Co-authored by SecurityScorecard KPMG

REPORT

Third-Party Breaches are the Top Threat for the U.S. Energy Sector

Executive Summary

This paper examines the cybersecurity posture of the U.S. energy sector. As an industry, energy is a confluence of sub-sectors — power and utilities, oil & gas, natural resources, and chemicals — that are experiencing significant transformations in the ways that they interact with customers and suppliers. Adding to this complexity are the parallel transformations of companies across the industrial spectrum, such as manufacturing, technology and automotive, all of which depend on energy. This paper will focus on vulnerabilities in the energy sector's supply chain. Through an in-depth analysis of 250 top U.S. energy companies, the report highlights prevalent cyber risks, especially from third-party sources, and evaluates the industry's preparedness against potential cyber attacks. With cybersecurity ratings based on SecurityScorecard metrics, the research identifies varying levels of security across different segments of the energy supply chain, from oil & gas production to renewable energy sources.

Key findings reveal that while the majority of the industry upholds strong security practices, a significant minority remains highly vulnerable to cyber disruptions, including ransomware and data breaches. **19% of the U.S. energy companies in our sample had unsatisfactory security ratings.** The report stresses the importance of addressing third-party cyber risks and underscores the need for enhanced security measures around renewable energy sources. It aligns with global and national cybersecurity initiatives, offering strategic insights to improve resilience against cyber threats in the energy sector. This analysis is crucial for stakeholders within the U.S. energy industry, policy makers, and cybersecurity professionals aiming to fortify the sector against the evolving landscape of cyber threats.

45% **of breaches were third-party related, and surprisingly not from the energy sector itself**

19% **of U.S. energy companies had unsatisfactory cyber risk ratings**

Introduction

This paper presents an analysis of cyber risks within the U.S. energy supply chain, focusing on third-party risks, by evaluating the cyber security ratings of 250 leading U.S. energy firms with SecurityScorecard metrics. By comparing different segments of the supply chain, the study uncovers where the energy supply chain is most susceptible to cyber disruptions. **45% of industry breaches involve third parties, mostly from outside the energy industry or in software/IT services and products.** The findings stress that while ransomware poses a significant threat, the prevalence of more conventional data breaches also presents a substantial risk to the industry's cybersecurity posture.

> *"The energy industry is a complex system that is undergoing a generational transition with a heavy reliance on a steady supply chain. With geopolitical and technology-based threats on the rise, this complex system is facing an equally generational risk exposure that could harm citizens and businesses alike. Organizations that are able to quantify these risks and establish mitigation measures will increase their odds of success in the energy transition journey."*
>
> **— Prasanna Govindankutty**
>
> Principal, Cyber Security US Sector Leader, KPMG

Relevance

This paper supports global efforts for bolstered cybersecurity measures across the energy supply chain, aligning with the global commitment to combat cyber threats highlighted during the June 2024 G7 summit. It underscores the partnership among key U.S. entities like the White House Council on Supply Chain Resilience, the Department of Energy, and the Idaho National Laboratory, emphasizing ransomware as a critical threat. The notorious May 2021 ransomware attack on the Colonial Pipeline, which disrupted U.S. fuel supplies, has magnified the urgency for enhanced security within the energy sector, catalyzing efforts to prevent future disruptions.

Concerns about cyber disruptions of the U.S. energy supply chain have often focused on its Industrial Control Systems (ICS) and Operational Technology (OT) for the extraction, transportation, and processing of energy supplies. While such concerns are well-founded, these scenarios may be described as "higher-impact, lower-probability" cases, as the number of actual ICS/OT attacks has been relatively low thus far. Our data-driven approach instead emphasizes more likely scenarios, such as ransomware attacks on and data breaches of conventional information technology (IT). Indeed, the Colonial Pipeline attack did not have to compromise any ICS/OT to disrupt the flow of energy; a disruption of the pipeline's IT billing system was sufficient to force it to suspend operations and thus disrupt the energy supply chain.

Another consideration is securing the shift to cleaner energy. A "greener" grid would be more interconnected and software-driven and thus more potentially exposed and vulnerable to attack. Reducing this risk is a key focus of the U.S. National Cybersecurity Strategy, specifically outlined as Strategic Objective 4.4. Our findings reveal that U.S. renewable energy companies now have security ratings below the industry average, signaling a critical need for heightened cybersecurity measures to safeguard these emerging sources of energy from potential cyber risks.

