Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Steps Oil And Gas Cos. Can Take To Manage Cyber Risk

By **Valerie Hatami** (June 2, 2021, 4:43 PM EDT)

Valerie Hatami

The U.S. oil and gas industry, central to all critical infrastructure sectors,[1] presents an attractive target for cybercriminals and other malicious actors, including geopolitical rivals and cyberterrorists.[2]

Of the top 25 publicly traded oil and gas companies, 52% report having experienced cyberattacks.[3] The facilitation of hard-to-track ransom payments by bitcoin and other cryptocurrencies further increases the risk.[4]

Cyberattacks have long-lasting legal implications that extend beyond immediate losses associated with business interruption. Cyberattacks can cause market value decline and damage to companies' environmental, social and governance efforts, exposing oil and gas companies to a variety of potential lawsuits:

CyberAttacks	Potential Legal Impacts
Company value decline	Shareholder class actions, shareholder derivative lawsuits
Environmental damage	Regulatory compliance violations, landowner lawsuits
Workplace accidents	Wrongful death lawsuits, personal injury lawsuits
Production damage	Breach of contract lawsuits, non-op / mineral owner lawsuits
Supply chain disruption	Consumer class actions, breach of contract lawsuits

To appreciate the magnitude of the potential legal exposure, one needs to look no further than a recent ransomware attack on Colonial Pipeline Co., operator of the largest fuel pipeline in the U.S.[5] On May 7, Colonial Pipeline announced that it had to disconnect certain operational technology systems to contain the threat posed by ransomware deployed against the company's information technology systems.[6]

It was later determined that the attack was perpetrated by DarkSide, a malicious cyber group that the U.S. Cybersecurity and Infrastructure Security Agency, or CISA, has said targets "large, high-revenue organizations, resulting in the encryption and theft of sensitive data."[7] Although the exact process of infiltration of Colonial Pipeline's IT systems remains unclear, CISA has reported that in the past, DarkSide has gained "initial access through phishing and exploiting remotely accessible accounts and systems."[8]

Disabling Colonial Pipeline's operational technology systems resulted in a five-day cessation of all pipeline operations, causing major supply chain disruption and fuel price increase.[9] To restart the system as quickly as possible, Colonial Pipeline paid a 75 bitcoin, or $4.4 million, ransom.[10]

This ransom payment may have enabled Colonial Pipeline to decrypt its data and resume operations, but it did not eliminate the company's legal exposure. In addition to suffering significant financial losses and reputational harm, the company is now facing a consumer class action for damages resulting from the company's alleged negligent failure to maintain adequate cybersecurity measures.[11]

Although some companies may be able to restore their operations without paying a ransom, those companies may still experience appreciable business disruptions. In February 2020, CISA published a security alert describing a ransomware attack on an unnamed natural gas compression facility and encouraging critical infrastructure asset owners and operators to familiarize themselves with the malicious actor's techniques and the applicable mitigations.[12]

According to CISA, after obtaining initial access to the facility's IT network, the attacker infiltrated the facility's operational technology network, and used ransomware to encrypt data on both networks.[13] Ultimately, the facility was able to procure replacement equipment and employ preattack configurations to facilitate the restoration process.[14]

Although the attack was limited to one facility, separate compression facilities in other geographic areas had to cease operations due to pipeline transmission dependencies, causing a two-day shutdown of the entire pipeline.[15]

Cryptocurrency Expansion

The proliferation of ransomware attacks has been linked to the rise of bitcoin and other cryptocurrencies, which are notoriously hard to trace.[16] By employing such strategies as "chainhopping" — exchanging funds in one cryptocurrency for another — and setting up fraudulent accounts, and by utilizing novel financial entities outside regulated financial payment markets, malicious actors can — and do — avoid detection.[17]

Ransomware is not the only tool in a cybercriminal's toolbox. At the upstream level, a variety of other tools capable of disrupting critical operations is available: from spyware capable of stealing competitive seismic data to malware capable of infecting operation control systems and causing wellsite and subsurface damage.[18]

In fact, one commonly used operation control system — known as supervisory control and data acquisition, or SCADA — which allows operators to remotely monitor and control entire sites is among key targets,[19] particularly if SCADA is cloud-based[20] or a vulnerable legacy system.

