International Journal of Multidisciplinary Innovation and Research Methodology (IJMIRM)
ISSN: 2960-2068, Volume 4, Issue 1, January-March, 2025, Available online at:https://ijmirm.com

Cyber Threats and their Impact on Energy Efficiency

Sultan Aljabri

Sr. CS Specialist in Saudi Energy Efficiency Center (SEEC), Saudi Arabia

ABSTRACT

This paper focuses on analyzing the impact of cyber threats on energy efficiency, specially examining the relationship between them.Cyber threats have a direct impact on energy efficiency levels as they disrupt the system that manages, monitors, and perfects the energy usage. The growing dependence on digital infrastructure has also exposed the sector to an increased probability of cyber-attacks, which in turn affects energy efficiency.The paper highlights the ways in which cyber threats affect energy efficiency levels, such as disruption of energy systems, loss of optimal efficiency, false data inputs, and increased energy usage during recovery. Ukraine Power Grid Attack 2015 and 2016 and Colonial Pipeline Ransom Ware Attack (2021) are real time examples illustrated in paper that highlight the impact of cyber threats over energy efficiency. At last the paper includes measures to manage cyber threats like strengthening of cyber security, segmentation of network, strong backup system, and recovery plan. Cyber security is a critical concern in Saudi Arabia, and the country is making continuous efforts to address the challenges of cyber attacksin order to support energy efficiency, reliability, and security.The prompt implementation of security measures, upgrading the operational technology, and fostering security collaborations are the focus of the country on managing cyber threats and mitigating their impact on energy efficiency.

Keywords: Cyber Security, Cyber Threats, Energy Efficiency, Security, Risks, Digital, Infrastructure, SEEC, Measures, Challenges, Attacks, Recovery, Plan

INTRODUCTION

Cyber threats pose a significant risk to energy efficiency as they lead to reduced efficiency and increased energy usage with potential system failure. These threats undermine the security of energy systems. The relationship between cyber threats and energy efficiency is critical as the infrastructure of companies not only includes physical infrastructure but is also dependent on the strength of the digital defenses it buys. Cyber-attacks usually attack energy infrastructure, which causes operational disruption, energy wastage, and affects the optimization of systems which ultimately causes increased energy consumption (IEA, 2017). On the other hand, the growing dependence on digital infrastructure has also exposed the sector to an increased probability of cyber-attacks. Therefore, there is an interconnection between cyber threats and energy efficiency levels.

Cyber threats have a direct impact on energy efficiency levels as they disrupt the system that manages,monitors, and perfects the energy usage. The modern age’s infrastructure consists of smart grids; energy efficient systems and automated systems. These systems tend to depend on digital technologies in order to improve their effectiveness in energy usage and performance optimization. When these systems are attacked or infected, their ability and effectiveness is also compromised.

WAYS IN WHICH CYBER THREATS AFFECT ENERGY EFFICIENCY LEVELS

Disruption of the energy systems

Smart grids and smart control systems are energy management technologies designed to operate automatically in order to achieve maximum energy efficiency. Cyber-attacks force systems to shut down or operate in emergency mode where operational efficiency isa minimal level and the prime focus of the systems is also to prioritize safety over efficiency by which energy efficiency is compromised (IEA, 2017). This causes prolonged or temporary energy wastage due to malfunctioning of the systems. To manage the situation, the systems are prone to switch on manual mode, which is less optimized and consumes high energy.

Loss of optimized level of Efficiency

Today’s digital infrastructure is designed with the integration of IoT and artificial intelligence, making systems more energy-efficient and capable of optimizing energy consumption in real time (Krause, T, 2016). However, cyber-attacks or threats often target and disable optimization software, leading to energy wastage, poor load management, and increased energy demand

False Data Inputs for System Malfunctioning

Cyber-attacks often involve injecting false data inputs to manipulate sensors and smart meters, potentially compromising security systems. This can result in overheating, overcooling, overproduction, or underutilization of equipment—each of which negatively impacts system performance and energy efficiency.

Increased level of energy usage for reaching recovery mode

When a cyber-attack occurs, the system often undergoes full resets, hardware damage, and rebooting processes, all of which require additional power. These recovery efforts typically lead to high energy consumption, resulting in significant energy wastage.

