Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2023, 10(12):233-242**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Cybersecurity in Utilities: Protecting Critical Infrastructure from Emerging Threats

Vijay Kartik Sikha[1], Satyaveda Somepalli[2]

[1]ORCID: 0009-0002-2261-5551,
vksikha@gmail.com
[2]ORCID: 0009-0003-1608-0527,
satyaveda.somepalli@gmail.com

Abstract: As utility corporations increasingly integrate digital technologies into their operations, they become more vulnerable to sophisticated cyber threats from nation-states, hackers, and criminal organizations. This paper examines the cybersecurity challenges faced by the utility sector, highlighting the vulnerabilities of modernized systems such as smart grids and SCADA systems, legacy equipment, and remote access points. It explores various types of threat actors and attack vectors, providing insights into advanced cybersecurity strategies like AI-driven threat detection, incident response planning, and zero-trust architecture. Additionally, the paper discusses regulatory and compliance considerations, including NERC standards and GDPR, and presents case studies of successful cybersecurity implementations. By fostering a cybersecurity culture through employee training and industry collaboration, utility firms can enhance their resilience against emerging threats and safeguard critical infrastructure, thereby supporting the economic and social well-being of communities worldwide.

Keywords: Cybersecurity, Utilities, Critical Infrastructure, Threat Actors, Smart Grids, SCADA Systems, Legacy Equipment, Remote Access, AI-driven Threat Detection, Zero Trust Architecture, Incident Response, NERC Standards, GDPR, Cyber Resilience, Employee Training, Industry Collaboration

Introduction

Cybersecurity has become a top responsibility for utility corporations, which run the key infrastructure that powers our modern world (Bologna, 2022). As the energy, water, and other utility sectors become more digital and interconnected, they confront a growing threat from sophisticated cyber actors such as nation-states, hackers, and criminal groups.

A successful cyber attack on vital utility infrastructure can have severe implications, including extensive service interruptions, environmental damage, and even dangers to public safety and national security. Utility operators must be proactive in hardening their systems and networks against growing threats. (Bologna 2022).

This study provides an extensive analysis of the cybersecurity issues plaguing the utility industry, while also highlighting the weaknesses inherent in modernized utility systems. Additionally, the paper delves into the strategies and best practices that leading companies are employing to enhance their cyber resilience. Utility firms would be able to play an important role in supporting the economic and social well-being of communities worldwide by comprehending the changing threat landscape and implementing strong security measures.

Trends And Projections

Cyberattacks on the energy sector have been rapidly increasing since 2018, reaching alarmingly high levels in 2022 following Russia's invasion of Ukraine (IEA, 2023). The average cost of a data breach hit a new record

high in 2022, reaching USD 4.72 million in the energy sector (IEA, 2023). Critical infrastructure, including gas, water and particularly power utilities, are favored targets for malicious cyber activity (IEA, 2023).

According to a survey by Trend Micro, 54% of 500 US critical infrastructure suppliers reported attempts to control systems, while 40% had experienced attempts to shut down systems. Over half said that they had noticed an increase in attacks, while three-quarters believed that those attacks were becoming more sophisticated (Allianz Commercial, 2022).

The growing digitalization and the "Internet of Things" (IoT) could create a perfect cybersecurity storm, as more everyday devices become connected and the trend of running devices, software and data through virtual networks, such as cloud computing, accelerates (Allianz Commercial, 2022).

Ransom Payments in the Utility Sector

In 2021, the Colonial Pipeline, a major US fuel pipeline, paid a ransom of $4.4 million to hackers who had shut down its operations (IFAC, 2020). While specific data on ransom payments in the utility sector is limited, the increasing frequency and sophistication of attacks suggest that many companies may be resorting to paying ransoms to restore their systems and operations.

Understanding The Cyber Threat Landscape

To effectively secure utility systems from evolving threats, it is critical to understand the varied spectrum of threat actors, their tactics, methods, and procedures (TTPs), and to identify common attack vectors used by these adversaries (Bailey et al, 2020). By analyzing both elements, utilities can create comprehensive defense plans suited to individual risk variables.

