Professional Perspective

Changing Cybersecurity Expectations for US Oil & Gas Companies

Stephen Lilley and Christopher Watts, Mayer Brown

Bloomberg Law

Changing Cybersecurity Expectations for US Oil & Gas Companies

Contributed by Stephen Lilley and Christopher Watts, Mayer Brown

Cyber risks facing the oil and gas industry continue to grow. Legal requirements likewise are continuing to expand. The cybersecurity directives issued by the Transportation Safety Administration (TSA) in 2021 and 2022, for example, imposed new requirements upon certain oil and gas pipelines, including new incident reporting obligations and required vulnerability assessments.

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) and the Securities and Exchange Commission's (SEC) proposed rule to require public companies to disclose material incidents within four business days promise further change. Moreover, the National Cybersecurity Strategy (Strategy) recently released by the Biden administration makes strengthening the cybersecurity of US critical infrastructure a top priority. Emphasizing an increase in government regulation and private-sector accountability to "rebalance" legal expectations for companies, the Biden administration's Strategy could have potentially significant consequences for the oil and gas sector, particularly if Congress passes legislation expanding regulatory authorities.

In short, further change is on the horizon. But what does this mean for companies in the oil and gas industry? While it is impossible to predict precisely how policymakers will shape cybersecurity requirements in the future, leaders in the oil and gas sector will benefit from understanding three key trends: first, a shift towards earlier reporting and public disclosure of cyber incidents; second, an increase in government oversight and regulation of cybersecurity within the industry; and third, a heightened focus on cyber governance, including by companies' boards of directors.

In this article, we summarize how these trends may affect oil and gas companies in the coming years and describe steps companies can take to stay ahead of the curve.

Earlier Reporting & Public Disclosure of Cyber Incidents

TSA substantially expanded cyber incident reporting requirements in the oil and gas industry when it required critical pipeline owners and operators to report any cybersecurity incident on a pipeline's network infrastructure to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) within 12 hours of identification. Policymakers are not stopping there.

The two forthcoming requirements discussed below will also further advance this trend towards earlier reporting of incidents to government agencies and, in some cases, public disclosure of cyber incidents. As a result of these and other impending changes, a broad range of US oil and gas companies should expect to be required to report, and possibly disclose, certain cyber incidents in the next few years.

In 2022, Congress dramatically expanded cyber incident reporting to the federal government with CIRCIA. That statute requires covered entities to report certain substantial cyber incidents to CISA within 72 hours. Covered entities will also need to disclose within 24 hours any ransom payments made.

The exact scope and mechanics of these requirements will be identified in a rulemaking effort led by the Director of CISA—a process that saw extensive industry comments in response to a request for information in September 2022. Some of these industry comments recommended that CISA cover only the most critical infrastructure and the most severe incidents in the forthcoming rule.

The tone of the National Cybersecurity Strategy appears to suggest, however, that the Biden administration may interpret CIRCIA broadly so that it covers a wide group of incidents experienced by a broad set of companies. While the implementation timeline provided in CIRCIA means that any final rule is unlikely to go into effect for at least a couple of years, oil and gas companies should not be caught flat-footed when the time comes.

Increasing public disclosure of cyber risks and cyber incidents to investors has been a focus of the Securities and Exchange Commission for over a decade. Having previously issued guidance, the SEC took the further step in March 2022 of

proposing a rule that would require publicly traded companies to publicly disclose cybersecurity incidents on a Form 8-K within four business days of determining that the incident is "material."

This proposed rule raised numerous concerns for industry stakeholders about its workability and unintended consequences. For example, numerous stakeholders across industries urged the SEC to permit delay of public disclosure of incidents when disclosure would impair law enforcement investigations, compromise national security, or otherwise have serious negative consequences for the victim company or third parties. It remains to be seen how the SEC will resolve the comments it received. Assuming the SEC moves forward with a final rule that roughly aligns to the proposal, publicly traded oil and gas companies should be prepared for early public disclosure of cyber incidents.