> *"The prioritization of software, IT products, operational and control systems will remain as the number one source of risk to your organization as well as the end-to-end sector supply chain."*
>
> **— Diana Keele**
>
> Managing Director, US Third Party Security Leader, KPMG LLP

Key Findings

Third-party risk was responsible for an unusually high proportion of these breaches (45%).

In contrast, the global rate is 29%. Furthermore, all but one (9 out of 10), or 90%, of attacks on companies breached more than once involved third parties.

Most of the third-party involvement in these breaches came from: a) outside the energy industry; and b) providers of software & IT products & services.

12 of these 18 third-party breaches involved third-party software & IT. Only 4 of the 18 third-party breaches involved other energy organizations.

Additional Findings

The U.S. energy industry has good security but still has problems.

Its average ratings (86/88) are on par with or slightly below other samples. Most companies (81%) have good ratings, but a minority (19%) with weak ones could imperil the supply chain.

Vertically integrated oil & natural gas companies score highest (93/94); renewable energy companies score lowest (81/85).

The former significantly outperformed industry averages, whereas the latter scored below industry averages by a noteworthy margin.

A vast majority (92%) of companies concentrated their lowest sub-scores in only 3 of 10 security risk factors.

Application Security (40%) and Network Security (23%) are common top sources of cyber risk across all industries. DNS Health, however, was more common (29%) as a source of cyber risk in this sample than in most others.

Overview

The mean rating for all 250 companies is 86; the median is 88. The small gap between the mean and median indicates that the sample is slightly "left-skewed," i.e. a small number of relatively low scores drag down the mean value. The median may be a better representative of the sample.

For comparison, the mean rating for all 12 million organizations worldwide that our platform covers is currently 82. The above mean and median scores are within the same range as, or a bit lower than, those of other samples that SecurityScorecard has analyzed recently, such as: the global aviation & aerospace industry (85/88); the U.S. healthcare and pharmaceuticals industry (88/89); top technology vendors (84/87); and the S&P 500 stock index (88/89).

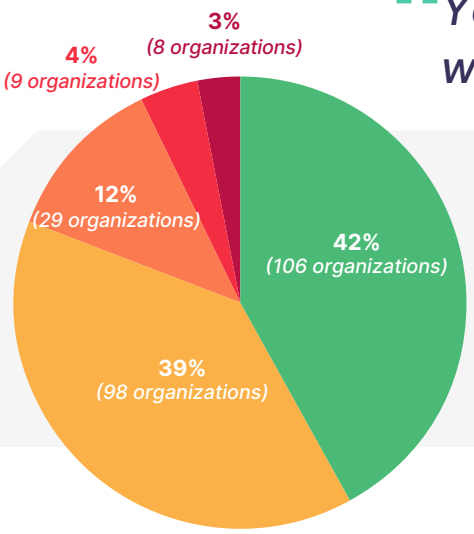
The S&P 500 report found that energy companies had some of the best ratings on that index (91/92). Expanding the scope to smaller U.S. energy companies paints a less favorable portrait of the industry's security. Security costs money. Prior SecurityScorecard research found a strong correlation between GDP and security ratings. Companies in richer countries can often afford stronger security. There is a growing gap of "cyber inequity" between "cyber haves" and "have notes," according to the World Economic Forum. By the same token, larger companies within the same country can often afford stronger security than their smaller counterparts.

Distribution of Letter Grades

This distribution of letter grades within the U.S. energy industry provides more nuance. According to our rating methodology, a "B" rating indicates a 2.9x greater likelihood of a breach than an "A"; a "C" indicates a 5.4x greater likelihood; a "D" indicates a 9.2x greater likelihood; and a "F" indicates a 13.8x greater likelihood. More loosely, an A rating is considered strong or excellent; a B is good or respectable; and C, D, and F ratings are weak, deficient, or bad.

In this case, 81% of the U.S. energy industry sample had either strong A or good B ratings; only 19% had weak, deficient, or bad C, D, or F ratings. This distribution illustrates the left-skewed nature of the sample; the low C, D, and F scores are reducing the mean value for a sample otherwise dominated by higher A and B scores. This 81% proportion of A & B ratings compares favorably with that of global aviation (77%) and top technology vendors (77%), but it is still less than that of the S&P 500 (88%) and the U.S. healthcare & pharmaceuticals industry (90%).

