THE AMERICAN OIL & GAS REPORTER®
DECEMBER 2017
The "Better Business" Publication Serving the Exploration / Drilling / Production Industry

# Insurance Mitigates Cyber-Related Risk

Lawrence J. Bracken II,
Michael S. Levine
and Geoffrey B. Fehling

ATLANTA–In today's interconnected society, cyber breaches are inevitable. As the saying goes, it is not a matter of if, but when, an organization will be breached. This is particularly true for businesses in the energy sector, which is one of the most frequently targeted industries for cyber attacks. From producers to pipelines and refineries, energy companies' computer systems are increasingly at risk of becoming the target of a sophisticated and targeted cyberattack, making cyber risk mitigation paramount.

Oil and gas companies face unique cyber risks, including a broad array of direct and indirect losses that can accompany a cyber breach. Companies can mitigate these risks by employing sound operational and incident response practices in conjunction with adequate cyber insurance and comprehensive traditional insurance policies such as pollution liability and general liability policies. An effective insurance program should minimize coverage gaps when pollution events, property damage, bodily injury or business interruptions result from cyber attacks.

A 2017 survey of cyber security risk managers indicated that implementing cyber security measures in the U.S. oil and gas industry lags behind the growth of digitalization in oil and gas operations. One report estimated that three of four oil and gas companies fell victim to at least one cyber attack last year, as hacking efforts against the industry became more frequent and sophisticated.

Technological advancements, while necessary and important for operational purposes, may exacerbate the risk of compromised computer systems. For example, implementing computer-controlled offshore platforms requires offshore-to-onshore communications and other processes, which are often controlled by onshore personnel using networked computers. This remote system, while likely improving safety and decreasing costs, provides opportunities for would-be hackers to target critical communications, supervisory and support systems.

The complex supply chain further complicates matters, as each party or innovative technology in the chain presents a new attack vector or potential "weak link" for hackers to exploit. In fact, the most robust encryption and sophisticated firewalls offer little protection if an operator or a vendor, supplier or customer is using a less sophisticated cyber security system. The complex nature of the oil and gas industry, which relies on a combination of state-of-the-art technology and outdated hardware that is often decades old, also makes cyber security more challenging because of the difficulty of balancing old and new technologies.

Three of the most worrisome attack vectors include manipulating stock information to dynamically change pricing information, hacking burner management systems to engineer oil tank explosions, and manipulating temperature or pressure measurements on remote plant equipment to trigger breakdowns in remote facilities. Other potential losses include plant shutdowns, service interruptions, facility shutdowns, compromised product quality, undetected spills, bodily injury resulting from equipment malfunctions, and release of personally identifiable information, trade secrets or other financial data.

The bottom line is that new technological features and the interconnectedness of many operations not only improve efficiency, but also create new and enhanced risks. Some cyber risks are not limited solely to lost data or productivity, and may even result in more serious environmental liability, property damage, or bodily injury arising from physical damage or malfunctioning equipment. A robust insurance program that insures resulting liability and property losses is an important part of risk management and mitigation efforts in the event of a cyber event.

### Insuring Residual Risk

The cyber threat landscape has developed so rapidly that it is insufficient to rely solely on traditional "prevention" strategies, such as implementing robust encryption, firewalls and data compartmentalization. Rather, businesses should expect that every network has been or will be compromised, which requires shifting the principal focus from prevention to building resilience and minimizing the impact of cyber events when they occur. One important way to minimize this exposure is by insuring residual risk for cyber events.

Generally speaking, mitigating cyber risk through insurance involves four key coverages:

- First-party coverage, which protects a policyholder for claims involving data loss, business interruption, network failure and other cyber losses suffered by the policyholder itself;
- Hybrid first-party coverage, which provides event management and breach response coverage for particular security/privacy events;
- Third-party coverage, which provides

liability and defense cost insurance for alleged security, privacy and professional service failures arising from claims brought by third parties such as vendors, customers, employees and government agencies; and

- Crime insurance, which provides coverage for dishonest acts by third parties, including computer fraud and forgery or alteration of financial instruments.

