Top 3 Trends Affecting Cyber Risk and Insurance in the Energy Sector

The beauty of the cyber insurance market is that it is evolutionary by nature – offering solutions to an ever-changing risk profile and strategy from threat actors. This article highlights cyber trends affecting the energy sector, helping identify current risks and market conditions so you can determine the best coverage solution for your client.

State of the Cyber Insurance Market

Before diving into the energy sector specifically, it's important to understand the current state of the cyber insurance market as a whole. Loss ratios are running high as a result of increased frequency and severity of claims – largely driven by ransomware, as well as traditional losses from failures of network security or privacy.

Since the loss ratio is the result of premiums collected vs. losses paid, this is a measurement that many insurers cannot afford to ignore. Combined ratios for some of the major players within the cyber insurance market are creeping closer to one – and over one in some cases. This means for every dollar of premium collected, there is close to one (and/or potentially more than one) dollar leaving the company in the form of claims payments or expenses.

Under these constraints, there is a need among carriers to correct the trend. Unfortunately, insureds tend to feel these measures most acutely. Though cyber insurance losses generally have a shorter tail in comparison to the rest of the market, there has been a significant uptick in not only purchasing cyber coverage, but also the limits purchased. Therefore, carriers are taking on more risk, while underwriting more profitably.

This correction to profitability has been seen through four key changes:

(1) **Rate increases** are material and widespread – historically low rates are no longer generating appropriate protection of capacity.
(2) **Decreased capacity** on any one type of risk to limit aggregation and increase the spread of risk has resulted in less limit for more rate for individual insureds.
(3) **Increased retentions** which shift onus onto insureds to keep adequate protections in place and contribute more financially in the event of a claim.
(4) **Strict underwriting guidelines** have been implemented around certain base-level network security controls, such as multi-factor authentication, endpoint decryption, segregated backups and business continuity plans, as well as limitations of coverage terms and conditions for higher hazard exposures or those with inadequate controls.

Top 3 Cyber Trends Facing the Energy Sector

1. Vendor and Supply Chain Risk

Summary

From production to the pump, there are an infinite number of connected enterprises, each operating with the same goal of delivering fuel (gas or oil) to the end consumer and user. If one of the entities along the supply chain is compromised or suffers a cyber incident which reduces their ability to complete the chain, the effective backlog would be substantial.

CONTACT

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

The cyber security community is also taking note of this vendor/supply chain risk – for good reason. According to recent research from the cybersecurity firm BlueVoyant, only 22.5% of organizations monitor their entire supply chain while 32% percent reassess and report their vendor's cyber risk position on a bi-annual or annual basis. The report also indicates that over 80% of breaches reported result from a weakness in their supply chain and/or third-party vendor systems.

Claim Example

It's estimated there were roughly 135-140 oil refineries operating in the U.S. in 2019. If a refinery in the U.S. were hit with a ransomware attack, the company may have to take their networks offline for three days in order to restore systems from backup and/or pay the ransom. For purposes of this example, we will assume an output of 75,000 barrels produced per day and oil trading around $60 per barrel. The loss would be in excess of $13.5M in total, or roughly $4.5M daily.

The subsequent impact to the refinery's partners should also be taken into consideration – transportation, distribution and stations offering fuel to consumers.

Solution

Most cyber policies now offer business interruption coverage for loss of earnings and extra expense as a result of a cyber-attack. These generally include a waiting period which acts similarly to a time retention, with market standard being 8-10 hours (though some carriers offer even further reduced options).

Additionally, this coverage can be extended to include cover for "contingent" business interruption. In other words, if a supplier or vendor on which the insured depends to operate their business suffers a cyber incident which then affects the insured's business, there could exist first-party cover under the cyber policy.

2. Targeted Attacks / Hacktivism

Summary

Coming off a particularly heated election year, there is a renewed focus on environmentally conscious operations and more pressure on fossil fuels. This is now beginning to extend beyond political candidates and opinions to materially affect the insurance market and threats to fossil fuel companies.

