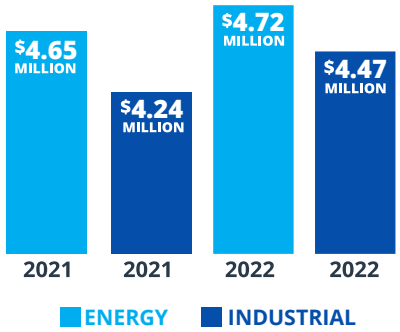
THREATQUOTIENT™

ThreatQ for Energy and Utilities Companies

The Energy and Utilities sector is the backbone of modern society, providing essential services that sustain everyday life. This critical infrastructure not only powers our homes but also serves as the foundation for various sectors, including healthcare, transportation, and communication to name a few. Given its indispensable role, the Energy and Utilities sector has become one of the most targeted industries for cyberattacks. This report will explore the primary threats faced by this industry, with a particular focus on ransomware, and key challenges it encounters in maintaining robust cybersecurity.

The attack surface in the Energy and Utilities sector is constantly expanding as additional utilities are introduced to the industry. The integration of digital technologies and smart infrastructure has undoubtedly improved operational efficiency, but it has also broadened the avenues through which attackers can breach systems. To combat these threats effectively, a comprehensive understanding of vulnerabilities and threats is paramount. However, utilities often lack the cybersecurity staff and resources needed to identify cyber assets and fully comprehend the intricate system and network architectures required for conducting comprehensive cybersecurity assessments, monitoring, and necessary upgrades.

AVERAGE COST OF A DATA BREACH BY INDUSTRY



IBM Security, Cost of a Data Breach Report 2022[3]

Electric utilities can be affected by cyberattacks across the whole chain.

GENERATION

Interference with the operation of power plants and renewable energy sources due to ransomware attacks and service interruptions.

TRANSMISSION

Remote disconnection of services causing widespread power disruptions for customers on a large scale.

DISTRIBUTION

Sabotage of substations resulting in the regional loss of power services and disruptions for customers.

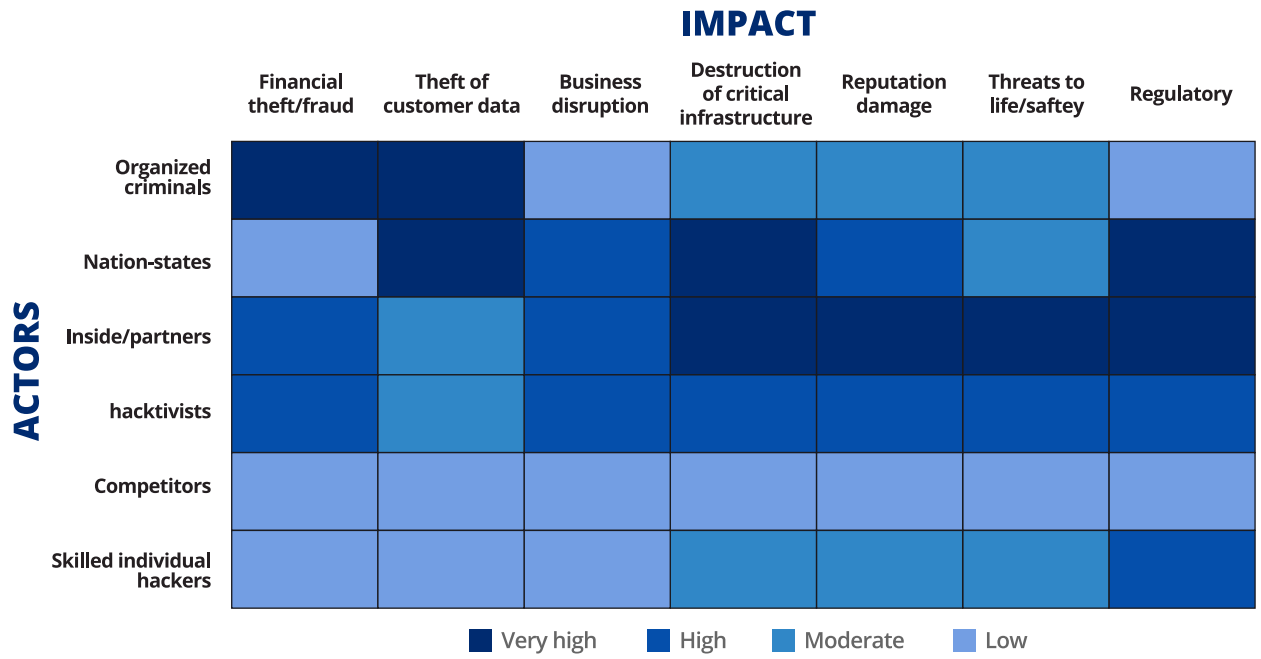
NETWORK

Theft of customer data, perpetration of fraud, and deliberate disruptions to services.

Credit: McKinsey & Company[2]

> "Total awareness of all vulnerabilities and threats at all times is improbable, but without enough cyber security staff and/or resources utilities often lack the capabilities to identify cyber assets and fully comprehend system and network architectures necessary for conducting cyber security assessments, monitoring, and upgrades."
>
> **- Idaho National Laboratory[1]**

The cyberthreat profile for the US electric power sector is highest from three key actors



Deloitte Insights[4]

KEY CHALLENGES

The Energy and Utilities sector faces several key challenges in safeguarding its critical infrastructure and digital assets. These challenges not only include ransomware but also extend to supply chain attacks, incomplete system integration, identity and access management (IAM) inefficiencies, and the growing problem of mobile device phishing[5].

