Specialist Cyber Protection:
For Oil & Gas Firms

The Key Exposures Facing Oil & Gas Firms

Attractive to Cybercriminals
The energy industry is critical to modern economies, making oil and gas companies attractive targets for cybercriminals. Further, the oil and gas sector may be leveraged during geopolitical conflict by attackers motivated by political, economic, or strategic interests.

Operational Disruptions
Increased reliance on technology leaves oil and gas companies vulnerable to operational disruptions that not only cause significant revenue losses but have the potential to tarnish reputation.

Aging Infrastructure
Updates to equipment can be costly and time consuming. Legacy systems pose significant cybersecurity risk as software updates and patches have become more essential. Without the appropriate investment in updated infrastructure, systems are increasingly susceptible to exploits and attacks.

Guidance and Standards
The publicity and awareness surrounding recent cyber-attacks penetrating oil and gas companies have brought increased scrutiny to the industry. To help protect the industry from these events, enhanced guidance may develop around critical infrastructure.

How Our Specialist Coverages Respond To The Threats

01 Broad definition of Dependent Business as a third-party entity that provides necessary products and services to the Insured Organisation pursuant to a written contract, including supply chain-related interruptions.

02 Incorporates a qualifying period approach to business interruption coverage instead of a waiting period.

03 Computer system definition includes technology such as Industrial Control Systems (ICS), Programmable Logic Controllers (PLCs) and Supervisory Control and Data Acquisition (SCADA).

04 Third party liability coverage for bodily injury claims arising from cyber incidents, available up to $250,000 sublimit.

05 Coverage for BYOD (bring your own device), as many on-site workers utilize their own mobile phones.

06 Third party liability for failure to supply coverage arising out of cyber incidents.

beazley

Reducing Risk:
Cybersecurity Advice For Oil & Gas Firms

01 **Multi-Factor Authentication.**
Implement two-factor authentication for all remote access, web-based email access, and for administrator access to key resources. Provide remote access only through secure channels and require strong passwords.

02 **Securing Operational Technology (OT).**
Create separate user credentials for the OT environment and require MFA for remote access. Develop a plan for end-of-life assets and annually assess the capability of security tools.

03 **Endpoint Protection (EPP) solution and Endpoint Detection and Response (EDR).**
Deploy an EPP/EDR solution across enterprise assets, including operational technology, to detect and block common viruses with advanced capabilities of active monitoring.

04 **Security Operation Center (SOC).**
Leverage an in-house or third-party managed SOC to monitor the entire enterprise, inclusive of operational technology.

05 **Email Security.**
Properly configuring spam filters, investing in antivirus protection, and adding multi-factor authentication can help employees avoid business email compromises, fraudulent instruction losses, and other cyber claims

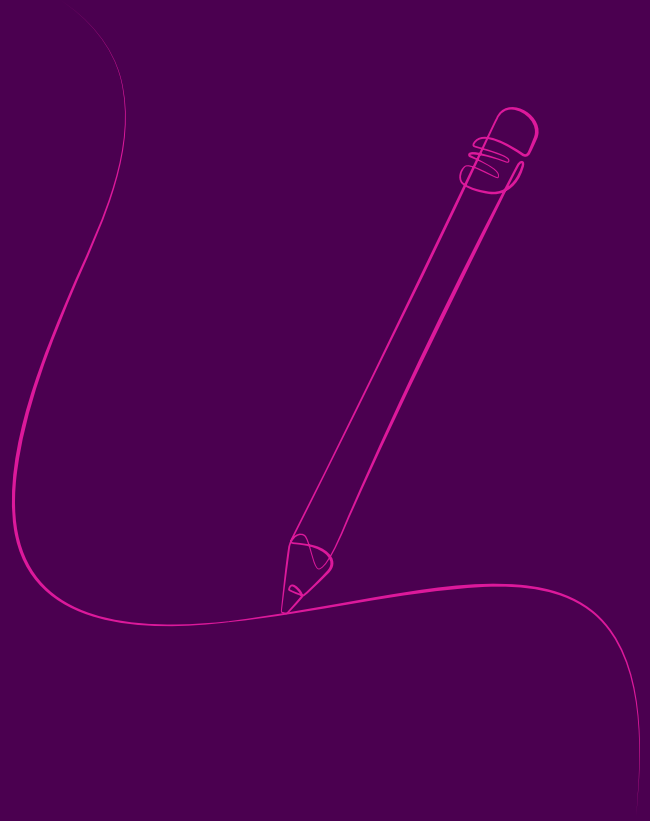
06 **Backups.**
Develop and test backup and recovery plans; keep copies of sensitive or proprietary data in a separate and secure location. Test back-ups regularly to ensure both the technology, and the people, can function during a crisis.

07 **Antivirus and Patching.**
Maintain updated antivirus software and configurations. Enforce a patch management process to address ongoing security updates and defend against critical vulnerabilities.

beazley

Claims examples

How our policy supports clients for the duration of the claim



A large oil wholesaler and retail gas station operator suffered a ransomware attack that paralyzed operations.

	How our solution responded
The policyholder immediately contacted their Beazley Cyber Services Manager. Within hours the Cyber Services Manager connected the policyholder to expert service providers to investigate.	**Cyber Services: Incident Helpline**
Digital forensic experts contained the incident and concluded that PII was exfiltrated from the policyholder's environment. Under the guidance of privacy counsel, notification and credit monitoring solutions were utilized to notify over 1,000 employees. A public relations team was also engaged to assist with media communications.	**Cyber Services: Digital forensics, Legal Services, Crisis Communications, Notification**
Widespread encryption rendered the organization inoperable. With the assistance of Cyber Services, a data recovery firm was immediately aligned to aid in restoration efforts. In less than one week, retail operations were restored, and sales resumed.	**First Party Loss: Data Recovery & Business Interruption**
The policyholder was able to restore systems without paying the $4M extortion demand. Beazley reimbursed $3M in business interruption losses and data recovery costs. Service provider fees and notification expenses were paid under the BBR Policy's separate Breach Response Coverage (outside the limit). Therefore, $2M in limit was preserved under the policyholder's $5M limit, in the event of any future claim during the policy period.	**Claims Support**

A large oil company was severely impacted by ransomware event.

	How our solution responded
The policyholder contacted their Beazley Cyber Services Manager, who immediately aligned the services of privacy counsel, digital forensics, and public relations.	**Cyber Services: Incident Helpline**
The investigation concluded that PII was not exfiltrated and, as a result, privacy counsel determined that there were no notification or regulatory reporting obligations.	**Cyber Services: Digital forensics, Legal Services**
Encryption shutdown all systems, including loading/unloading, logistics, retail sales, and tank delivery. To mitigate the mounting business income loss, the Cyber Services Manager quickly arranged for support from a data recovery firm to aid in restoration. Despite these efforts, the organization sustained massive business interruption losses.	**First Party Loss: Business Interruption**
Excellent cooperation between the policyholder and Beazley resulted in the speedy reimbursement of business interruption losses. Within a short period of time, Beazley paid the full $10M policy limit.	**Claims Support**

beazley

Oil & Gas Appetite

Key coverages include:

- **Breach response:** Notifications, Forensics, Public Relations, Legal, Crisis Management
- **First party:** Cyber Extortion, Business Interruption, Dependent Business Interruption, Data Recovery, Extra Expense
- **Third party:** Data and Network Liability, Regulatory Defense and Penalties, Payment Card Liability
- **eCrime:** Fraudulent Instruction, Funds Transfer Fraud, Telephone Fraud