# **Cybersecurity Threats and Issues Facing the Oil and Gas Industry in 2025**

## **1. Executive Summary**

The oil and gas industry forms a cornerstone of the global economy, providing the energy that underpins numerous sectors and daily life 1. However, this critical role also renders it an increasingly attractive target for cyber adversaries. The frequency and sophistication of cyber threats aimed at this sector are escalating, necessitating a proactive and robust approach to cybersecurity 1. This report analyzes the key cybersecurity challenges confronting the oil and gas industry in 2025, drawing upon recent annual cybersecurity reports from leading firms such as Dragos and Nozomi Networks, alongside insights from other reputable sources. The findings highlight the persistent danger of ransomware attacks, the activities of specific threat actor groups with varying motivations, and the common vulnerabilities that these malicious entities seek to exploit 1. This document outlines the structure of the threat landscape, the specific risks posed, and the significant incidents that have occurred, providing a foundation for informed cybersecurity strategies within the oil and gas industry. The insights presented are crucial for understanding the current state of cyber threats and for developing effective mitigation measures to protect critical infrastructure.

## **2. The 2025 Cybersecurity Threat Landscape for the Oil and Gas Industry**

### **2.1 Analysis of Key Findings from 2025 Annual Cybersecurity Reports**

The Dragos 2025 OT Cybersecurity Year in Review underscores a significant rise in ransomware attacks targeting industrial organizations 8. The report identifies new threat groups, notably GRAPHITE and BAUXITE, which are active in the energy sector 5. Furthermore, it highlights the continued operations of VOLTZITE, a threat group with a focus on operational technology (OT) data and the potential to develop disruptive attack capabilities, targeting critical infrastructure including the oil and gas industry 5. The analysis from Dragos emphasizes the increasing focus on OT data, suggesting a trend towards attacks that could directly impact physical processes and safety within oil and gas operations 11.

The Nozomi Networks 2025 OT/IoT Cybersecurity Trends & Insights report indicates that the energy sector, which includes oil and gas, is among the industries most frequently targeted by ICS vulnerabilities 15. This report also points to the prevalence of data manipulation as a common attack technique within energy environments 15. The risks associated with inadequately protected wireless networks in critical infrastructure are also highlighted, as is the ongoing use of brute-force attacks aimed at IoT devices 7.

Insights from other sources corroborate these findings. CrowdStrike's 2025 Global Threat Report emphasizes the emergence of "enterprising adversaries" who employ sophisticated techniques and execute attacks with increasing speed 6. Google's Cybersecurity Forecast 2025 (Mandiant) draws attention to the growing danger of infostealer malware and the potential for AI-powered attacks 16. Silverline Solutions identifies remote access exploitation, ransomware incidents, vulnerabilities in OT systems, phishing attempts, and insider threats as primary cybersecurity concerns for the oil and gas sector in 2025 1, B3, B61. The Business Research Company's report on the global oil and gas security market notes that the market's growth is being driven by the increasing incidence of cybercrime threats 18. The consistent appearance of ransomware and the targeting of the energy sector across multiple independent analyses suggests that these are significant and widespread issues requiring immediate attention. The increasing focus on OT data by threat actors indicates a concerning evolution towards attacks that could have severe physical and operational consequences. The presence of both sophisticated, potentially nation-state aligned groups and hacktivist entities in the threat landscape points to a complex environment with diverse motivations behind cyber intrusions.

### **2.2 Increasing Sophistication and Frequency of Cyberattacks**

The overall trend indicates a rise in cybercrime impacting critical infrastructure 3. Adversaries are employing increasingly advanced techniques, including AI-powered attacks and methods that do not rely on traditional malware 6. A notable development is the perceived lowering of the barrier to entry for those seeking to target OT and ICS environments 11. This suggests that even actors with less advanced capabilities may now view these systems as viable targets for disruption and exploitation. Furthermore, the speed at which attacks are executed is increasing, demanding faster detection and response capabilities from defenders 6. The fact that less sophisticated threat actors are now capable of targeting OT/ICS potentially stems from the availability of more accessible tools and the sharing of knowledge within the cybercriminal community. This implies that the oil and gas industry must prepare for a broader spectrum of attackers, making basic security measures even more critical. The rise in attacks that do not use malware suggests that traditional signature-based security solutions may be less effective in OT environments, necessitating a greater emphasis on behavioral analysis and anomaly detection.

