CYBER LIABILITY IN THE ENERGY SPACE: CRITICAL COVERAGE FOR CRITICAL ASSETS

CONTACT

To learn more about how AmWINS can help you place coverage for your clients, reach out to your local AmWINS broker.

LEGAL DISCLAIMER

Views expressed here do not constitute legal advice. The information contained herein is for general guidance of matter only and not for the purpose of providing legal advice. Discussion of insurance policy language is descriptive only. Every policy has different policy language. Coverage afforded under any insurance policy issued is subject to individual policy terms and conditions. Please refer to your policy for the actual language.

ABOUT THE AUTHOR

This article was authored by Megan North, a Professional Lines broker with AmWINS Brokerage of Texas in Dallas and a member of AmWINS' national professional lines practice,

In 2018, companies within the energy sector, from suppliers to producers, rely heavily on operational technology to perform daily operations. Internet-connected networks and systems for activities such as pipeline management, workflow automation, real-time monitoring of equipment, reservoir modeling, use of electronic data interchange (EDI), and many other activities utilize connected networks and software in order to optimize efficiencies, save money, and ultimately, increase profits. With this increased connectivity comes increased cyber risk. Despite this fact, nearly 65 percent of respondents in the Ponemon Institute's 2017 study rated their operational technology response readiness as less than "high."

The energy sector has experienced numerous cyber-attacks. Significant security breaches include:

- 2013 – The United States Department of Energy disclosed two separate breaches of their network.Attic ventilation openings
- 2015 – The United States Industrial Control Systems Cyber Emergency Response Team issued an advisory for a vulnerability found in a widely used, small-scale turbine for homes or farms.
- 2016 – A Vermont utility company serving less than 20,000 households found Russian malware on one of its computers. The motive was unclear.
- 2017 – The "Wannacry" ransomware hit numerous energy companies, crippling their networks.
- 2018 – The United States Department of Homeland Security issued a warning concerning Russian hackers targeting U.S.-based energy companies.

While it's clear that the threat is persistent and that preparedness is minimal, the number of energy-related companies purchasing Cyber Liability coverage is lower than it should be compared to other industries. If the coverage isn't purchased, it cannot respond, and companies will be left to fend for themselves in the event of a network security or privacy breach incident.

HOW CAN A STAND-ALONE CYBER LIABILITY POLICY ADD VALUE TO YOUR COVERAGE OFFERING FOR ENERGY RISKS?

- **Comprehensive Coverage** – Cyber insurers are highly adept at comprehensively underwriting industry-specific risks, as well as providing highly valuable resources to assist insureds before, after and throughout a cyber event.
- **Limit Capacity** – Even if some limited Cyber coverage is purchased in a multiline package policy, small sublimits are not enough. Having dedicated coverage built to respond to cyber losses preserves policy limits for each type of risk. In some cyber forms, breach response expenses are outside the policy limit, which also helps preserve limits.

(continued on next page)

(continued from previous page)

- **Regulatory** – The energy sector produces critical resources. As such, it is not only a heightened target for threat actors, but also for regulators. State-specific privacy laws are enforced by state attorney generals, who can investigate and levy fines and penalties. Federal bodies, such as the Department of Homeland Security, monitor the cyber threat activity surrounding the energy sector. A Cyber Liability policy can provide coverage for fines and penalties – where insurable – as well as for costs associated with regulatory investigations.

- **Response and Pre-Emptive Resources** – Stand-alone Cyber policies generally include cyber security risk management packages that may feature web-based learning platforms, legal white papers on security matters, discounted rates with IT security vendors, network penetration testing, table-top breach exercises, assistance with incident response plans and, in some cases, real-time network security monitoring.

CURRENT AND FUTURE CLAIM TRENDS

Emerging trends in the network security world are increasing the need for energy and energy-related companies to consider purchasing Cyber Liability coverage.

1. **Unintentional or Negligent Insider Threats** – Recent reports are showing threats from insiders are growing. Bad actors are exploiting internal users in an effort to gain access to networks by exploiting misconfigured servers, as well as Man-in-the-Middle (MitM) and phishing attacks.

