LRO SNAPSHOT
A brief from the Legislative Research Office July 2022

Power Down: Legislative Considerations for Utility Cybersecurity

By Dillon Cornett, Research Analyst

A ransomware cyberattack in May of 2021 on the largest pipeline system for refined oil products in the nation, Colonial Pipeline Company (Colonial), caused the energy supplier to proactively shut off their own systems, which curbed fuel supplies on the East Coast. The U.S. Department of Energy's Office of Cybersecurity, Energy Security and Emergency Response (CESER) performs the important duties of monitoring and responding to cyber threats. CESER also manages the response to disruptions in operations and played a pivotal role in assisting Colonial with the restoration of its systems.

Image Courtesy of Hover Solutions LLC

Nearly a year later, the federal government passed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022. This Act requires all critical infrastructure companies to report significant cyber-incidents within 72 hours and to report any ransomware payments within 24 hours. Incident reports are sent to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency.[1] However, there remains no national definition of reasonable cybersecurity for the country's utilities. Many of the policies for how to prevent and respond to cyber-incidents are left up to the states and the utility companies themselves. Regarding energy emergencies, like a cyberattack, the legislative role often includes the creation of planning requirements, the granting of powers, and the appropriation of funding for planning and response activities.

Energy companies and utilities are responsible for the efficient operation of their vastly complicated functions that include information technology (IT) and operational technology (OT) systems. The business and communication networks that store, process and deliver data encompass IT networks whereas OT incorporates hardware and software to monitor and manage the physical controls that operate industrial equipment. Both types of technology are susceptible to breaches and outages could result if either system is attacked. Over the years, these physical and digital structures controlled by utilities have gradually merged. For example, utilities are increasingly installing internet-enabled devices like smart meters on the electric grid. This convergence of IT and OT networks has made energy supply more reliable, increased system awareness, and has lowered costs, but unfortunately it has also made utilities more vulnerable to cyberattacks.[2]

The Cyberattack on Colonial

Leaders in government and industry often simulate cyberattacks originating from terrorists or a hostile state with the intention to shut down energy supply. However, Colonial was targeted by a criminal extortion ring called DarkSide, believed to be operating out of Russia, which instead intended to hold Colonial's corporate data for ransom. The criminals used a ransomware attack, which was deployed through the company's IT network.

1. 117th Congress. (2022, March 15). H.R.2471 - 117th Congress (2021–2022): Consolidated Appropriations Act, 2022. Library of Congress. https://www.congress.gov/bill/117th-congress/house-bill/2471
2. Shea, D. (2021, October 26). Lessons From the Colonial Pipeline Attack: Heading Off Cyberthreats. National Conference of State Legislatures. https://www.ncsl.org/research/energy/lessons-from-the-colonial-pipeline-attack-heading-off-cyberthreats-magazine2021.aspx

Cybersecurity Definitions

Ransomware

- **A type of malware from cryptovirology that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion.**

Phishing

- **A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.**

After detecting the attack, Colonial made the unprecedented decision to shut down its pipelines. Colonial was concerned that malware had infected their billing functions and that it may spread further into their OT systems. Colonial controls nearly half of the gasoline, jet fuel, and diesel distributed across the East Coast, and news of the shutdown resulted in panicked drivers flooding gas stations, which caused delays at the pump.

Soon after the attack, the Energy and Homeland Security Departments drafted a confidential assessment that came to the conclusion that if the pipeline shutdown continued for another three to five days, then buses and mass transit would need to limit services due to a lack of fuel. Furthermore, industrial factories and refineries would have had to power down because distribution operations were unavailable. Alternative methods of fuel distribution were explored by the White House, but no plans were readily available, due in part to a shortage of truck drivers and train containers. Eventually, actions were taken to begin distribution prior to the pipeline system restart, and the President signed a first-of-its-kind executive order that sought to mandate cybersecurity changes. Additionally, U.S. Cyber Command, the military's cyberwarfare force, reportedly took retaliatory action against DarkSide and several other ransomware gangs. Ultimately, but possibly only temporarily, these groups ended their criminal operations.[3]

Colonial waited four days after the attack to engage in substantive discussions with the federal government, which delayed the response. Even after the company paid almost $5 million in Bitcoin to recover its stolen data, the process of decryption and restarting the pipeline system still took several days. Since the attack, Colonial has not publicly released information about exactly how DarkSide first infiltrated their systems.