### **2.3 Specific Threats Identified for 2025**

Ransomware remains a significant threat and will be discussed in detail in Section 3. Remote access exploitation is another major concern, with adversaries targeting vulnerabilities in technologies like VPNs and RDPs to gain unauthorized access to OT networks 1, B3, B61. Inadequate security controls for remote access points are a key weakness, emphasizing the importance of implementing multi-factor authentication (MFA) and ensuring that remote access software is regularly updated and patched 19, B31. Supply chain compromises also pose a substantial risk, as attackers increasingly target third-party vendors and suppliers to infiltrate primary targets within the oil and gas sector 1. The interconnected nature of the oil and gas supply chain makes it particularly vulnerable, and maintaining visibility and control over the security practices of third-party vendors presents a significant challenge 1. Other persistent threats include phishing attacks, which can lead to compromised credentials and unauthorized access, and insider threats, whether malicious or unintentional, which can also compromise security 1, B3, B61. The consistent highlighting of remote access exploitation as a major threat underscores the difficulties in securing the geographically dispersed operations of the oil and gas industry, especially with the increasing need for remote work and vendor access to OT systems. The emphasis on supply chain compromises indicates a growing understanding that attackers are targeting less secure entities within the broader ecosystem to reach their ultimate targets, necessitating a comprehensive security approach that extends beyond individual organizations.

## **3. Ransomware: A Persistent Threat to the Oil and Gas Sector**

### **3.1 In-depth Analysis of the Ransomware Threat Landscape in 2025**

The prevalence of ransomware attacks targeting industrial organizations is on the rise 8. Financial gain remains a primary motivation for these attacks, with threat actors seeking large ransom payments in exchange for decrypting compromised systems 1. The use of "quadruple extortion" tactics, which can include encryption, data theft, denial-of-service attacks, and even harassment, is becoming more common, increasing the pressure on victims to pay the ransom 25. The energy sector, including oil and gas, is a particularly attractive target for ransomware due to the potential for significant operational disruption, which can lead to substantial financial losses and even impact critical infrastructure 21. Notably, exploited vulnerabilities are frequently cited as the initial entry point for ransomware attacks within the energy sector, highlighting the importance of effective vulnerability management 21. The emergence of quadruple extortion tactics indicates that ransomware attacks are evolving to become more impactful, requiring organizations to develop more comprehensive incident response plans that address not only data recovery but also potential reputational damage and operational downtime. The fact that exploited vulnerabilities are a major pathway for ransomware underscores the critical need for robust vulnerability management programs within the oil and gas industry, including timely patching and regular security assessments.

### **3.2 Ransomware Variants Known to Target OT/ICS Environments**

While specific ransomware groups are continuously evolving, there have been instances of ransomware potentially targeting the oil and gas sector. For example, the RansomHub group was suspected to be behind the attack on Halliburton 26. The potential for ransomware to cause physical damage to infrastructure is a significant concern in the oil and gas industry, given the critical nature of OT/ICS systems that control physical processes 1. Reports indicate an increasing level of sophistication in ransomware attacks specifically designed to target OT environments, suggesting a growing understanding of industrial control systems by threat actors 19. The development of ransomware variants tailored for OT/ICS demonstrates a concerning trend towards attacks aimed at disrupting physical operations, which can have severe safety and environmental consequences in the oil and gas sector. This necessitates specialized security solutions and expertise in OT cybersecurity, as traditional IT-centric security approaches may not be adequate.

### **3.3 Data on the Financial and Operational Impact of Ransomware Attacks**

The financial costs associated with ransomware attacks in the energy sector can be substantial. The cyberattack on Halliburton in August 2024, suspected to be a ransomware incident, resulted in a reported loss of $35 million 26. Operational disruptions caused by ransomware can also be severe, as demonstrated by the Colonial Pipeline attack in 2021, which led to widespread fuel shortages 4. Such attacks on oil and gas infrastructure can impact production, distribution, and ultimately the availability of essential resources 1. Furthermore, the recovery process for energy and water utilities following ransomware attacks often takes longer compared to other sectors, highlighting the complexity of restoring critical infrastructure 27. The significant financial losses and prolonged recovery times associated with ransomware attacks in the energy sector underscore the critical need for robust business continuity and disaster recovery plans specifically designed for cyber incidents in OT environments. Recovering from an OT ransomware attack can be a complex and time-consuming process, making well-tested recovery procedures essential for minimizing downtime and financial impact.