> *"Your security is only as strong as its weakest link - including your vendors."*



DISTRIBUTION OF LETTER GRADES IN U.S. ENERGY INDUSTRY SAMPLE

- A — 90 or higher
- B — 80 to 89
- C — 70 to 79
- D — 60 to 69
- F — less than 60

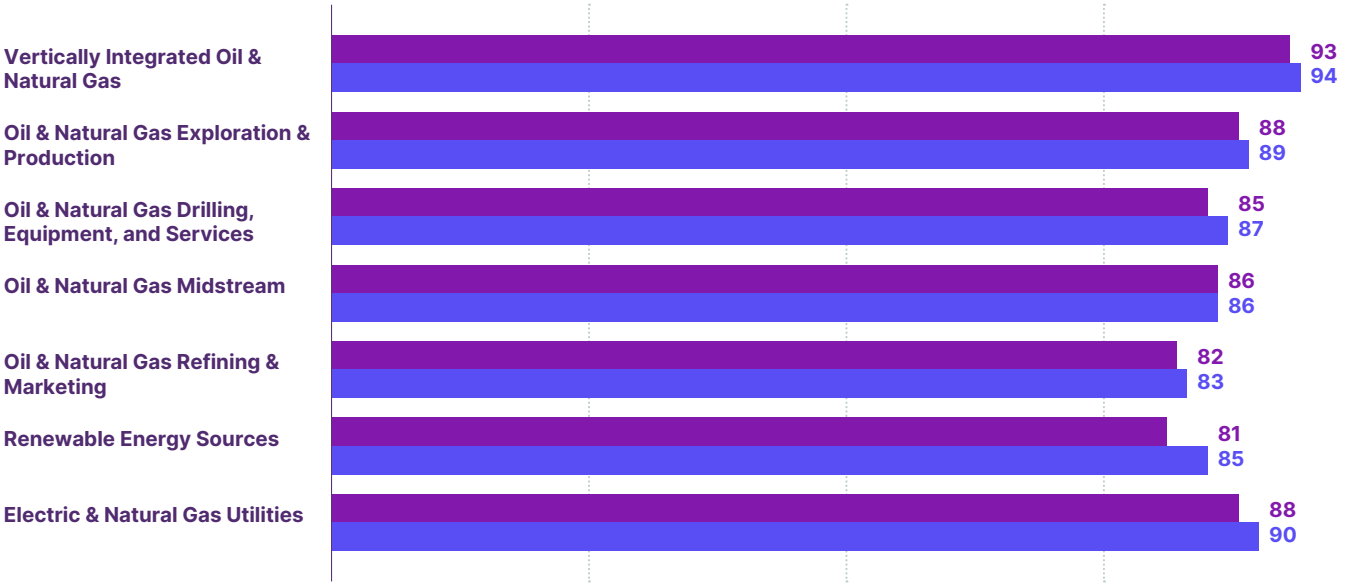
While these statistics may paint a moderately favorable portrait of the security of the U.S. energy industry, one must remember that security is only as strong as its weakest link. The good security ratings of 81% of the industry mean little if a weakness in the security posture of the remaining 19% of the industry enables third-party breaches of the other 81% or disrupts their supply chain.

Comparison of Energy Supply Chain Segments

A comparison of the security ratings of various sectors of an industry, or the various segments of its supply chain, sheds light on where the greatest risk of compromise or disruption lies.

- For example, in the U.S. healthcare & pharmaceuticals industry, medical device manufacturers score lowest. This finding compounded existing concerns about the vulnerable medical devices in healthcare providers' attack surfaces. Relationships with device vendors, beyond installations of their potentially vulnerable products, are thus another source of extra supply chain risk for their customers among healthcare providers.
- In the case of global aviation, airlines' security ratings outperformed all categories of vendors that support them, and that aviation-specific software & IT vendors had the lowest scores in the industry. Airlines are thus incurring elevated third-party risk from all their vendors, but more so from their specialized software & IT vendors.