Implementing high security systems to avoid cyber threats

To mitigate the risk of cyber threats, companies often implement robust security systems featuring multiple layers of authentication and regular security updates, which can increase energy consumption and infrastructure costs. Additionally, companies frequently overbuild backup systems and operate with high safety margins to safeguard their intellectual property. This strategy of excessive data and asset protection typically results in elevated baseline energy usage

SOME REAL-WORLD EXAMPLES THAT HIGHLIGHT THE IMPACT OF CYBER THREATS OVER ENERGY EFFICIENCY

Ukraine Power Grid Attack 2015 and 2016

In this attack, the hackers used spear-phishing emails to infect the systems with malware. Through this attack, the hackers gained control of the circuit breakers of energy distribution companies and disrupted the power supply to about 230,000 people for several hours (He, H., & Yan, 2016). To manage the situation, the operators had to switch the systems to manual mode which is a slower and less optimized version of operation. The frequent switching of the system to manual mode caused damage to the equipment, which led operators to operate the systems at a less efficient level in the future as well.

Colonial Pipeline Ransom Ware Attack (2021)

Darkside is a ransomware group that hacked the IT system of Colonial Pipeline. To avoid the attack affecting the entire pipeline operational system, the companyproactively shut down the entire pipeline operational system. These pipelines were the most energy efficient way to transport fuel and after their shutdown the fuel had to be transported by trucks and railways,which are less energy efficient modes. This resulted in a major fuel supply disruption across the East Coast of the United States that affected the fuel supply for cars and planes as well as for industries. Therefore, this cyber threat not only affected the fuel supply but also caused a chain reaction that rendered the entire fuel supply system less energy efficient, even several weeks after the attack.

Managing Cyber Threats to Affect Energy Effectiveness

The ways by which companies can fix energy effectiveness by limiting the chances of getting cyber threats are listed below:

Strengthening Cyber security for Energy Systems

Installing strong firewalls is an effective way to enhance energy efficiency while maintaining cybersecurity. The implementation of an intrusion detection system and enabling secure access controls are also effective ways to manage security against cyber threats, which ultimately lead to energy optimization. Regular updates to security software and systems are equally important to keep the security protocols updated with the latest cyber threats and to keep the system secure from cyber-attacks (He, H., & Yan, 2016). The Saudi Energy Efficiency Center (SEEC) has launched several initiatives to reduce energy consumption in Saudi Arabia’s Industrial sector. It has set policies and targets to improve energy efficiency in the industrial sector in the Kingdom. It also plans to study non targeted industrial sectors and identify appropriate mechanisms to improve the energy consumption efficiency. The implementation of energy management systems and the adoption of energy efficient technologies have resulted in substantial energy savings. Hence, Saudi Arabia is making significant strides in energy efficiency through comprehensive government policies, programs, and technological advancements.

Segmentation of Network

Segmenting energy control systems from IT operational units or systems can effectively reduce level of loss, as an attack on one system may not affect the other side of the network, whether it involves energy control or business operations. The use of strong authentication is also an effective method to avoid cyber-attacks such as multiple factor authentications for all critical controls (Gawade, A, 2022). Therefore, this segmentation can help in reducing the level of loss to the organization.

Usage of Strong Backup and Recovery Plan

Maintaining regular backups of system settings and data is essential for managing cyber incidents and minimizing data loss. Backups enable faster data restoration after an attack, reducing the impact on business operations. Coupled with a robust recovery plan, this approach helps ensure a swift, energy-efficient recovery with minimal downtime. Additionally, training employees to recognize phishing attempts and cyber-attacks—and to respond quickly—plays a crucial role in limiting the effects of such incidents.

Cyber Threats effect on the Energy Sector in Saudi Arabia

Cybersecurity remains a critical priority for Saudi Arabia, especially as the nation confronts increasing cyber-attacks targeting its vital infrastructure. Ongoing efforts to strengthen cyber defenses are essential to ensure the energy sector's efficiency, reliability, and overall security. Saudi Arabia has experienced 88 ransom ware incidents with the manufacturing sector closely linked to energy accounts for 25.41% of these attacks in 2024 (SOCRadar@Cyber Intelligence inc, 2025). Essential measures involve the swift deployment of security protocols, modernization of operational technologies, and the promotion of collaborative security efforts to effectively address cyber threats and reduce their impact on energy efficiency.Additionally, Saudi Arabia is strengthening regulatory compliance by enforcing mandatory cyber security regulations, ensuring that organizations align with established legal and security standards. The National Cybersecurity Authority (NCA) plays a central role in this effort by developing cyber security legislation and overseeing the enforcement of these regulations across all sectors.

