Emerging Legal Issues In Managing Cyber Risk for Pipelines

Pipeline & Gas Journal

February 2013

Section: Pg. 53; Vol. 240; No. 2; ISSN: 0032-0188

Length: 2288 words

Byline: Wolff, Evan D

Delionado, John J

Simpson, Aaron P

Hogfoss, Robert E

Body

Oil and gas pipelines provide a significant amount of America's energy demands. Like most energy infrastructure, pipelines rely on Industrial Control Systems (ICS), including Supervisory Control And Data Acquisition (SCADA) systems, that function on computerized and communication networks. As a result, these networks present vulnerability and can be targets of cyber threats.

Development of new tight oil and gas fields, new pipeline construction and related corporate mergers and acquisitions result in increasing stresses on existing SCADA systems. Attention to cybersecurity is therefore more critical than ever.

The federal government has been debating national cybersecurity standards for critical infrastructure, including pipelines. Congress considered a comprehensive bill in 2012 and President Obama is expected to issue an Executive Order on the issue in light of congressional inaction. In the meantime, pipeline companies must maintain constant vigil by assessing risks to their command and control components, including SCADA. This includes managing risks from litigation, compliance activities, data security and privacy issues.

Not only must pipeline companies protect against these risks for business reasons, they now must contend with emerging regulatory and industry-developed standards. The pipeline industry has long been regulated by performance-based standards rather than prescriptive rules. This article suggests that such an approach is well-suited to cybersecurity issues, and provides an overview of these emerging legal issues.

Evolving Cybersecurity Regulatory Landscape

Pipelines are subject to a complex web of regulatory requirements and voluntary standards developed by both the government and the private sector to protect the nation's critical infrastructure from bad actors. Given the pervasiveness of recent threats and the pace of technological change, a state of flux has ensued from a cybersecurity perspective, making compliance with these standards challenging in the pipeline sector.

The landscape of cyber threats faced by pipeline control systems has shifted dramatically. Historically, due to their built-in redundancy and unique designs, the risks were considered low. With the recognition of a cyber intrusion campaign against the sector, openly acknowledged by the federal government, the risk level clearly is heightened. This nefarious campaign has been a factor in the recent push by the federal government to empower federal agencies to develop or strengthen cybersecurity standards for critical infrastructure and incentivize critical infrastructure owners, including pipeline owners, to implement enhanced security practices.

For example, the Department of Homeland Security's (DHS) Chemical Facility AntiTerrorism Standards require companies that store, handle or use high-risk chemicals, including many pipelines, to comply with stringent performance standards when securing cyber systems, including industrial control systems.

In addition to DHS compliance obligations, the Securities and Exchange Commission's Division of Corporation Finance issued disclosure guidance in late 20 1 1 regarding the reporting of material cyber events by publicly traded companies. Although non-binding, it provides specific guidance regarding existing disclosure obligations in the context of cybersecurity matters and cyber incidents, and will no doubt be utilized in SEC enforcement proceedings and/ or by plaintiffs' counsel in litigation.

Pursuant to the guidance, registrants are encouraged to consider disclosing both known and threatened cyber events, depending on the nature of the event and the underlying business context. For those publicly traded companies in the pipeline sector, disclosure and cybersecurity business teams, along with counsel, should coordinate carefully on any response to the SEC's guidance.

Industry Self-Regulatory Efforts

Outside of the regulated sphere, the 9/1 1 Act of 2004 authorized the Transportation Security Administration to promulgate physical and cybersecurity regulations for the pipeline sector, but it has not done so to date. Instead, TSA has developed cybersecurity guidance and best practice recommendations through an industry-wide consensus process. This guidance has been used widely in the pipeline industry as a baseline for security requirements and planning by many pipeline companies.

TSA also has established a public/private partnership-based cybersecurity program supporting the National Infrastructure Protection Plan. This process has been widely viewed as a positive example of cooperation between the government and industry in developing guidance and information sharing.

From a purely industry self-regulation perspective, the Interstate Natural Gas Association of America maintains its own extensive cybersecurity guidelines for natural gas pipeline control systems, and similarly the American Petroleum Institute maintains an industry standard for oil pipeline control system security. Pipeline operators also participate in the DHS Industrial Control Systems Joint Working Group, which facilitates information sharing between federal agencies and departments and the owners and operators of industrial control systems.

As industrial standards have proliferated through cooperative public-private partnerships and opportunities for information sharing have increased, so have the responsibilities for the private sector to address the standards in a meaningful way and to respond to notice of increased threats. Failure by pipelines to institute changes consistent with the standards or to respond to threats may result in a greater risk of liability.

Traditional Privacy And Information Security Concerns

In addition to emerging critical infrastructure regulations and industry guidance focused on control systems, pipelines are subject to a panoply of state and federal privacy and information security requirements focused on the protection of information as well. For example, there is a divergent body of law in the U.S. that regulates how all businesses, including those in the pipeline sector, process personal information regarding individuals with whom they have a relationship, including customers, employees, consultants and contractors.

In 46 states (plus Guam, Puerto Rico, the U.S. Virgin Islands and Washington, DC) there is an obligation to notify affected individuals (and often regulators) in the event personal information for which a business is responsible has been acquired or accessed by an unauthorized person. Notification triggers in these laws are broadly drafted, and thus even in circumstances where a cyber event in the pipeline context is focused on control systems and not data, a legally cognizable information security breach involving personal information can result.

