Updates
May 17, 2021

Ransomware, Cyberattacks, and Cybersecurity for Pipelines and LNG Facilities

Colonial Pipeline shut down 5,500 miles of its East Coast pipeline on May 7, 2021, in an effort to contain a security breach resulting from a ransomware attack. Colonial's pipeline is one of the nation's largest and carries refined gasoline and jet fuel from Texas up the East Coast to New York. This represents nearly 45% of the fuel consumed on the East Coast. Ransomware attacks have increased in recent years, affecting many industries from banks, universities, and cities. Generally, a ransomware attack is a coordinated effort by computer hackers to lock up and freeze computer systems in order to demand large sums of money to then free up the computer systems. The recent cyberattack on Colonial Pipeline has resulted in gas shortages and panic buying across the southeastern United States, and highlights concerns over the security of critical infrastructure.

Regulatory Oversight of Physical and Cybersecurity of U.S. Energy Infrastructure

Unlike the electric grid, U.S. pipeline infrastructure reliability is not regulated by a single federal agency, and the Colonial Pipeline ransomware attack highlights a regulatory gap that exposes pipelines to cyberattack. The authority to regulate the safety of pipelines lies with the Transportation Security Administration (TSA). The Implementing Recommendations of the 9/11 Commission Act of 2007 directed TSA to promulgate pipeline security regulations and carry out necessary inspection and enforcement. 6 U.S.C. § 1207. However, TSA has yet to issue such regulations and instead relies upon voluntary guidelines on pipeline physical and cybersecurity.[1] A 2018 Government Accountability Office (GAO) report identified a number of weaknesses with TSA's program, including that "TSA does not have a strategic workforce plan to help ensure it identifies the skills and competencies—such as the required level of cybersecurity expertise—necessary to carry out its pipeline security responsibilities."[2] These findings highlight that TSA is not necessarily the best equipped agency to address cybersecurity issues.

By comparison, the electric industry has been subject to mandatory reliability standards since 2005, including those that address in detail cybersecurity. Pursuant to Section 215 of the Federal Power Act (FPA), the Federal Energy Regulatory Commission (FERC) maintains regulatory oversight over the reliability of the transmission grid and other elements of the bulk electric system. 16 U.S.C. § 824o(d). In accordance with FPA Section 215, FERC certified the North American Electric Reliability Corporation (NERC) to act as the nation's Electric Reliability Organization—an independent entity that enforces electric reliability standards on all users, owners, and operators of the U.S. transmission system. 16 U.S.C. § 824o(a)(2). Under this authority, NERC developed the Critical Infrastructure Protection (CIP) reliability standards that provide detailed requirements for maintaining cybersecurity. Section 215 also grants FERC and NERC authority to impose civil penalties for an entity's failure to comply with reliability standards, including the CIP standards. 16 U.S.C. § 824(e). Compliance with these reliability standards is consistently one of the highest priorities for FERC's office of enforcement.[3]

FERC does not have jurisdiction under either the Natural Gas Act (NGA) or the Interstate Commerce Act (ICA) to impose similar cybersecurity requirements on pipelines. However, following the cyberattack, FERC's Chairman Richard Glick issued a joint statement with Commissioner Alison Clements on May 10, 2021, calling for mandatory pipeline cyber standards. During his keynote address at the Energy Bar Association Annual Meeting on May 11, 2021, Chairman Glick repeated this call to action, advocating that either the TSA adopt

mandatory cybersecurity standards or Congress take legislative action to address the perceived regulatory gap.

Congressional Fix?

The Colonial Pipeline cyberattack brought new life to two pieces of bipartisan cybersecurity legislation. On May 11, 2021, the U.S. House of Representative's Energy and Commerce Committee reintroduced two pieces of legislation aimed at strengthening the U.S. Department of Energy's ability to respond to both physical and cybersecurity related threats to U.S. pipelines and liquified natural gas facilities. The proposed Pipeline and LNG Facility Cybersecurity Preparedness Act would require the Department of Energy to implement a program to ensure the security of pipelines and LNG facilities. The proposed Energy Emergency Leadership Act would assign the energy emergency and energy security functions to the assistant secretary of energy. This includes responsibilities related to infrastructure and cybersecurity.

The House is not alone in considering legislative change. In the U.S. Senate, there have been calls for more aggressive oversight of private companies operating critical infrastructure, like pipelines, and to seek more civil and criminal penalties, including personal accountability for CEOs in charge of such companies. Others in Congress have called for more investment in voluntary public-private partnerships such as the Cybersecurity & Infrastructure Security Agency (CISA), a standalone federal agency dedicated to reducing and eliminating threats to critical physical and cyber infrastructure. CISA is working with Colonial Pipeline on the May 7 ransomware attack among other cybersecurity initiatives. But CISA's program is voluntary and lacks the necessary teeth to enforce regulatory requirements.

Conclusion

It is unclear whether the Colonial Pipeline ransomware attack will result in strict mandatory reliability standards—closing a regulatory gap for pipelines and LNG facilities. Moreover, whether mandatory reliability standards—which take time to design, implement, and amend—are able to mitigate constantly evolving cybersecurity risks in a timely fashion is also uncertain. However, it is clear that the nation's gasoline panic buying has shined an even brighter spotlight on this weak spot in our infrastructure protection programs.

Endnotes

[1] TSA, Pipeline Security Guidelines (April 2021)

[2] U.S. GAO, Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Management (Dec. 2018)

[3] FERC, 2020 Report on Enforcement, Docket No. AD07-13-014 (Nov. 19, 2020)

Authors

Jane Rueger

Partner
JRueger@perkinscoie.com 202.661.5834

Jane E. Carmody

Associate
JCarmody@perkinscoie.com 206.359.3545

Explore more in

Environment, Energy & Resources | Infrastructure Development | Energy Infrastructure & Clean Technology

Related insights

Update

Wrapping Paper Series: Issues and Trends Facing the Retail Industry During the Holiday Season

Update

Department of Commerce Adopts Final Rule Restricting Tech and Telecom Supply Chain Transactions With Foreign Adversaries