## **4. Key Threat Actors Targeting the Oil and Gas Industry**

### **4.1 Profiles of Prominent Threat Actor Groups**

Several threat actor groups have been identified as actively targeting the oil and gas industry. **VOLTZITE** is a crucial group to monitor, with a focus on exfiltrating OT data, including GIS data and OT network diagrams, suggesting a potential for developing disruptive capabilities 5. This group shares technical overlaps with Volt Typhoon and primarily targets US-based critical infrastructure, including the electric, oil and gas, water, and government sectors, often using "living off the land" techniques and exploiting vulnerabilities in VPNs and firewalls 11. Their activity is expected to continue targeting US and Western-aligned nations in 2025. **KAMACITE** has shifted its focus to European oil and natural gas (ONG) entities, employing spear-phishing campaigns, such as those leveraging the 2024 Gas Infrastructure Europe (GIE) conference, and deploying custom Windows malware 5. This group has historical links to disruptive ICS attacks. **GRAPHITE** is a newly identified threat group targeting the energy (oil & gas, electric), logistics, and government sectors in Eastern Europe and West Asia 8. With strong technical overlaps with APT28 (a Russia-based group), GRAPHITE focuses on organizations relevant to the military situation in Ukraine and conducts spear-phishing campaigns. **BAUXITE** is another new group implicated in global campaigns targeting industrial entities, including the energy (oil & gas, electric), water, food & beverage, and chemical manufacturing sectors 8. This group shares technical overlaps with the hacktivist persona CyberAv3ngers, which has affiliations with Iran's IRGC-CEC. Finally, **CyberArmyofRussia\_Reborn (CARR)**, a hacktivist group with suspected connections to state-sponsored entities, has launched attacks on industrial facilities, including an oil and gas facility in Texas, demonstrating the ability to manipulate HMI devices 5. The emergence of new threat groups with suspected nation-state ties underscores the increasing geopolitical aspect of cyber threats against critical infrastructure. The connection between state-sponsored groups and hacktivist personas suggests a strategy to potentially obscure the origin and intent of attacks. VOLTZITE's emphasis on reconnaissance and data theft indicates a possible long-term campaign aimed at preparing for future disruptive actions.

### **4.2 Analysis of Motivations, Targeting Patterns, and Known TTPs**

The motivations behind these threat actors vary. Some, like those with suspected nation-state affiliations (GRAPHITE, BAUXITE), may be driven by geopolitical objectives, such as espionage or disruption aligned with national interests. Others, like ransomware groups, are primarily motivated by financial gain. Hacktivist groups like CyberArmyofRussia\_Reborn may have disruptive goals driven by ideological or political agendas. Targeting patterns also differ. VOLTZITE focuses on critical infrastructure in the US and Western-aligned nations, while KAMACITE has recently targeted European oil and gas organizations. GRAPHITE's targets are concentrated in Eastern Europe and West Asia, aligning with geopolitical tensions in the region. BAUXITE's activity has been observed globally across various industrial sectors. Common tactics, techniques, and procedures (TTPs) employed by these actors include spear-phishing campaigns for initial access, exploitation of known vulnerabilities in VPNs and other internet-facing devices, the use of "living off the land" techniques to blend in with normal network activity, data manipulation within OT systems, lateral movement to gain access to critical assets, manipulation of Human Machine Interfaces (HMIs) to disrupt operations, deployment of ransomware and wiper malware for financial extortion or destructive purposes, and supply chain attacks targeting less secure third-party vendors. Some groups, like VOLTZITE, have also been observed compromising SOHO routers to use as part of their attack infrastructure, and others, like those leveraging brute-force attacks, target weak or default credentials on remote access services and IoT devices. The prevalence of spear-phishing highlights the ongoing importance of employee training in mitigating cyber risks. The exploitation of VPN vulnerabilities emphasizes the need for robust patch management.

