THE FOSTER REPORT
Independent and In-Depth Reporting on the Energy Industry

Oil and Gas Companies Warned on Cyber Threats, Data Security

This article appears as published in The Foster Report No. 3203, June 15, 2018

Natural gas and oil pipelines and gas utilities need to be diligent in how they handle and store data and learn from others facing cybersecurity threats, a speaker advised at the Northeast LDC Gas Forum in Boston.

Electric utilities have national reliability standards and FERC has approved standards to bolster supply chain protection for equipment used in power grid operations. That step, taken in early 2018, is designed to augment critical infrastructure protection (CIP) standards for protection against cybersecurity risks in the power sector.

But the natural gas industry can take steps of its own to enhance its protection against cyber intrusions that could affect pipeline or local distribution companies, said Jerrod Montoya, deputy chief information security officer at OATI. The company, which grew from Open Access Technology International Inc., provides an online trading platform for natural gas customers that includes load forecasting, gas scheduling and services certified by the North American Energy Standards Board (NAESB), Montoya noted.

OATI operates data centers, has software as a service for energy companies and hosts servers with cloud computing for customers, he said. The company was created in the mid-1990s and learned through experience how to manage risks for companies as energy markets were restructured, with less regulation, Montoya noted.

When computer servers are at a company site, companies must manage them, with trained staff and requirements that can be costly, including physical security issues. Using servers through cloud computing increases vulnerability to cyberattacks. "The threat is real" and "the energy sector is in the cross hairs" of entities targeting oil and natural gas infrastructure, Montoya said.

The U.S. Computer Emergency Readiness Team issued an alert earlier this year about Russian cyber actions targeting organizations in the energy, nuclear and water sectors to try and breach networks. Federal government agencies sent the alert to help network defenders identify and reduce their exposure to malicious activity.

Montoya referred to an incident in early April in which electronic data interchange (EDI) transactions for several pipelines were halted due to a cyber attack on Latitude Technologies Inc., which is owned by Energy Services Group LLC.

EDI transactions can involve the nomination and scheduling process for pipeline customers and the submittal/exchange of other information. They are not part of pipeline operations, and pipeline owners affected by the incident emphasized that operations were not affected. Latitude Technologies did not believe any customer data was compromised, it said in a notice sent to pipeline customers.[1]

"That was a pretty significant event" and it illustrated the need for pipelines to be aware of data integrity and security risks as cyber intrusion attempts become more common, Montoya told the LDC Forum audience.

"It is inevitable that something will happen" that affects data security or perhaps pipeline network operations, so the key for the industry will be protecting systems and keeping staff informed of the latest developments, he said. "Look at your vulnerabilities, learn from others" such as companies or government agencies that suffered consequences for exposed Wi-Fi passwords or simple human errors, he said.

Gas and oil companies can choose to have audits of their cyber risks, but make sure such audits are thorough and independent from any company providing services to the company, Montoya advised.

Also, "be careful selecting a vendor. Choose one that knows you and your business" and the importance of energy infrastructure in today's society.

The Interstate Natural Gas Association of America (INGAA) on April 17, said its board of directors approved new commitments to pipeline safety and security, addressing physical and cyber security based on new guidelines from the Transportation Security Administration. The revised TSA guidelines superseded a 2011 version and was updated due to advancements in security practices to meet cyber and physical security threats to pipelines.

By Tom Tiernan TTiernan@fosterreport.com

To Subscribe contact **Gina Smith**, (508) 263-6263; GSmithFosterreport.com

Follow us on Twitter @Foster_Report

[1] For past story, *see*, *Pipelines Say Cyber Attack on EDI Systems Had No Impact on Operations*, FR No. 3193, pp. 8-9.

Published by Concentric Energy Publications, Inc.,
a Concentric Energy Advisors, Inc. Company

Copyright © 2018 by Concentric Energy Publications, Inc.
All Rights Reserved. Concentric Energy Publications Trademark used under license from Concentric Energy Advisors, Inc.