# Surge in ransomware attacks highlights cybersecurity risks in energy sector



Recent research conducted by Trustwave has highlighted a concerning trend in the cybersecurity landscape, particularly within the energy and utilities sector, which has witnessed a significant surge in ransomware attacks. This sector's growing reliance on interconnected devices such as smart meters, sensors, and home automation systems has created numerous potential cyber vulnerabilities, making it an attractive target for cybercriminals.

The report, which analyses data from mid-2022 to mid-2023, indicates that there were 137 ransomware attacks reported, a figure that alarmingly increased by over 80% in the subsequent year, reaching 257 attacks by mid-2024. Although there has been a slight decline in the frequency of attacks in the second half of 2024, the total number remains to be fully assessed as the year concludes. Trustwave's data also reveals that nearly half of these attacks originated from the United States, with approximately 10% occurring in the European Union. A small number of specific groups are responsible for the majority of these attacks, including LockBit, which initiated 85 attacks since mid-2022, and AlphV, which followed with 36 attacks. Emerging groups, such as Hunters International and Qilin, have also begun to increasingly target utilities in the latter part of 2024.

Phishing is identified as a primary method used by attackers, accounting for 84% of breaches within the sector, while 96% of the attackers exploited remote services to navigate through systems. The financial repercussions of data breaches are substantial, with the average cost nearly $500,000 exceeding the cross-industry average.

The Trustwave report outlines multiple factors contributing to the energy and utilities sector's vulnerability to cyberattacks. These include the sector's nature as a profitable domain with substantial revenues, which makes it a lucrative target; the interconnected framework of the industry that opens numerous entry points for potential attackers; and the considerable societal impact that such breaches can cause. Furthermore, recovery from these incidents typically takes longer in this sector compared to others, incurring high operational costs due to disruption.

Cybersecurity within the energy and utilities sector presents distinct challenges, attributed to a strong dependence on integrating physical infrastructure with digital systems, increasing regulatory scrutiny, and outdated legacy systems. Trustwave emphasizes the importance of developing resilient cybersecurity strategies that can proactively identify, mitigate, and respond to breaches.

In response to these challenges, the report recommends several measures, including implementing network segmentation between Operational Technology (OT) and Information Technology (IT) systems to limit lateral movements by attackers. Investment in threat detection and response tools is urged in addition to maintaining regular system updates and conducting frequent security assessments. Moreover, employee awareness and training constitute critical components of a comprehensive cybersecurity framework.

Kory Daniels, Chief Information Security Officer at Trustwave, noted that "to achieve effective threat resilience, asset and exposure management, infrastructure and code testing, OT and IT cyber defence and business continuity and disaster recovery programmes," innovative collaboration between public and private sectors is becoming increasingly necessary.

Additionally, the World Economic Forum has drawn attention to the complexities facing cybersecurity on a broader scale. While larger organisations have made steady progress in bolstering their cyber resilience, smaller firms are reportedly struggling, with many reaching a critical point where securing their operations has become increasingly difficult. Regionally, disparities exist, particularly in Africa and Latin America, where confidence in national responses to cyber incidents targeting critical infrastructure is markedly lower than in regions such as Europe and North America. Public sector bodies are also disproportionately affected, predominantly due to a shortage of skilled personnel capable of achieving cybersecurity goals.

Another pressing issue identified is the vulnerability of supply chains, which has emerged as a significant cyber risk. Increasing complexities within supply chains, coupled with inadequate visibility into the security measures of suppliers, raise concerns about software vulnerabilities introduced by third parties and the potential for wider propagation of cyberattacks within the ecosystem. Furthermore, the rapid integration of artificial intelligence into business processes presents new security challenges, as generative AI is reportedly enhancing cybercriminal capabilities and leading to a rise in social engineering attacks, with nearly half of the organisations surveyed reporting such incidents in 2024.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.trustwave.com/en-us/resources/library/documents/trustwave-spiderlabs-research-cybersecurity-challenges-for-energy-and-utilities-in-2025/> - This link supports the claim about the surge in ransomware attacks and cybersecurity challenges in the energy and utilities sector, as highlighted by Trustwave's research.
* <https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/upcoming-trustwave-spiderlabs-report-investigates-threats-against-the-energy-and-utilities-sector/> - This article discusses the increasing threats to the energy and utilities sector, including an 80% rise in ransomware attacks, and provides details on upcoming reports from Trustwave SpiderLabs.
* <https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/trustwave-spiderlabs-the-ransomware-trends-confronting-the-energy-and-utilities-sector/> - This blog post details the trends in ransomware attacks against the energy and utilities sector, including the rise of ransomware-as-a-service and the involvement of new threat groups.
* <https://html.spec.whatwg.org> - This link does not directly support the article's claims but is a general resource on HTML standards, which might be relevant in a broader cybersecurity context.
* <https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/how-generative-ai-is-shaping-the-future-of-cybersecurity-key-insights-for-cisos-and-enterprises/> - This article explores how generative AI is impacting cybersecurity, which aligns with the article's mention of AI enhancing cybercriminal capabilities.
* <https://www.weforum.org/agenda/archive/cybersecurity/> - The World Economic Forum has discussed cybersecurity challenges, which supports the broader context of cybersecurity issues mentioned in the article.
* <https://www.noahwire.com> - This is the source of the original article but does not provide additional supporting information beyond the text itself.
* <https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/trustwave-spiderlabs-ransomware-attacks-against-the-energy-and-utilities-sector-up-80/> - This article further details the increase in ransomware attacks against the energy and utilities sector, aligning with Trustwave's findings.
* <https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/why-vulnerability-scanning-alone-isnt-enough-the-case-for-penetration-testing/> - This article discusses the importance of comprehensive cybersecurity measures, which supports the article's recommendations for robust security strategies.