## **5. Data-Driven Analysis of Cybersecurity Threats and Trends**

### **5.1 Presentation of Data on Targeted Sub-Sectors**

While the provided research snippets do not offer granular data on the specific sub-sectors within the oil and gas industry most frequently targeted in 2025, general trends can be inferred. The focus on OT data and the manipulation of HMIs suggest that the operational aspects of the industry, likely spanning upstream, midstream, and downstream operations, are of significant interest to threat actors 5. The Colonial Pipeline attack, a notable incident from the recent past, targeted midstream operations, highlighting the potential for disruption in transportation and distribution 4. The targeting of European oil and natural gas organizations by KAMACITE indicates a focus on the natural gas supply chain 10. The reasons for these targeting patterns likely stem from the criticality of the infrastructure in each sub-sector and the potential for significant economic and societal impact if operations are disrupted.

### **5.2 Visualization of Trends in Attack Vectors, Initial Access Methods, and Data Types Targeted**

To better understand the cybersecurity threats facing the oil and gas industry in 2025, visualizing key trends is beneficial.

**Graph/Chart Opportunity 1: Attack Vectors:** A bar chart could illustrate the prevalence of different attack vectors based on the analyzed reports. Categories might include ransomware, malware (excluding ransomware), data breaches, denial-of-service attacks, and others. The height of each bar would represent the frequency or impact (if quantifiable) of each attack vector mentioned across the sources. This visualization would clearly show that ransomware remains a dominant threat, but other vectors like data breaches and potentially targeted malware attacks also pose significant risks.

**Graph/Chart Opportunity 2: Initial Access Methods:** A pie chart could depict the common initial access methods used by threat actors. Segments of the pie could represent spear-phishing, exploitation of VPN vulnerabilities, supply chain compromise, brute-force attacks, and others. The size of each segment would correspond to the frequency with which each method is reported as a point of entry. This would likely show that spear-phishing and VPN exploitation are significant initial access vectors, highlighting the need for strong email security and secure remote access protocols.

**Graph/Chart Opportunity 3: Data Types Targeted:** If sufficient data were available across the reports, a bar chart could display the types of data most frequently targeted. Categories might include OT data (control system configurations, operational processes), customer data, financial data, intellectual property (drilling technologies, reservoir data), and personally identifiable information (PII). The height of each bar would indicate the frequency of each data type being targeted. This visualization would underscore the diverse objectives of attackers, ranging from disrupting operations to stealing valuable information.

These visual representations would provide a clear and concise overview of the key cybersecurity threats, making it easier for stakeholders to grasp the most pressing risks and prioritize their defensive strategies.

### **5.3 Analysis of the Increasing Convergence of IT and OT Security Risks**

The increasing connectivity between information technology (IT) and operational technology (OT) systems within the oil and gas industry is creating new avenues for cyberattacks and exposing previously isolated OT environments to a broader range of threats 1. This convergence, driven by the need for greater efficiency and data-driven decision-making, introduces vulnerabilities as attackers can potentially leverage weaknesses in IT systems to gain access to critical OT infrastructure, and vice versa. Securing these heterogeneous environments is particularly challenging due to the presence of legacy OT systems that were not designed with modern cybersecurity threats in mind and often run on outdated software and hardware 4. The differing lifecycles and patching requirements of IT and OT systems further complicate security efforts. This situation necessitates the adoption of integrated security strategies that address the unique challenges and requirements of both IT and OT environments, moving away from traditional, siloed approaches 35. A unified perspective on security is crucial to effectively monitor, detect, and respond to threats that may traverse both IT and OT networks within the oil and gas industry.

## **6. High-Profile Cybersecurity Incidents in the Oil and Gas Sector (2024)**

The year 2024 witnessed several significant cybersecurity incidents affecting the oil and gas sector, highlighting the ongoing threats.

