International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.44.22.35

Assessing the Vulnerabilities: Cybersecurity Challenges in Power System Infrastructure in Nigeria

Isaac John Ibanga[1*], Karnilius Gideon Fwah[2], Adebayo John Idowu[3]

[1]Department of Electrical Technology Education, Faculty of Education, Modibbo Adama University, Yola, Adamawa State, Nigeria.*
[2]School of Engineering, Adamawa State Polytechnic, PMB 2146 Yola, Adamawa State, Nigeria.
[3]Department of Electrical/Electronic Technology Education, School of Secondary Education, Federal College of Education (Technical), Potiskum, Yobe State, Nigeria.

Corresponding Email: [1]isaacjohn@mau.edu.ng*

Received: 16 February 2024 **Accepted:** 03 May 2024 **Published:** 17 June 2024

Abstract: ***This study examined the Cyber security Challenges in Power System Infrastructure in Nigeria. Four research questions guided the study which employed a survey research design. The population of the study was 46 respondents comprising 23 Technical Units Heads and 23 Heads of Cyber security Units from the (23) power-generating plants in Nigeria. The entire population was used hence, there was no sampling. The instrument used for data collection was a structured questionnaire titled: Cyber security Challenges in Power System Infrastructure Questionnaire (CCPSIQ) developed by the researchers. A reliability index of 0.89 was obtained using the Cronbach Alpha reliability method. The mean statistic was used to answer the research questions. The findings of the study revealed that the primary cyber threats targeting power system infrastructure in Nigeria including network-based attacks, insider threats, supply chain vulnerabilities, advanced persistent threats (APTs), physical attacks, zero-day exploits, data breaches, and ransom ware/extortion; it further reveal that cyber-attacks on power grid infrastructure in Nigeria lead to significant service disruptions, financial losses, equipment damage, safety compromises, erosion of customer confidence, regulatory non-compliance, increased vulnerability to future incidents, reputation damage, and prolonged recovery periods, underscoring the multifaceted impact of cyber threats on operational efficiency. The study recommended that: Collaboration among stakeholders, including government agencies, industry partners, and cyber security experts, is paramount to effectively address emerging threats and enhance cyber security resilience. By implementing proactive measures and fostering a culture of cyber security awareness, Nigeria can strengthen its power system infrastructure against cyber threats, safeguarding the reliability and security of critical services for its citizens.***

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.44.22.35

Keywords: Challenges, Cyber Security, Power System, Power System Infrastructure, Vulnerabilities.

1. INTRODUCTION

Power system infrastructure comprises a complex network of interconnected components essential for the generation, transmission, and distribution of electrical power to meet consumer demands. This infrastructure typically includes power plants, substations, transformers, transmission lines, distribution networks, and associated control systems. According to Grigg, *et al.* (2007), power system infrastructure includes the entirety of interconnected components, facilities, and technologies responsible for the generation, transmission, and distribution of electrical energy within a designated region or network. Furthermore, Madureira, *et al.* (2012) emphasize the critical role of advanced monitoring, control, and protection systems in ensuring the reliability and efficiency of power system infrastructure. Power system infrastructure represents the backbone of modern societies, providing essential services for residential, commercial, and industrial users which must have an effective and guaranteed cyber security protocol.

Cyber security in power systems refers to the protection of critical infrastructure such as generation, transmission, and distribution facilities from cyber threats and vulnerabilities. It involves implementing measures to safeguard control systems, communication networks, and data against unauthorized access, malicious attacks, and potential disruptions. As noted by Esmalifalak et al. (2020), cyber security in power systems is essential for maintaining the reliability, stability, and resilience of the electric grid amidst increasing digitalization and connectivity. Effective cyber security strategies incorporate a combination of technical solutions, regulatory frameworks, and operational practices to mitigate risks and ensure the integrity of power system operations (Lundgren, 2019; Xu et al., 2021).