Ransomware
Ransomware, a malicious software that encrypts a victim's data and demands a ransom in exchange for a decryption key, stands out as one of the most significant threats to the Energy and Utilities sector. In 2021, a notable example of this threat became painfully apparent when the Colonial Pipeline fell victim to a cyberattack6. This incident was deemed a national security threat, as it disrupted the transportation of fuel across a large portion of the United States, causing panic buying and fuel shortages. While the situation was eventually resolved within a week, it underscored the severity of the ransomware threat. Ransomware attacks not only disrupt operations but also create a sense of helplessness in victims, compelling them to consider paying a ransom to the attacker in exchange for the decryption key and a chance to restore their critical systems.

Supply Chain Attacks: The Utilities industry is susceptible to supply chain attacks, which target the software and hardware components that form the backbone of its operations. Attackers may compromise these supply chains to introduce vulnerabilities into the infrastructure, potentially affecting numerous utilities at once.

Incomplete integration of systems: The sector's rapid adoption of digital technologies has often led to incomplete integration of systems. This fragmented architecture can create security gaps and weaknesses that attackers can exploit, as the sector's interconnected systems rely heavily on data flow and communication and can create security gaps and weaknesses that attackers can exploit.

Identity and access management (IAM) inefficiencies: IAM systems are critical for ensuring that only authorized personnel access sensitive systems. Inefficiencies, misconfigurations, or weak authentication mechanisms in IAM can expose the sector to unauthorized access, data breaches, and other malicious activities.

Mobile device phishing: The proliferation of mobile devices in the sector's operations introduces another vector for attack. Phishing attacks targeting mobile devices can compromise sensitive information and access to critical systems, further challenging the sector's cybersecurity posture.

The Energy and Utilities sector is undeniably the lifeblood of modern society, making it a prime target for a range of cyber threats. While it faces a multitude of dangers, ransomware, with its disruptive and financially damaging nature, stands out as a particularly pressing concern. The sector must remain vigilant, continuously assess vulnerabilities, and

invest in robust cybersecurity measures to protect the essential services it provides to everyday life. Addressing the key challenges, from supply chain security to identity and access management, is crucial in safeguarding the sector's critical infrastructure against evolving threats in an increasingly digital world. To ensure the sector's continued stability and the uninterrupted provision of vital services, it must work tirelessly to defend itself against the persistent, evolving threats it faces.

CREATING A LEADING THREAT INTELLIGENCE OPERATION

A robust data-driven threat intelligence platform gives energy and utilities providers the context and prioritization they need to make better decisions, accelerate detection and response, and advance team collaboration and learning for continuous improvement. Serving as the hub of intelligence operations for many industries, the ThreatQ Platform aggregates and combines unstructured and structured data from any source, internal and external. There's no need to alter existing security infrastructure or workflows; all tools and technologies work seamlessly with ThreatQ's open architecture. Automation eliminates repetitive, time-consuming tasks so analysts can focus on high-priority and strategic work. The platform also provides flexibility to share curated threat intelligence, advisories and reports with a range of internal and external stakeholders, including energy and utilities sectors, quickly.

ACHIEVE MORE WITH THREATQ:

- **CONSOLIDATE** all sources of external (e.g., E-ISAC, OSINT) and internal (e.g., SIEM) threat intelligence and vulnerability data in a central repository.
- **ELIMINATE** noise and easily navigate through vast amounts of threat data to focus on critical assets and vulnerabilities.
- **PRIORITIZE** what matters most for your environment.
- **PROACTIVELY HUNT** for malicious activity which may signal malicious activity, denial of service attacks and other disruptions and potential harm to customers, employees and constituents.
- **FOCUS** on known security vulnerabilities in currently active exploits which may impact regulatory status and security posture.
- **ACCELERATE ANALYSIS AND RESPONSE** and response to attacks through collaborative threat analysis that enables shared understanding and coordinated response.
- **AUTOMATING** threat detection and response.

Request a live demo of the ThreatQ Platform and ThreatQ TDR Orchestrator at www.threatq.com/demo.

1. https://www.energy.gov/policy/articles/cyber-threat-and-vulnerability-analysis-us-electric-sector
2. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities
3. https://www.ibm.com/downloads/cas/3R8N1DZJ
4. https://www2.deloitte.com/content/dam/insights/us/articles/4921_Managing-cyber-risk-Electric-energy/DI_Managing-cyber-risk.pdf
5. https://energydigital.com/technology-and-ai/the-top-5-cyber-threats-to-the-energy-sector
6. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

ABOUT THREATQUOTIENT™

ThreatQuotient improves security operations by fusing together disparate data sources, tools and teams to accelerate threat detection and response. ThreatQuotient's data-driven security operations platform helps teams prioritize, automate and collaborate on security incidents; enables more focused decision making; and maximizes limited resources by integrating existing processes and technologies into a unified workspace. The result is reduced noise, clear priority threats, and the ability to automate processes with high fidelity data. ThreatQuotient's industry leading data management, orchestration and automation capabilities support multiple use cases including incident response, threat hunting, spear phishing, alert triage and vulnerability prioritization, and can also serve as a threat intelligence platform. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe, MENA and APAC. For more information, visit www.threatquotient.com.

THREATQUOTIENT™

20130 Lakeview Center Plaza, Suite 400 Ashburn, VA 20147 • ThreatQ.com
Sales@ThreatQ.com • +1 703 574-9885

TQ-IDB08-1223-01