MEAN AND MEDIAN SECURITY RATINGS FOR EACH ENERGY INDUSTRY SECTOR



The distribution of cybersecurity scores across the energy sector highlights several critical insights. Vertically integrated oil & gas companies boast the highest security scores, likely due to their larger size and greater financial capacity to invest in security programs. In contrast, renewable energy firms, often newer and smaller with a market capitalization of $1 billion USD or less, exhibit some of the lowest scores, which raises concerns amid efforts to transition from fossil fuels to renewable sources. The vulnerability of these companies to cyber disruptions and espionage, exemplified by the activities of state-sponsored groups like Volt Typhoon, poses a significant threat to the sector's competitiveness and the broader adoption of renewable energy.

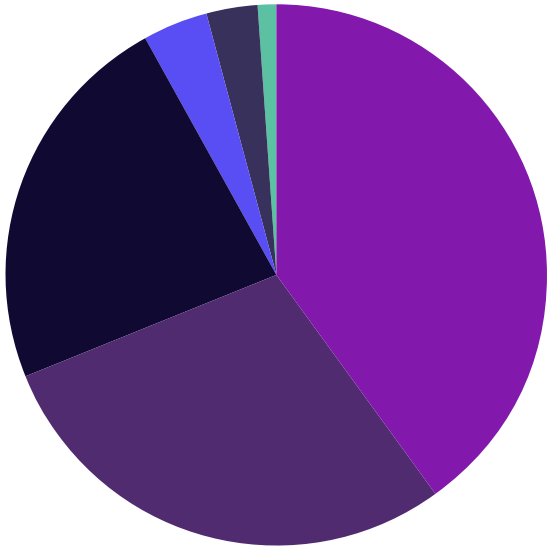
Additionally, a noticeable decline in security scores is observed as one moves downstream in the oil and gas supply chain, with the exception of electric and natural gas utilities, which have above-average scores. This trend suggests a heightened risk of cyber disruptions in the later stages of the supply chain, emphasizing the need for targeted cybersecurity enhancements across all segments, particularly in downstream operations, where average scores are lowest.

The observed decline in security scores toward the downstream segments of the energy supply chain implies an increased likelihood of cyber-induced disruptions as resources progress toward the consumer end, with such risks diminishing closer to the original point of production. Consequently, energy companies need to shift their contingency planning focus from potential halts in production and supply to addressing the challenges of surplus supplies that fail to reach consumers due to disruptions in downstream operations. For instance, in the event of a cyberattack impacting a downstream refinery or marketer, upstream producers and midstream transporters might find themselves compelled to either scale back production or manage the storage of excess supplies, highlighting the necessity for robust cybersecurity measures throughout the entire supply chain to ensure the uninterrupted flow of energy to the end users.

General Cyber Risk Factors and Specific Security Issues

To identify top sources of cyber risk, we noted the 1 of 10 security factors for which each company received its lowest sub-score. We used these values to calculate mean and median sub-scores for those same risk factors among those companies scoring lowest in those areas.

PERCENTAGES OF COMPANIES WITH THEIR LOWEST SUB-SCORES IN EACH SECURITY FACTOR; MEAN/MEDIAN SUB-SCORES OF THOSE COMPANIES FOR THOSE SECURITY FACTORS



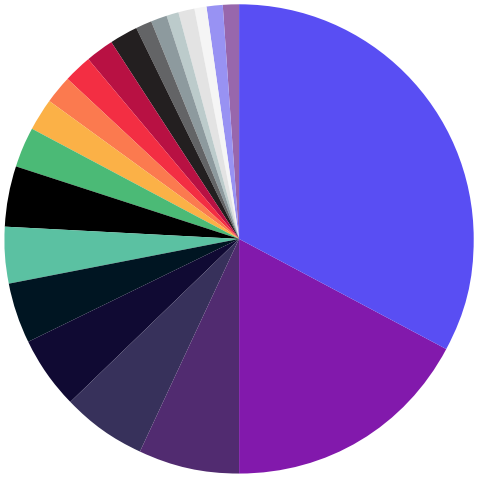
- **Application Security:** 40%, 76/77
- **DNS Health:** 29%, 78/80
- **Network Security:** 23%, 79/81
- **Patching Cadence:** 4%, 72/71
- **Endpoint Security:** 3%, 81/83
- **IP Reputation:** 1%, 60/60

The data reveals a notable concentration of vulnerabilities within specific security domains. Among the ten evaluated security factors, four were not represented in the analysis of the lowest scores at all. Remarkably, 92% of the lowest scores were concentrated within just three areas: Application Security, DNS Health, and Network Security. Application Security and Network Security frequently emerge as significant risk areas across various industries. However, the proportion of companies scoring lowest in DNS Health (29%) is higher than usual in this case.