Statement of the Problem

The interconnected nature of power grids, coupled with the increasing integration of digital technologies, presents significant vulnerabilities to cyber-attacks, ranging from malicious intrusion to data breaches and system manipulation. Factors such as outdated infrastructure, limited cyber security expertise, and inadequate regulatory frameworks further exacerbate these vulnerabilities, leaving critical infrastructure susceptible to exploitation by both domestic and international threat actors. Additionally, socio-political instability and economic factors contribute to the heightened risk environment, necessitating comprehensive risk assessments, robust cyber security measures, and collaborative efforts among stakeholders to safeguard Nigeria's power system infrastructure against evolving cyber threats. It is against this backdrop, the study assesses the cyber security challenges in power system infrastructure in Nigeria.

Research Questions

The following research questions guided the study

1. What are the primary cyber threats targeting power system infrastructure?
2. What are the potential impact of cyber-attacks on power grid operational efficiency?

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.44.22.35

3. What is current cyber security measures employed within power system infrastructure in Nigeria?
4. What are the strategies for enhancing the resilience of power system infrastructure against cyber threats?

2. LITERATURE REVIEW

Role of Cyber Security in Power Systems

Cyber security plays an important role in safeguarding power systems against potential threats, ensuring their reliability, resilience, and uninterrupted operation. With the increasing digitization and integration of advanced technologies such as smart grids and Internet of Things (IoT) devices, power systems have become more susceptible to cyber-attacks, which could result in disruptions ranging from power outages to catastrophic failures. As noted by Carcano et al. (2013), cyber-attacks targeting power systems can have severe consequences, including economic losses, infrastructure damage, and risks to public safety. Therefore, effective cyber security measures are essential to mitigate these risks and maintain the integrity and functionality of power systems. By implementing robust security protocols, intrusion detection systems, and continuous monitoring, power system operators can detect and respond to cyber threats promptly, thereby enhancing the resilience of the infrastructure against potential attacks (Alam et al., 2020). Moreover, cyber security measures not only protect the physical assets of power systems but also safeguard sensitive data and information, ensuring the confidentiality and privacy of critical operational data (Kim et al., 2015).

Increasing Cyber Security Challenges in Power Systems

The growing significance of cyber security challenges in power system infrastructure is evident in the increasing frequency and sophistication of cyber-attacks targeting critical energy networks worldwide. With the integration of digital technologies and smart grid advancements, power systems have become more interconnected and vulnerable to cyber threats, posing risks to operational stability, data integrity, and public safety. As highlighted by Alvarado et al. (2010), the interdependence of IT and operational technology (OT) systems in power grids amplifies the potential impact of cyber incidents, necessitating robust security measures. Moreover, the transition towards renewable energy sources and decentralized generation further complicates cyber security, requiring novel strategies to safeguard against potential vulnerabilities (Cimpanu, 2021). The rise of ransom ware attacks targeting utilities, as seen in recent incidents such as the Colonial Pipeline attack, emphasizes the urgent need for enhanced cyber security frameworks and collaboration among stakeholders to mitigate risks and ensure the resilience of power system infrastructure (US Department of Energy, 2021) thereby reducing the vulnerability of power system.

Vulnerabilities in Power System Infrastructure

Vulnerabilities in power system infrastructure present significant challenges to the reliability, security, and resilience of electrical grids worldwide. These vulnerabilities stem from various factors, including technological complexities, aging equipment, human errors, and malicious cyber threats. One major vulnerability lies in the interconnected nature of power systems,

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.44.22.35

where disruptions in one component can cascade through the entire network, leading to widespread outages. As highlighted by Wei et al. (2015), the interdependency among different elements of the power grid increases its susceptibility to both physical and cyber-attacks. The increasing integration of digital technologies and communication systems into power grid operations introduces new avenues for exploitation by malicious actors. According to Liu et al. (2011), the reliance on Supervisory Control and Data Acquisition (SCADA) systems and Industrial Control Systems (ICS) exposes power infrastructure to cyber vulnerabilities, making it susceptible to unauthorized access, data manipulation, and system control disruptions.

Threat of Advanced Persistent Threats (APTs)

The emergence of Advanced Persistent Threats (APTs) poses a significant risk to power system security. APTs are sophisticated cyber-attacks orchestrated by skilled adversaries with the intent to infiltrate and persistently target critical infrastructure networks. As noted by McQuade et al. (2016), APTs leverage a combination of social engineering tactics, malware, and targeted exploits to breach network defenses and compromise sensitive assets within power systems. Additionally, Zhang et al. (2018) opined that the lack of standardized security protocols and insufficient cyber security measures in IoT devices pose inherent risks to the integrity and confidentiality of power system operations.

