered several state agencies to exercise interstate and intrastate inspection and enforcement authority.

Congress gave further attention to pipeline cybersecurity last year, when it unanimously passed the Pipeline Safety Act of 2016 (PIPES Act). Among other changes, the PIPES Act amended the existing standards for natural gas pipeline facilities to require that the DOT, through PHMSA, propose regulations that enact cybersecurity measures for such pipelines. Despite this mandate, PHMSA's most recent strategic plan fails to make any mention of cybersecurity, and the agency has been slow to execute Congress's PIPES Act mandate.

Industry Takes a Brief Solo Turn

In 2012, around the time that DHS discovered Chinese hacking of pipeline SCADA systems, the Christian Science Monitor reported that an earlier industry effort to defend pipeline SCADA infrastructure that had been scuttled. The report focused on a 2006 comprehensive study that had the goal of creating a powerful encryption system to shield pipeline compressors, substations, and other pipeline infrastructure from cyberattack, and which had self-destructed on the eve of its being rolled out.

The five-year effort, sponsored by the American Gas Association, had charged the "AGA 12 Cryptography Working Group" with developing a suite of open standards to protect the data transmitted by SCADA systems, authenticate the originators of messages on SCADA systems, and ensure data integrity. Since support for AGA-12 was pulled, industry collaboration on pipeline cybersecurity has been anemic.

Public-Private Cybersecurity Partnerships

Frustrated by Congress's failure to pass comprehensive cybersecurity legislation, President Barack Obama issued Executive Order 13636 in early 2013. In the order, the President directed the National Institute of Standards and Technology (NIST) – a non-regulatory agency of the Department of Commerce – to follow the public-private approach and develop a set of voluntary cybersecurity guidelines for use by companies managing critical infrastructure, including those in the oil and gas industry. The February 2014 NIST Framework is a widely adopted set of practices, standards, and guidelines created to help critical infrastructure owners and operators manage cyber risks.

See "*Demystifying the FTC's Reasonableness Requirement in the Context of the NIST Cybersecurity Framework (Part One of Two)*" (Oct. 19, 2016); *Part Two* (Nov. 2, 2016).

Today, four years after Executive Order 13636 was issued, full confidence that pipeline SCADA system are protected continues to be out of reach. In no small part, this is attributable to the lack of coordination among government agencies and between the public and private sectors. Many experts worry that such initiatives are running short on time.

Despite the lack of coordination, the pipeline industry does appear to be embracing the NIST Framework. Its LNG trade group has also announced the formation of an industry threat sharing center, the Downstream Natural Gas Information Sharing and Analysis Center (DNG ISAC). The DNG-ISAC represents a recognition that "a meaningful partnership between the private sector and the federal and state governments is the key to addressing cybersecurity threats to our nation's critical infrastructure."

Information Sharing: Another Core Component of Pipeline Cybersecurity

While cyber intrusions are increasing, reporting cyber attacks remains voluntary and not all attacks are disclosed. DHS encourages such information sharing, which it says contributes to a useful understanding of the rapidly changing threat landscape, including the vectors attackers are using, varieties of malware, and other data DHS then uses to assist contributors in preventing further deleterious impacts on the nation's critical infrastructure.

The enactment of the Cybersecurity Information Sharing Act of 2015 (CISA) will put the public-private model to the test. CISA was passed in part as a response to North Korea's notorious hack of the cyber assets of Sony Pictures Entertainment, and is designed to create a voluntary cybersecurity and cyber-threat-information sharing process to further encourage public-private sharing of cyber threat information by removing legal barriers and the threat of litigation.

See "*Opportunities and Challenges of the Long-Awaited Cybersecurity Act of 2015*" (Jan. 6, 2016).

For private entities, CISA offers certain liability protections from causes of action related to monitoring information systems and shields companies from lawsuits based on disclosure of information under CISA, so long as the party sharing the information about cyber threat indicators and defensive measures follows DHS guidance published in June 2016. The industry tide now appears to be turning towards more cooperation for the shared goal of greater security.

What Will the Trump Administration Bring to the Cybersecurity Table?

The impact of the new U.S. presidential administration on private-sector information sharing is unknown. Shortly after taking office in January 2017, President Donald Trump signed an executive order severely restricting the issuance of new federal regulations, requiring government agencies to eliminate two regulations for every new rule enacted. This measure does foster concern that efforts to regulate privately owned critical assets may be stymied. While the EO does exempt "national-security" regulations, arguments over the definitions can be expected.

Administration officials, however, have also expressed an intent to give focus to critical infrastructure cybersecurity. President Trump may well go further than President Obama's Order 13636, and, through his own executive order or legislative initiative, find ways to engage private companies in the energy critical infrastructure sector with federal agencies. Whether that or any other Trump administration initiative will result in comprehensive cybersecurity in the pipeline industry is a question that all Americans should take seriously.

See "*Presidential Commission Recommends Ways For Public and Private Sectors to Improve Cybersecurity*" (Dec. 14, 2016).