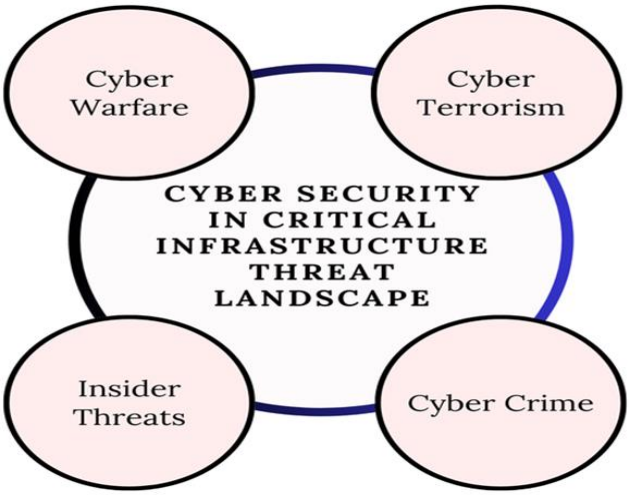

Figure 1: *Cyber Threat Landscape*

Types of Threat Actors

Utility firms face a wide variety of cyberthreats from a variety of skilled actors with varying motivations (Warikoo, 2021). These include:

Nation-State Actors:

Government-sponsored entities that engage in cyber espionage, sabotage, or other offensive acts to further their country's geopolitical goals. They frequently have superior capabilities and extensive resources (Warikoo, 2021).

Hacktivists:

Individuals or groups motivated by political, social, or ideological reasons rather than monetary gain. They could attack utility systems and infrastructure to promote their ideals or make a statement.

Criminal Organizations:

Cybercriminal organizations that use cyberattacks as part of their larger criminal operations, such as fraud, extortion, and money laundering. Their main motivation is financial gain.

Insider Threats:

Malicious insiders that abuse their access to systems and data for sabotage, espionage, or personal gain, such as resentful workers or contractors (Warikoo, 2021).

Attack Vectors

Utility companies face a range of common attack vectors that threat actors leverage to compromise their systems and networks:

Phishing:

Attackers use fraudulent emails or messages to trick users into revealing sensitive information or downloading malware (Zeng & Li, 2020).

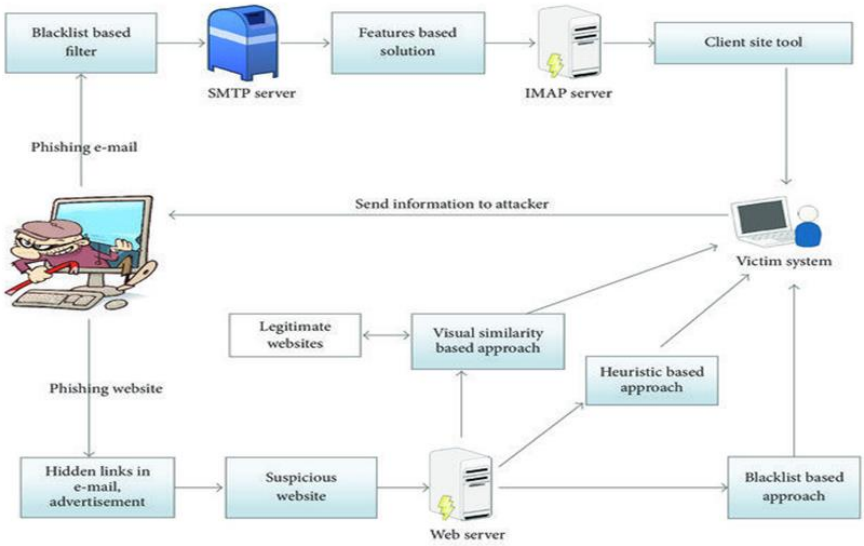

Figure 2: *Phishing Attack*

Ransomware:

Ransomware is a form of malicious software that encrypts a victim's data, rendering it inaccessible until a ransom payment is made for the decryption key. This type of attack can severely disrupt critical utility operations by locking essential data and systems, leading to significant downtime and operational disturbances. For example, the Colonial Pipeline ransomware attack in 2021 exemplifies the severe impact ransomware can have on critical infrastructure. Attackers targeted Colonial Pipeline, one of the largest fuel pipelines in the United States, encrypting its data and demanding a ransom payment. This led to a temporary shutdown of the pipeline, causing fuel shortages and widespread disruption across several states. Although Colonial Pipeline eventually paid the ransom to regain access to their data, the attack resulted in substantial operational and financial consequences (Zeng & Li, 2020).