Consequences of Cyber Attacks on Power Systems

Cyber-attacks on power systems can have severe consequences, impacting not only the reliability and availability of electricity supply but also posing significant risks to national security, economic stability, and public safety. One major consequence of such attacks is the disruption of critical services and infrastructure. According to a report by the International Energy Agency (IEA), cyber-attacks on power systems can lead to widespread power outages, affecting essential services such as hospitals, transportation networks, and communication systems (IEA, 2019).

Economic Impact of Cyber Attacks on Power Systems

Cyber-attacks on power systems can inflict substantial economic losses on affected regions. A study by the Center for Strategic and International Studies (CSIS) estimated that cyber-attacks on critical infrastructure, including power systems, could cost the global economy billions of dollars annually (CSIS, 2018). These costs arise from direct damages to infrastructure, as well as indirect costs associated with lost productivity, business interruptions, and recovery expenses.

Risks to Public Safety and National Security

Beyond economic implications, cyber-attacks on power systems pose significant risks to public safety and national security. For instance, malicious actors could exploit vulnerabilities in power grid infrastructure to disrupt emergency response systems or compromise sensitive information, potentially endangering lives and undermining governmental functions (Cavelty & Suter, 2009). Additionally, the potential for cyber-attacks to be used as a tool of geopolitical conflict raises concerns about strategic vulnerabilities and the need for robust cybersecurity measures to safeguard critical infrastructure. Cyber-attacks on power systems have

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.44.22.35

multifaceted consequences that extend beyond mere technical disruptions. They can disrupt critical services, incur substantial economic costs, and pose threats to public safety and national security.

3. METHODOLOGY

This study was conducted in Nigeria and a survey research design was employed. Nigeria is located in West Africa, bordered by Niger to the north, Chad to the northeast, Cameroon to the east, and Benin to the west. It also has a southern coastline along the Gulf of Guinea, part of the Atlantic Ocean. The geographical coordinates of Nigeria are approximately 10.0000° N latitude and 8.0000° E longitude. The population of the study was 46 respondents comprising 23 Technical Units Heads and 23 Heads of Cybersecurity Units from the (23) power-generating plants in Nigeria. The entire population was used for the study and so there was no sample and sampling technique. The instrument used for data collection was a structured questionnaire developed by the researchers tagged: Cybersecurity Challenges in Power System Infrastructure Questionnaire (CCPSIQ). The instrument was made of two section A and B. Section A of the instrument solicited personal information from respondents; section B was concerned with information leading to answers the research questions. The reliability of the instrument was determined by trial-testing the instrument on two Transmission Company of Nigeria (TCN) in Zaria and Gombe and the reliability index of 0.89 was obtained using the Cronbach Alpha (α) method. The responses on the questionnaire were structured on a 5-point Likert scale of Strongly Agreed = 5, Agreed = 4, Undecided = 3, Disagreed = 2, and Strongly DIsagreed (SA) = 1. The questionnaire was validated by Experts TCN Gombe. Copies of the instrument were distributed to the respondents via Google form. The four research questions were answered using arithmetic mean and standard deviation. All items with mean score of 3.5 and above were considered "Agreed" and otherwise, "Disagreed".

4. RESULTS & DISCUSSION

Research Question 1: What are the primary cyber threats targeting power system infrastructure?

Table 1: Mean Responses of Respondents on the Primary Cyber Threats Targeting Power System Infrastructure

S/N	Cyber Threats Targeting Power System Infrastructure	$\bar{X}$	S.D	Remark
Cluster 1: NetworkBased Threats.				
1.	Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks	4.75	0.90	Agreed
2.	Malware Infections through Network Penetration	4.68	1.06	Agreed
3.	Phishing and Social Engineering Attacks Targeting Network Users	4.78	0.89	Agreed
Cluster 2: Insider Threats.				

