Cybersecurity Issues To Consider In Oil And Gas M&A

By **Eric Otness, William Ridgway and Daniel Scime** (October 7, 2019, 3:12 PM EDT)

Eric Otness

William Ridgway

Daniel Scime

One of the foremost threats companies face today is that posed by cybercriminals, and the unique vulnerabilities of companies in the oil and gas sector create heightened cybersecurity risks for those pursing transactions in the sector. A recent study by KPMG found that oil and gas CEOs rank cybersecurity as the largest threat to their organizations' growth. Over half of CEOs in the sector believe that their organization will at some point fall victim to a cyberattack.

While there is growing recognition that cybersecurity is a key risk factor in mergers and acquisitions generally, executives and directors contemplating an acquisition in the oil and gas sector need to be aware of the unique cybersecurity challenges within the industry, in order to properly assess transaction risks and value target companies.

As in other industries, companies in the oil and gas sector face the prospect of paralyzing ransomware, data breaches and intellectual property theft — common risks that are all too familiar to executives today. Yet cybersecurity risks are magnified in the oil and gas industry for a number of reasons.

Unlike in the power and nuclear sectors, federal regulators do not require companies in the oil and gas sector to adhere to baseline cybersecurity standards. Despite efforts by industry leaders to develop their own best practices and standards, companies in the sector sometimes lag behind other industries in their response to digital threats. And because oil and gas companies are not required to report when hackers infiltrate their systems, there is limited visibility into the volume of attacks and performance of existing cybersecurity controls.

The scale of oil and gas operations also complicates the job of defending against hackers. Sprawling networks of computers, automated controls and sensors mean a multitude of access points for attackers. Moreover, the equipment and software used to run these networks is often decades old and lacking modern security features. Seemingly straightforward upgrades can cost millions of dollars and halt operations for days.

Midstream and other oil and gas companies that own and operate critical infrastructure are particularly alluring targets for sophisticated hackers, including state actors and cyber terrorists. Increasingly, these actors seek to infiltrate and manipulate operational controls — raising the specter that malicious hackers could disrupt systems in a key industry, or cause a catastrophe such as a spill or an explosion.

Failing to appreciate and account for these unique risk factors during the due diligence process can haunt acquirers of oil and gas companies. Where target companies fail to invest in effective cybersecurity controls and protect the proprietary extraction, processing and delivery technologies and processes that provide them with competitive advantages, acquiring companies risk watching the value of their purchase erode.

Worse yet, compromised systems at the target company could, when merged with the acquiring company's network, permit hackers to circumvent the acquiring company's own cyber defenses and spread the breach.

Similarly, acquiring companies can emerge from the transaction to find that they have significant unexpected capital costs and potential exposure — outdated digital infrastructure in need of repair, the prospect of production disruptions, and vulnerabilities that could lead to a spill, worker injuries or an explosion. These hidden costs could significantly reduce the value of the transaction.

As with any due diligence effort, the scope will depend on the transaction dynamics and timeline. Still, key considerations for which companies contemplating an acquisition in the oil or gas sector should account include the following.

Industry Standards

Although there are no mandatory cybersecurity standards against which to measure cybersecurity programs and practices for companies in the oil and gas sector, the U.S. Department of Energy has developed a best practices model. Additionally, trade groups, including the American Petroleum Institute, have adopted industry standards.

One threshold question for the diligence team is whether the target company's cybersecurity program adheres to a particular standard. To answer this question, diligence teams should at minimum:

- Interview key staff;
- Analyze the results of any vulnerability assessments, penetration testing and vendor audits;
- Review incident response plans and incident reports for adherence to best practices; and
- Assess the maturity of the company's cybersecurity governance and vendor management programs, including: (1) the terms of any indemnification and cyber insurance policies; (2) the existence of past cybersecurity incidents and how they were handled; and (3) whether the company has interacted with regulators, law enforcement or other third parties regarding actual or potential cybersecurity incidents.

Target Company's Network Security

Diligence teams should not rely on a target company's assurances without independent verification. Companies with serious security gaps seldom recognize the problem.

Acquirers should consider retaining a third-party forensic firm to conduct vulnerability assessments and penetration testing, particularly where the target has never engaged one. That effort may uncover hackers lurking in the target's network. More likely, however, the result will be a risk calculation based on the target company's governance and the information security controls.

Deal Terms

Diligence results should inform deal terms, addressing both costs to remediate gaps in cybersecurity governance and risk management as well as any post-deal indemnity claims. Well-crafted representations and warranties can protect acquirers; at minimum, these terms should cover:

- The absence of unauthorized access to the target's networks;

- The confidentiality of key proprietary technology, plans, data and intellectual property;

- Compliance by the target (and affiliates and vendors) with relevant cybersecurity and data privacy laws; and

- Compliance with the target's own internal cybersecurity policies and practices.

The target will likely request qualifications limiting these representations and warranties. An acquirer's willingness to acquiesce will depend in part on what the diligence investigation revealed.

Indemnity provisions may also be used to hold the target liable for its representations as well as for hidden or undisclosed cybersecurity liabilities that arise after closing. The parameters for indemnity provisions should likewise flow from the diligence findings.

Cyber Insurance

Representation and warranty insurance — which is now commonplace in M&A transactions — and standalone cyber insurance can help shield acquirers from cyber risks.

In either case, an underwriter will likely consider the quality and depth of the acquirer's diligence review when analyzing insurable risks and determining premiums, deductibles and caps. A robust diligence investigation, thus, will likely pave the way for more favorable insurance policy terms.

Eric C. Otness and William Ridgway are partners and Daniel J. Scime is an associate at Skadden Arps Slate Meagher & Flom 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.