**Table 1: High-Profile Cybersecurity Incidents in the Oil and Gas Sector (2024)**

| **Date of Incident** | **Targeted Organization** | **Nature of Attack** | **Impact on Sector** | **Attributed Threat Actor (if known)** | **Source(s)** |
| --- | --- | --- | --- | --- | --- |
| January 2024 | Texas Oil and Gas Facility | Cyberattack | Disruption of operational processes | CyberArmyofRussia\_Reborn (CARR) | 5 |
| August 2024 | Hitachi Energy | Data Breach | Energy, Various | CLOP (suspected) | 21 |
| August 2024 | Halliburton | Ransomware Attack, Data Exfiltration | Oilfield Services | RansomHub (suspected) | 21 |
| May 2024 | Danish Energy Sector | Firewall Exploitation | Energy | Sandworm (initially suspected, later questioned) | 21 |
| July 2023 (Ongoing Impact in 2024) | Suncor (Petro-Canada) | Cybersecurity Breach | Downstream (Retail) | Unknown | 21 |

*Note: The STORMOUS cyberattack on PVC-MS occurred in September 2023 but its impact and reporting continued into 2024 21.*

These incidents illustrate the diverse nature of cyber threats, ranging from hacktivist activity to sophisticated ransomware attacks and data breaches, impacting various segments of the oil and gas industry. The table demonstrates that no single type of organization or region within the oil and gas sector is immune to cyberattacks. The attribution of some attacks provides valuable intelligence for understanding the motivations and tactics of adversaries. The recurring theme of exploited vulnerabilities underscores the importance of proactive security measures.

## **7. Common Vulnerabilities and Tactics, Techniques, and Procedures (TTPs) in the Oil and Gas Sector**

### **7.1 Common Vulnerabilities**

Several recurring vulnerabilities make the oil and gas industry a prime target for cyberattacks. These include unpatched software and systems, which leave known weaknesses open for exploitation 4. Weak or default passwords continue to provide easy access for attackers 15. Insecure remote access configurations, often necessary for managing geographically dispersed operations, present significant entry points for malicious actors 1, B3, B61. A lack of proper network segmentation between IT and OT environments allows attackers to move laterally within a network once a breach occurs 1. Vulnerabilities specific to Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, which are critical for controlling physical processes, are also frequently targeted 4. The increasing adoption of IoT devices introduces new exploitable vulnerabilities 34. Even physical security vulnerabilities can be leveraged to gain access to critical systems 24. The reliance on legacy systems, many of which were not designed with modern security in mind, further exacerbates these issues 4. Finally, a lack of visibility into wireless networks can leave critical communications unprotected 7. The persistence of basic vulnerabilities indicates a fundamental challenge in maintaining cybersecurity hygiene within the industry, potentially due to its complexity. The specific vulnerabilities in ICS/SCADA systems highlight the need for specialized OT security measures.

### **7.2 Tactics, Techniques, and Procedures (TTPs)**

Threat actors targeting the oil and gas industry employ a range of TTPs. Spear-phishing campaigns are a common method for gaining initial access to networks 5, B1, B41. Exploitation of known vulnerabilities in software and hardware is another frequently used technique 4. Brute-force attacks are often directed at remote access services and poorly secured IoT devices to guess credentials 5. Many advanced threat actors utilize "living off the land" (LOTL) techniques, using legitimate tools and processes already present on compromised systems to evade detection 11. Data manipulation within OT systems is a concerning tactic that can lead to operational disruptions 15. Lateral movement within networks allows attackers to spread from initial points of compromise to reach critical assets 11. Manipulation of Human Machine Interfaces (HMIs) can directly impact industrial processes 5. The deployment of ransomware and wiper malware is a common objective, either for financial gain or to cause destruction 5. Supply chain attacks target third-party vendors as a means to access the primary target's network 1. Some actors compromise SOHO routers to establish command and control infrastructure 5, B1, B410. Replacing public SSH keys for persistent access is a more sophisticated technique observed in some attacks 15. The combination of both sophisticated and common TTPs indicates that attackers are adapting their strategies to exploit various weaknesses within the oil and gas industry. The use of compromised routers highlights the potential for attackers to leverage less secure devices on the network periphery.