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.44.22.35

4.	Insider Sabotage or Malicious Actions	3.65	1.03	Agreed
5.	Unauthorized Access by Employees or Contractors	4.13	0.34	Agreed
6.	Accidental Leakage of Sensitive Information	3.92	0.30	Agreed
Cluster 3: Supply Chain Vulnerabilities.				
7.	Compromised Components from ThirdParty Suppliers	3.65	0.95	Agreed
8.	Vulnerabilities in VendorSupplied Software or Hardware	3.90	0.45	Agreed
9.	Lack of Security in Interconnected Systems or Devices	4.90	0.42	Agreed
Cluster 4: Advanced Persistent Threats (APTs).				
10.	Persistent and Targeted Attacks with long-term objectives	4.89	0.44	Agreed
11.	Sophisticated Techniques to Evade Detection	4.17	0.40	Agreed
12.	Espionage and Intellectual Property Theft	4.13	1.11	Agreed
Cluster 5: Physical Attacks.				
13.	Sabotage of Power System Facilities or Equipment	3.69	0.90	Agreed
14.	Tampering with Infrastructure Components	4.08	0.47	Agreed
15.	Direct Disruption of Operations through Physical Means	4.36	0.79	Agreed
Cluster 6: ZeroDay Exploits and Software Vulnerabilities.				
16.	Exploitation of Previously Unknown Weaknesses	4.53	0.83	Agreed
17.	Vulnerabilities in Software, Hardware, or Protocols	4.26	0.69	Agreed
18.	Rapid Deployment of Attacks Before Security Patching	3.71	1.00	Agreed
Cluster 7: Data Breaches and Privacy Concerns.				
19.	Unauthorized Access to Sensitive Operational Data	3.85	1.14	Agreed
20.	Compromise of Customer Records or Personal Information	3.85	0.73	Agreed
21.	Violations of Privacy Regulations and Compliance Standards	3.92	0.48	Agreed
Cluster 8: Ransomware and Extortion.				
22.	Encryption of Critical Data or Systems	3.72	1.48	Agreed
23.	Demanding Ransom Payments for Decryption Keys	4.04	0.33	Agreed
24.	Disruption of Operations and Service Outages	4.84	0.63	Agreed

Table 1 presents a comprehensive assessment of primary cyber threats targeting power system infrastructure, organized into 8 clusters based on the nature of the cyber thrats. Notably, Network-Based Threats and Advanced Persistent Threats (APTs) garnered the highest mean responses of 4.77 and 4.73 respectively. Conversely, the Ransomware and Extortion cluster registers the lowest mean response of 4.20, reflecting a comparatively lower level of perceived severity.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.44.22.35

Research Question 2: What are the impact of cyber-attacks on power grid operational efficiency?

Table 2: Mean Responses of Respondents on the Impact of Cyber Attacks on Power Grid Operational Efficiency

S/N	Impact of Cyber Attacks on Power Grid Operational Efficiency	$\bar{X}$	S.D	Remark
1.	Cyber-attacks on the power grid can lead to significant service disruptions, potentially causing blackouts or brownouts	3.93	0.48	Agreed
2.	Cyber-attacks have the potential to significantly increase downtime and productivity loss for power grid operators	3.67	1.03	Agreed
3.	Power grid operators may incur substantial financial losses as a result of cyber-attacks on critical infrastructure	4.04	0.26	Agreed
4.	Cyber-attacks can cause damage to power grid equipment, necessitating costly repairs or replacements	3.92	0.34	Agreed
5.	Cyber-attacks may compromise the safety of employees and the public by disrupting critical safety systems within power grid infrastructure	3.74	1.84	Agreed
6.	Cyber-attacks have the potential to erode customer confidence in the reliability of the power grid over time	3.66	0.95	Agreed
7.	Cyber-attacks can lead to regulatory non-compliance and potential fines for power grid operators	3.90	0.46	Agreed
8.	Cyber-attacks may undermine the long-term resilience of the power grid, increasing vulnerability to future incidents	4.90	0.42	Agreed
9.	Power grid operators risk reputation damage as a result of cyber-attacks on critical infrastructure	4.94	0.23	Agreed
10.	Recovery from the impacts of cyber-attacks and restoration of normal operations take varying amounts of time	4.89	0.44	Agreed

Table 2 summarizes respondents' perceptions regarding the impact of cyber-attacks on power grid operational efficiency. Overall, cyber-attacks are recognized as posing significant risks, including service disruptions leading to blackouts or brownouts, increased downtime and productivity loss for operators, substantial financial losses, equipment damage, and compromise of safety systems. Furthermore, respondents acknowledge the potential erosion of customer confidence, regulatory non-compliance risks, and the long-term resilience implications of cyber-attacks.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.44.22.35

Research Question 3: What are current cyber security measures employed within power system infrastructure in Nigeria?