   The IBM X-Force Threat Intelligence Index 2018 report indicates that clients in the education, energy, and financial services sectors experienced a "notably higher percentage" of insider threat activity. They noted a higher than average volume of targeted phishing emails as one potential cause.

   Furthermore, 65 percent of respondents in a recent Ponemon Study said that the top cyber security threat is the negligent or careless insider.

2. **Nation State and Political Threats** – Black hats or bad actors' most common motivations are financial gain. With the global political climate in a heightened state of unrest, however, more and more "hacktivist" activities are targeting critical assets – such as energy and/or manufacturing – to bring awareness to a cause or hinder the production and operations of a perceived enemy state (and domestic companies). As a result of such attacks, energy firms have recently experienced, and will likely continue to see, business interruption losses. These interruptions cause not only loss of revenues, but also a host of other liability issues for those that depend on their products.

3. **Contingent Bodily Injury and Property Damages** – Inherently, the implications of a network security incident for an energy firm go beyond traditional financial loss. A hijacked pipeline management or industrial control system could easily lead to widespread issues involving threat to human life and property alike. Generally, most Cyber policies exclude coverage for claims arising or relating to bodily injury or property damage; however, there appears to be a shift in the market as carriers consider a provision of this coverage. Some carriers can also provide contingent Pollution coverage as a result of a network security incident. Energy buyers should always ask about – and coordinate coverage between – Cyber, General Liability and Pollution. The peril of flood will usually have a higher deductible than other perils on the policy.

4. **Supply Chain Vulnerabilities** – Companies within the energy sector rely heavily on certain supply chains. Upstream, midstream, and downstream companies in the oil and gas sector, for example, all experience some reliance on suppliers and other vendors. Often, these vendors pose a cyber security threat even in the absence of unscrupulous motives. With access to a company's network, negligent or insufficient security protocols used by a vendor can allow threat actors to access the network via the vendor's system and wreak havoc. Per the 2017 Ponemon Oil & Gas Cyber Security Preparedness study, 69 percent of respondents believe their organization is at risk because of uncertainty about the cybersecurity practices of third parties in the supply chain. Furthermore, 61 percent say their organization has difficulty in mitigating cyber risks across the oil and gas value chain. Vendor access will continue to be an issue given that even the best prevention measures cannot stop all threats.

(continued on next page)

(continued from previous page)

INSURANCE SOLUTIONS FOR CYBER THREATS TO ENERGY COMPANIES

Energy companies should utilize table-top exercises with their leadership teams, risk managers, IT leaders and others to create a game plan for every possible cyber threat. Nevertheless, we know that some attacks will still be successful. Here are some examples of threats and possible insurance solutions.

THREAT	POSSIBLE INSURANCE SOLUTION
Lost revenue from a network interruption arising from ransomware.	Cyber insurance covers the ransom payment if necessary, as well as the forensic investigation to determine the scope of the threat and to shut it down. Insurance pays for business interruption losses and extra expenses to return to full operation.
Network shutdown at a critical third-party vendor reduces or completely stops operations for the named insured.	Cyber insurance with the proper system failure insurance wording covers business interruption losses and extra expenses until the vendor recovers or coverage period runs out.
Hackers enter the network and turn off safety measures, leading to a massive pollution event.	A Pollution policy without a network security exclusion would have primary responsibility for assisting with clean-up expenses. A Cyber policy with proper pollution exclusion amendments assists with IT forensics, regulatory investigations, and possibly, business interruptions.
Cyber thieves spoof the corporate controller into wiring $500,000 to a fictitious vendor account.	Crime insurance assists with repayment of unrecoverable funds. Cyber insurance assists with the forensic investigation to ensure that the client's computer network hasn't been compromised. A Cyber policy may have a sublimit for cybercrime, as well.
Hackers enter the client network and exfiltrate thousands of personal health and financial records of current and former employees.	Cyber insurance helps with legal and IT forensics, notification and public relations expenses, regulatory investigations, establishment of call centers, credit and identity monitoring, fraud resolution and more.

As threats continually evolve, it is virtually impossible to adequately prepare for every type of cyber-attack; however, appropriate coverage can play a key role in mitigating risk. As a result, brokers are advised to ask their clients numerous and detailed questions regarding their threats, in order to assist brokers and underwriters in effectively matching risks with insurance solutions.