## **8. Recommendations for Enhancing Cybersecurity Posture**

To mitigate the identified threats, oil and gas organizations should implement several key cybersecurity measures. Multi-factor authentication (MFA) should be enforced for all remote access points and critical systems 1, B31. Regularly updating and patching all software and firmware, particularly for internet-facing devices and OT/ICS systems, is crucial 1, B31. Enhancing network segmentation to isolate critical OT systems from IT networks and other less trusted zones is essential to limit the impact of a breach 1, B31. Developing and regularly testing comprehensive incident response plans specifically tailored for OT/ICS environments will enable a more effective response to cyber incidents 1, B31. Conducting regular security assessments, penetration testing, and vulnerability assessments of both IT and OT environments can help identify and address weaknesses proactively 1, B31. Implementing robust access controls and adhering to the principle of least privilege will limit the potential damage from compromised accounts 1. Strengthening security measures for third-party vendors and throughout the supply chain, including security audits and stringent security requirements, is vital 1. Deploying continuous monitoring and anomaly detection solutions for both IT and OT networks can help identify malicious activity in real-time 2. Strengthening wireless network security through regular audits and continuous monitoring is necessary to protect these increasingly used communication channels 15. Fostering a strong security culture through regular employee training and awareness programs on phishing, social engineering, and other threats is a critical element of defense 1. Developing and maintaining robust backup and recovery procedures for critical IT and OT systems will ensure business continuity in the event of an attack 1, B31. Considering the adoption of a Zero Trust security model can further enhance defenses 18. Finally, enhancing collaboration and information sharing with industry peers and government agencies can contribute to a stronger collective defense 1. These recommendations emphasize a multi-layered security approach that combines technical and organizational controls.

## **9. Conclusion**

The cybersecurity landscape for the oil and gas industry in 2025 presents a complex and evolving array of threats. The persistent danger of ransomware, the diverse motivations and tactics of identified threat actor groups, and the prevalence of common vulnerabilities underscore the need for constant vigilance and proactive defense. This report has highlighted the key findings from recent cybersecurity reports, analyzed significant incidents from 2024, and detailed the common weaknesses and attack methods observed. The increasing sophistication and frequency of attacks demand that oil and gas organizations prioritize cybersecurity investments and implement the recommended best practices. By adopting a proactive and adaptive security posture, the industry can better protect its critical infrastructure, ensure operational resilience, and mitigate the potentially severe consequences of cyber intrusions.

