Energy and Renewables Sector:

CYBERSECURITY RISKS *(And How To Be Prepared)*

As the energy and renewables sector undergoes digital transformation, the risk of cyberattack has increased significantly. These threats can disrupt operations, compromise data and cause significant financial loss.

Here's what you need to know to stay protected.

WHY THE HIGH RISK?

Large Attack Surface:
Vulnerabilities extend from power plants to energy transmission networks, IoT devices, and weak third-party security.

Industry Change:
Shifts towards digitization use of IoT and SaaS platforms (AI-power optimization tools) increase vulnerabilities.

Critical Infrastructure:
Energy sector provides essential services, making it an attractive target for politically motivated or nation-sponsored attacks.

High Profits:
Soaring profits attract potential hackers seeking financial gain.

COMMON ATTACKS

Phishing Attacks:
Cybercriminals target employees to gain unauthorized access.

Digitization Threats:
As operational technology becomes digitized, hackers gain new points of attack.

SCADA Vulnerabilities:
Supervisory control and data acquisition (SCADA) systems, responsible for managing industrial networks, are particularly susceptible to infiltration.

Third-party vendor security:
Partners with weak security postures can open energy companies to cyberattacks.

Weak device security:
IoT devices with poor encryption or open remote access are attack vectors.

Shared Account Threat:
Shared operator accounts in energy monitoring systems can pose a security risk.

IN THE NEWS

Increasing Vulnerability:
The independent risk management and quality assurance provider DNV conducted a survey that revealed that 60% of C-suite respondents in the energy sector feel more vulnerable to a cyberattack now than ever before.

Neglected Supply Chain Security:
Only 28% of energy professionals feel that their companies are investing adequately in supply chain security.

Attack on Critical Infrastructure:
Notable attacks have already targeted power grids with the intent to cut off power to entire regions or to collect sensitive intelligence. In 2021, Colonial Pipeline, a US-based pipeline system was hit with a ransomware attack marking one of the worst supply chain attacks in recent years.

Prevalent Unpreparedness:
The energy sector became the 3rd most targeted industry in 2020, rising six places compared to 2019.

HOW ENERGY AND RENEWABLES SECTOR CAN BE PREPARED

Invest in cybersecurity basics like email protection, endpoint protection, and privilege account abuse detection.

Partner with an external vendor for 24/7 monitoring and response services.

Implement strong password management and two-factor authentication.

Ensure due diligence in vetting third-party partners for adequate security measures.

Get organization-wide buy-in on your cybersecurity plan and regularly communicate security best practices.

With the right knowledge, strategies, and partnerships, companies in the energy and renewables sector can significantly reduce their risk of cyberattacks. Partnering with experts like SolCyber can help ensure you have the necessary tools and monitoring in place to stay secure.

It's essential to ensure your entire organization understands the threats and their roles in preventing cyber attacks. This understanding spans from the C-suite to the frontline employees. Comprehensive, regular training can empower your employees to spot and avoid common threats such as phishing attacks and maintain best practices in data management and security.

Don't wait for a cyberattack to disrupt your operations. Take action now to secure your infrastructure and safeguard your business. Reach out to SolCyber, the experts in cybersecurity for the energy and renewables sector, and start building your cyber resilience today.

Take Action Now

SolCyber

solcyber.com