# Cyberattacks on renewable energy infrastructure surge amid accelerating energy transition



When you glance at your smart meter to check your electricity usage, the notion of a cyberattack is likely far from your mind. Yet, Internet of Things (IoT) devices like smart meters can serve as vulnerable entry points for cybercriminals. In 2023, there was a staggering 200% increase in cyberattacks targeted at utilities, with the energy sector facing an average data breach cost surpassing $4 million. This trend is especially pronounced in Europe, where cyberattacks in the power sector doubled between 2020 and 2022, and in the United States, where cyber incidents against utilities surged by nearly 70% year-on-year during 2024.

This intensifying threat environment arises amid the ongoing energy transition, where the renewables sector has become a prime target for cybercriminals. As the industry accelerates its adoption of digital technologies to manage and integrate renewable sources, potential vulnerabilities proliferate. The necessity for sophisticated software to coordinate these technologies—from battery energy storage systems to solar panels—opens new avenues for cyberattacks. Furthermore, the increasing number of stakeholders involved in these initiatives encompasses not only traditional power companies but also businesses from diverse sectors, enhancing the risk landscape.

The International Renewable Energy Agency (IRENA) reported that global renewable power capacity rose by 473 gigawatts (GW) in 2023—a 14% increase from the previous year. However, this expansion comes with its own challenges, as new systems are often more dispersed and less established, creating ripe opportunities for cyber threats. Digital tools, including IoT and artificial intelligence, have become essential for optimising energy management and forecasting demand, yet they also compound the complexity of cybersecurity.

The vulnerabilities affecting renewable energy infrastructure can manifest in numerous ways. For instance, solar networks face six distinct types of cyberattacks, and both wind farms and battery storage facilities are susceptible to remote control disruptions. A cautionary message from the Federal Bureau of Investigation (FBI) highlights that “malicious cyber actors may seek to disrupt power-generating operations.” An illustrative case involved a denial-of-service attack on a private solar firm, which resulted in a significant operational setback across several states.

In the UK alone, renewable companies endured approximately 1,000 attempted cyberattacks every day. Many of these incidents go unreported, in stark contrast to notable attacks, such as the 2022 incident where a cyberattack on a satellite communications network led to a significant operational halt of 5,800 wind turbines in Germany. These incidents signal the pressing need for robust cybersecurity measures across the sector.

As the cyber threat landscape evolves, the shortage of skilled cybersecurity personnel exacerbates the issue. A survey by the Boston Consulting Group indicates that there is a staggering 42% shortfall in cybersecurity specialists within the energy sector. While almost three-quarters of companies in the industry are leveraging generative AI for cybersecurity, the shortage poses a critical risk to effective defence strategies.

Recent policy initiatives aim to address this skills gap. In the US, the proposed Cyber PIVOTT Act seeks to create scholarship programs for students pursuing cybersecurity careers in exchange for government service. Meanwhile, Europe has launched the Cybersecurity Skills Academy and is reinforcing regulatory measures, such as the Network and Information Security Directive, to standardise cybersecurity practices among member states, particularly in critical sectors like energy.

Experts universally concur that energy companies must take decisive action to bolster their cybersecurity posture. Basic steps, including comprehensive training programs and the implementation of advanced monitoring systems like InteRSePT—developed by Mitsubishi Heavy Industries—are pivotal. These systems are designed to identify abnormal behaviour across the control networks of energy infrastructures.

As the energy transition accelerates, utilities must find a balance between leveraging digital innovations and establishing strong cybersecurity measures. With grids becoming increasingly digital and decentralised, the potential disruptions from cyberattacks loom larger, threatening not only operational stability but also the overarching goal of establishing sustainable energy systems worldwide. To navigate this precarious landscape, collaboration between utilities, governments, and technology providers will be essential for fortifying cybersecurity frameworks and devising advanced solutions for modern threats.