To prevent ransomware attacks, organizations can adopt several best practices. Regularly updating and patching software and operating systems is crucial, as it addresses known vulnerabilities that ransomware can exploit. Implementing robust backup solutions is also essential; regular, secure backups of critical data ensure that organizations can recover their information without having to pay a ransom. These backups should be stored offline or in a secure cloud environment to prevent them from being encrypted during an attack. Additionally, employee training and awareness are vital; educating staff about recognizing phishing attempts and other common attack vectors can reduce the likelihood of falling victim to ransomware schemes. Network segmentation, which involves dividing networks into segments, limits the spread of ransomware within an organization and helps contain the impact of an attack. Strong access controls, including least privilege policies and multi-factor authentication (MFA), further protect sensitive systems and data from unauthorized access. Finally, having a well-developed and regularly updated incident response plan ensures that organizations can act swiftly and effectively in the event of a ransomware attack, isolating affected systems and restoring operations as quickly as possible (Zeng & Li, 2020).

Supply Chain Attacks:

Supply chain attacks involve targeting third-party vendors and service providers to gain access to a utility's network and systems. These attacks exploit the trust and connections between organizations and their suppliers or partners, often bypassing traditional security defenses by compromising less-secure third-party systems.

Example: A notable example of a supply chain attack is the SolarWinds cyberattack discovered in December 2020. In this incident, attackers inserted malicious code into an update for SolarWinds' Orion software, a widely used IT management platform. When SolarWinds customers, including several utility companies, applied the update, the malware was deployed within their networks. This sophisticated attack allowed the threat actors to gain unauthorized access to sensitive data and systems across numerous organizations, including government and private sector entities (Bellekens, 2022).

Supply chain attacks are particularly concerning because they exploit the inherent trust between organizations and their vendors. Once a third-party vendor is compromised, attackers can potentially move laterally within the utility's network, access critical infrastructure, and conduct malicious activities without triggering traditional security alarms. To mitigate these risks, utility companies need to implement stringent vetting processes for third-party vendors, enforce security standards and controls, and continuously monitor their supply chain for potential vulnerabilities (Bellekens, 2022).

Exploiting Vulnerabilities:

Taking advantage of unpatched software flaws or misconfigurations to gain unauthorized access.

Example: In 2017, the WannaCry ransomware attack demonstrated the dangers of exploiting unpatched vulnerabilities. The ransomware exploited a flaw in Microsoft Windows, known as EternalBlue, which had been leaked from the National Security Agency (NSA). Many organizations, including utilities, had not applied the necessary security updates to address this flaw. As a result, WannaCry spread rapidly, encrypting data on affected systems and demanding ransom payments. This incident highlighted how unpatched vulnerabilities can be exploited to cause widespread disruption and financial loss (Microsoft, 2017).

Advanced Persistent Threats (APTs):

Sophisticated, targeted attacks by nation-state actors or highly skilled criminal groups, often involving a combination of techniques to infiltrate and maintain access to utility networks over an extended period (Bellekens, 2022).

By understanding the diverse threat landscape and the common attack vectors, utility companies can develop comprehensive cybersecurity strategies to protect their critical infrastructure and operations.

Vulnerabilities In Utility Systems

Interconnected systems, while providing numerous benefits, also introduce distinct vulnerabilities that could be exploited by malicious actors (Bailey et al, 2020). Two prominent examples illustrating these weaknesses are smart grids and Supervisory Control and Data Acquisition (SCADA) systems. Additionally, legacy equipment presents considerable challenges concerning adequate cybersecurity protections. Finally, remote access points warrant careful consideration due to the associated hazards stemming from external connectivity.

