Deloitte.

Powering the future of the energy industry 5x5 series: Insights and actions

Grids and guardrails: Securing the power and utilities sector

As technology continues to play a critical role in the power and utilities sector, it also introduces a range of cybersecurity challenges.
A proactive and layered approach to cybersecurity is essential to safeguard critical infrastructure and maintain the reliable delivery of essential services.

***5** insights you should know*		***5** actions you can take*
Integration of digital technologies and the Internet of Things (IoT) has improved efficiency and control but has also **expanded the attack surface through increased connectivity of Operational Technology (OT) devices** with IT infrastructure. The power and utilities sector has seen an increase in attacks on the OT devices environment resulting from compromised IT systems that allowed attackers into the OT/Industrial Control Systems (ICS) networks.	1	**Segment the OT network** to isolate critical infrastructure and control systems from less critical parts of the network. This reduces the potential impact of a breach spreading throughout the entire infrastructure. Implement OT Security program policies, training, and awareness to educate plant operations teams on identifying and responding to cyber-attacks on their connected OT systems.
The power and utilities sector often relies on **legacy systems and equipment** that are not designed with cybersecurity in mind. These **outdated systems might be more vulnerable to attacks** and lack necessary security updates and patches.	2	**Conduct regular risk assessments and vulnerability scans** to identify weaknesses and potential entry points into your network and systems. Address and prioritize remediation of critical vulnerabilities to decrease the risk of exploitation.
The power and utilities sector relies on a complex supply chain. **Attackers are exploiting supply chains** targeting third-party vendors, which could indirectly impact the organization's operations.	3	**Strengthen your third-party risk management program.** Assess the cybersecurity posture of third-party vendors and suppliers before collaborating with them. Establish precise cybersecurity requirements and standards for vendors with access to systems or data.
The power and utilities sector is an increasingly attractive target for cyberattacks on critical infrastructure. A successful attack on these facilities could have severe consequences on a national or regional level, disrupting electricity supply, water management, and other essential services.	4	Have a strong understanding of the critical assets within your environment and the impact on the business if these assets are compromised. **Implement an effective Attack Surface Management (ASM) program** to understand, triage, and reduce organizational attack surfaces. Regularly update software, applications, and systems with the latest security patches and updates. All this helps address known vulnerabilities before they can be exploited.
Ransomware attacks have become increasingly common across industries. For power and utilities organizations, a successful ransomware attack could disrupt operations and result in significant challenges in restoring services.	5	**Be prepared to prevent, detect, and respond to a ransomware event.** Update and regularly exercise Security Operations Center (SOC) processes and playbooks for monitoring and responding to a ransomware event. Reduce the risk of ransomware through network segmentation, robust Multi-Factor Authentication (MFA), and Privileged Account Management (PAM) practices. Improve organizational resilience through regularly exercising data backups, disaster recovery, and incident response processes.

Connect with us learn more:

Lynne Challender
Managing Director
Deloitte & Touche LLP
lchallender@deloitte.com

Dave Nowak
Principal
Deloitte & Touche LLP
danowak@deloitte.com

Anne Robbins
Senior Manager, Cyber IoT
Deloitte & Touche LLP
anrobbins@deloitte.com

Allison White
Senior Manager
Deloitte & Touche LLP
alliwhite@deloitte.com

Akhilesh Bhangepatil
Senior Manager
Deloitte & Touche LLP
abhangepatil@deloitte.com