Energy Intelligence

Reproduced with permission by Energy Intelligence for Jackson Walker
Issue Vol. 68, No. 69, Day, April 9, 2018

OIL DAILY®

Vol. 68, No. 69 Monday, April 9, 2018

Cyber Security Risks Rise as Energy Industry Modernizes

Technological innovation made the shale revolution possible, but a recent cyberattack that impacted four natural gas pipelines is raising the question of whether the energy industry's embrace of digitalization makes it more vulnerable to cyber risks.

The online hack this month targeted a third-party electronic data interchange (EDI) service provider that is widely used throughout the energy space. Oneok, Energy Transfer Partners, Boardwalk Pipeline Partners and Chesapeake Utilities Corp.'s Eastern Shore Natural Gas all reported a break in communications with their customers. Oneok said it was the result of an apparent cyberattack on a third party.

Industry and government leaders should expect aggressive attempts to compromise the nation's infrastructure, said John Gibson, senior adviser on energy technology at investment bank Tudor Pickering Holt in Houston (TPH).

"We have entered an era where we are unsure if the ratio of attackers to defenders provides sufficient coverage," he said.

TPH associate researcher Deanna Zhang said EDI systems have become a regular part of doing business (OD Feb.28'18). Companies and their customers use EDI for orders, information-sharing and documents — in short, they have replaced mailing and faxing.

"Putting aside cost and time savings, these old systems were subject to errors because of human intervention and security risk from the number of middlemen involved," she told Oil Daily. "So increased digitalization does increase the risk of cyberattacks, but it also increases overall security compared to old school systems."

Still, communications systems are a regular target of hackers looking for information such as network access and credentials, said Sara Hollan Chelette, co-chair of the cybersecurity litigation practice of Jackson Walker in Dallas.

"They want to ultimately gain access to operational systems they can then disrupt," she told OD.

Any industry could be targeted by cyberattacks (OD Sep.8'17). However, the energy industry has certain risk factors that aren't apparent in retail or finance, said Phil Bezanson, managing partner at Bracewell's Seattle office.

"The challenges that are presented with energy are something like service disruption or environmental releases or something else that could cause physical harm to people or property or to the environment," he told OD. "If something goes wrong, it could go really, really wrong. To the extent that energy is an attractive target to hackers, that's why."

Planning for Cyberattacks

It's important that companies prepare a plan of action in the event of a cyberattack, just as they might prepare for a natural disaster, Bezanson said.

"Being prepared doesn't mean a hurricane or earthquake won't happen," he said, adding that it does mean a company can better manage the threat and recover more quickly.

A good plan is composed of instructions for opening and maintaining vital communications lines, even if a company's primary communications mechanisms are compromised, he said. Some companies use an offline drive — that is routinely updated to store business-essential data — that can be used as a backup in the event of an attack.

Hollan Chelette said companies should be vigilant with the basics. Strong passwords, two-factor authentication and data encryption are among the first defenders.

Even physical security remains a critical element to protecting valuable information, TPH's Gibson said.

"There are very advanced methods being developed to reduce risk, but one should assume an equal effort is being made to wreak havoc," he said. "Physical access lowers the defensive shields."

US Department of Energy (DOE) Secretary Rick Perry has announced plans for a $96 million Office of Cybersecurity, Energy Security and Emergency Response. The DOE division will be designed protect the nation's power grid and infrastructure against cyberattacks (OD Dec.19'17).

The origin of the attack that impacted the natural gas pipelines remains unknown. In March, however, the US Department of Homeland Security and the FBI warned that Russian government cyber actors had infiltrated US government entities as well as companies in the energy, nuclear, commercial facilities, aviation and critical manufacturing sectors for at least the past two years.

The warning noted that hackers used peripheral organizations such as trusted third-party suppliers with less secure networks to infiltrate their intended targets.

"Increased digitalization does increase the risk of cyberattacks at oil gas companies, in the same sense that driving a car increases one's risk of getting into a car crash," TPH's Zhang said. "This shouldn't be equated with a reduction in security of the overall system."

Deon Daugherty, Houston