Most cyber insurance policies provide several or all these coverages.

First-party cyber coverage typically insures losses sustained directly by the policyholder as a result of a covered cyber event, including the cost of reconstructing or retrieving data destroyed or corrupted by a computer attack, lost revenue and extra expense arising from a computer attack, the cost of investigating and paying extortion demands related to a threatened computer attack, and certain reputational harms (such as diminution of business income due to lost customers).

While sometimes overlooked in the news in favor of high-profile consumer data breach lawsuits, system interruptions following a cyber event can have a significant impact on operations, with very high recovery costs. For example, in 2012, one of the world's largest oil companies was targeted by a virus that erased data on 75 percent of its computers, forcing the company to shut down its information technology network. Last summer, multiple oil and gas companies, port operators and other energy facilities were hit with the Petya virus, which disabled computers and demanded that users pay cryptocurrency ransoms to unlock the compromised systems.

Each of these cyber events stopped short of disrupting actual production or supply operations, but they unquestionably imposed significant direct losses in the form of forensic investigation, data restoration and retrieval costs, and business interruption losses.

### Hybrid Cyber Coverage

Hybrid cyber insurance provides coverage for particular types of security and privacy events, such as computer system breaches, malicious use of computer code or "denial of service" attacks, and dissemination or compromise of personal and confidential business information. Costs commonly covered by these security or privacy events include the cost of forensic accountants to determine the existence, cause and scope of the attack; associated legal and public relationships costs, required (and sometimes voluntary) breach notification costs; data restoration costs; and the cost to implement call centers and credit and identity monitoring services for customers following a breach.

The oil and gas industry has faced many security and privacy breaches that may have resulted in losses that would be covered under hybrid cyber insurance policies. For example, a 2011 cyber attack stole confidential exploration and bidding data from several major oil companies. The coordinated attack, which had been secretly targeting energy companies for as many as four years, utilized both traditional methods of exploiting software vulnerabilities in computer operating systems and "social engineering" techniques such as spear-phishing. Security and privacy losses tied to social engineering are particularly crucial components of cyber risk mitigation, given that they may not be covered by traditional insurance policies.

### Third-Party Cyber Coverage

As its name suggests, third-party cyber insurance protects policyholders from liabilities to third parties harmed by cyber attacks, and may cover civil penalties and other costs imposed by regulators or government agencies. Covered costs under such policies can include defense costs, judgments, and settlement payments, as well as certain fines and penalties. However, third-party cyber liability policies do not automatically provide full coverage for all possible claim scenarios involving a cyber liability, such as situations where a hacking incident causes bodily injury, property damage, business interruption or other physical losses.

Many businesses have redoubled efforts to protect their most important digital assets, intellectual property and critical infrastructure in light of recent cyber attacks targeting so-called "crown jewels." But more traditional consumer-facing aspects of many oil and gas operations still are being targeted by hackers.

For example, an international oil company learned that an employee of a vendor had utilized employees' personal information to facilitate an unemployment insurance claim scam in Texas, underscoring the importance of protecting information in all aspects of a company's operations, however routine. In 2014, that same company reportedly had personal information of approximately 7,000 customers in New Zealand and Australia stolen by online hackers. Loss arising from data breach claims may result in both first-party (e.g., recovering stolen data) and third-party (e.g., data privacy lawsuit) losses.

### Crime Coverage

Crime insurance protects policyholders from dishonest acts of third parties, including employee theft, forgery and alteration, computer fraud and funds transfer fraud, ransom and extortion, robbery, and counterfeiting. While not a traditional "cyber" coverage, crime insurance has become critical to any comprehensive cyber insurance program because it can protect against financial loss caused by social engineering threats.

As oil and gas companies continue to increase the strength and resilience of their computer systems, many hackers simply choose to target the one entry point that cannot be protected with software updates: employees. Last February, the cause of an attempted spyware infection at a Middle Eastern company was one employee opening an infected spreadsheet, which he had received from an elaborate but fraudulent online "person" with whom the employee had been communicating for more than a month. Using this persona, criminals had cultivated social media connections with numerous mid-level technicians, software developers, and administrators at oil and gas, technology, and consulting companies.

