

# [***Cyberattack puts pipeline industry in hot seat***](https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:5S2W-GGS1-J9XT-P23N-00000-00&context=1516831)

Plus Company Updates(PCU)

April 10, 2018 Tuesday

Copyright 2018 Plus Media Solutions Private Limited All Rights Reserved



**Length:** 916 words

**Body**

Houston: WorldOil.com has issued the following press release:

NEW YORK -- A cyberattack that U.S. natural gas pipeline owners weren’t required to report has lawmakers taking a closer look at how the industry is handling such threats, raising the prospect of tighter regulation.

In website notices to customers this week, at least seven pipeline operators from Energy Transfer Partners to TransCanada said their third-party electronic communications systems were shut down, with five confirming the service disruptions were caused by hacking. But the companies didn’t have to alert the U.S. Transportation Security Administration, the agency that oversees the nation’s more than 2.6 million mi of oil and gas conduits in addition to providing security at airports.

Though the cyberattack didn’t disrupt the supply of gas to U.S. homes and businesses, it underscores that energy companies from power providers to pipeline operators and oil drillers are increasingly vulnerable to electronic sabotage. It also showed how even a minor attack can have ripple effects, forcing utilities to warn of billing delays and making it more difficult for analysts and traders to predict a key government report on gas stockpiles.

“These attacks are a wake-up call that addressing our aging energy infrastructure needs to be a priority,” Congressman Robert Latta, a Republican from Ohio who serves on the House Committee on Energy and Commerce, said in an emailed statement on April 5. “Bad actors are looking at any way to weaken the American energy sector.”

This isn’t the first time hackers have had oil and gas pipes in their sights: The Congressional Research Service reported intrusions targeting pipeline communication systems back in 2012. A web attack could “disrupt pipeline service and cause spills, explosions, or fires -- all from remote locations,” the service said in a report.

The electronic systems that were targeted in the recent cyberattack help pipeline customers communicate their needs with operators via a computer-to-computer exchange of documents, such as contracts and invoices. The attacks didn’t affect operational control of the pipelines.

Even before the most recent pipeline web attack, there were signs that the government was intensifying its focus on web-based energy threats. Last month, the TSA issued a 27-page report on pipeline security that included a section on cybersecurity. In the report, the agency urged pipelines to take measures including establishing a cybersecurity plan, limiting network access and changing default passwords.

But TSA doesn’t require operators to report web intrusions, and it’s not clear whether the agency would have jurisdiction over an attack on a third-party communications provider. TSA requests voluntary notifications of “security incidents that are indicative of a deliberate attempt to disrupt pipeline operations or activities that could be considered precursors to such an attempt,” according to the report last month.

“TSA will continue to work with the pipeline industry to assess any vulnerabilities associated with this incident,” Lisa Farbstein, a spokeswoman for the agency, said in an email Friday. “TSA, in consultation with cyber experts, will make recommendations, as appropriate, to the pipeline industry to mitigate concerns.”

The American Gas Association, an industry group that represents more than 200 gas supply companies, supports voluntary reporting of cyberattacks, said Dave McCurdy, the association’s president. Mandatory reporting could be counterproductive because it may set the bar too low and create a false sense of security, especially in an ***environment*** where cyber threats evolve quickly, McCurdy said by phone Friday.

“Just asking for reporting and requirements is not the answer,” he said. “We need to understand the nature of attacks. Every industry in a critical area receives attacks mostly daily.”

$96 Million

In February, Energy Department Secretary Rick Perry announced the department would use $96 million in funding to create an office to address cyber threats to energy. Though Homeland Security, which oversees TSA, has the legal authority to oversee energy cybersecurity, “DOE works closely with the sector on cyber security and threat information sharing,” Shaylyn Hynes, a spokeswoman for the department, said in a statement. But some lawmakers say it’s not enough.

At a congressional hearing in March, Maria Cantwell, a Democratic senator from Washington, told Perry that budget cuts could make it more difficult to shield the energy sector from cyber intrusions.

“Our energy infrastructure is under attack,”’ Cantwell said. “A year ago, I called for a comprehensive assessment of cyber-attacks to our grid by Russians. We don’t need rhetoric at this point – we need action.”

The threat appears to be widespread. Two years ago, the Department of Energy’s Pacific Northwest National Laboratory in Richland, Washington, said its firewall system blocks 25,000 cyberattacks a day.

Though the energy industry and regulators are looking more closely at cybersecurity risks, the shift may not be happening fast enough, said Edgard Capdevielle, chief executive officer of Nozomi Networks Inc. in San Francisco, a company that provides cybersecurity applications for customers including power producers and oil and gas pipeline operators.

The industry’s perception is that addressing energy cyber threats “is important, but mañana is OK,” said Capdevielle. “Mañana is not OK."

**Load-Date:** April 10, 2018

**End of Document**