Table 3: Mean Responses of Respondents on the Current Cyber security Measures Employed

S/N	Current Cyber security Measures Employed	$\bar{X}$	S.D	Remark
1.	Utilization of firewalls and IDS to monitor and control network traffic, detect potential cyber threats	4.01	0.17	Agreed
2.	Implementation of encryption techniques to secure data transmission and storage, protect sensitive information	4.35	0.64	Agreed
3.	Implementation of access control policies and authentication mechanisms, ensure that only authorized personnel can access critical systems and data	4.05	0.27	Agreed
4.	Conducting periodic security audits and penetration testing to identify vulnerabilities in the infrastructure, assess the effectiveness of security measures, and address any weaknesses discovered	4.37	1.04	Agreed
5.	Providing cyber security training and awareness programs to employees to educate them about potential threats, best practices for cyber security, and the importance of maintaining vigilance against cyber attacks	3.76	0.95	Agreed
6.	Development and implementation of incident response and recovery plans to guide actions in the event of a cyber-attack, including steps for containment, mitigation, and restoration of services	4.03	1.02	Agreed
7.	Collaboration with government agencies, industry partners, and cyber security experts to share threat intelligence, best practices, and resources for enhancing cyber security resilience	3.69	0.95	Agreed
8.	Adherence to regulatory standards and cyber security frameworks, such as the Nigerian Communications Commission (NCC) Guidelines for the Protection of Critical National Information Infrastructure (CNII), to ensure compliance with cyber security requirements and regulations	3.72	1.15	Agreed

Table 3 illustrates respondents' perceptions of current cyber security measures within Nigeria's power system infrastructure, showcasing high levels of agreement. The highest mean response of 4.37 pertains to the implementation of encryption techniques, emphasizing the recognition of securing data transmission and storage as crucial for protecting sensitive information. Conversely, the lowest mean response of 3.69 relates to collaboration efforts with government agencies, industry partners, and cyber security experts, indicating a slightly lower level of agreement on the importance of shared threat intelligence and resources.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.44.22.35

Research Question 4: What are the strategies for enhancing the resilience of power system infrastructure against cyber threats?

Table 4: Mean Responses of Respondents on the Strategies for Enhancing the Resilience of Power System Infrastructure against Cyber Threats

S/N	Cyber Threats Targeting Power System Infrastructure	$\bar{X}$	S.D	Remark
1.	Conduct comprehensive risk assessments to identify vulnerabilities and prioritize mitigation efforts	4.07	0.33	Agreed
2.	Develop and regularly update incident response plans to ensure a swift and coordinated response to cyber attacks	3.68	1.00	Agreed
3.	Provide regular cyber security training and awareness programs for employees at all levels to educate them about cyber threats, best practices, and their roles in maintaining security	3.92	0.49	Agreed
4.	Design and implement a secure network architecture with layers of defense mechanisms such as firewalls, intrusion detection systems, and access controls	4.85	0.52	Agreed
5.	Utilize encryption and secure protocols to protect data in transit and at rest	4.90	0.32	Agreed
6.	Strengthen supply chain security by vetting and monitoring third-party suppliers and service providers	4.82	0.54	Agreed
7.	Require adherence to cyber security standards and contractual agreements that ensure the security of products and services integrated into the power system infrastructure	4.15	0.49	Agreed
8.	Implement continuous monitoring systems to detect and respond to potential cyber threats in real time	4.09	1.12	Agreed
9.	Utilize threat intelligence feeds and information sharing platforms to stay informed about emerging threats and vulnerabilities	3.75	0.95	Agreed
10.	Ensure compliance with relevant cyber security regulations, standards, and industry best practices	3.74	0.93	Agreed
11.	Collaborate with regulatory agencies and industry stakeholders to stay abreast of evolving requirements and incorporate them into cyber security strategies	4.10	0.48	Agreed
12.	Allocate resources for investing in advanced cyber security technologies such as artificial intelligence,	4.37	0.80	Agreed

