Stephens Insurance, LLC

bms.

Cyber Insurance as a Risk Management Tool in the Oil & Gas Industry

The current view of cyber insurance as a viable risk transfer tool for Oil & Gas companies is reflected in the relatively low take-up of meaningful cyber insurance limits purchased across the industry. According to an assessment from credit rating agency Moody's[1], only half of sector firms carry cyber insurance, well below the corporate average of 80%.

The hesitation to embrace cyber insurance seems to mirror the electric and gas utility industry's view of cyber risk management from 10-12 years ago. At that time, there was a common industry belief that cyber insurance only addressed data privacy and data breaches, while the industry's true concern centered on the operational exposure to a cyber event and the potentially catastrophic impact it could have to operations, balance sheets, customers, and shareholders.

It was at this point in the evolution of cyber insurance that a small number of specialized insurance brokers and insurance carriers or syndicates began to craft solutions tailored specifically to the exposures faced by the broader utility industry. Coverage provisions such as failure to supply liability, spot market power extra expense, voluntary shutdown, system failure triggers for business interruption and contingent business interruption, and specific industrial control systems (ICS), SCADA, and other operational technology (OT) provisions were incorporated into highly manuscript policies. This tailored approach resulted in a decade which has seen the majority of Electric & Gas Utilities begin to purchase meaningful cyber insurance limits ($50M+) as part of their overall risk management programs.

Oil & Gas companies face increasing cyber threats that cannot be fully mitigated through technology alone. Cyber insurance provides financial protection and an injection of capital against operational disruptions, ransom demands, and regulatory penalties that are lawfully insurable. A comprehensive risk management approach that combines cybersecurity measures with insurance ensures resilience against evolving threats.

Evolving Threat Landscape and ICS Malware

Attacks targeting OT, especially those carried out with an intention to cause physical disruption, are much rarer than those targeting IT systems. That said, the Oil & Gas sector is a lucrative target for cybercriminals due to the money involved, especially for ransomware groups who understand the cost of downtime to such companies[2].

ICS vendor Waterfall Security Solutions identified 68 cyber-attacks in 2024 which caused physical consequences to OT – a significant increase over the previous year, though still less than the estimated thousands of cyber-attacks per day targeting IT systems.[3]

Furthermore, Oil & Gas was among the top four industries targeted by ransomware in 2024[4], with 44 reported attacks, and threat actors refining ICS-specific malware:

- Nation-state actors are investing in ICS-specific malware (e.g., ELECTRUM, KAMACITE)
- Cybercriminals and hacktivists lowering the barrier for OT attacks
- ICS malware becoming more accessible through repurposed tools

Notably, the PIPEDREAM malware discovered by Dragos in 2022 remains a significant concern. Designed to target industrial controllers in Oil & Gas infrastructure, the malware's capabilities include:

- Disabling safety controllers
- Manipulating PLCs
- Disrupting SCADA and control systems
- Bypassing network security measures

Attack Surface and Exposure

While many buyers in the past considered cyber insurance to be primarily a liability product (associated with the confidentiality and integrity of data), today's cyber insurance has evolved into a first- and third-party product tailored to address the unique exposures and operations of specific sectors. The Oil & Gas industry relies on E&P, midstream, contract services, and transportation companies to keep operations running, but these critical sectors face significant cyber threats that can disrupt supply chains and impact the global economy.

Remote Operations and Access: Increasing reliance on remote operations and IoT devices in the drive for efficiency and real-time monitoring have introduced new cybersecurity challenges to the Oil & Gas industry. The use of remote access technologies increases the overall attack surface, creating potential entry points for threat actors to gain unauthorized access and the deployment of malware.

ICS Vulnerabilities: Vulnerabilities in ICS can have catastrophic consequences when misused, including equipment damage, environmental hazards, and even loss of life.

Supply Chain Risks: The interconnected nature of the Oil & Gas industry introduces weaknesses through third-party vendors and suppliers. A compromised supply chain can result in the

introduction of malicious software or ransomware, leading to potential security breaches, unauthorized access to critical systems, data exfiltration, and potential disruption of operations.

Insider Threats: Disgruntled employees, contractors, or others who have been granted prior authorized access can intentionally or unintentionally compromise critical systems and sensitive data.

Joint Venture Vulnerabilities: An often-overlooked exposure across the industry is that introduced through joint ventures. Collaborative networks, shared resources, shared IT and OT systems, and joint operational data create potentially critical system weaknesses. Lack of proper network segmentation and security controls between joint venture partners can lead to unauthorized access to sensitive data, potential disruption of joint operations, and increased risk of cyber-attacks through partner networks.

Cyber Events Impacting Oil & Gas Companies

Ransomware attacks have become a significant threat to the industry. High-profile incidents demonstrate that even with sophisticated cybersecurity measures, adversaries can and will continue to successfully breach systems:

- **Sector 16 and Z-Pentest Attack on Texas SCADA System (2025):** Russian hacktivists gained unauthorized access to a U.S. Oil & Gas facility.
- **Halliburton (2024):** An oilfield services company experienced a cyber attack and the exfiltration of sensitive data requiring the organization to proactively take certain IT systems offline to contain the breach, disrupting access to critical business applications.
- **Suncor Energy Cyber Attack (2023):** Disrupted payment systems, resulting in millions of dollars in losses.
- **Amsterdam-Rotterdam-Antwerp Storage Terminals (2022):** Malware was deployed onto the automation systems that control the scheduling and execution of fuel transfers between storage tanks, pipelines, and transport vehicles, disrupting key terminal management systems.
- **Colonial Pipeline Attack (2021):** Led to widespread fuel shortages and a ransom payment of $4.4 million.
- **ExxonMobil Ryuk Ransomware Attack (2019):** Disrupted refining operations.
- **Triconex Controller Attack at Saudi Aramco (2017):** Targeted safety controllers, highlighting industrial vulnerabilities.

