International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 04 Apr. 2024, pp: 904-913 www.ijaem.net ISSN: 2395-5252

Advancing Cybersecurity Resilience in Edo State through Effective Cyber Hygiene Initiatives

Clement Agbeboaye[1], Joshua Okoekhian[2]
[1,2]*Department of Electrical/Electronic Engineering Technology, National Institute of Construction Technology and Management, Uromi, Edo State, Nigeria.*

Date of Submission: 18-04-2024 Date of Acceptance: 28-04-2024

ABSTRACT
Like many other regions, Edo State faces evolving cyber threats that necessitate proactive measures to safeguard critical infrastructure, sensitive data, and individual privacy. This research investigates the state of cybersecurity resilience in Edo State, Nigeria, considering various stakeholders across public and private sectors. The study employs a multifaceted approach, combining surveys, interviews, and documentary analysis to gather comprehensive data on cybersecurity practices and challenges. A total of 300 survey questionnaires were distributed, with 294 valid responses received, complemented by semi-structured interviews with key stakeholders. Thematic analysis techniques were applied to qualitative data obtained from interviews. Quantitative data collected from the survey questionnaires underwent statistical analysis using descriptive statistics such as frequencies and percentages. The study reveals a diverse demographic profile of respondents and highlights gaps in cybersecurity knowledge, awareness, and practices. Findings indicate varying levels of awareness and adherence to cybersecurity measures, with notable challenges including awareness gaps, inconsistent software updates, and limited resources for cybersecurity initiatives. Additionally, the study identifies critical disparities between the current state and the ideal state of cybersecurity resilience, emphasizing the need for concerted efforts to bridge these gaps. Based on the findings, recommendations were proposed to enhance cybersecurity resilience in Edo State.

Keywords: Cybersecurity Resilience, Cyber Hygiene Initiatives, Edo State, Cyber Threats, Information Security

I. INTRODUCTION

In an increasingly digitized world, where interconnected systems and ubiquitous internet connectivity underpin critical aspects of society, cybersecurity has emerged as a paramount concern. Globally, over one million users fall prey to some form of cybercrime every day [1] – [4]. The proliferation of cyber threats, ranging from data breaches and ransomware attacks to sophisticated state-sponsored cyber espionage, underlines the imperative of robust cybersecurity measures to safeguard individuals, organizations, and nations against malicious actors seeking to exploit vulnerabilities in digital infrastructure. The Internet and increased use of personal computer in recent years has provided a refuge for a multitude of computer-based crimes [5]. Within this setting, Nigeria, like many other countries, faces significant cybersecurity challenges, characterized by a rapidly evolving threat, inadequate cybersecurity awareness, and the growing digitization of services across various sectors.

Edo State, located in the southern region of Nigeria, has made significant strides in embracing digital technologies for various aspects of governance, commerce, and daily life. The state has witnessed a surge in internet penetration, mobile device usage, and the adoption of online platforms for communication, transactions, and data sharing. While these advancements have brought immense convenience and opportunities, they have also exposed the state to a myriad of cybersecurity threats. The escalating cyber threats in Edo State encompass a wide range of issues, including data breaches, phishing attacks, ransomware, identity theft, critical infrastructure vulnerabilities, insufficient cyber hygiene, and limited cybersecurity resources.

In addressing these multifaceted challenges, it is crucial to recognize that cybersecurity is not solely a technical matter; it is also deeply rooted in human behaviour, awareness, and practices. Cyber hygiene, akin to personal hygiene, represents the collective habits, routines, and behaviours that individuals and organizations

adopt to maintain their digital well-being. Effective cyber hygiene initiatives encompass a spectrum of activities, including education and awareness, password management, safe browsing, regular software updates, incident response plans, and collaboration and partnerships.

This research aspires to empower individuals, businesses, educational institutions, and government agencies in Edo State with the knowledge and tools they need to navigate the digital world securely. Through effective cyber hygiene initiatives, we envision a future where Edo State's citizens are better equipped to protect themselves and their digital assets from cyber threats, ultimately contributing to a safer and more secure digital environment.

II. REVIEW OF RELATED LITERATURE

In an era dominated by digitalization, the importance of cybersecurity cannot be overstated. With cyber threats becoming increasingly sophisticated and pervasive, individuals, organizations, and governments alike are compelled to fortify their digital defenses. This section examines existing research and practices, offering insights into the current trends and paving the way for a comprehensive investigation into how effective awareness campaigns can enhance cybersecurity resilience in Edo state.