Lessons from the Attack

Much of the country's critical infrastructure, more than 80 percent, is in the hands of private companies. Historically, the only sector of critical infrastructure that had mandatory and federally enforceable security standards was the electric grid.[4] The Transportation Security Agency (TSA) supervised and maintained voluntary cyber and physical security guidelines for the country's natural gas, oil, and hazardous materials pipeline systems until the Colonial attack. In July 2021, the TSA implemented new mandatory directives including ransomware and other cyber threat protections, recovery plans, and security reviews.[5]

A significant yet basic tenant of cybersecurity for energy utilities is the separation between their business management and operation systems. Cybersecurity experts have noted that if Colonial had possessed the utmost confidence in the separation of their IT and OT networks, the shutdown of their pipeline systems would not have been necessary.

3. Sanger, D. E., & Perlroth, N. (2021, June 8). Colonial Pipeline Hack Reveals Weaknesses in US Cybersecurity. The New York Times. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html
4. Shea, D. (2020, January 24). Cybersecurity and the Electric Grid | The state role in protecting critical infrastructure. National Conference of State Legislatures. https://www.ncsl.org/research/energy/cybersecurity-and-the-electric-grid-the-state-role-in-protecting-critical-infrastructure.aspx
5. Department of Homeland Security. (2021, July 20). DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators | Homeland Security. DHS. https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators
6. The White House. (2021, July 28). National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. Briefing Room. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

Many pipeline owners and operators across the country have installed such a firewall, never allowing data to flow into the pipeline OT system. This type of security feature would prevent a ransomware attack from spreading, for example. Colonial has not confirmed whether that same level of security is deployed in their systems. A security installation of this kind can be complicated and expensive but is potentially still cheaper than losses from a shutdown.[3]

The White House announced a cybersecurity initiative for the critical infrastructure community in July 2021, soon after the Colonial incident. The initiative intends to increase visibility, detection, and response capabilities in the energy sector. Over 150 electric utilities have joined the voluntary program and the administration has expanded the parameters to include natural gas pipeline companies.[6,7]

Unfortunately, not only were lessons learned by American industry and government officials, but by adversaries as well. In the case of the Colonial cyberattack, a basic ransomware virus was sufficient to shut down operations and cause panic across a large portion of the nation. To incite such chaos, bad actors learned they would not need to affect the more heavily secured core of the electric grid or the OT systems that distribute fuel or water throughout the country.

"It's all fun and games when we are stealing each other's money. When we are messing with a society's ability to operate, we can't tolerate it."

- Sue Gordon, former Deputy Director of National Intelligence[3]

State Legislature Considerations

With oversight over public service or utility commissions, state legislatures have the authority to improve cybersecurity policy. Some states approach cybersecurity laws either by specifically defining reasonable standards, like in California, or by providing a bevy of options and empowering firms to select the policies best suited for their purposes in return for liability protections, as in Ohio.

The most common legislative topics that have been recently introduced include requiring government agencies to implement cybersecurity training, policies, and plans for incident response. Recently enacted legislation in Connecticut and Utah provides incentives for private businesses to implement security guidelines and have those protocols in place prior to a breach of their cybersecurity. Several states, including Nebraska, also recently exempted particular cybersecurity information from public records laws. In 2021, North Carolina passed a law that prohibits ransomware payments by government entities.[8]

In addition, at least 30 states (not including Nebraska) have created a statewide task force, commission or advisory council in order to study or advise on cybersecurity issues. Most of these task forces were created via executive order, but 11 states have taken legislative action to create these initiatives.[9] The Nebraska Legislature did, however, create the Nebraska Information Technology Commission, which has as one of its stated goals, to "[e]nsure the security of the State's data and network resources and the continuity of business operations."

In terms of best practices for energy cybersecurity, officials at CESER advise the development of comprehensive state plans and incident response procedures, which are important to prepare for generally low-probability but high-impact events like cyberattacks. In addition, it is important to ensure the proper and rapid flow of information, like threat intelligence, across state agencies and with the private sector through entities such as the state fusion center, the Nebraska Information Analysis Center.[10] Finally, CESER recommends enabling public utility commissions to fulfill requests for new response mechanisms due to the significant investment in equipment and personnel that cybersecurity requires.

7. The White House. (2021b, August 26). FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity. Briefing Room. https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/
8. Greenburg, P. (2022, January 12). Cybersecurity Legislation 2021. National Conference of State Legislatures. https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2021.aspx
9. Greenburg, P. (2022b, April 4). Statewide Cybersecurity Task Forces. National Conference of State Legislatures. https://www.ncsl.org/research/telecommunications-and-information-technology/statewide-cybersecurity-task-forces636129887.aspx
10. Nebraska State Patrol. (2022, January 4). Nebraska Information Analysis Center. NAIC. https://statepatrol.nebraska.gov/divisions/investigative-services/nebraska-information-analysis-center