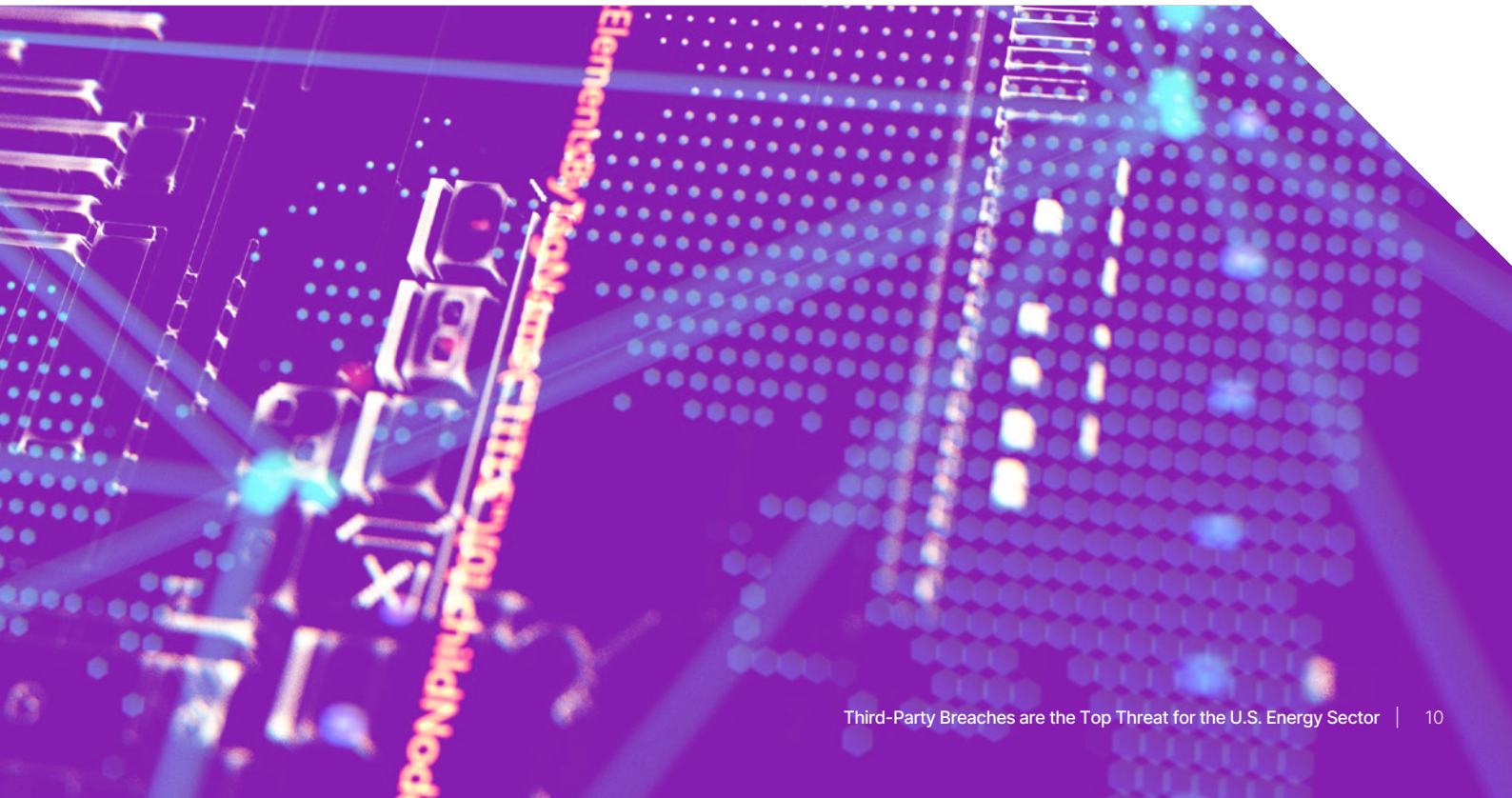
We further analyzed the individual security issues that had the most negative impact on each company's scores. In parentheses next to the description of the specific issues are the broader security factors to which they contribute. Where applicable, we consolidated issues that occurred only once on this list under the rubric of "Miscellaneous" issues for the relevant security factor.