## Reference Map:

* Paragraph 1 – [[1]](https://spectra.mhi.com/why-the-energy-transition-means-more-cyberattacks), [[2]](https://www.armis.com/2024/02/29/cyberattacks-utilities-rise-200-2023/), [[4]](https://www.eurelectric.org/news/press-releases/2023/2023-11-15-eurelectric-press-release-cybersecurity-in-the-power-sector/)
* Paragraph 2 – [[1]](https://spectra.mhi.com/why-the-energy-transition-means-more-cyberattacks), [[6]](https://www.energymonitor.ai/renewables/renewable-energy/cybersecurity-in-the-renewable-energy-sector)
* Paragraph 3 – [[3]](https://www.securityintelligence.com/articles/cost-data-breach-energy-utilities/), [[5]](https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04/)
* Paragraph 4 – [[3]](https://www.securityintelligence.com/articles/cost-data-breach-energy-utilities/), [[6]](https://www.energymonitor.ai/renewables/renewable-energy/cybersecurity-in-the-renewable-energy-sector)
* Paragraph 5 – [[1]](https://spectra.mhi.com/why-the-energy-transition-means-more-cyberattacks), [[2]](https://www.armis.com/2024/02/29/cyberattacks-utilities-rise-200-2023/), [[4]](https://www.eurelectric.org/news/press-releases/2023/2023-11-15-eurelectric-press-release-cybersecurity-in-the-power-sector/)
* Paragraph 6 – [[6]](https://www.energymonitor.ai/renewables/renewable-energy/cybersecurity-in-the-renewable-energy-sector), [[7]](https://www.ul.com/energy/renewable-energy/cybersecurity-in-renewable-energy)
* Paragraph 7 – [[1]](https://spectra.mhi.com/why-the-energy-transition-means-more-cyberattacks), [[5]](https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04/)
* Paragraph 8 – [[1]](https://spectra.mhi.com/why-the-energy-transition-means-more-cyberattacks), [[2]](https://www.armis.com/2024/02/29/cyberattacks-utilities-rise-200-2023/), [[6]](https://www.energymonitor.ai/renewables/renewable-energy/cybersecurity-in-the-renewable-energy-sector)

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

## Bibliography

1. <https://spectra.mhi.com/why-the-energy-transition-means-more-cyberattacks> - Please view link - unable to able to access data
2. <https://www.armis.com/2024/02/29/cyberattacks-utilities-rise-200-2023/> - A report from cybersecurity firm Armis reveals that cyberattacks on utilities increased by over 200% in 2023, with overall cyberattacks rising by 104%. The report highlights that many companies are running outdated operating systems and neglecting critical security patches, making them more vulnerable to attacks. Utilities and manufacturing sectors saw the greatest increase in attacks, with 93% of wearable devices not patched for common security vulnerabilities. The rise in cyber threats is partly attributed to geopolitical tensions and cybercriminals targeting outdated devices and operating systems. ([exponent.com](https://www.exponent.com/article/cyberattacks-utilities-rise-200-2023?utm_source=openai))
3. <https://www.securityintelligence.com/articles/cost-data-breach-energy-utilities/> - According to IBM's 2024 Cost of a Data Breach Report, the average cost of a data breach in the energy sector is $4.65 million, a decrease from $6.39 million in 2020. The report indicates that nearly half of the analyzed breaches involved compromised personally identifiable information (PII), with the average cost per record at $180. Roughly 8% of breaches involved ransomware, with an average cost of $4.62 million. The study is based on breaches where between 2,000 and 101,000 records were compromised. ([securityweek.com](https://www.securityweek.com/ibm-average-cost-data-breach-exceeds-42-million/?utm_source=openai))
4. <https://www.eurelectric.org/news/press-releases/2023/2023-11-15-eurelectric-press-release-cybersecurity-in-the-power-sector/> - A report by Eurelectric highlights a doubling of cyberattacks in the European power sector between 2020 and 2022. The report emphasizes the need for enhanced cybersecurity measures to protect critical infrastructure and ensure the reliability of the power supply. It also discusses the challenges posed by the increasing digitalization of the energy sector and the growing sophistication of cyber threats. ([cmitsolutions.com](https://cmitsolutions.com/blog/cost-of-a-data-breach/?utm_source=openai))
5. <https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04/> - The U.S. electric grid is increasingly vulnerable to cyberattacks, with susceptible points in electrical networks growing by about 60 per day, according to the North American Electric Reliability Corporation (NERC). Vulnerable points in the grid's software or hardware increased to 23,000-24,000 last year, up from 21,000-22,000 in 2022. The rise in cyber threats is partly due to geopolitical conflicts, such as Russia's invasion of Ukraine and the war in Gaza, alongside ongoing threats from China. With the upcoming U.S. presidential election, the potential for attacks on the grid is expected to rise. ([reuters.com](https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04/?utm_source=openai))
6. <https://www.energymonitor.ai/renewables/renewable-energy/cybersecurity-in-the-renewable-energy-sector> - The renewables sector has become a prime target for cybercriminals as digital technologies are rapidly adopted to integrate and manage renewable energy sources. The integration of more renewable projects and battery energy storage systems requires software that allows the technologies to interact and work together, introducing cybersecurity risks across the system. As renewables develop and scale, the number of stakeholders involved is increasing, including businesses from various sectors alongside power companies, which could increase the likelihood of cyber threats.
7. <https://www.ul.com/energy/renewable-energy/cybersecurity-in-renewable-energy> - Integrating more renewable projects and battery energy storage systems requires software that allows the technologies to interact and work together, introducing cybersecurity risks across the system. The increasing number of stakeholders involved in renewable energy projects, including businesses from various sectors alongside power companies, could increase the likelihood of cyber threats.