Oil and Gas Digitalization

Faced with fluctuating commodity prices and operational challenges exacerbated by the COVID-19 pandemic, oil and gas companies are accelerating digitalization in an attempt to reduce costs, enhance margins and generate positive free cash flow.[21]

In addition to such well-known and widely used technologies as remote monitoring and control, mobile platforms/apps and cloud computing, the oil and gas industry is also adopting, albeit at a slower pace, more advanced digital technologies.[22] However, this digital revolution[23] has a downside: an increasing risk of cyber breaches.

For publicly traded oil and gas companies, legal exposure due to cyber breaches may be even greater. Unlike privately held entities, publicly traded companies are required to make certain disclosures under the federal securities laws, which have been interpreted by the U.S. Securities and Exchange Commission to include disclosures relating to "cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences."[24]

In addition to potential regulatory ramifications, failure to disclose may result in multiple shareholder class actions. For instance, in January, several shareholders of SolarWinds Corp., a publicly traded infrastructure management software provider,[25] brought three class action lawsuits against the company and its management, alleging SolarWinds violated the federal securities laws.[26]

According to shareholders, SolarWinds misrepresented the adequacy of its cybersecurity measures and failed to disclose a cyber breach affecting the company's products, which resulted in an artificial inflation of the market price of SolarWinds' stock.[27] Shareholders further alleged that when information about the cyber breach became public, the market value of SolarWinds' shares experienced "precipitous decline," resulting in significant losses and damages to shareholders.[28]

SolarWinds' experience is a cautionary tale for publicly traded oil and gas companies — and yet another example of far-reaching consequences of cyberattacks.

Five Considerations to Manage Oil and Gas Cyber Risk

In light of growing threats posed by cyberattacks, the oil and gas industry can expect the imposition of future minimum cybersecurity standards by government.[29] Although oil and gas companies utilize various technological measures to prevent potential cyber-related disruptions,[30] leadership should consider the following steps to further manage oil and gas cyber risk.

1. Implement Cybersecurity Policies and Procedures

The oil and gas industry is adept at managing business risks by developing internal policies and procedures to create value, increase safety and enhance efficiency.[31] Escalation of potential cyber threats is a recognized business risk.[32]

Therefore, implementing robust cybersecurity policies and procedures, which outline cybersecurity expectations, roles and responsibilities within an organization, as well as set internal standards of behavior, is critical to managing this type of risk.[33]

These cybersecurity policies and procedures cannot be static. As new cyber threats emerge, companies should periodically review and update their policies and procedures to address gaps and weaknesses.[34]

2. Prepare a Cyber Incident Response and Recovery Plan

Having a cyber incident response and recovery plan allows a company affected by a cyber breach to quickly detect the breach, ensure business continuity, minimize losses and avoid costly mistakes.[35]

Based on the company's size and identity, an effective cyber incident response and recovery plan will include elements specific to that company. Nevertheless, at least two key elements that warrant mentioning will be the same.

First, the company's plan should establish an incident response team,[36] so that its members can gain appropriate response experience via training and emergency exercises.[37] Second, the company's plan should establish an appropriate reporting structure.[38]

Based on applicable statutory, regulatory or contractual requirements, a company may have certain notification and/or disclosure obligations. Thus, in addition to identifying internal players, the reporting structure should also identify all outside parties who will need to be notified.[39]

For cyber breaches with potential adverse legal consequences, notification requirements should include outside counsel to maximize the protections of the attorney-client privilege.

3. Increase Employee Awareness

For decades, employees in the oil and gas industry have been trained to recognize and address various safety hazards to prevent fatalities and avoid catastrophic accidents. The same level of diligence and regimented training is required with respect to cybersecurity hazards.

A survey conducted by Ernst & Young LLP in 2019 identified employee awareness as one of the most important cybersecurity issues currently facing the oil and gas industry.[40] Untrained, unaware employees are viewed by malicious actors as the weakest link.[41]

To address this issue, employees should be trained to recognize cyber threats they are likely to encounter and encouraged to adopt simple best practices, such as creating strong passwords and avoiding clicking on suspicious links.[42] Additionally, employee awareness must be regularly tested, to assess the effectiveness of internal training and to understand what further training might be necessary.

4. Assess Cyber Practices of External Parties

Even companies with robust cyber protections in place could still be vulnerable if vendors and/or contractors, who may have access to company's systems and data, do not maintain adequate cybersecurity practices.