DISTRIBUTION OF SECURITY ISSUES WITH MOST NEGATIVE IMPACT ON SCORES

- **SSL/TLS Service Supports Weak Protocol (Network Security):** 33%
- **Redirect Chain Contains HTTP (Application Security):** 17%
- **SPF Record Contains a Soft Fail without DMARC (DNS Health):** 7%
- **Session Cookie Missing "Secure" Attribute (Application Security):** 6%
- **Unsafe Implementation of Subresource Integrity (Application Security):** 5%
- **Website References Object Storage (Application Security):** 4%
- **Website Copyright is Not Current (Application Security):** 4%
- **SPF Record Missing (DNS Health):** 4%
- **Outdated Web Browser Observed (Endpoint Security):** 3%
- **Session Cookie Missing "HTTPOnly" Attribute (Application Security):** 2%
- **Miscellaneous Application Security Issues (Application Security):** 2%
- **FTP Service Observed (Network Security):** 2%
- **Miscellaneous Network Security Issues (Network Security):** 2%
- **Telephony/VoIP Device Accessible (Network Security):** 2%
- **Miscellaneous Patching Cadence Issues (Patching Cadence):** 1%
- **Site Emits Visible Browser Logs (Application Security):** 1%
- **DNS Server Accessible (Network Security):** 1%
- **UPnP Accessible (Network Security):** 1%
- **HTTP Proxy Service Detected (Network Security):** 1%
- **SPF Record Found Ineffective (DNS Health):** 1%
- **Malformed SPF Record (DNS Health):** 1%



Despite Application Security being identified as the most commonly encountered low-scoring factor overall, it ranks a close second when it comes to the sources of the most detrimental impacts on security scores, accounting for 41% of such issues. By a slim margin, Network Security issues lead as the primary contributors to significant negative score impact, representing 42%. This slight edge is primarily attributed to the prevalent issue of weak encryption or misconfigurations in SSL/TLS services, a common challenge in Network Security that represents a third (33%) of all identified concerns. This issue is not unique to any one sector but is instead a widespread vulnerability noted across various industries. Beyond this, other Network Security problems contributing to negative impacts were notably less common.



Malware Infections and Device Compromises

Our IP Reputation security factor tracks signs of malware infections or device compromises through intelligence collection methods such as sinkholes and honeypots. It indicates that approximately 8% (21 out of 250) of the organizations sampled showed evidence of network compromises over the past year. This rate is significantly lower compared to other sectors, such as the global aviation industry, which stands at 17%. While these instances do not necessarily point to widespread breaches of these organizations, they highlight potential vulnerabilities and unreported breaches, serving as initial indicators or access points for broader network infiltration. Importantly, the scope of these compromises appears limited, with most cases involving minimal data points. Only 2 of the 21 potentially compromised companies in our sample had data points of this kind reaching double digits, suggesting that the overall impact on the energy sector's network security may be contained but warrants vigilant monitoring and preventive measures.

Previous Attacks and the Roles of Third Parties

Statistics and Third-Party Risk

SecurityScorecard gathers intelligence on cybersecurity breaches from a variety of sources, including mainstream media, legal actions, corporate disclosures, government announcements, and insights from underground criminal circles. This comprehensive documentation allows us to refine our analytics, identifying patterns between the signals we collect and actual breach events. It is important to note that experiencing a breach can significantly impact an organization's score, especially if sensitive data is disclosed, as such incidents often provide actionable intelligence for other cybercriminals (including technical details, such as credentials or network reconnaissance).

In our dataset, 40 breaches were publicly reported across 35 of the 250 companies, translating to 14% of the sample. Notably, 5 of these companies experienced more than one breach, contributing to a higher risk profile. Compared to our S&P 500 study, where 21% of companies reported breaches within a year, the 14% figure appears more favorable. However, a striking finding from our analysis is the significant role of third-party risk, implicated in 45% of the reported breaches. This is substantially higher than the global average of 29%, underscoring the critical impact third-party risk has on this industry's security. Particularly telling is that among companies with repeated breaches, third-party involvement was nearly universal, emphasizing the amplified risk third parties contribute to an organization's cybersecurity landscape. The vast majority (9 out of 10, or 90%) of breaches at companies breached more than once also involved third parties. Most companies in our sample may have done well in securing their own attack surfaces, but that success is undone when they experience a breach via a less secure vendor.