In their work [6] examined the intricate landscape of Cyber Security Awareness Campaigns, aiming to pinpoint key factors contributing to their inability to effect behavioral change effectively. This study takes a psychological perspective, emphasizing the significance of comprehending individuals' risk perceptions in shaping effective awareness campaigns. Effective behavioural change necessitates not only the provision of risk information but also the recipients' capacity to understand and implement the guidance, coupled with the motivation to do so. The study explores the appropriateness of persuasion techniques, including the common use of 'fear appeals,' and identifies essential components and success/failure factors for awareness campaigns. Additionally, it offers insights by examining awareness campaigns in different cultural contexts, such as the UK and Africa.

The study carried out by [7] investigated cyber-hygiene as a key concept of cybersecurity in cyberspace. Cyberspace, interconnecting various devices and technologies, demands meticulous rules and regulations, referred to as 'Cyber-hygiene,' to ensure its cleanliness and security. The study explores cyberspace, its associated challenges, and the importance of maintaining proper cyber-hygiene practices. The authors emphasize that Cyber Hygiene is pivotal for safeguarding individuals and organizations against cyber threats, attackers, and risks, offering enhanced protection, security, and network maintenance.

The authors of [8] carried out an in-depth examination of optimizing investments in Cyber Hygiene, specifically aimed at safeguarding healthcare users. Cyber hygiene measures are crucial for enhancing an organization's security, particularly against social engineering attacks. The study introduces the Optimal Safeguards Tool (OST), an innovative framework that leverages game theory and combinatorial optimization to select cyber hygiene safeguards optimally. The model factors in various elements, including the probability of user group attacks, asset value, control effectiveness, and indirect costs associated with employee training. The study evaluates OST in a healthcare context, showcasing its advantages over alternative defending strategies.

In his work [9] conducted a critical analysis of cyber security and resilience in Nigeria. This study explores the extent of cyber security and resilience in the country, focusing on professionals in computer science, computer engineering, and security agents with exposure to computer science. Utilizing a descriptive survey research design and stratified random sampling, the study collects data through the "Cyber Security and Resilience Questionnaire" (CSRQ). Analysis of the data reveals that Nigeria has faced significant cyber-attacks, emphasizing the importance of cyber security and resilience in countering cyber risks. The study recommends building upon initiatives like the Global Community Engagement and Resilience Fund (GCERF) to enhance resilience against cyber-attacks.

The study carried out by [10] investigated digital forensic analysis for enhancing information security. The study aimed to simulate digital crime scenarios and conduct forensic and anti-forensic analyses to fortify security measures. Employing various forensic and anti-forensic tools and techniques, data from the simulations were analyzed. The findings highlighted that, despite the challenges posed by digital crimes, sophisticated forensic and anti-forensic tools can facilitate successful investigations.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 04 Apr. 2024, pp: 904-913 www.ijaem.net ISSN: 2395-5252

III. RESEARCH METHODOLOGY

.A. Study Area

The study was conducted in Edo State, Nigeria, targeting various stakeholders including government officials, IT professionals, business owners, employees (non-IT), and students within public and private sector organizations across the state. Edo State's diverse setting, spanning urban areas, rural communities, government institutions, and private enterprises, provides a rich context for examining cybersecurity resilience. With a population exceeding 3 million people, Edo State offers a representative snapshot of Nigeria's socio-economic environment. Key areas of focus include urban centers like Benin City, rural communities, government institutions, and private enterprises across industries such as manufacturing, finance, and healthcare.

B. Method of Data Collection

To collect comprehensive data on the current state of cybersecurity practices and challenges in Edo State, a multifaceted approach was utilized. This involved the distribution of structured survey questionnaires to professionals, employees (both IT and non-IT), business owners, and students across various sectors in the state. These surveys covered topics such as cybersecurity knowledge, awareness, cyber hygiene practices, experiences with cyber threats, and perceptions of existing cybersecurity initiatives. Additionally, semi-structured interviews were conducted with key stakeholders including government officials, IT administrators, cybersecurity specialists, and business leaders to obtain qualitative insights into the existing cybersecurity infrastructure, policies, challenges, and perceptions of cybersecurity resilience. Simultaneously, relevant documents such as cybersecurity policies, reports, and public awareness campaigns were collected and analyzed to supplement the data obtained from surveys and interviews. This comprehensive approach, combining survey questionnaires, in-depth interviews, and documentary analysis, aims to provide a thorough understanding of cybersecurity awareness, practices, and challenges in Edo State.