Practically speaking, this trend toward early reporting—and possibly public disclosure—will require relevant businesses to maintain procedures that allow them to quickly and appropriately assess the cyber incidents they face and then, provide accurate information to key internal decisionmakers so that they can determine whether notification or disclosure is required. Companies that do not maintain well-defined internal procedures for responding to cyber incidents that involve their legal counsel and escalate key decisions to executive stakeholders will likely struggle to meet forthcoming requirements and to manage the consequences of incident reporting or disclosure.

As a result, oil and gas companies will likely benefit from assessing and exercising their incident response policies, particularly after more clarity is available around the scope and substance of future regulatory requirements.

Increases in Government Oversight & Regulation

The National Cybersecurity Strategy prioritizes establishing cybersecurity requirements for critical infrastructure. To that end, the Strategy explains that the "Federal Government will use existing authorities to set necessary cybersecurity requirements in critical sectors." The Strategy further explains that the Administration will work with Congress to close gaps in existing authorities. And it further explains that "[w]here states or independent regulators have authorities that can be used to set cybersecurity requirements, the Administration will encourage them to use those authorities in a deliberate and coordinated manner."

While it is difficult to predict how Congress and state governments will view these goals, it is clear that many policy leaders share widely held concerns about cyber threats to energy infrastructure. For example, just weeks after the Administration announced the Strategy, the Senate Energy and Natural Resources Committee conducted a hearing to examine cybersecurity vulnerabilities in US energy infrastructure. In that hearing, the witnesses testified to the shift in the cyber threat landscape and the need for collaborative action—including the federal government—to address an ever-growing threat.

To address these issues, the Biden administration and like-minded states are likely to take available actions to close perceived gaps in government oversight. To that end, a recent report by the Government Accountability Office (GAO) on the cybersecurity of offshore oil and gas facilities provides an example of an area in which government action may be forthcoming. Likewise, legislation in New York state may provide an example of how state governments will try to steer cybersecurity practices within the industry.

Together, these examples suggest that greater government oversight—and possibly direct regulation—of cybersecurity in the oil and gas industry likely lies ahead.

GAO Study on Offshore Oil & Gas Cybersecurity

GAO's October 2022 report described offshore infrastructure as facing significant threats from a broad range of cybercriminals, hackers, and state actors. Given these threats and vulnerabilities in critical systems, including operational technology (OT), GAO concluded that an attack could cause significant physical, environmental, and economic harm, and that disruptions to oil and gas production and transmission in the aftermath of a cyberattack could have a direct impact on global supplies and markets. GAO called on the Bureau of Safety and Environmental Enforcement (BSEE), and agency within the Department of the Interior, to immediately develop and implement a cybersecurity strategy for offshore oil and gas facilities.

It remains to be seen how exactly BSEE will move forward and what implications this will have for oil and gas companies. However, in light of the National Cyber Strategy, companies should likely expect the Biden administration to use available

authorities to drive changes in cybersecurity practices in offshore facilities, as well as other areas that the administration itself identifies as not being subject to relevant cybersecurity requirements.

Companies that are currently subject to limited regulation on this front will consequently likely benefit from engaging with the Biden administration on potential policy approaches and specific proposals to ensure that chosen approaches actually improve cybersecurity and do not have unintended consequences. At the same time, such companies will likely benefit from reviewing regulatory requirements or guidance in related sectors, as well as relevant industry best practices. While not required by law, confirming that their cybersecurity management programs are generally aligned with these guideposts will likely help prepare an oil and gas company for any future regulation or guidance applied directly to its business.

State-Level Action

Recent action in New York state may provide an indication of how state legislatures and regulators may weigh in on cybersecurity in the oil and gas industry. There, Governor Kathy Hochul signed legislation (A.3904B/S.5579A) increasing cybersecurity oversight of New York's energy industries at the end of 2022.

Amongst other things, the new law will provide the Public Service Commission, which regulates New York's energy industries, with enhanced auditing powers. This includes the authority to perform "an annual audit of gas corporations and electric corporations relating to the adequacy of cyber-security policies, protocols, procedures and protections." The statute, among other provisions, also requires utility companies to prepare for cyberattacks as part of their annual response plans and directs the Public Service Commission to establish rules requiring gas corporations and electric corporations to develop and implement capabilities to detect unauthorized network activity.