Smart Grids and SCADA Systems

The increasing interconnectivity and digitization of utility systems, particularly smart grids and Supervisory Control and Data Acquisition (SCADA) systems have introduced new vulnerabilities that threat actors can exploit (Aloul et al., 2012).

The integration of information and communication technologies (ICT) with the physical power grid creates complex cyber-physical interdependencies. This allows cyber attacks on the digital components to potentially cascade into physical disruptions of electricity generation, transmission, and distribution (Aloul et al., 2012). For example, a successful cyberattack could remotely disable or manipulate intelligent electronic devices (IEDs) that regulate and protect the electric power grid.

Legacy Equipment

Many utility companies still rely on aging legacy systems and equipment that were not designed with modern cybersecurity in mind. These legacy components often lack built-in security features, use outdated software and protocols, and are difficult to patch or upgrade, leaving them vulnerable to exploitation (Aloul et al., 2012).

Integrating these legacy systems with newer, more interconnected technologies creates additional points of vulnerability that attackers can target. Utility operators must carefully balance the need to modernize their infrastructure with the challenges of securing legacy equipment that may be critical to ongoing operations (Aloul et al., 2012).

Remote Access Points

The increasing use of remote access and control capabilities in utility systems, such as for maintenance and monitoring, introduces significant cybersecurity risks. Threat actors can potentially exploit these remote access points to gain unauthorized entry into utility networks and systems, enabling them to disrupt operations, steal sensitive data, or deploy malware (Mirzaee et al, 2022).

Inadequate access controls, weak authentication mechanisms, and a lack of visibility into remote activities can all contribute to the vulnerability of utility systems to remote attacks. Utility companies must implement robust access management, multifactor authentication, and continuous monitoring to mitigate these risks (Mirzaee et al, 2022).

Cybersecurity Strategies for Utilities

Advanced Threat Detection

Organizations are increasingly relying on advanced threat detection technologies driven by artificial intelligence (AI) and machine learning (ML) to counter the sophisticated and ever-evolving cyber threats that target utility systems (Hasan et al., 2019).

Massive volumes of network traffic, system records, and user activity can all be analyzed by AI-driven anomaly detection algorithms to find odd patterns or behaviors that might point to a possible cyberattack. These systems can swiftly identify and notify on abnormalities by setting up a baseline of typical activity, allowing for quick reaction and mitigation. (Hasan and associates, 2019).

Behavioral analytics is another effective AI-based technique that focuses on studying and modeling the normal behaviors of people, devices, and apps in the utility's environment. Any variations from these defined behavioral patterns can activate alarms, allowing security teams to analyze and handle potential risks before they cause substantial damage.

Incident Response Plans

For utility firms to handle and recover from cybersecurity issues, they need to have strong and well-practiced incident response strategies in place. To mitigate the consequences of an attack and restore essential operations as soon as possible, it is crucial to incorporate protocols for rapid detection, isolation, and restoration within these plans.

Key elements of an effective incident response plan include:

- Identified roles and responsibilities for security, IT, and operations teams.
- Developed communication protocols and procedures to alert key stakeholders.
- Detailed playbooks for responding to various cyber situations.
- Regularly tested backup and disaster recovery procedures.
- Undertaking extensive post-incident analysis and extracting valuable insights to continually enhance the plan.

Zero Trust Architecture

Given the dynamic nature of cyber threats and the growing intricacy of utility systems, the conventional "castle-and-moat" security concept is deemed inadequate. A zero-trust strategy is being adopted by utility firms, which operates under the premise that all users, devices, and applications—including those connected to the organization's trusted network—could pose a threat.

Regardless of the user's location or device, the zero-trust architecture (ZTA) mandates constant verification and validation of each access request. This entails putting in place strict access controls, robust multi-factor authentication, and real-time analytics and monitoring to identify and address any questionable activity.

The zero-trust paradigm assists utility businesses in reducing the risks associated with insider threats, remote access, and the expanding attack surface of their linked systems by removing implicit trust and requiring verification of every contact. This method improves the vital utility infrastructure's overall security and resilience.