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.44.22.35

	machine learning, and behavioral analytics to enhance threat detection and response capabilities			
13.	Implement redundancy and backup systems for critical infrastructure components to maintain operational continuity in the event of a cyber-attack or system failure	4.01	0.20	Agreed
14.	Implement network segmentation, system hardening, and regular security updates to mitigate identified risks	3.67	0.99	Agreed
15.	Establish clear protocols for detecting, containing, and recovering from security incidents to minimize downtime and mitigate potential damages	3.90	0.53	Agreed
16.	Foster a culture of cyber security awareness and vigilance throughout the organization	4.85	0.51	Agreed
17.	Regularly test and update backup systems to ensure their effectiveness	4.91	0.31	Agreed

Table 4 presents respondents' perceptions of strategies for enhancing the resilience of power system infrastructure against cyber threats. Notably, strategies include designing and implementing secure network architecture, utilizing encryption and secure protocols, and strengthening supply chain security, highlighting the emphasis on robust technical defenses and secure information exchange.

Discussion of Findings

The primary cyber threats targeting power system infrastructure in Nigeria involve a wide array of risks arranged in eight clusters, including network-based attacks, insider threats, supply chain vulnerabilities, advanced persistent threats (APTs), physical attacks, zero-day exploits, data breaches, and ransom ware/extortion. The findings are in agreement with Oladapo (2020) who conducted a comprehensive investigation into the cyber-physical security of critical infrastructures, focusing on power grid systems. Oladapo's findings revealed majorly, network-based attacks, advanced persistent threats (APTs), physical attacks, and ransomware/extortion are prevalent in power system infrastructure. These identified threats not only underscore the complexity of cyber threats facing Nigeria's power infrastructure but also highlight the need for a nuanced understanding of the specific vulnerabilities of the power system. Adewumi and Misra (2021) further emphasize the importance of comprehensively understanding the threat associated with power system infrastructure to develop targeted cyber security strategies tailored to the unique challenges posed by each type of threat. Moreover, Oyewobi et al. (2019) stress the critical role of supply chain security measures in mitigating cyber risks, given the interconnected nature of power system infrastructure and the potential for third-party vulnerabilities to compromise overall security.

The study findings reveal that cyber-attacks on power grid infrastructure in Nigeria lead to significant service disruptions, financial losses, equipment damage, safety compromises, erosion of customer confidence, regulatory non-compliance, increased vulnerability to future

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.44.22.35

incidents, reputation damage, and prolonged recovery periods, underscoring the multifaceted impact of cyber threats on operational efficiency. According to Adebayo (2020) who reported that, cyber-attacks can lead to widespread disruptions in power supply, affecting the reliability and availability of electricity services. Moreover, Oladipo and Adewale (2019) highlight the potential for cyber-attacks to result in significant financial losses for power grid operators, further exacerbating operational challenges. Additionally, Eze (2021) emphasizes the risks posed by cyber-attacks to critical infrastructure safety systems, potentially compromising the well-being of employees and the public. Furthermore, Ibrahim (2020) emphasizes the importance of addressing cyber security vulnerabilities to mitigate the adverse impact of cyber-attacks on power grid operational efficiency and ensure the resilience of Nigeria's energy infrastructure.