New York's action aligns with the Biden administration's interest in states helping to set minimum cybersecurity requirements for critical infrastructure. How many other states will follow suit remains to be seen. However, oil and gas companies should be prepared to see more state-level actions akin to those in New York, especially in states where significant oil and gas infrastructure is located. As at the federal level, tracking these proposals and engaging effectively with state legislators and regulators will likely help make future requirements both more effective and more practical.

Heightened Focus on Governance

Effective cybersecurity requires strong collaboration between technical stakeholders, safety teams, legal, communications, and other functions. Strong cybersecurity programs are typically documented in appropriate policies and procedures, and oversight is performed by senior executives and the board of directors. Expectations around these governance best practices are rapidly increasing.

The anticipated revision to the NIST Cybersecurity Framework will introduce a new "Govern" function, for example, and the SEC's proposed rule regarding cybersecurity disclosures by registrants would emphasize governance in the required disclosures. Oil and gas companies should expect this focus on governance to continue to grow in the coming months and years, and refine their own cyber risk management and oversight approaches accordingly.

NIST Framework v.2.0

The Framework for Improving Critical Infrastructure Cybersecurity, issued in 2014 by the National Institute for Standards and Technology (NIST), has become a broadly utilized tool for managing cyber risk to oil and gas companies, among others. After making limited updates to this framework in 2018, NIST now anticipates making more substantive revisions in an upcoming version 2.0.

To that end, in January 2023, NIST released a concept paper describing its intended approach and soliciting public comment. This concept paper flagged NIST's intent to highlight governance in version 2.0, elevating it in a new "Govern" function that would join the existing five functions—identify, protect, detect, respond and recover.

According to NIST, this "new crosscutting Function will highlight that cybersecurity governance is critical to managing and reducing cybersecurity risk." This function "may include determination of priorities and risk tolerances of the organization, customers, and larger society; assessment of cybersecurity risks and impacts; establishment of cybersecurity policies and procedures; and understanding of cybersecurity roles and responsibilities."

NIST explains that these "activities are critical to identifying, protecting, detecting, responding, and recovering across the organization, as well as in overseeing others who carry out cybersecurity activities for the organization, including within the supply chain of an organization." In NIST's estimation, elevating governance to a function "would also promote alignment of cybersecurity activities with enterprise risks and legal requirements."

In short, oil and gas companies—many of which have long employed the NIST Cybersecurity Framework—should expect governance to be a core and expected feature of their cybersecurity programs in the future, if not already. To that end, oil and gas companies would be well served to confirm that existing policies and procedures, and other governance tools, adequately address the governance goals previewed by NIST.

SEC Rulemaking

The SEC's proposed cybersecurity rule likewise highlights cybersecurity governance. It would require detailed disclosures regarding: policies and procedures, if any, for identifying and managing cybersecurity risks and the company's cybersecurity governance; the board of directors' role in oversight of cybersecurity risks; and management's role in managing cybersecurity-related risks and implementing the company's cybersecurity policies and procedures.

For example, it would require a registrant to explain:

- Whether the registrant has a cybersecurity risk assessment program, and if so, provide a description of such program.
- Whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risk; and how the board is informed about cybersecurity risks, and the frequency of its discussions on this topic.
- Whether and how the board considers cybersecurity risks as part of its business strategy, risk management and financial oversight.

In addition, under the rule as proposed, a registrant would be required to disclose whether any board member has cybersecurity expertise, and, if so, the nature of such expertise.

While the details of any final rule remain to be seen, the SEC's approach confirms the increasing expectations for governance of cyber risk by registrants. Oil and gas companies—even including those that are not public companies—will be well served to evaluate their own cyber governance practices and to confirm that their senior leaders provide effective oversight.

Conclusion

Cybersecurity expectations for US oil and gas companies have increased in recent years and further change is on the way. Companies should engage with policy makers to ensure that future policies effectively advance the cybersecurity of the industry. US oil and gas companies also generally will be well served by anticipating three key trends:

- Earlier required reporting or disclosure of cyber incidents.
- Increased government oversight or regulation of cybersecurity practices.
- Increased expectations for cyber governance.

While the details of future cybersecurity expectations for the industry remain to be seen, understanding and responding to these three trends will allow US oil and gas companies to manage the legal, financial, and reputational risks associated with the many cyber threats that they face.