REPORT

Energy Sector Cybersecurity Report:

Navigating Third-Party Cyber Risk

SecurityScorecard

CONTENTS

Introduction

SecurityScorecard threat researchers have identified that 90% of the world's largest energy companies experienced a third-party breach in the past 12 months.

Fueling the global economy and daily life, reliance on the energy sector elevates it as a prime target for cyberattacks. Amid economic and political uncertainties, concerns about safeguarding this vital sector intensifies. Attacks on energy not only result in financial losses and disruptions but also ripple through manufacturing, healthcare, and transportation sectors.

Key research findings

Third-Party breaches in the energy industry

- 90% of the world's largest energy companies experienced a third-party breach in the past 12 months.
- All top 10 U.S. energy companies had a third-party breach.

The hidden threat of fourth-party vendors

- 92% of the energy companies evaluated have been exposed to fourth-party breaches.

Security Ratings and breach likelihood

- One-third of energy companies had a C Security Rating or lower, which indicates a higher likelihood of breaches.

Recent breach incidents

- In the last 90 days alone, SecurityScorecard identified 264 breach incidents related to third-party compromises.

MOVEit takes center stage

- MOVEit emerged as the most prevalent third-party vulnerability in the last six months, affecting hundreds of companies globally.

Methodology

SecurityScorecard conducted an extensive analysis of the cybersecurity posture of the 48 largest energy companies across five key nations: the United States, United Kingdom, France, Germany, and Italy. These companies, representing the coal, oil, natural gas, and electricity industries, were selected based on their current revenue rankings, ensuring a focus on major players in the industry.

SecurityScorecard examined over 21,000 domains, reflecting a diverse range of third-party and fourth-party vendors. This approach offers unique insights into the complex supply chain dependencies that characterize modern critical infrastructure.

*While only 4% of over 2,000 third-party vendors experienced direct breaches, **90% of the evaluated energy companies facing third-party breaches**.*

The ripple effect

This disparity underscores a critical vulnerability in the energy sector's supply chain security, where a small number of breaches can cascade into widespread security incidents.

The situation was particularly acute in the United States, where every single energy company included in the study suffered from a third-party breach. This not only highlights the interconnected nature of cybersecurity risks in the energy sector but also illustrates the rapid and extensive spread potential of supply chain attacks.

Ryan Sherstobitoff, Senior Vice President of Threat Research and Intelligence at SecurityScorecard, stated: "More than two years after the major U.S. pipeline ransomware incident, the world still lacks a common framework for measuring cyber risk. Transparency and information sharing about cybersecurity is critical for national security."

Shining a light on fourth-party cyber risk

The study sheds light on the significant, yet often overlooked, risk that fourth-party vendors pose.
It was revealed that an alarming 92% of the energy companies assessed were exposed to fourth-party breaches

This finding emphasizes the need to extend security assessments and mitigation strategies beyond immediate third-party vendors to include the entire digital supply chain. It also illustrates the intricate web of dependencies in the supply chain and the importance of a comprehensive approach to security that takes into account not just direct partners, but all entities within the digital ecosystem.

The link between Security Ratings and breach probability

33% of energy companies rated 'C' or lower. Notably, U.K. companies had the highest average Security Rating, while Italy had the lowest.

Cybersecurity Ratings can be compared to financial credit ratings. Just as a poor credit rating is associated with a greater probability of default, a poor cybersecurity rating is associated

with a higher probability of sustaining a data breach or other adverse cyber events. In fact, organizations with a cybersecurity grade of F are 7.7 times more likely to sustain a breach compared to organizations with an A.

Minimize disruption from third-party cyber risks

Enterprises globally continue to be plagued by third-party-originating cyber incidents. In the past, third-party cybersecurity risk management has been too resource-intensive, overly process-oriented, and has little to show for in terms of results.

Jim Routh, Fortune 500 CISO and Senior Advisor and Chairman of the SecurityScorecard Cybersecurity Advisory Board, commented: "Hope and prayer may be useful but are clearly not sustainable strategies. Preventing the surge of supply chain attacks requires systematically applying real-time data triggering automated workflow to manage risk in the digital ecosystem."

Effective third-party cyber risk management depends on delivering three key outcomes:

1. Resource efficiency
2. Risk management and resilience
3. Influence on business decision making

CISOs can take five key actions to manage third-party cyber risk:

1. Operationalize cybersecurity oversight across the supply chain
2. Ensure continuous monitoring and detection of third- and fourth-parties
3. Conduct third-party cyber incident response planning
4. Work with critical third-parties to mature security posture
5. Report on third-party cyber risk to the board to create a risk-informed partnership

Together, we can cultivate transparency and collaboration to secure the digital ecosystem.

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.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.com

United States: (800) 682-1707
International: +1(646) 809-2166