By SUPPLY CHAIN CONNECT STAFF

Energy Sector's Achilles' Heel: Third-Party Vulnerabilities

New report finds that third-party risk is responsible for 45% of all cybersecurity breaches impacting the energy sector's supply chains.

The U.S. energy sector could be facing more vendor-related supply chain security risks in the near future according to a new report from SecurityScorecard and KPMG. In fact, nearly two-thirds of all breaches (12 of 18, to be precise) now come from the software and IT vendors that energy organizations work with. And, third-party risk is responsible for 45% of breaches, compared to a global rate of 29%.

These are some of the eye-opening findings highlighted in *A Quantitative Analysis of Cyber Risks in the U.S. Energy Supply Chain*, which offers up a detailed analysis of cybersecurity vulnerabilities across the energy sector and its supply chains.

SecurityScorecard and KPMG say frequent threats like ransomware attacks on conventional IT systems are often enough to cause widespread disruption across the energy sector.

Much attention has also been paid to potential attacks on industrial control systems (ICS) and operational technology (OT), which will continue to be a focus for risk mitigation. Clean energy initiatives are another prime target for bad actors looking for systems to exploit. "As the shift to cleaner energy accelerates," the reports states, "the sector's vulnerabilities may grow, as a greener, more interconnected grid becomes increasingly reliant on software, making it more susceptible to cyberattacks."

SUPPLY CHAIN connect™

Disproportionately High Third-Party Risks

In their new report, SecurityScorecard and KPMG say third-party risks are disproportionately high in the energy sector. In fact, third-party risk drives almost half (45%) of breaches in the sector—a number that's significantly higher than the global rate of 29%. Additionally, 90% of companies that suffered multiple breaches were hit via third-party vendors.

"The energy sector's growing dependence on third-party vendors highlights a critical vulnerability — its security is only as strong as its weakest link," SecurityScorecard's Ryan Sherstobitoff continues, in a press release. "Our research shows that this rising reliance poses significant risks. It's time for the industry to take decisive action and strengthen cybersecurity measures before a breach turns into a national emergency."

Here are some of the other key report findings:

- The U.S. energy industry scores a "B" on average based on SecurityScorecard's scoring methodology. 81% of companies have either an A or B rating, but the remaining 19% with weak scores pose a significant risk to the entire supply chain.

- Software and IT vendors are the leading cause of third-party breaches: Software and IT vendors outside the energy sector are the main source of third-party breaches. Of the incidents studied, 67% of third-party breaches were due to software and IT vendors, with only four involving other energy companies.

- Oil & natural gas companies scored well above average with an "A–," while renewable energy firms lagged behind with a "B–" score.

- 92% of companies had their lowest scores in just three of 10 risk factors: application security (40%), network security (23%), and DNS (Domain Name System) health (29%).

5 Ways to Manage the Growing Problem

SecurityScorecard's STRIKE team offers these tips for energy organizations that want to improve their cybersecurity stances and take proactive steps to thwart the "bad actors" that could exploit vulnerabilities in their systems:

1. **Prioritize software and IT vendors.** Focus on mitigating risks from software and IT vendors, which pose the highest third-party risks.

2. **Emphasize product security in new acquisitions.** Help ensure that new technology acquisitions are secure, following initiatives like CISA's "Secure by Design" and integrating the U.S. Department of Energy Supply Chain Cybersecurity Principles.

3. **Prioritize the improvement of security around renewable energy sources.** Strengthen security programs to protect against potential supply chain risks and geopolitical threats, particularly from nation-states.

4. **Prepare for disruptions and balance other risks.** Prepare for disruption without neglecting the pervasive risk of data breaches and other common cyberthreats.

5. **Learn from attacks on foreign targets.** Gain valuable insights by studying ransomware attacks on foreign counterparts to improve resilience and cybersecurity defenses.