Brown & Brown

PROPERTY & CASUALTY

Protecting Critical Infrastructure from Evolving Cyber Threats

Overview

As digital enhancements continue, power producers and utilities face a rapidly evolving landscape of cyber threats. From ransomware attacks on SCADA systems to regulatory exposure from privacy breaches, a cyber event can cripple operations, interrupt revenue and damage stakeholder trust.

Cyber insurance provides tailored financial protection and response services to help utility operators, independent power producers (IPPs) and renewable developers recover from these incidents and maintain business continuity.

Why It Matters for the Energy Sector

Operational Downtime Is Costly

Every minute of power interruption affects revenue, reliability ratings and customer confidence.

SCADA and ICS Are Vulnerable

Industrial control systems often rely on legacy software not designed for cybersecurity, increasing exposure to attacks.

Regulators Are Watching

Entities like NERC, FERC and regional energy authorities are increasing scrutiny and enforcement around cyber preparedness.

Third-Party Dependency Is Rising

Cloud platforms, grid operators and software vendors introduce new risks, often outside of customers' direct control.

Core Cyber Insurance Coverage

- **Network Security and Privacy Liability:** Protects against liability for failure to prevent unauthorized access, malware spread or breach of confidential data
- **Regulatory Investigation and Fines:** Covers legal defense and fines from cyber-related regulatory actions (e.g., NERC CIP violations, GDPR, CCPA)
- **Business Interruption (BI):** Reimburses lost income and extra expenses when operations are disrupted by a cyber event, including SCADA outages
- **Contingent Business Interruption (CBI):** Extends BI coverage to losses caused by outages at critical third-party vendors or service providers
- **Digital Asset Restoration:** Covers costs to repair or replace corrupted, encrypted or deleted operational data and control system software
- **Ransomware / Cyber Extortion:** Pays ransom (where legal), plus costs for negotiation, system recovery and forensic investigation
- **Incident Response and Breach Costs:** Includes access to legal, IT forensics, crisis communications and notification/ credit monitoring services
- **Social Engineering and Funds Transfer Fraud:** Reimburses financial losses from phishing and deception-based fraud leading to unauthorized wire transfers
- **Media and Content Liability:** Covers exposures from public-facing communications, including websites and digital marketing
- **Operational Technology (OT) / ICS Endorsements:** Optional coverage enhancements to include industrial control systems, often excluded in standard cyber policies

Bespoke Energy Enhancements

- **Pre-Breach Risk Assessments:** Optional services to identify cyber vulnerabilities in SCADA and IT environments
- **Incident Response Panel:** Preferred access to top-tier forensic, legal and public relations firms at pre-negotiated rates
- **Customized Limits and Retentions:** Structured to align with enterprise risk appetite and existing cyber controls
- **Global Applicability:** Coverage can be extended to multinational IPPs and cross-border energy operations
- **War and Terrorism Clarifications:** Structured Negotiated carve-backs to protect against state-sponsored cyberattacks

Recent Energy Cyber Incidents

The following outlines two recent examples of cyber incidents that cyber insurance could help protect against.

Ransomware Attack on U.S. Natural Gas Pipeline Operator (Late 2024)

A major U.S. natural gas pipeline company was targeted in a ransomware attack that began with phishing and escalated through lateral movement into operational technology systems. The incident, attributed to the Base ransomware group, resulted in a temporary shutdown of pipeline operations and caused disruption to the regional gas supply.

Iranian-Linked Espionage Campaign on Middle Eastern Oil Refineries (2024)

In 2024, multiple oil refineries in the Gulf region were targeted in an espionage campaign suspected to be orchestrated by an Iranian APT group. Attackers used credential harvesting and ICS reconnaissance to infiltrate systems. While there was no confirmed physical damage, the incident resulted in significant operational risk and data exfiltration.

Why Brown & Brown Global Energy

We specialize in the energy and renewables sector and understand the unique cyber exposures you face.

Our cyber coverage solutions are:

- Backed by leading cyber carriers
- Tailored for OT/ICS environments
- Supported by benchmarking data and analytics
- Integrated with your broader risk management strategy

Let us help you build a resilient and responsive cyber insurance program that aligns with your operational needs and regulatory landscape.

About Brown & Brown

Growth has no finish line. No matter where you are on your growth journey, we can help you find solutions to meet your ever-evolving insurance and risk management needs. If you are a highly complex multinational company, an individual or anything in between, our experienced teams can help every step of the way.

Brown & Brown

Find Your Solution at BBrown.com