It ensures that organizations adhere to rigorous cyber security standards, with a particular focus on protecting critical infrastructure such as the energy sector. In addition to these initiatives, Saudi Arabia has made significant investments in developing a skilled cyber security workforce. Taweiq Academy, in partnership with leading educational institutions, is responsible for delivering comprehensive training programs tailored to employees across various sectors. The academy focuses on equipping professionals with the expertise needed to address emerging cyber threats, while also preparing them to earn internationally recognized certifications such as CISA and CISM. These efforts are vital for cultivating a highly trained workforce capable of protecting critical infrastructure and securing the nation's energy systems against cyber threats.The AI driven cyber security segment is valued at $456.3 million in 2024 and is expected to reach $4.28 billion in 2033 (openpr.com, 2025).

CONCLUSION

Cyber threats pose a significant risk to energy efficiency by disrupting operations, damaging IT infrastructure, and forcing energy systems to operate below optimal efficiency. As companies increasingly rely on digital technologies, the threat of cyber-attacks is growing more alarming, driven by the rising demand for smart management and technological optimizationSecurity breaches result in energy losses, reduced system responsiveness, and diminished operational performance, all of which ultimately increase operational costs and management challenges. Therefore, to protect energy efficiency, organizations must prioritize cyber security alongside energy management by implementing robust defense systems (Venkatachary, 2025). Robust defense strategies and real-time management of the data with an effective response plan may lead to a situation where the limit of the loss can be facilitated with faster recovery and less data or operational loss (Gawade, A, 2022). This ultimately results in improved outcomes, ensuring greater energy efficiency, reduced downtime, and a faster recovery process for IT infrastructure.

Saudi Arabia is actively working to enhance its national cyber security framework and has established the National Cyber security Authority (NCA) as a regulatory body responsible for overseeing cyber security matters. The NCA develops guidelines, formulates regulations, enforces legal frameworks, and manages issues related to cyber threats across the country. Saudi Arabia created NCA with authority to take care of rules and regulations of cyber security governance and also to spread awareness about cyber security among all Saudi workers. Managing cyber security and reaching secured operations is considered as a national priority and is also important to achieve the Vision 2030 goals. The Saudi Energy Efficiency Center (SEEC) is aimed at improving energy effectiveness by building a strong balance between energy production and consumption for optimal management. This vision is reached through collaborating with local and international partners in both the private and public sectors (SEEC.gov.salen, 2025). Cyber threats not only compromise an organization's security but also negatively impact energy efficiency by making systems unstable, less optimized, and more conservative in their operations. To address this challenge, Saudi Arabia established the National Cyber security Authority (NCA), which is responsible for governing cybersecurity regulations and raising awareness among the national workforce. By ensuring the protection of critical energy systems, the NCA plays a vital role in maintaining and enhancing energy efficiency in today's increasingly connected world.

REFERENCES

[1]. International Energy Agency (IEA). (2017). Digitalization and Energy. https://www.iea.org/reports/digitalisation-and-energy

[2]. He, H., & Yan, J. (2016). Cyber-physical attacks and defenses in the smart grid: A survey. IET Cyber-Physical Systems: Theory & Applications, 1(1), 13-27. https://doi.org/10.1049/iet-cps.2015.0008

[3]. Gawade, A., &Shekokar, N. M. (2022). Impact of cyber security threats on IOT Applications. Cyber Security Threats and Challenges Facing Human Life, 71–80. https://doi.org/10.1201/9781003218555-8

[4]. *Cyber threats against the energy sector surge as global tensions mount*. Resecurity. (n.d.). https://www.resecurity.com/blog/article/cyber-threats-against-energy-sector-surge-global-tensions-mount

[5]. SEEC | Saudi Energy Efficiency Center | KSA. (n.d.). SEEC | Saudi Energy Efficiency Center | KSA. https://www.seec.gov.sa/en

[6]. Venkatachary, S. K. & P. (2025, January 1). *Cybersecurity and cyber-terrorism challenges to energy-relat*. International Journal of Critical Infrastructure Protection. https://ideas.repec.org/a/eee/ijocip/v45y2024ics1874548224000180.html

[7]. Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021, September 16). *Cybersecurity in power grids: Challenges and opportunities*. Sensors. https://pmc.ncbi.nlm.nih.gov/articles/PMC8473297/

[8]. *Welcome to Socradar's 2024 Saudi Arabia Threat Landscape Report!*SOCRadar® Cyber Intelligence Inc. (2025, January 2). https://socradar.io/socradars-2024-saudi-arabia-threat-landscape-report/?utm_source=chatgpt.com