Regulatory And Compliance Considerations

Understanding the many important frameworks, standards, and laws regulating the activities of the utility industries is essential for navigating the complex world of cybersecurity demands (Zeng & Li, 2020). Of these, the rules set forth by the North American Electric Reliability Corporation (NERC) serve as the cornerstones of safe power grid architectures, while the General Data Protection Regulation (GDPR) has a substantial influence on data processing techniques. Additional direction on bolstering comprehensive security postures can be found in industry standardizations such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

NERC Standards

One of the most important organizations for protecting North America's power grids is the North American Electric Reliability Corporation, or NERC. Each regional reliability council applies the operating requirements that NERC establishes to guarantee security and dependability within its own boundaries (Zeng & Li, 2020). .

The goals of NERC standards are to control and guarantee the quality of the bulk power system in North America by establishing minimal criteria for safety, efficiency, dependability, and risk management. Resource and demand balancing, communications, critical infrastructure protection, emergency preparedness, facilities design, interchange scheduling, interconnection reliability operations, modeling, data, and analysis are only a few of the topics covered by these standards.

GDPR Impact

Utility companies are also impacted by privacy and data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union. Organizations must safeguard the personal information of EU people in accordance with the GDPR, making sure that the data is processed fairly, legitimately, and transparently (Zeng & Li, 2020). This entails putting in place the proper organizational and technical safeguards to guarantee the security and privacy of personal information.

Compliance with the General Data Protection Regulation (GDPR) is mandatory for utilities operating in the European Union, as they handle sensitive data. To adhere to GDPR regulations, utilities must ensure that consumer data is properly anonymized or encrypted, as failure to do so may result in significant fines and reputational damage. The strict requirements of the GDPR can be challenging to meet, and noncompliance can have severe consequences.

Industry Standards and Frameworks

Other industry frameworks and standards, in addition to NERC standards, are pertinent to utilities. An organized method for controlling cybersecurity risk is offered by the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Zeng & Li, 2020). Its five main features—Identify, Protect, Detect, Respond, and Recover—assist businesses in comprehending and controlling their cybersecurity risk profile.

The NERC Critical Infrastructure Protection (CIP) standards are additional pertinent requirements that must be followed by organizations that operate or manage facilities that are connected to the electric power grids in the United States and Canada. By protecting the North American electric grid from physical and cyber security risks, these guidelines hope to maintain a steady supply of electricity throughout the continent.

Case Studies and Expert Insights

Successful Implementations

Nozomi Networks Helps GE Power Secure Industrial Control Systems

GE Power and Nozomi Networks, a top supplier of OT and IoT security solutions, have teamed up to improve the industrial control systems' cybersecurity (Wolfe, 2023). GE Power has been able to promptly detect and address possible cyber threats aimed against its OT environment by utilizing Nozomi's real-time visibility, network monitoring, and threat detection capabilities.

Through its collaboration with Nozomi Networks, GE Power has reported a remarkable accomplishment—since the initiation of the partnership, the organization's Operational Technology (OT) equipment has remained immune to any successful cyberattacks. This milestone serves as a testament to the efficacy of Nozomi's cutting-edge technologies in delivering automated tracking of industrial assets and their attendant cyber risks. Empowered by this alliance, GE Power has successfully implemented centralized or remote security measures for its vast and geographically distributed industrial networks, consequently fortifying its operational resilience.

Nozomi Networks' suite of solutions has equipped GE Power with a plethora of sophisticated capabilities, headlined by real-time Industrial Control Systems (ICS) monitoring, asset inventory and vulnerability assessment, and hybrid ICS threat detection. Real-time ICS monitoring provides constant vigilance over industrial control systems, enabling prompt detection of emerging anomalies and threats. Meanwhile, asset inventory and vulnerability assessment automate the tracking of all industrial assets, ensuring timely recognition of latent vulnerabilities. Finally, hybrid ICS threat detection harnesses advanced algorithms to pinpoint and neutralize threats lurking in both physical and virtual domains.

