Drilling Down on Cybersecurity

Brittany Bacon and Adam Solomon, Hunton Andrews Kurth LLP, provide a comprehensive overview of cybersecurity risks, regulations, and best practices in the US oil and gas industry.

It is no surprise that the oil and gas industry continues to be a high-value target for cyber criminals, hacktivists, and nation-state actors alike. As the US$6 trillion oil and gas sector embraces the adoption of new digitisation and automated technologies, many operational technology (OT) systems are built on legacy infrastructure plagued with unpatched vulnerabilities, outdated software, and weaker security controls that can make them more difficult to protect. Moreover, the industry's attack surface is broader than ever with geographically dispersed assets and a heavy reliance on complex supply chains with third-party dependencies.

This article summarises the key state and federal cyber regulations that apply to the oil and gas industry, executive and board liability and oversight responsibilities in the breach context, and practical steps for cyber risk mitigation and preparedness.

Key cybersecurity regulations for critical infrastructure

The oil and gas industry is among the more highly regulated operators of critical infrastructure for cybersecurity in the US. There are various regulatory frameworks that apply to different segments of the oil and gas industry depending on their upstream, midstream, and downstream operations, resulting in a complex, often duplicative, and burdensome assortment of requirements for oil and gas companies to navigate when securing their infrastructure and responding to cybersecurity incidents.

Since 2021, there has been an uptick in cybersecurity rules that apply to companies in the oil and gas supply chain. Key US cybersecurity regulatory frameworks for oil and gas companies include:

Pipeline owners and operators

Following the ransomware attack on Colonial Pipeline in 2021, the Transportation Security Administration (TSA) issued two security directives aimed at enhancing the cybersecurity defenses of critical oil and gas pipelines. These security directives require owners and operators of critical pipelines to report cybersecurity incidents to TSA within a 24 h period, conduct vulnerability assessments on their systems and implement a baseline set of mandatory cybersecurity measures to protect the security and resiliency of their pipeline infrastructure. Covered owners and operators are required to memorialise their compliance programmes in a cybersecurity plan that explains their defense-in-depth strategy for protecting critical systems, which must be tested and audited annually. Following criticism from industry stakeholders and a reform to make the mandatory measures more adaptable, TSA began a rulemaking process to replace the security directives with a more holistic set of cybersecurity regulations for entities that own or operate pipeline facilities and systems. In November 2024, TSA released a draft of the proposed regulations for public comment. The draft regulations adopt many of the existing principles and measures found in the security directives and propose combining physical security and cybersecurity requirements into a single set of rules.

Public companies

Like other public companies, oil and gas companies that are issuers of public securities are subject to the Securities and Exchange Commission's (SEC's) cybersecurity disclosure regulations. These rules require public companies to disclose material cybersecurity incidents to investors through a Form 8-K within four business days of making a materiality determination and also impose obligations to include information about the company's cybersecurity governance and risk management programme in their annual reports.

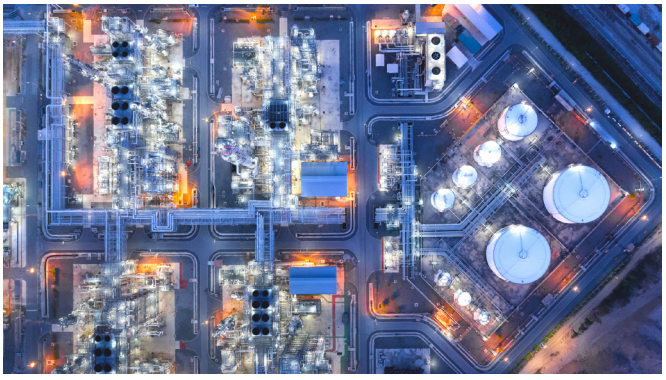

Figure 1. *Boards and executive leadership are expected to play an active role in cyber oversight and preparedness.*

Critical infrastructure entities

In 2022, Congress passed a groundbreaking new incident reporting rule for critical infrastructure entities, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). The Cybersecurity and Infrastructure Security Agency (CISA) has noted that it "anticipates that many oil and natural gas subsector entities will be considered covered entities" required to report incidents to federal authorities under this reporting framework. CIRCIA will require covered entities to report certain substantial cyber incidents to CISA within 72 h from learning of a reportable event and ransom payments made in response to a ransomware attack within 24 h after a payment has been made. The CIRCIA reporting requirements are not yet in effect and are being fleshed out in implementing regulations. While CISA released a much anticipated draft of the CIRCIA rules in April 2024, the agency has postponed the finalisation of the regulations and announced that the final rules are not expected to be released until May 2026.

Public utilities

Some oil and gas companies also may have compliance obligations under federal and state utility cybersecurity rules. At the state level, utility regulators have been focused on enhancing their cybersecurity regulations, including in Maryland and New York, which have issued or proposed new cybersecurity regulations for public utilities in their states in recent years. These regulations are particularly relevant for gas companies with downstream operations that may fall within the scope of these state regimes. At the federal level, the North American Electric Reliability Corp.'s (NERC) Critical Infrastructure Protection (CIP) standards are a federally enforced framework that applies to entities operating in the electric power sector within the oil and gas industry. NERC CIP requires covered entities to comply with a range of security control standards for protecting their OT that supports North America's bulk electric system.

Maritime stakeholders

Oil and gas companies involved in upstream and midstream operations also could be impacted by the recently released cybersecurity regulations for the maritime industry. In January 2025, the US Coast Guard released a final rule formalising cybersecurity requirements for owners or operators of US-flagged vessels, facilities, and Outer Continental Shelf facilities. The regulations, which are similar to the TSA security directives for oil and gas pipelines, include requirements on maintaining a cybersecurity plan, implementing a baseline set of prescribed cybersecurity measures for protecting the Marine Transportation System, and reporting cybersecurity incidents to the National Response Centre.