It is thus worth identifying specific types of third-party relationships that have enabled these 18 third-party breaches, so as to set priorities for third-party risk management (TPRM) teams

THIRD-PARTY RISK PLAYED TWICE AS LARGE A ROLE IN THE MISFORTUNE OF COMPANIES BREACHED TWICE

- **MOVEit vulnerability at affected energy companies:** 3
- **Unspecified vendors/contractors:** 3
- **Energy efficiency software & services:** 2
- **MOVEit vulnerability at Pension Benefits International:** 2
- **MOVEit vulnerability at payroll services provider:** 1
- **MOVEit vulnerability at unspecified vendor:** 1
- **Electronic data interchange (EDI) for pipeline:** 1
- **Joint venture overseas with foreign oil & gas company:** 1
- **Managed Service Provider:** 1
- **Cloud service:** 1
- **Payment processor:** 1
- **Accounting firm:** 1

The most common cause of third-party breaches was the large-scale exploitation of the zero-day vulnerability (CVE-2023-34362) in Progress Software's MOVEit file transfer software by the criminal group "C10p" in mid-2023. This massive cross-industry campaign caused 7 of the 18 third-party breaches in question, or more than one-third of them (approximately 39%).

3 of the 7 MOVEit compromises involved energy companies using MOVEit. The other 4 were fourth-party breaches, in which energy companies experienced third-party data breaches via vendors who had suffered breaches of their own via their MOVEit installations. 2 of those fourth-party MOVEit compromises involved the same vendor: Pension Benefit International (PBI), a company that tracks the beneficiaries of company benefits for employers. Another fourth-party MOVEit compromise was at a payroll services provider for an energy company. The remaining fourth-party MOVEit compromise involved an unidentified vendor.

Only 4 of the 18 third-party breaches involved other energy companies.

12 of the 18 third-party breaches, or two-thirds of them (67%), involved providers of software & IT products and services. Aside from the 7 that exploited the MOVEit vulnerability, 2 others involved specialized industry-specific software. Others involved cross-industry products and services, such as a cloud service and a Managed Service Provider (MSP).

Ransomware and Other Disruptive Threats

Ransomware stands as a predominant threat across various sectors, with the energy industry being no exception. The sector's limited tolerance for operational downtime makes it an attractive target for ransomware operators, mirroring the vulnerability that has also placed healthcare providers in the crosshairs of cyber extortionists. A recent case in point involves an oil services giant, which reportedly fell victim to a ransomware attack in summer of 2024. This cyber assault led to the shutdown of multiple systems within the company. Despite the severity of the attack, there have been no immediate reports of disruptions to the energy supply, highlighting its resilience yet underscoring the vulnerability within the industry.

Ransomware groups, notably Nefilim and BlackCat/ALPHV, have shown a marked interest in the energy sector, targeting companies across the globe. For example, Nefilim attacked W&T Offshore, a Texas-based oil and natural gas producer, compromising significant data without impacting industrial control systems. BlackCat/ALPHV attacked U.S. entities like Mammoth Energy as well as international targets, including Canada's Trans-Northern Pipelines and energy utilities in Spain, among others, before going dark in March 2024. These incidents underscore the global nature of ransomware threats to the energy sector, driven by the lure of profitability and the relative ease of executing attacks, rather than geographical preferences.

Employee and Customer Data

Despite well-founded concerns about possible disruption of energy supplies, many compromises of energy companies are simply data breaches with no impact on the energy supply chain. Such data breaches, as represented by cases in our sample, typically involve the personally identifiable information (PII) of a company's employees and/or retail customers, along with other data points that could be useful for identity theft, bank fraud, phishing, or other malicious activities.

Security researchers often highlight the healthcare sector for its wealth of personally identifiable information (PII), given the depth of patient records that typically include critical data such as dates of birth (DOBs) and Social Security numbers (SSNs) — vital for identity theft. However, breaches in other industries, such as energy, also expose these sensitive details. HR, payroll, and benefits documentation often reveal DOBs, SSNs, and even banking details for direct deposits.