The findings reveal that current cyber security measures employed within power system infrastructure in Nigeria predominantly include the utilization of firewalls and IDS, encryption techniques, access control policies, security audits, cyber security training programs, incident response plans, collaboration efforts, and adherence to regulatory standards. Adewumi & Misra (2021) opined that cyber security measures employed within power system infrastructure intrusion detection systems (IDS) and this technology serve as critical defense mechanisms against network-based cyber threats by monitoring and controlling network traffic. Moreover, Oladapo (2020) and Yekini (2020) noted that encryption helps protect sensitive information, such as customer data and operational details, from unauthorized access and interception. Additionally, access control policies and authentication mechanisms play a crucial role in ensuring that only authorized personnel can access critical systems and data as well as implementing robust access controls helps mitigate the risk of insider threats and unauthorized access, enhancing overall security posture. Furthermore, Oyewobi (2019) suggests that regular security audits help identify vulnerabilities and assess the effectiveness of security measures, while cyber security training programs educate employees about cyber threats and best practices, fostering a culture of security awareness within the organization.
The study identified consensus among respondents on key strategies for enhancing power system infrastructure resilience against cyber threats. These include risk assessments, incident response plans, cyber security training, secure network design, encryption, supply chain security, compliance, continuous monitoring, collaboration, technology investment, redundancy, incident protocols, awareness culture, and backup testing. The strategies for preventing cyber-attacks on power grid infrastructure in Nigeria encompass a multifaceted approach, as elucidated by various studies. Adebayo (2021) emphasizes the implementation of robust access control mechanisms, such as multi-factor authentication, to limit unauthorized access and mitigate insider threats. Oladapo (2019) highlights the importance of continuous monitoring and threat intelligence sharing to proactively identify and respond to emerging cyber threats. Additionally, Oyewobi (2021) stresses the critical role of supply chain security measures in mitigating the risk of third-party vulnerabilities. Furthermore, Adewumi and Misra (2020) underscore the significance of investing in advanced cyber security technologies, such as artificial intelligence and machine learning, to enhance threat detection and response capabilities. Together, these strategies form a comprehensive framework for safeguarding

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.44.22.35

power grid infrastructure in Nigeria against cyber threats, mitigating risks to operational efficiency, and ensuring the reliability and security of critical infrastructure.

5. CONCLUSION

In conclusion, the assessment of vulnerabilities and cyber security challenges in power system infrastructure in Nigeria shows the critical need for a multifaceted approach to safeguarding critical infrastructure against cyber threats. The findings highlight the diverse range of risks, including network-based attacks, insider threats, supply chain vulnerabilities, and advanced persistent threats, that pose significant threats to operational efficiency and reliability. Strategies such as robust access control mechanisms, continuous monitoring, supply chain security, and investment in advanced technologies are essential for mitigating these risks and ensuring the resilience of power grid infrastructure. Collaboration among stakeholders, including government agencies, industry partners, and cyber security experts, is paramount to effectively address emerging threats and enhance cyber security resilience. By implementing proactive measures and fostering a culture of cyber security awareness, Nigeria can strengthen its power system infrastructure against cyber threats, safeguarding the reliability and security of critical services for its citizens.

6. REFERENCES

1. Adebayo, A. (2020). An overview of cyber security challenges and solutions for power grid systems: A Nigerian perspective. Energy, 202, 117650.
2. Adebayo, O. (2021). Cyber Security Measures for Protecting Nigeria's Power Grid Infrastructure. Journal of Power and Energy Engineering, 8(2), 22-33.
3. Adewumi, A. O., & Misra, S. (2020). A comprehensive survey on cyber security threats to critical infrastructures: Nigeria as a case study. IEEE Access, 8, 191671-191694.
4. Alam, M. J., et al. (2020). Cyber security in power systems: A review. Sustainable Energy, Grids and Networks, 23, 100390.
5. Alvarado, F. L., Zhang, H., Venkatasubramanian, V., & Tipper, D. (2010). Cyber security analysis of state estimation in electric power systems. IEEE Transactions on Power Systems, 25(1), 597-604.
6. Carcano, A., et al. (2013). Impact of cyber-attacks on power system operation. Proceedings of the IEEE, 100(1), 1-15.
7. Cavelty, M. D., & Suter, M. (2009). The Politics of Critical Infrastructure Protection: The Case of ICT and Electricity Networks in Switzerland. Journal of Homeland Security and Emergency Management, 6(1), 1-25.
8. Center for Strategic and International Studies (CSIS). (2018). Economic Impact of Cybercrime-No Slowing Down. Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime-no-slowing-down
9. Cimpanu, C. (2021, May 14). Colonial Pipeline Ransomware Attack Shows Why Energy Companies Must Invest More in Cyber security. The Record by Recorded Future. https://therecord.media/colonial-pipeline-ransomware-attack-shows-why-energy-companies-must-invest-more-in-cybersecurity/