#### Works cited

1. Top Cybersecurity Threats Facing the Oil and Gas Industry in 2025 - Silverline Solutions, accessed March 22, 2025, <https://www.silverlinesolutions.com/top-cyber-threats-facing-the-oil-and-gas-industry-in-2025/>
2. ICS/OT Security for the Oil and Gas Utility Industry - Cyberintelsys, accessed March 22, 2025, <https://cyberintelsys.com/ics-ot-security-for-the-oil-and-gas-utility-industry/>
3. Advancing cybersecurity posture through a comprehensive maturity program in the oil industry - CEE Multi-Country News Center, accessed March 22, 2025, <https://news.microsoft.com/en-cee/2025/03/13/advancing-cybersecurity-posture-through-a-comprehensive-maturity-program-in-the-oil-industry/>
4. (PDF) CYBERSECURITY CHALLENGES IN THE OIL AND GAS INDUSTRY: PROTECTING CRITICAL INFRASTRUCTURE FROM EMERGING THREATS - ResearchGate, accessed March 22, 2025, <https://www.researchgate.net/publication/389348125_CYBERSECURITY_CHALLENGES_IN_THE_OIL_AND_GAS_INDUSTRY_PROTECTING_CRITICAL_INFRASTRUCTURE_FROM_EMERGING_THREATS>
5. 2025 OT Cybersecurity Report | Dragos, accessed March 22, 2025, <https://www.dragos.com/ot-cybersecurity-year-in-review/>
6. 2025 Global Threat Report | Latest Cybersecurity Trends & Insights | CrowdStrike, accessed March 22, 2025, <https://www.crowdstrike.com/en-us/global-threat-report/>
7. Nozomi Networks Labs Report Finds Wireless Networks Unprotected as Threats to Critical Infrastructure Escalate, accessed March 22, 2025, <https://www.nozominetworks.com/press-release/nozomi-networks-labs-report-finds-wireless-networks-unprotected-as-threats-to-critical-infrastructure-escalate>
8. Dragos: Attackers have moved beyond mere access and reconnaissance | SC Media, accessed March 22, 2025, <https://www.scworld.com/news/dragos-attackers-have-moved-beyond-mere-access-and-reconnaissance>
9. Dragos Reports OT/ICS Cyber Threats Escalate Amid Geopolitical Conflicts and Increasing Ransomware Attacks, accessed March 22, 2025, <https://www.dragos.com/resources/press-release/dragos-reports-ot-ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks/>
10. Dragos Reports OT/ICS Cyber Threats Escalate Amid Geopolitical Conflicts and Increasing Ransomware Attacks - Business Wire, accessed March 22, 2025, <https://www.businesswire.com/news/home/20250225734979/en/Dragos-Reports-OTICS-Cyber-Threats-Escalate-Amid-Geopolitical-Conflicts-and-Increasing-Ransomware-Attacks>
11. Ransomware, state actors, hacktivists exploited geopolitical tensions to target critical infrastructure in 2024 - Industrial Cyber, accessed March 22, 2025, <https://industrialcyber.co/reports/ransomware-state-actors-hacktivists-exploited-geopolitical-tensions-to-target-critical-infrastructure-in-2024/>
12. Dragos Reports OT/ICS Cyber Threats Escalate Amid Geopolitical Conflicts and Increasing Ransomware Attacks | Morningstar, accessed March 22, 2025, <https://www.morningstar.com/news/business-wire/20250225734979/dragos-reports-otics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks>
13. VOLTZITE | Dragos, accessed March 22, 2025, <https://www.dragos.com/threat/voltzite/>
14. Connecting the Dots: State Actors, Hacktivists, and Critical Infrastructure Attacks in 2024, accessed March 22, 2025, <https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2025/february/State-Actors-Hacktivists-Critical-Infrastructure-Attacks/>
15. OT/IoT Cybersecurity Trends & Insights 2025 - Nozomi Networks, accessed March 22, 2025, <https://www.nozominetworks.com/ot-iot-cybersecurity-trends-insights-february-2025>
16. Cybersecurity Forecast 2025 report - Google Cloud, accessed March 22, 2025, <https://cloud.google.com/security/resources/cybersecurity-forecast>
17. Cybersecurity Annual Report 2025 - FlippingBook, accessed March 22, 2025, <https://online.flippingbook.com/view/66100556>
18. Oil And Gas Security And Service Global Market Report 2025, accessed March 22, 2025, <https://www.thebusinessresearchcompany.com/report/oil-and-gas-security-and-service-global-market-report>
19. Top 5 Cybersecurity Threats to Oil & Gas - Dragos, accessed March 22, 2025, <https://www.dragos.com/blog/top-5-cybersecurity-threats-to-oil-gas-and-how-to-protect-against-them/>
20. Cyber Attack News - Risk Roundup - 2024 Retrospective - Xage Security, accessed March 22, 2025, <https://xage.com/blog/cyber-attack-news-2024-attacks-on-critical-infrastructure/>
21. Biggest Cybersecurity Attacks in Oil And Gas Extraction Industry (2023-2024) - SOCRadar, accessed March 22, 2025, <https://socradar.io/cyber-attacks-in-oil-and-gas-industry-2023-2024/>
22. The cyber threats to watch in 2025, and other cybersecurity news to know this month, accessed March 22, 2025, <https://www.weforum.org/stories/2025/02/biggest-cybersecurity-threats-2025/>