The energy industry as a whole is generally known to be particularly vulnerable to third-party attacks, and 67% of energy sector breaches are linked to initial infections through software and IT vendors, rather than the target themselves.[5] Energy companies often have large attack surfaces, which are only growing as more companies utilize internet-connected devices.[2] According to the 2025 Dragos' Year In Review report, 65% of sites assessed had insecure remote access conditions, which is particularly concerning for offshore Oil & Gas operations that rely heavily on remote connections.[4]

Cyber Insurance – Coverage Gaps and Solutions

When cyber exclusions are applied to property policies, there are gaps created in coverage related to resultant physical damage and business interruption loss, meaning that organizations are no longer protected if there is a physical loss or damage arising out of the use of computers or data. The extent to which these gaps exist is dependent on the language of the cyber exclusions applied and can range between absolute exclusions, which take out coverage for anything related to the use of computers or data (directly or indirectly), to exclusions that try to delineate between malicious cyber events and non-malicious or accidental events.

In every case, these cyber exclusions take away certainty of coverage for organizations, and an affirmative insurance policy covering physical damage loss and business interruption caused by cyber events (accidental or malicious) should be considered for risk transfer. The availability of cyber physical damage insurance policies for malicious events is prevalent. However, it remains unclear whether accidental events that cause physical damage should be covered by the property market or the cyber insurance market, with the former currently taking the majority of that exposure given that cyber events are considered fortuitous in nature similar to other physical perils, such as fire, explosion, wind etc.

Cyber property damage can be obtained in either the property market or the stand-alone cyber market with varying degrees of coverage clarity and certainty.

	Cyber Market		**P&C Market**
	Affirmative Cyber PD	**Buy-Back Cyber PD**	**Cyber Exclusion** *(with certain carvebacks)*
Overview	Ground up primary policy that responds to property damage arising from a malicious cyber attack.	Buy-back policy that wraps exclusionary language and responds to the % of loss not covered within the property policy, arising from a malicious cyber attack.	Ground up primary policy for any property damage, however losses arising from a malicious cyber attack are typically excluded.
Coverage	First party property damage, debris removal and ensuing business interruption only.	Mirrors first party property damage and extensions of the property policy being wrapped.	First party property damage and extensions per property policy.
Trigger	Malicious cyber attack e.g. 'cyber act.' No coverage for non-malicious events e.g. 'cyber incident.'	Malicious cyber attack e.g. 'cyber act. No coverage for non-malicious events e.g. 'cyber incident.'	Malicious cyber attack e.g. 'cyber act' excluded. Some coverage provided for non-malicious events e.g. 'cyber incident.'
Limits	Dedicated limit for a malicious cyber attack resulting in damage to first party property.**	Dedicated limit for a malicious cyber attack resulting in damage to first party property and other extensions contained within the property policy.**	Policy limit could be unaggregated or an aggregate limit could apply for certain perils contained within property policy.

Underwriting Requirements	TIV's & Cyber Application.	TIV's & Cyber Application.	Typical property underwriting submission.
Pros	• Ring-fenced limit for cyber property damage • Single claims contact and handling in event of a loss • Pricing credits if purchased in tandem with non-damage cyber from same insurer.	• Terms and conditions align with coverage contained in property policy • Pricing typically cheaper than a standalone cyber property damage tower.	• Typically offered for free.
Cons	• Policy language may not align directly with language contained within the property policy.	• Claim must work through property policy and be excluded before buy-back coverage responds, which may take additional time in obtaining recovery.	• Very little cyber-related coverage typically provided, leaving large gaps in coverage and inclusive of often onerous cyber exclusions.

**LMA cyber exclusions exclude 'cyber act' and carveback certain perils arising from a 'cyber incident' depending on the exclusionary language used.*

***Sometimes cyber property damage limits are aggregated with non-damage cyber limits if purchased under the same policy with the same insurers.*

Sources

1 https://www.govinfosecurity.com/oil-gas-firms-aware-cyber-risks-a-26525

2 XCyber, *Oil and Gas Cyber Threat Landscape* (February 26, 2025)

3 https://waterfall-security.com/wp-content/uploads/2024/04/2024-Threat-Report.pdf

4 Dragos, Inc., *2025 OT/ICS Cybersecurity Year in Review: 8th Annual Report* (Hanover, MD: Dragos, 2025), https://www.dragos.com/)

5 https://securityscorecard.com/company/press/67-of-energy-sector-breaches-linked-to-software-and-it-vendors-securityscorecard-reports/

Authors

Mark Green
Senior Vice President
Cyber Practice Leader
Stephens Insurance

Mark Alvarez
Senior Vice President
Cyber Practice Leader
Stephens Insurance

Daniel Leahy
LLB Hons ACII
Cyber Practice Leader
BMS

Monica Tigleanu
CISSP, GICSP
Cyber Strategy Director
BMS