SpencerFane®

Cybersecurity in Oil and Gas: Protecting Critical Infrastructure and Operations in the Digital Age

Cybersecurity is hard. The odds are against you from the beginning requiring the defenders to get everything right 100 percent of the time and the attackers needing only one lucky shot. Cybersecurity in the oil and gas industry is even harder. While cyber criminals are usually motivated by money, the oil and gas sector faces threats not only from financially motivated criminals but also from nation-state actors, hacktivists, and others seeking to disrupt critical infrastructure or cause environmental damage.

The Colonial Pipeline Cyber Incident is only one example of the sector's vulnerability. The cyberattack, which occurred on May 7, 2021, targeted computerized equipment managing the pipeline, leading to a shutdown of operations. The pipeline, which carries gasoline and jet fuel mainly to the Southeastern U.S., was forced to halt operations to contain the attack. On May 8, 2021, the company paid a ransom to the hacker group Darkside of 75 Bitcoin ($4.4 million at the time of the transaction) in order to restore their systems. Approximately 12,000 gas stations were affected. Operations were restored on May 13, 2021.

The criminals will try to disrupt operations through ransomware attacks, steal sensitive operational data, and threaten to publish confidential information if ransom demands aren't met. Smaller and mid-size oil and gas companies are as much of a target as industry giants because attackers know they usually have fewer resources for cyber defense, yet their operations are often interconnected with larger players in the industry.

Even worse, cybersecurity is not a static problem that can be fixed, like a technical glitch such as Y2K; instead, it is more like warfare where an active adversary is

continuously attacking and every time you implement new defenses, they counter by adapting, changing tactics, and finding another way to circumvent those defenses. This is particularly critical in oil and gas operations where a successful attack could lead to environmental disasters, safety incidents, or disruption of essential energy supplies.

Reality, not a feel-good message. I apologize that this is not a pleasant "feel good" message, but it is the reality and the only way we can fulfill our responsibilities to our stakeholders, employees, and the communities we serve is by having a realistic understanding of the challenges we face because there are many things that can be done to become much harder and resilient targets.

In my role as breach counsel, I have advised on thousands of cyber incidents and hundreds of ransomware attacks over my career. Being in that detached role, seeing the overall process from a strategic vantage point, that perspective has shown me several things that organizations could have done differently to avoid those situations. These observations are particularly relevant for the oil and gas sector, where operational technology (OT) and information technology (IT) systems are increasingly interconnected.

Cybersecurity requires an ongoing and continuous process. Threat actors are continuously adapting and changing their tactics. The only way to defend critical energy infrastructure is to have an ongoing process that is evolving and maturing with them.

Risk assessments are essential. All organization's risks are unique and depend on a multitude of different factors. Because you cannot protect against what you do not know, you must have an understanding of your unique risks, not only from a technical standpoint but also from an operational safety and environmental perspective. This risk assessment is essential for prioritizing mitigations efforts.

Data governance is critical. Your objective includes protecting both operational data and intellectual property. This means you must know what sensitive data you have, not collect or maintain more than is needed, and when you no longer need it, securely archive or dispose of it.

Data equals risk. If you want to reduce that risk, reduce the data you have available to threat-actors. The same principles apply to employee data and other forms of sensitive operational information.

Know the law. Cybersecurity, and especially compliance, is a legal issue that requires a thorough understanding of the laws and regulations that are applicable to your organization, including environmental and safety regulations. Do not forget about your contracts. Many organizations have far more "law" governing them through their contracts than any other source.

Know your service providers. Your organizational risk assessment should include third parties you rely on for services or that have access to your operational systems. As the Colonial Pipeline attack showed, a successful attack on one service provider in the energy sector can shut down operations across multiple organizations and regions. What service providers does your organization depend on and how will you continue to operate if something happens to them?

Cyber risk is an overall organizational risk, not just an "IT risk." Your organization must have a team-oriented approach to managing cyber risk, both internally and externally (with the partners you rely on or will rely on if you have an incident). Your team's different perspectives are invaluable.

At a minimum, no matter the size of the organization, the risk team should include members (internal or external) that focus on: (1) information security, (2) operational technology security, (3) industrial control systems, (4) legal, compliance, environmental health and safety, (5) audits, (6) operations, (7) human resources, and (8) communications.

For smaller organizations, one person may wear a lot of hats in an attempt to fulfill many of those roles, but each organization must have access to external partners with specific expertise who can fill the gaps that inevitably appear.

This blog was drafted by Shawn Tuma, an attorney in the Spencer Fane Plano, Texas office and the leader of the firm's Cyber | Data | Artificial Intelligence | Emerging Technology team. For more information, visit www.spencerfane.com.

Click **here** to subscribe to Spencer Fane communications to ensure you receive timely updates like this directly in your inbox.