Traditional liability policies may present significant coverage gaps that do not apply to cyber-related losses, in part because cyber threats are a relatively new phenomenon from an insurance perspective. As a result, court rulings are inconsistent about whether cyber losses are covered under general liability policies, differing over whether traditional terms such as "publication" and "tangible property" apply to electronic theft or compromise of digital information.

For that reason, policyholders should not assume that their legacy insurance policies are adequate to protect against claims involving cyber attacks. Furthermore, many traditional policies now contain express exclusions for cyber-related losses.

That said, legacy policies still can play an important role in certain cyber claim scenarios. The inherent risk of physical loss resulting from a cyber event underscores the importance of minimizing coverage gaps between traditional and cyber insurance policies, such as where third-party cyber liability policies contain

bodily injury and property damage exclusions. For that reason, in the event of a loss involving a cyber event, it is essential that the policyholder examine potential coverage under both traditional and cyber insurance coverage.

**Common Coverage Issues**

Both legacy policies (general liability, excess liability, pollution liability and property) and cyber-specific insurance products may not provide adequate coverage for all risks that arise from a cyber event. There are some challenging exclusions and other limitations to evaluate when assessing coverage for cyber risks.

The first is environmental liability. Liability policies of all kinds may include various forms of "pollution" exclusions, which bar coverage for loss arising from the discharge or release of pollutants. Cyber attacks on oil and gas companies frequently pose a risk of environmental liability, but cyber insurance policies may limit or bar coverage entirely for claims involving the release of pollutants. Even where companies purchase pollution-specific coverage, the definition of a pollutant may not adequately cover liability arising from cyber attack-related releases.

As noted, many cyber insurance policies also exclude coverage for claims involving bodily injury, property damage or other physical loss, even where such loss is caused by a cyber event. The industry faces significant exposures for physical loss following hacks of drilling platforms, pipelines, storage tanks and other equipment. Policyholders should maintain coverage for physical losses through environmental and traditional general liability insurance to minimize coverage gaps.

Liability policies also commonly include broadly worded exclusions barring coverage for any loss arising from "war" or "terrorism." Many cyber attacks may have direct or indirect ties to terrorism. This is particularly true in the oil and gas sector, where certain industry participants are state-sponsored and often targeted by extremists. Companies should attempt to exempt cyber terrorism from these exclusions through negotiations with their insurers at the time of program renewal.

Another common exclusion is "liability assumed by contract," which bars coverage for fees, indemnification or other costs that the policyholder is obligated to pay due to a contract. One federal district court case rejected a policyholder's attempt to recover fees paid following a 2013 breach in which hackers obtained and posted on the Internet 60,000 credit card numbers belonging to the policyholder's customers. The court held that the fees, which were imposed by the bank under its servicing agreement with the policyholder, were excludable under the policy's contractual liability exclusion. The court reached this conclusion notwithstanding evidence that the policyholder had expected coverage for such fees.

Insurance policies typically exclude coverage for "criminal" or "dishonest" acts of employees. Many cybercrimes involve the bad acts of former employees or independent contractors no longer employed by the company, but who still can disrupt computer systems. Businesses should seek amendments to these exclusions so that criminal acts of former employees are covered.

Another factor to consider is coverage triggers. Viruses, ransomware and other malicious code may lie dormant in a company's systems for years before they are discovered. Even when breaches are discovered, companies may not understand the scope or impact of the loss for some time. As a result, "occurrence-based" policies, which traditionally apply only where a covered incident "occurs" during the policy period, should be amended to ensure they cover data breaches discovered during the policy period, rather than only those that took place during the policy period. Where the coverage is under a claims-made policy, it is important to ensure retroactive dates and other time-based exclusions will not exclude coverage once an intrusion or damage is discovered.