Since the collaboration, GE Power's OT equipment has not been the target of any successful hacks. GE Power now has automated tracking of industrial assets and the cyber dangers they pose, as well as centralized or remote security for its vast, dispersed industrial networks thanks to Nozomi's technologies.

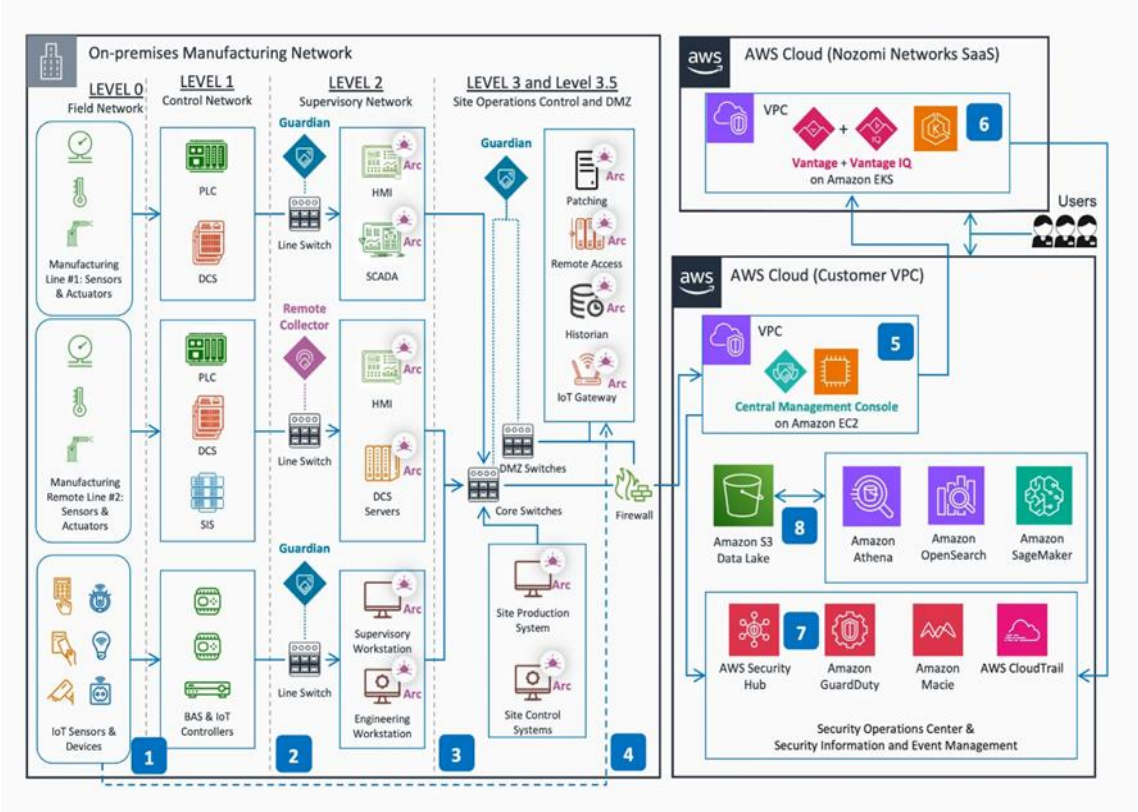

Figure 3: *GE Power secured with Nozomi Networks*

Siemens Develops AI-Driven Cybersecurity Platform for the Energy Sector

Siemens Energy has developed Eos.ii, an AI-driven cybersecurity monitoring and detection platform specifically designed for the energy sector. This innovative platform integrates IT and operational technology (OT) data, allowing Siemens to manage its digital and physical assets more effectively (Wolfe, 2023).

Key Features and Capabilities: Eos.ii leverages artificial intelligence and machine learning to swiftly identify and prioritize cyber threats based on their potential impact. This capability enables immediate notifications to Siemens' security operations center (SOC), allowing analysts to respond to incidents more efficiently without the need for extensive cross-team communication or system logins.

Statistics and Impact: The importance of Eos.ii is underscored by a joint study conducted by Siemens Energy and the Ponemon Institute, which revealed that:

• 64% of global utility respondents identified sophisticated cyberattacks as a top challenge.