In late 2019, at least three major insurers announced changes to their corporate strategy in respects to coal mining organizations. These changes ranged from commitments to discontinue providing insurance to such organizations to reducing investment in these and other similarly classified businesses.

While the insurance industry is not yet focusing on oil and gas in such a way, it's understandable that the volatility surrounding the environmental impact of production and related activities has increased the risk of cyber incidents. Threat actors have proven repeatedly they can cause significant damage to companies they perceive as threatening or not in alignment with their agendas – from a political, social, nation state or otherwise.

Claim Example

A hacktivist group launches a large-scale distributed denial-of-service (DDoS) attack against a production and exploration company's website. They also launch social media campaigns and digital defacement of the company causing reputational harm and a subsequently loss in profit due to the event.

Solution

Many cyber policies offer reputational harm cover as an enhancement over the base coverage form. The extent of this cover can range from public relations costs to the addition of coverage for lost income. Depending on the extent of the event, there are also additional first-party coverages available, including business interruption and breach response costs which may assist with the response and recovery.

3. Bodily Injury / Property Damage

Summary

Cyber policies were initially designed to cover only financial damages as a result of a cyber incident. As the risk has evolved, so have the damages and types of loss that can result. At the same time, society has become more technologically dependent as have the businesses which drive our economy and daily lives.

Oil and gas companies are no different. From industrial control systems at refineries to EMV compliance requirements at retail gas stations, and everything midstream and beyond, technological dependence is only increasing. This shift has increased productivity, efficiency and creativity, but also increased risk.

Claim Example

Modern gas pumps have monitoring systems or automatic tank-gauging (ATG) systems. These internet-connected systems are used to track certain metrics such as fuel levels and temperature. If these systems are infiltrated by a threat actor, many issues could occur. Assume the hacker changes the tank overflow settings to an amount beyond its capabilities, this could lead to spillage, lost profits or worse – an explosion which would cause devastating damages to people and property.

Solution

Most cyber policies include a specific exclusion for loss arising out of bodily damage or property damage due to a cyber incident. If this coverage is amended and endorsed, it's generally limited to a small sublimit which could easily be eroded by the above example.

Most people think of a general liability policy to respond to bodily injury losses – which it is designed to do. However, more insurance carriers are facing regulatory pressures to provide affirmative (or exclusionary) language around losses arising from a cyber incident. These exclusions are becoming mainstream and are anticipated to continue to permeate the insurance offerings we see moving forward.

So, if cyber policies exclude the type of loss (bodily injury or property damage) and property and casualty policies cover that type of loss but exclude the trigger (as a result of a cyber incident), where can insureds find cover?

This conundrum is called silent cyber. Affirmative cover is elusive, but it is available via certain niche cyber insurance products – most notably, Amwins' exclusive cyber umbrella policy, CyberUP.

Summary

Despite challenging market conditions in the energy sector, and specific risks facing firms within the oil and gas space, it's imperative to note the industry's growth in remote control and access to network systems. This shift has increased productivity, efficiency and creativity, but has also exponentially increased the attack surface and potential vulnerabilities in the vendor/supply chain – from production to the pump. At the same time, the industry is facing renewed focus on environmental consciousness, mounting pressure on fossil fuels and the threat of silent cyber exposure.

The first line of defense must begin internally with people, followed by processes and systems. There must be an acute focus from the board-level down to the employee body on cyber security and awareness. To complement this effort, a robust cyber insurance program can provide added peace of mind as well as additional services to bolster the security posture.

Because all cyber policies are **not** created equal, and written in complex language, it's important to work with a specialized insurance broker who not only has access to the appropriate markets, but is knowledgeable of the nuances of each available coverage offering.

Amwins has specialists dedicated to placing cyber coverage for risks across the globe. We have the expertise, resources and insurance products to help retailers protect their clients from a myriad of evolving cyber risks.

About the Author

This article was written by Megan North, Vice President and Cyber specialist with Amwins Brokerage in Seattle, WA.