Finally, many cyber insurance forms provide coverage for fraudulent or wrongful acts by hackers who "directly" cause the loss at issue. Insurers in many cases have argued that this direct causation requirement bars coverage because the wrongful conduct (e.g., spoofed e-mails, fraudulent communications with employees) was only an "incidental" part of the scheme. Direct causation language should not be fatal to most claims, but policyholders should negotiate more favorable insuring agreements that address this potential insurer defense.

**Best Practices**

In addition to addressing these specific coverage provisions, oil and gas companies should conduct detailed risk analysis at the time of traditional and cyber insurance policy placement or renewal. Insurance analysis often focuses on claim analysis in light of policy terms, but the insurance application and renewal process also is an important step in addressing a company's specific risks to maximize potential insurance recoveries in the event of a loss or claim.

There are specific best practices oil and gas companies should follow for insurance placement and renewal applications. First, critical personnel need to be involved in the process to ensure the business is submitting the most accurate information from employees most likely to have knowledge of the relevant facts, especially with respect to information technology, computer systems and prior cyber events.

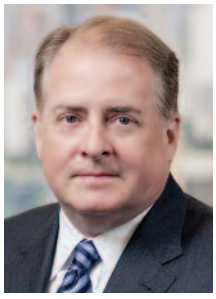
Prior applications should be reviewed at renewal to identify any key changes or areas to supplement, and to ensure that the company follows through with implementing procedures and risk controls identified in an insurance application. Questions should be answered fully whenever possible, but companies also should not be afraid to qualify answers when necessary. For example, it is prudent to be wary of responding to questions about existing cyber events because such events could go undiscovered for months or even years.

The impact of breaches involving critical suppliers or infrastructure also needs to be considered. The oil and gas industry relies on various links in the supply chain to ensure products are obtained, transported, delivered, and consumed as efficiently and safely as possible. The success of oil and gas companies is intertwined with the operations and viability of other related entities. For that reason, companies should consider whether additional coverage extensions or endorsements, such as dependent service provider or contingent business interruption coverage, are needed.

Not all cyber insurance forms are created equal, making it paramount to ensure cyber coverage addresses current risks. Recent cyber coverage decisions have demonstrated that seemingly basic cyber losses may not be covered under an insurance policy based on the policyholder's type of business, the type of claim, or the specific computer systems, databases, or network at issue. Do not stop thinking about insurance after policies are in place, as significant obligations

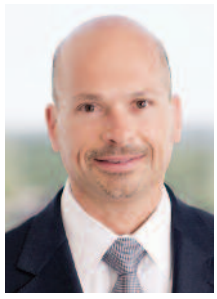
or revisions may be necessary to maintain adequate coverage following a change in control, a change in the scope of services or work performed, the introduction of new cyber risks, or the implementation of new contracts or additional insureds.

An insurance policy is a specialized contract. Like any other contract, a policy can be negotiated and amended to address specific risks and concerns of the policyholder. Experienced insurance brokers and coverage counsel can help policyholders identify and negotiate appropriate policy endorsements to address those risks and concerns, and aggressively protect a policyholder's rights to maximize recovery in the event of a claim. ❐

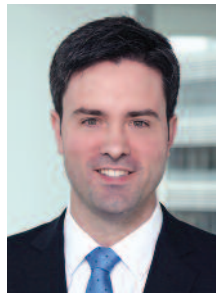
**LAWRENCE J. BRACKEN II**

*Lawrence Bracken is a partner in the Atlanta office of Hunton & Williams LLP, where he is a member of the firm's commercial litigation and insurance coverage practices. He has represented oil and gas industry clients in litigation and insurance coverage matters for more than 30 years.*



**MICHAEL S. LEVINE**

*Michael Levine is a partner in the Washington, D.C., office of Hunton & Williams LLP, where he is a member of the firm's insurance coverage practice. He regularly advises and represents clients in the oil and gas industry.*



**GEOFFREY B. FEHLING**

*Geoffrey Fehling is an associate in the Washington, D.C., office of Hunton & Williams LLP, where he is a member of the firm's insurance coverage and commercial litigation practices. Fehling represents clients in insurance coverage disputes involving a variety of cyber, environmental and other liability and property claims.*