In addition to notification obligations, it has now become commonplace for individuals and businesses impacted by such events to bring private actions seeking remuneration for damages they claim to have suffered as a result of the breach. Both the Federal Trade Commission and state attorneys general are increasingly bringing enforcement actions resulting from information security breaches as well.

The Prospect Of Comprehensive Federal Action On Cybersecurity

Given the importance of securing our nation's critical infrastructure and the cybersecurity compliance web that owners of critical infrastructure find themselves in, there has been significant action in Washington to create a more consolidated legal regime. At the center of this activity most recently was the Cybersecurity Act of 2012.

Although this bipartisan bill failed to pass, it was an important effort that sought to enact a comprehensive, federal cybersecurity law. The Act would have directed DHS to set "voluntary" cybersecurity standards for companies that operate infrastructure considered vital to U.S. national security, which includes pipelines. It also proposed standards for companies and the government regarding informationsharing requirements regarding cyber threats.

While the pipeline sector generally supported the information-sharing provisions, many were concerned that even voluntary standards could expose them to new liability and that the Act did not provide adequate liability protection to address those risks.

In the absence of comprehensive, federal cybersecurity legislation, the Obama Administration has publicly declared that it is considering taking action through an Executive Order. A recently released draft Executive Order would institute a voluntary cybersecurity standards structure for critical infrastructure similar to the Cybersecurity Act of 2012 but without the liability protections.

Under the draft Order, the National Institute of Standards and Technology would coordinate development of a Cybersecurity Framework, and DHS would invite critical infrastructure owners and operators to participate in a voluntary program to encourage the adoption of the Framework. Sector-specific agencies would report to the President on their existing authority to regulate cybersecurity and would be encouraged to propose additional regulations as appropriate.

Some business sectors expressed concern that, like the failed cybersecurity legislation, such an Order may create additional liability for companies as even voluntary standards might morph into a legal standard of care. In addition, private companies have raised legitimate concerns about just how voluntary the standards would be if implemented as currently drafted.

If, for example, a company decides against participation and is victimized by a threat, it seems plausible that it still may need to contend with the voluntary standards, particularly if adherence to such standards would have nullified or mitigated the threat. Businesses are concerned, moreover, that insurers may rely on the voluntary standards in evaluating or underwriting insurance policies, and regulators may use them when evaluating indirect action, such as the disclosure obligations set forth above.

Pipelines have always been regulated by the federal Office of Pipeline Safety on the basis of performance-based standards (49 C.F.R. Parts 190 - 199), as opposed to prescriptive standards where "one size fits all." That approach allows individual pipeline systems to develop regulatory programs individually tailored to their location and characteristics.

Cybersecurity systems must be similarly tailored in order to accommodate varying system attributes, and such a performance-based approach could, in fact, improve security for the industry as a whole, as threats against the industry as a whole could be minimized.

What Companies Can Do Now

Cyber threats come from many sources, including terrorist groups, internal sabotage, state-sponsored entities, and political activists. Increasingly, the government has been more active in identifying these threats and sharing related information with interested private sector partners.

As a matter of due diligence, companies can participate in information-sharing organizations and networks in order to receive appropriate indicator and warning documents. It is equally important for companies to review and consider such information and have a welldocumented response process containing both internal and external elements. As a part of this process, companies should work with their counsel to identify potential risks and undertake risk-mitigation activities such as network-security assessments and penetrations tests.

As the debate regarding cybersecurity regulation continues, it has become de rigeur for businesses of all stripes to develop comprehensive information governance frameworks. While the precise components of such a framework will depend on the nature of a business's data processing activities, all well-designed information governance frameworks should share certain key features.

At the foundation of the framework should be an in-depth understanding of the business's proprietary and personal information. In particular, it is important to understand the flow of information from its creation to its ultimate disposal, including with respect to what information is maintained by die business, where it is stored, how it is secured, and whether and to whom it is disclosed.

Based on this assessment, the business should then develop or revise its information governance framework to ensure appropriate administrative, technical and physical safeguards are in place to manage business and compliance risks from a strategic information management perspective.

The pipeline industry should continue to work with DHS and the administration to allow flexibility in any cybersecurity mandates, as that approach could act to increase the rigor of pipeline security systems.

By Evan D.Wolff, John J. Delionado, Aaron P. Simpson, and Robert E. Hogfoss, Hunton &; Williams LLP

Authors: Evan D. Wolff is director of Hunton &; Williams LLP's homeland security practice, advising clients on homeland security, chemical facility security regulation, cybersecurity and critical infrastructure. He can be reached at *ewolff@hunton.com*

John J. Delionado 's practice focuses on the defense of businesses and individuals investigated by the government on cybersecurity matters. He can be reached at jdelionado@ hunton.com.

Aaron P. Simpson advises clients on a broad range of complex privacy and security matters, as well as the remediation of large-scale data security incidents. He can be reached at asimpson@ hunton.com.

Robert E. Hogfoss's practice focuses on energy, environmental and administrative law, with emphasis on Pipeline Safety Act, Clean Water Act, Oil Pollution Act, NEPA, RCRA, CERCLA and TSCA issues. He can be reached at *rhogfoss@hunton.com*

Graphic

Photographs

Load-Date: March 15, 2013