23. Cybersecurity considerations 2024: Energy and natural resources sector, accessed March 22, 2025, <https://kpmg.com/us/en/articles/2024/cybersecurity-considerations-2024-energy-and-natural-resources-sector.html>
24. OT/ICS Security for Oil & Gas: A Comprehensive Guide - Sectrio, accessed March 22, 2025, <https://sectrio.com/blog/complete-guide-ot-ics-cybersecurity-oil-and-gas/>
25. How the Oil and Gas Industry Will Combat Ransomware in 2025 - Netdata | Blog, accessed March 22, 2025, <https://blog.netdatanetworks.com/en/ransomware-oil-and-gas>
26. Oil Giant Halliburton Lost $35 Million Due to the August 2024 RansomHub Ransomware Data Breach - CPO Magazine, accessed March 22, 2025, <https://www.cpomagazine.com/cyber-security/oil-giant-halliburton-lost-35-million-due-to-the-august-2024-ransomhub-ransomware-data-breach/>
27. Ransomware Remains a 'Brutal' Threat in 2024 - GovTech, accessed March 22, 2025, <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/ransomware-remains-a-brutal-threat-in-2024>
28. Cyberattack Cost Oil Giant Halliburton $35 Million - SecurityWeek, accessed March 22, 2025, <https://www.securityweek.com/cyberattack-cost-oil-giant-halliburton-35-million/>
29. Halliburton Cyberattack Update: Losses Worth $35 Million Hit The Firm, accessed March 22, 2025, <https://latesthackingnews.com/2024/11/15/halliburton-cyberattack-update-losses-worth-35-million-hit-the-firm/>
30. Protecting Critical Infrastructure: Defending Against Threats to OT/ICS Systems, accessed March 22, 2025, <https://www.criticalstart.com/protecting-critical-infrastructure-defending-against-threats-to-ot-ics-systems/>
31. The Halliburton Cyberattack: A Wake-Up Call for Critical Infrastructure Cybersecurity, accessed March 22, 2025, <https://www.juvare.com/the-halliburton-cyberattack-a-wake-up-call-for-critical-infrastructure-cybersecurity/>
32. Your first line of defense against adversaries - Dragos, accessed March 22, 2025, <https://www.dragos.com/threat-groups/>
33. KAMACITE Threat Group Operations - Dragos, accessed March 22, 2025, <https://www.dragos.com/threat/kamacite/>
34. Cybersecurity for Oil and Gas: Vulnerabilities & Solutions | Darktrace, accessed March 22, 2025, <https://darktrace.com/cyber-ai-glossary/cybersecurity-for-oil-and-gas>
35. Oil Rig Security: Preparing for 2025 and Beyond - Identec Solutions, accessed March 22, 2025, <https://www.identecsolutions.com/news/oil-rig-security-preparing-for-2025-and-beyond>
36. Hitachi Energy UNEM/ECST - CISA, accessed March 22, 2025, <https://www.cisa.gov/news-events/ics-advisories/icsa-25-063-05>
37. ICS Vulnerability Report: Hitachi Energy Network Management Flaw Scores a Perfect 10, accessed March 22, 2025, <https://cyble.com/blog/hitachi-energy-critical-risk/>
38. Hitachi Energy UNEM - ICS Advisory - CISA, accessed March 22, 2025, <https://www.cisa.gov/news-events/ics-advisories/icsa-25-030-01>
39. Cybersecurity Alerts and Notifications | Hitachi Energy, accessed March 22, 2025, <https://www.hitachienergy.com/products-and-solutions/cybersecurity/alerts-and-notifications>
40. The cyber threat against Denmark 2024 - Center for Cybersikkerhed, accessed March 22, 2025, <https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/cfcs---the-cyber-threat-against-denmark-2024.pdf>
41. Attacks against Denmark 's energy sector were not carried out by Russia-linked APT, accessed March 22, 2025, <https://securityaffairs.com/157438/hacking/denmark-energy-sector-attacks-attribution.html>
42. 2024 Annual Report - Suncor, accessed March 22, 2025, <https://www.suncor.com/-/media/project/suncor/files/investor-centre/annual-report-2024/2024-annual-report-en.pdf?modified=20250226230952&created=20250225185554>
43. Top Utilities Cyberattacks of 2023 and Their Devastating Impact on Critical Infrastructure, accessed March 22, 2025, <https://asimily.com/blog/top-utilities-cyberattacks-of-2023/>
44. The Suncor Cybersecurity Incident: Unveiling The Depths Of Network Security Threats - TeckPath, accessed March 22, 2025, <https://teckpath.com/a-deep-dive-into-the-suncor-cybersecurity-incident/>
45. Microsoft reveals ransomware attacks against its customers nearly tripled last year, accessed March 22, 2025, <https://www.cybersecuritydive.com/news/microsoft-customers-ransomware-attacks-triple/730011/>
46. Addressing Cybersecurity Threats in the Oil & Gas Industry | Pumps & Systems, accessed March 22, 2025, <https://www.pumpsandsystems.com/addressing-cybersecurity-threats-oil-gas-industry>
47. Threat Actor Profile: OilRig - Cyble, accessed March 22, 2025, <https://cyble.com/threat-actor-profiles/oilrig/>