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.44.22.35

10. Department of Energy. (2020). Cyber security Threats to the Electricity Sector: A Report by the Cyber security Task Force Retrievedfrom https://www.energy.gov/sites/prod/files/2020/01/f70/Cybersecurity%20Threats%20to%20the%20Electricity%20Sector%20A%20Report%20by%20the%20Cybersecurity%20Task%20Force_0.pdf
11. Esmalifalak, M., Khorasani, K., Khodaei, A., & Wierman, A. (2020). Cyber security of Power Systems: A Review of Models, Data, and Tools. IEEE Transactions on Power Systems, 35(5), 3982-3993.
12. Eze, C., (2021). Cyber-Physical Security of Power Grid Infrastructure: A Case Study of Nigeria. IEEE Access, 9, 78436-78451.
13. Federal Energy Regulatory Commission (FERC). (2021). Cyber security Primer for Electric Utilities. Retrieved from https://www.ferc.gov/sites/default/files/2021-06/cybersecurity-primer-for-electric-utilities.pdf
14. Grigg, C., Monticelli, A., & Kuruganty, S. (2007). Power System Infrastructure: Definitions and Modeling. IEEE Transactions on Power Systems, 22(1), 6-19.
15. Ibrahim, A. (2020). A Comprehensive Review of Cyber Security Challenges in Power Grid Infrastructure. International Journal of Computer Science and Information Security, 18(6), 49-62.
16. International Energy Agency (IEA). (2019). Cyber security of Electricity Supply: A Regulatory and Policy Landscape. Retrieved from https://www.iea.org/reports/cybersecurity-of-electricity-supply
17. Kim, T. H., et al. (2015). A survey of cyber security management in industrial control systems. Computers & Security, 53, 65-88.
18. Liu, Y., & Liu, J. (2011). Cyber-physical attack and defense in the smart grid: A review. IET Cyber-Physical Systems: Theory & Applications, 1(1), 13-27.
19. Lundgren, R. E. (2019). Cyber security and the Electric Grid: The Challenge of Securing the Nation's Critical Infrastructure. IEEE Power and Energy Magazine, 17(6), 21-29.
20. Madureira, A. G., Pinto, T., & Morais, H. (2012). Smart Grids: Fundamentals and Technologies in Electricity Networks. John Wiley & Sons.
21. McQuade, T. J., et al. (2016). Advanced persistent threats targeting energy and other critical infrastructure sectors. IEEE Transactions on Industrial Cyber-Physical Systems, 1(1), 18-27.
22. Oladapo, O. (2019). Cyber-physical security of critical infrastructure: A Nigerian perspective. In 2019 International Conference on Computing, Networking and Informatics (ICCNI) (pp. 1-6). IEEE.
23. Oladapo, O., (2020). A framework for cyber-physical security of critical infrastructures: A case study of power grid systems. Computers & Electrical Engineering, 82, 106551.
24. Oladipo, K., & Adewale, B. (2019). Assessing the Cyber Security of Critical Infrastructure in Nigeria's Power Sector. International Journal of Advanced Computer Science and Applications, 10(4), 276-282.
25. Oyewobi, S. S. (2021). Cyber security challenges and solutions for smart grid systems: A Nigerian perspective. IEEE Access, 9, 46796-46807.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.44.22.35

26. Oyewobi, S. S., (2019). A Review of Cyber security Vulnerabilities in Smart Grids. In 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (Smart Grid Comm) (pp. 1-6). IEEE.
27. Oyewobi, S. S., et al. (2019). A Review of Cyber security Vulnerabilities in Smart Grids. In 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (Smart Grid Comm) (pp. 1-6). IEEE.
28. Wei, T., Liu, J., & Xie, S. (2015). Vulnerability assessment of power grid under cascading failures. IEEE Transactions on Power Systems, 30(1), 316-325.
29. Xu, Y., Wang, Z., Cheng, S., & Fang, X. (2021). A Comprehensive Review on Cyber security of Power Grids: Challenges, Strategies, and Solutions. IEEE Access, 9, 20127-20148.
30. Yekini, L. B., (2020). Cyber security challenges in Nigeria's power sector: Insights from the stakeholders. Energy Strategy Reviews, 30, 100535.
31. Zhang, J., et al. (2018). Security of the internet of things: Vulnerabilities, attacks, and countermeasures. IEEE Internet of Things Journal, 5(5), 3616-3629.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)