Conducting due diligence and evaluating external parties' cybersecurity before giving those parties access to critical systems and data is another measure that could prevent potential cyber breaches.[43] As a corollary to this task, a company should monitor user access to ensure there are no anomalies that need to be investigated.[44]

5. Evaluate Contracts with Third-Party Service Providers

Because some of the digital technologies used in the oil and gas industry are owned and managed by third-party service providers, evaluating contracts may be warranted. For instance, does a contract between a company and a cloud-based SCADA provider contain an expansive indemnity provision, obligating the company to indemnify the provider against any and all conceivable claims and losses resulting from provider's performance of the contract?

Does the contract contain an unreasonable limitation of liability clause, limiting provider's liability for company's damages only to the value of the contract, regardless of the cause and nature of damages? Does the contract provide any recourse in the event of a cyber breach?

Answering these questions is critical in evaluating the scope of company's potential exposure and the need for potential renegotiating.

Valerie V. Hatami is an associate at Conner & Winters LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Energy Sector, Cybersecurity and Infrastructure Secuirty Agency, https://www.cisa.gov/energy-sector (last visited May 23, 2021).

[2] Ransomware Guidance and Resources, Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/ransomware (last visited May 16, 2021) [hereinafter "Ransomware Guidance"]; Anshu Mittal, Andrew Slaughter and Paul Zonneveld, Protecting the Connected Barrels: Cybersecurity for Upstream Oil and Gas, Deloitte Univ. Press 3 (2017), https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/energy resources/DUP_Protecting-the-connected-barrels.pdf [hereinafter "Protecting the Connected Barrels"].

[3] Based on review of the 2020 SEC filings of top 25 publicly traded oil and gas companies (based on market capitalization May 21, 2021).

[4] Combating Ransomware: A Comprehensive Framework for Action, Inst. for Sec. and Tech. 14 (2021), https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf [hereinafter "Combating Ransomware"].

[5] About Us / Our Company, Colonial Pipeline Co., https://www.colpipe.com/about-us/our-company (last visited May 16, 2021); Grace Segers, Cyberattack Prompts Major Pipeline Operator to Halt Operations, CBS News.Com (May 9, 2021), https://www.cbsnews.com/news/colonial-pipeline-cyberattack-shut-down/.

[6] Media Statement Update: Colonial Pipeline System Disruption, Colonial Pipeline Co. (May 8, 2021), https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption.

[7] Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks, Cybersecurity and Infrastructure Security Agency, https://us-cert.cisa.gov/ncas/alerts/aa21-131a (last revised May 20, 2021).

[8] Id.

[9] Sara Morrison, How a Major Oil Pipeline Got Held for Ransom, Vox.com (May 19, 2021), https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices.

[10] Colonial Pipeline Confirms It Paid $4.4m Ransom to Hacker Gang After Attack, The Guardian (May 19, 2021), https://www.theguardian.com/technology/2021/may/19/colonial-pipeline-cyber-attack-ransom.

[11] See Dickerson v. CDPQ Colonial Partners, L.P., No. 1:21-cv-02098 (N.D. Ga. May 18, 2021).

[12] Alert (AA20-049A) Ransomware Impacting Pipeline Operations, Cybersecurity and Infrastructure Security Agency, https://us-cert.cisa.gov/ncas/alerts/aa20-049a (last revised Oct. 24, 2020).

[13] Id.

[14] Id.

[15] Id.

[16] Combating Ransomware, supra note 4.

[17] Id.

[18] Protecting the Connected Barrels, supra note 2, at 14.

[19] Charles Drobny, Cyber Security Key to SCADA, The Am. Oil & Gas Rep. (July 2013), https://www.aogr.com/web-exclusives/exclusive-story/cyber-security-strategy-key-to-scada.

[20] Rusty Gavin, Implementing a Cybersecurity Strategy for Cloud-Based SCADA, Oil & Gas Engineering (Aug. 14, 2018), https://www.oilandgaseng.com/articles/implementing-a-cybersecurity-strategy-for-cloud-based-scada/.

[21] Irina Slav, Digitalization Is The Only Way Oil Companies Can Survive, Oilprice (Sept. 30, 2020), https://oilprice.com/Energy/Energy-General/Digitalization-Is-The-Only-Way-Oil-Companies-Can-Survive.html.

