Stephens Insurance, LLC

bms.

Cyber Insurance in the Oil & Gas Industry

Evolving cyber threats facing Oil & Gas companies require a comprehensive risk management approach that combines cybersecurity measures with insurance to offer financial protection against operational disruptions, ransom demands, and regulatory penalties.

Common O&G Cyber Vulnerabilities

Remote Operations & Access create additional entry points for unauthorized access

Supply Chain Risks occur with only one "weak link" in your vendor network

Insider Threats can take the shape of disgruntled employees, former contractors or those with unauthorized access

Joint Ventures often lack proper network segmentation and security controls

Attacks on the Rise

68

cyber attacks in 2024 caused some form of physical damage to industrial control systems

Major Attacks

- Sector 16 and Z-Pentest Attack (2025)
- Pipedream (2023)
- Colonial Pipeline (2021)
- Triconex Controller Attack Saudi Aramco (2017)

Benefits of Cyber Insurance

- **Recovery for severe financial losses** attributed to physical damage or nonphysical damage including affirmative coverage for Business Interruption
- Incident response and management of public relations following a cyber event which helps to limit liability
- Manage risk tolerance levels and the threat of severe damages arising from malicious threat actors as well as operational, unplanned outages