In addition to laws and regulations, oil and gas companies often have cybersecurity obligations imposed on them in customer and business partner contracts. These agreements often require oil and gas companies to align their cybersecurity programs with well-known industry frameworks such as the National Institute of Standards and Technology's Cybersecurity Framework, American Petroleum Institute's Standard 1164, CISA's Cross-Sector Cybersecurity Performance Goals, and the Bureau of Safety and Environmental Enforcement's OT Cybersecurity Strategy.

Outside the US, cybersecurity rules for oil and gas companies are emerging just as rapidly, such as in the EU, which has expanded the scope of essential entities subject to the incident reporting and cybersecurity resilience requirements of the NIS2 Directive. Other countries have similarly developed or enhanced their cybersecurity frameworks for critical infrastructure operators doing business within their borders.

Board oversight

Cybersecurity has become a central compliance risk to most oil and gas companies that is mission critical and deserving of executive and board-level oversight. As a result, it is crucial for senior leadership, including the Board of Directors, to monitor and oversee a company's cybersecurity strategy and risk posture, including by receiving adequate and timely briefings about the company's compliance programme, preparedness efforts, and response to significant cybersecurity incidents and threats. Such cybersecurity oversight has become even more important over the years due to the rise in shareholder lawsuits seeking to impose personal liability on the officers and directors of companies for oversight failures related to cybersecurity attacks. Moreover, the SEC views cybersecurity risk management to be a key element of an enterprise-wide risk management programme and increasingly important to complying with US securities law. Public companies are now required to include disclosures in their annual reports on cybersecurity oversight roles and processes, including descriptions of the roles of the board of directors in overseeing risks from cybersecurity threats and management in assessing and managing the material risks from cybersecurity threats.

Practical steps for mitigating risk

We have outlined below critical steps oil and gas companies should take to help limit legal liability and mitigate operational, financial and reputational damage if an intruder is able to penetrate the company's IT or OT environments. These recommended actions supplement the technical efforts the company's IT and IS groups take to prevent cyber-attacks and data breaches in the first instance.

Enhancing multi-stakeholder incident response plan and procedures

An incident response plan should function as a company-wide framework that provides a comprehensive list of key activities and responsibilities to assist the company in identifying, evaluating, responding to and resolving cybersecurity incidents. The plan should draw on multiple functions across the company, including information security, legal, IT/OT, communications, insurance, physical security, HR, finance, and others. A Security Incident Legal Response Procedure can supplement the Plan by setting forth key protocols for the Legal Department to follow in responding to cybersecurity incidents.

Developing a ransomware incident playbook

We increasingly see companies (particularly in oil and gas) supplement their general incident response plan with a playbook that explains the unique steps and considerations for addressing ransomware incidents and other cyber extortion events. This playbook sets out key protocols to follow in the event of a ransomware or other cyber extortion demand, including steps and considerations for assessing payment decisions and the response strategy.

Conducting a cybersecurity tabletop exercise

An executive-level cybersecurity tabletop exercise helps prepare companies for a cybersecurity incident and identify gaps in the company's incident response processes. This exercise brings together senior stakeholders at the company, draws on actual events and applies the facts to a complex cybersecurity hypothetical. The tabletop is designed to help prepare a company to take a multi-functional, coordinated approach to cyber incidents, raising various scenarios and hypotheticals for the incident response functions within the company to consider and discuss.

Managing supply chain risk

The oil and gas industry relies heavily on a complex supply chain of myriad third-party vendors and contractors. A compromise of one link in the chain can have cascading effects on the broader operation. A robust vendor management programme helps manage these security risks throughout the lifecycle of the business relationship, including during due diligence, contracting, onboarding, ongoing monitoring and offboarding. Key components include developing an IT and OT security diligence questionnaire, developing robust vendor contractual security provisions, and developing audit questionnaires for monitoring third-party business partners' ongoing compliance with their cybersecurity obligations during the term of the agreement.

Consider external expert engagements

It is helpful to identify key vendors and preferred partners in advance of an incident. This includes forensic firms, cyber extortion specialists, outside counsel, PR firms, and other outside advisors with appropriate experience in managing crises so that the advisors can spring into action if need be.

Review cyber insurance policy

Oil and gas companies are well advised to assess their insurance portfolio, including current policies covering cybersecurity, directors and officers, errors and omissions, fidelity and crime, and general commercial liability to help ensure adequate coverage should the need arise.

Hardening OT security

OT devices can be vulnerable targets that may lack the key controls more widely applied by their IT counterparts. OT security can be bolstered by segmenting IT and OT networks; removing OT connections to the Internet; changing default passwords quickly and requiring complex, unique passwords; limiting and securing remote access to OT networks; inventorying OT assets; and ensuring business continuity and disaster recovery plans are in place to minimise downtime in the event of an incident.

Preparation is key

With little tolerance for operational downtime, oil and gas leaders are faced with unique challenges in this newly connected world and an increasingly ominous cyber threat landscape, marked by ransomware attacks, nation-state actors and advanced persistent threats, exploitation of ICS vulnerabilities, disgruntled insiders, and the growing threat of foreign workers infiltrating US companies to steal sensitive data and extort victim companies. Companies in this industry increasingly will be judged – by courts, regulators, boards of directors, shareholders and the public – by how well they prepared for and responded to these events.