For example, a late 2023 data breach at a state utility reportedly exposed data on 500,000 customers and contractors. A threat actor known as username "anazon" on an underground criminal forum offered to sell a sample of this data, which comprised not only names and contact details but also billing-related service information. The incident highlights the critical need for robust security measures to protect both employee and customer data, as such breaches not only risk the privacy and security of individuals but also erode trust in the institutions tasked with safeguarding their information.

Recommended Actions

1. **Prioritize Software & IT Vendors for Third-Party Risk Management**
   Given their critical role in enabling third-party breaches, software and IT vendors must be at the forefront of third-party risk management (TPRM) strategies. SecurityScorecard's MAX program, launched in 2024, exemplifies a proactive approach by offering TPRM as a managed service, addressing the complexities this essential task entails. Continuous monitoring of cross-industry threats, as well as those targeting specialized software and IT systems crucial to energy efficiency and pipelines, is imperative.

2. **Emphasize Product Security in New Acquisitions**
   Aligning with the U.S. Cybersecurity & Infrastructure Security Agency's "Secure by Design" initiative, companies should insist on inherent security in the technology products they adopt, ensuring they are built with security as a foundational element – key security features should be available at no extra cost. CISA provided this list of sample questions to ask prospective vendors, including whether or not they signed the Secure by Design pledge and if/how they have followed up on that commitment. The U.S. Department of Energy also advocates for integrating its Supply Chain Cybersecurity Principles to bolster security measures, highlighting the need for international cooperation, as supply chains may extend well beyond U.S. borders.

3. **Prioritize the Improvement of Security around Renewable Energy Sources**
   The relatively low scores for U.S. renewable energy companies in our sample raises concerns about the future of their role in the broader industry, as government policymakers, energy business leaders, and environmental advocates push to diversify away from fossil fuels. Another risk factor is the cyber-attacks launched by countries to support their competitive goals. Many of these companies are still relatively new and small and may thus simply need more time and investment to build and mature security programs on par with those of their peers in other energy sectors. Cyber attacks could damage these businesses via financial loss, intellectual property compromise, exposure of competitive intelligence, and disruption of end-to-end supply chain confidence.

4. **Preparing for Disruptions and Balancing Other Risks**
   Energy companies must prepare for disruption risks, particularly in downstream operations, without neglecting the pervasive risk of data breaches and other common cyber threats. By the same token, such disruptive attacks seem to be a "higher-impact, lower-probability" scenario. In contrast, the reporting on breaches that affected companies in our sample emphasizes more common "lower-impact, higher-probability" scenarios, such as data breaches that expose employee or customer data and enable fraud. Preparing for large-scale disruptions is important, but it should not distract energy organizations from more mundane, everyday threats.

Learn from Attacks on Foreign Targets

As we saw with at least two ransomware groups targeting U.S. energy companies, they also targeted their foreign counterparts. While state-sponsored actors may have political reasons to target the United States, their more common criminal counterparts are less geographically selective and may attack whatever targets they deem most cost-effective. The attack surfaces of foreign energy companies should resemble those of their U.S. counterparts enough that cyber threat intelligence (CTI) on the tactics, techniques, and procedures (TTPs) of attacks on them would be useful to security teams at U.S. energy companies. The experiences of foreign energy targets at the hands of ransomware groups offer valuable lessons in resilience and response that U.S. companies can adapt to enhance their own cybersecurity practices.

Methodology - Reference

SecurityScorecard researchers compiled a sample of 250 top U.S. energy companies, based on market capitalization and the various sectors of the industry that they represent. These sectors cover: the successive stages of the traditional oil & gas supply chain; the existence of vertically integrated oil & gas companies covering that whole supply chain; the consumption of some energy via utilities; and the emergence of companies devoted to renewable energy sources.

- Vertically Integrated Oil & Natural Gas
- Oil & Natural Gas Exploration & Production
- Oil & Natural Gas Drilling, Equipment, and Services
- Oil & Natural Gas Midstream
- Oil & Natural Gas Refining & Marketing
- Electric & Natural Gas Utilities
- Renewable Energy Sources

For each company, we noted:

- its overall numerical security score, based on our analysis of its attack surface;
- the one security risk factor where it scored the lowest and the value of that sub-score;
- the specific security issue that had the most negative impact on its overall score;
- previously unreported malware infections or compromised devices within the past year;
- any publicly reported breaches.

To learn more and create your free account, visit SecurityScorecard.com

ABOUT SECURITYSCORECARD

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

Security Scorecard

KPMG