[22] Oil and Gas Digital Transformation and the Workforce Survey, Ernst & Young (2020), https://assets.ey.com/content/dam/ey-sites/ey-com/en_us/topics/oil-and-gas/ey-bmc-oil-and-gas-global-survey-report-final-v1-wo-jw-single-web.pdf.

[23] Anil Pandey and David Branson, 2020 Digital Operations Study for Energy, Strategy& (2020), https://www.strategyand.pwc.com/gx/en/insights/2020/digital-operations-study-for-oil-and-gas/2020-digital-operations-study-for-energy-oil-and-gas.pdf.

[24] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, U.S. Securities and Exchange Commission (Feb. 26, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[25] SolarWinds: We Make It Look Easy, SolarWinds, https://www.solarwinds.com/company/home (last visited May 19, 2021).

[26] See Bremer v. SolarWinds Corp., No. 1:21-cv-00002 (W.D. Tex. Jan. 4, 2021); Azpurua v. SolarWinds Corp., No. 1:21-cv-00047 (W.D. Tex. Jan. 14, 2021); N.Y.C. Dist. Council of Carpenters Pension Fund v. SolarWinds Corp., No. 1:21-cv-00138 (W.D. Tex. Feb. 9, 2021).

[27] Complaint at 6 and 20, Bremer v. SolarWinds Corp. et al., No. 1:21-cv-00002 (W.D. Tex. Jan. 4, 2021), ECF No. 1.

[28] Id. at 8.

[29] Morgan Conley, Energy Chief Urges Better 'Cyber Hygiene' In Budget Hearing, Law360 (May 19, 2021), https://www.law360.com/cybersecurity-privacy/articles/1386267/energy-chief-urges-better-cyber-hygiene-in-budget-hearing.

[30] Defense-in-Depth: Cybersecurity in the Natural Gas and Oil Industry, Nat. Gas Council 10 (2018), https://www.api.org/-/media/Files/Policy/Cybersecurity/2018/Defense-in-Depth-Cybersecurity-in-the-Natural-Gas-and-Oil-Industry.pdf.

[31] Id.

[32] Based on review of the 2020 SEC filings of top 25 publicly traded oil and gas companies (based on market capitalization May 21, 2021); see also Cyber Essentials Starter Kit: The Basics for Building a Culture of Cyber Readiness, Cybersecurity and Infrastructure Security Agency (Spring 2021), https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf [hereinafter "Cyber Essentials Starter Kit"].

[33] How Cybersecurity Policies and Procedures Protect Against Cyberattacks, McAfee, https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/cybersecurity-policies.html (last visited May 20, 2021); see also Cybersecurity and Resiliency Observations, Off. of Compliance Inspections and Examinations, U.S. Securities and Exchange Commission (2020), https://www.sec.gov/files/OCIE-Cybersecurity-and-Resiliency-Observations-2020-508.pdf.

[34] Cybersecurity and Resiliency Observations, supra note 33.

[35] Paul Cichonski, Tom Millar, Tim Grance and Karen Scarfone, NIST Special Publication 800-61 Revision 2: Computer Security Handling Guide, Nat'l Inst. of Standards and Tech. 1, 18 (Aug. 2012), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf#page=31 [hereinafter "NIST Computer Security Guide"]. While this document has been created for federal agencies' use, it may also be used by the organizations in the private sector on a voluntary basis. Id. at 4.

[36] Id. at 10-13, 16.

[37] Ransomware Guidance, supra note 2.

[38] NIST Computer Security Guide, supra note 35, at 33.

[39] Id. at 33-34.

[40] Piotr Cipiela, Six Cyber Security Issues for Oil and Gas Companies, EY (Apr. 12, 2019), https://www.ey.com/en_gl/oil-gas/six-cybersecurity-issues-for-oil-and-gas-companies.

[41] Creating a Cybersecurity Strategy, McAfee, https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/creating-cybersecurity-strategy.html (last visited May 20, 2021).

[42] Cyber Essentials Starter Kit, supra note 32, at 5-6.

[43] Mark Lanterman, Cyberattacks and the Costs of Reputational Harm, 75 Bench & B. Minn. 10 (Oct. 2018); Cybersecurity and Resiliency Observations, supra note 33, at 8.

[44] Cybersecurity and Resiliency Observations, supra note 33, at 4.