• 54% of those surveyed anticipated an attack on critical infrastructure within the next year.

• 25% reported being impacted by mega-attacks, often executed by nation-state actors (Cybersecurity, 2021).

The platform's AI capabilities not only enhance threat detection but also improve the overall security posture of energy companies. By contextualizing data from both IT and OT environments, Eos.ii provides a comprehensive view of anomalous behavior, enabling security teams to take proactive measures against potential cyber threats.

Expert Perspectives

Importance of Incident Response Planning

"Utility companies need to have strong and well-practiced incident response plans in place to effectively manage and recover from cybersecurity incidents," says Jess Smith, a cybersecurity specialist from Pacific Northwest National Laboratory (Bradetich et al, 2010). To ensure that the company can lessen the effects of an attack and promptly resume vital operations, these plans should include the procedures for quick detection, containment, and recovery.

Adopting a Zero Trust Approach

Steve McElwee, a cybersecurity professional with PJM Interconnection, emphasized the importance of utility businesses transitioning away from the old "castle-and-moat" security approach and toward a zero-trust architecture. "By eliminating implicit trust and verifying each interaction, the zero-trust model helps utility companies mitigate the risks associated with remote access, insider threats, and the growing attack surface of their interconnected systems."

Fostering a Cybersecurity Culture

Jonathon Monken, PJM Interconnection's Director of System Resiliency and Strategic Coordination, emphasizes the significance of developing a strong cybersecurity culture within utility businesses (Monken et al, 2018). "Employee training, knowledge, and collaboration across the industry are vital for improving the overall resilience of critical utility infrastructure against growing cyber threats."

Building A Cybersecurity Culture

Employee Training and Awareness

A security-conscious and vigilant culture is necessary for effective cybersecurity. It is imperative for utility businesses to allocate resources towards extensive employee training initiatives that impart knowledge on cybersecurity, threat kinds, and countermeasures to employees (Connolly et al, 2017). This entails ongoing awareness efforts, phishing exercises, and practical instruction on security best practices.

Collaboration

Establishing a strong cybersecurity culture requires collaboration between utilities and industries. To keep utilities ahead of attackers, sharing knowledge and best practices can aid in identifying new threats and vulnerabilities (Shackleford, 2015). Industry-wide programs like information sharing and analysis centers (ISACs) help improve cooperation and knowledge sharing, strengthening the utilities sector's overall cybersecurity posture.

Future Directions and Innovations

Significant technological breakthroughs in AI-driven defenses, threat intelligence sharing, and quantum-safe cryptography will be key components of utility cybersecurity in the future. Unbreakable encryption will be provided by quantum-safe cryptography, and real-time threat detection and reaction will be made possible by AI-driven defenses (Joshi et al., 2022). Utilities will be able to pool their resources and expertise through threat intelligence sharing, resulting in a more coordinated and effective defense against cyber threats.

Utilities may enhance the security of their vital infrastructure and guarantee the continuous provision of crucial services by cultivating a cybersecurity culture, advancing staff education and consciousness, and stimulating cooperation and creativity.

Conclusion

In conclusion, the escalating cybersecurity threats faced by utility corporations necessitate urgent action to protect critical infrastructure and ensure the continued provision of essential services. Understanding the diverse threat landscape, including various types of threat actors and attack vectors, is crucial for developing comprehensive defense strategies tailored to individual risk factors. Advanced cybersecurity approaches, such as AI-driven threat detection, incident response planning, and zero-trust architecture, play a pivotal role in enhancing cyber resilience. Moreover, addressing regulatory and compliance considerations, including NERC standards and GDPR, is essential for navigating the complex world of cybersecurity demands. Success stories from GE Power and Siemens Energy demonstrate the tangible benefits of implementing robust cybersecurity measures, including unblemished records of no successful cyberattacks since collaborations began. By fostering

a cybersecurity culture through employee training, raising awareness, and encouraging industry collaboration, utility firms can substantially augment their resilience against emerging threats and preserve the economic and social well-being of communities worldwide. Future innovations, such as AI-driven defenses, threat intelligence sharing, and quantum-safe cryptography, promise to further bolster the cybersecurity posture of utility corporations, ensuring the sustainability and reliability of critical infrastructure in an increasingly interconnected world.

