Cybersecurity in Utilities/Energy:

Defend against hackers, breaches, and cybercrime

Cyberattacks have hit all segments of the Utilities value chain. Cybercriminals can use malware and IoT devices to gain unauthorized access to your network. Once in, they can launch attacks, causing power outages, stolen or ransomed data, destroyed assets, threats to human life, and more.

Utilities need to defend themselves better. Especially as their operations continue to become more connected and digitized. Investment in security from an IT perspective can support operational technology (OT) and the continuous modernization and growth of their business.

$3.2B

how much will be spent worldwide on smart-grid cybersecurity by 2026.

Navigant Research

61%

of the organizations represented by **600+ utilities professionals surveyed experienced some sort of physical or cyberattack over the last year.**

Utility Dive's sixth annual State of the Electric Utility Survey

49%

of power and utility CEOs surveyed say that **becoming a victim of a cyberattack is a case of when, not if—yet only half say their organizations are well prepared.**

Global Energy World

Why AT&T Business?

- Unparalleled data, analytics, cyber expertise, and threat intelligence enable us to detect and respond to threats to your network
- A premier team of cybersecurity trusted advisors
- Insight and visibility from protecting one of the largest IP networks in the world
- We deliver innovation to keep up with the changing threat landscape

The realization is growing across the energy industry that the major cybersecurity threats to upstream, midstream and downstream data and operations are often aimed at operational technology (OT) systems and equipment – usually older, legacy models – rather than at the information technology (IT) side. Those operational technologies typically include industrial control systems (ICS), supervisory control and data acquisition (SCADA) devices and other related technologies implemented at operational facilities, such as plants, pipelines, terminals and rigs. We have vast experience in delivering highly secure IT and can help you to protect your customer data, maintain your customers' trust, and rapidly recover from attack.

Current energy sector challenges	AT&T Cybersecurity solutions
• Achieving cybersecurity resilience and compliance • Managing cyber risk tied to grid modernization strategy, planning, and execution	• Cybersecurity risk assessment • Agency wide security programs • Internationally recognized frameworks: - ISA 99 (Industrial Autom. & Control Systems Security) - ISA/IEC 62443 4 1/2 (Indus. Network & System Security - WIB M 2784 (Process Control Domain Security Requirements for Vendors) - NIST 800 82 (Guide to Industrial Control Systems - ISO 27002 (Enterprise Cyber Security)
• Meeting Compliance with NERC/CIP Requirements CIP 004-6 • Preparing workforce to detect and protect against threats	• Security Awareness Training • Social Engineering Assessment to measure effectiveness
• Strengthening energy sector cybersecurity preparedness • Coordinating cyber incident response and recovery	• Incident Response Table Top Exercises • Incident Response Retainer • Vulnerability Assessment & Penetration Testing
• Monitor and protect SCADA infrastructure continuously	• Evaluate key risks in the ICS/SCADA network architecture • Identify the network vulnerabilities and test the connectivity to the enterprise network • Assist with the development of a vulnerability management program specific to ICS/SCADA • Threat Manager to analyze security/network event data
• Enhancing safety, reliability, resilience • Securing critical industrial infrastructures • Securing connected devices	• Security assessment services for connected devices, systems, applications, cloud services, and platforms.
• Securing digital transformation in Energy and Utilities • Use computing advances to increase security posture • Shortage of skilled security resources to handle internal security operations	• Next Gen Security Transformation • IT and OT Integration Strategy • Security Operations Consulting • Security Orchestration and Automation • Security Staff Augmentation

Our solutions help you understand trends, rapidly react to change, prepare for future events, and maintain compliance. We help you create effective practices to manage risk and meet changing regulatory requirements.

To learn more about AT&T Cybersecurity Consulting, visit www.att.com/security-consulting.