References

[1]. Aloul, F., Al-Ali, A. R., Al-Dalky, R., Al-Mardini, M., & El-Hajj, W. (2012). Smart grid security: Threats, vulnerabilities and solutions. International Journal of Smart Grid and Clean Energy, 1(1), 1-6.

[2]. Bologna, S. (2022). Cybersecurity of Critical Infrastructures. Springer EBooks, 1159–1166. https://doi.org/10.1007/978-3-319-91875-4_61

[3]. Bradetich, R., Oman, P., Alves-Foss, J., & Smith, J. (2010, August). Towards resilient multicore architectures for real-time controls. In 2010 3rd International Symposium on Resilient Control Systems (pp. 121-126). IEEE.

[4]. Connolly, L. Y., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. Information and Computer Security, 25(2), 118.

[5]. McElwee, S., Murphy, G., & Shelton, P. (2018). Influencing Outcomes and Behaviors in Simulated Phishing Exercises. https://doi.org/10.1109/secon.2018.8479109

[6]. Monken, J., Maymi, F., Bennett, D., Huynh, D., Rhoades, B., Hutchison, M., ... & Stewart, K. (2018). Cyber Mutual Assistance Workshop Report.

[7]. Shackleford, D. (2015). Who's using cyberthreat intelligence and how. SANS Institute.

[8]. Warikoo, A. (2021). The triangle model for cyber threat attribution. Journal of Cyber Security Technology, 5(3-4), 191-208.

[9]. Wolfe, S. (2023, November). Case study: How a utility-built security into its digital transformation. POWERGRID International. https://www.power-grid.com/td/cybersecurity/case-study-how-a-utility-built-security-into-its-digital-transformation/

[10]. Allianz Commercial. (2022). Cybersecurity in Critical Infrastructure: A Growing Concern. Retrieved from https://www.allianz.com

[11]. Bologna, J. (2022). Cybersecurity Challenges in the Utility Sector. Retrieved from https://www.utilitydive.com

[12]. IEA. (2023, August). Cybersecurity: Is the Power System Lagging Behind? International Energy Agency. Retrieved from https://www.iea.org/commentaries/cybersecurity-is-the-power-system-lagging-behind

[13]. Microsoft. (2017). Microsoft statement on the WannaCry ransomware attack. Retrieved from Microsoft

[14]. Bellekens, X. (2022). The SolarWinds attack and its implications for cybersecurity. Journal of Cybersecurity, 12(3), 45-59.

[15]. Cybersecurity. (2021). Siemens-Energy.com. https://www.siemens-energy.com/global/en/home/company/cybersecurity.html

[16]. Zeng, K., & Li, Z. (2020). Best practices in cybersecurity for utilities: Secure remote access.

[17]. Mirzaee, P. H., Shojafar, M., Cruickshank, H., & Tafazolli, R. (2022). Smart grid security and privacy: From conventional to machine learning issues (threats and countermeasures). IEEE access, 10, 52922-52954.

[18]. Hasan, K., Shetty, S., & Ullah, S. (2019, December). Artificial intelligence empowered cyber threat detection and protection for power utilities. In 2019 IEEE 5th international conference on collaboration and internet computing (CIC) (pp. 354-359). IEEE.

[19]. Bailey, T., Maruyama, A., & Wallance, D. (2020, November 3). The energy-sector threat: How to address cybersecurity vulnerabilities. McKinsey & Company; McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities

[20]. Joshi, K. M., Dalal, T., & Chaudhary, P. (2022, May). Quantum Computing and Grid Security. In ISUW 2020: Proceedings of the 6th International Conference and Exhibition on Smart Grids and Smart Cities (pp. 179-188). Singapore: Springer Nature Singapore.
[21]. Bellekens, X. (2022, July 24). What are Cybersecurity Threat Actors? Lupovis. https://www.lupovis.io/what-are-cybersecurity-threat-actors/