C. Sample Size and Sampling Technique

The sample size for this study was determined based on the population of interest and the desired level of precision. A total of 300 survey questionnaires were distributed to professionals, employees, business owners, and students across various sectors in Edo State. The sampling technique employed was a combination of convenience sampling and stratified random sampling. Convenience sampling was used to select participants who were readily accessible and willing to participate in the study, thereby facilitating the data collection process. However, to ensure the representation of diverse demographics and sectors within the state, the sample was stratified based on factors such as occupation, industry, and geographic location. This allowed for the inclusion of participants from urban and rural areas, different sectors (e.g., government, private, academia), and various job roles (e.g., IT professionals, non-IT employees, business owners). Out of the 300 questionnaires distributed, a total of 294 were returned, resulting in a response rate of 98%. The high response rate indicates a strong level of engagement from the participants and enhances the reliability of the collected data. The sample size of 294 provides sufficient statistical power to analyze the data, identify trends, and draw meaningful conclusions regarding cybersecurity awareness, practices, and challenges in Edo State.

D. Data Analysis

The data obtained from the survey questionnaires, in-depth interviews, and documentary analysis was subjected to a rigorous analysis process to extract meaningful insights into cybersecurity awareness, practices, and challenges in Edo State. The analysis consisted of the following:

a. Quantitative Analysis

The quantitative data collected from the survey questionnaires were subjected to statistical analysis using Microsoft Excel statistical software. Descriptive statistics, including frequencies and percentages were used to summarize the respondents' demographics, cybersecurity knowledge, awareness levels, cyber hygiene practices, threats and incidents, and public campaigns and initiatives awareness.

b. Qualitative Analysis

The qualitative data obtained from in-depth interviews and documentary analysis was analyzed using thematic analysis techniques. Transcripts of the interviews and relevant documents were categorized to identify key themes, issues, and challenges related to cybersecurity resilience and cyber hygiene practices in Edo State. These thematic categories were then systematically analyzed to uncover patterns, discrepancies, and insights that emerge from the qualitative data.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 04 Apr. 2024, pp: 904-913 www.ijaem.net ISSN: 2395-5252

c. Gap Analysis

The gap analysis was conducted and defined by the following:

- Identifying and defining the current state of cybersecurity practices in Edo State
- Defining an ideal state based on established cybersecurity standards and best practices
- Identifying the gaps between the two states.

This analysis helped to highlight areas where improvements and cyber hygiene initiatives are needed, guiding the development of recommendations and strategies for enhancing cybersecurity resilience in the state.

IV. RESULTS AND DISCUSSION

a. Quantitative Analysis

Table 1: Age of Respondents

Age Group (Yrs)	Frequency	Percentage	Cumulative Percentage
18 – 25	126	42.9	42.9
26 – 35	84	28.6	71.5
36 – 45	63	21.4	92.9
46 – 55	21	7.1	100
Total	294	100	

Source: Field Data, 2024.

The age distribution of the respondents indicates a diverse demographic profile, with the majority (42.9%) falling in the 18-25 age group. This suggests a significant presence of younger individuals, potentially reflecting their higher exposure to digital technologies and online activities. The distribution across other age groups is relatively evenly distributed, indicating representation across different age cohorts.

Table 2: Gender of Respondents

Sex	Frequency	Percentage	Cumulative Percentage
Male	147	50	50
Female	147	50	100
Total	294	100	

Source: Field Data, 2024.

The gender distribution of respondents is evenly split, with 50% male and 50% female participants. This gender parity suggests a balanced representation of perspectives and experiences in the study, contributing to the overall validity and reliability of the findings. It also reflects a positive trend towards gender inclusivity in discussions around cybersecurity resilience.

Table 3: Respondents' Occupation

Occupation	Frequency	Percentage	Cumulative Percentage
Students	89	30.3	30.3
IT Professionals	54	18.4	48.7
Business Owner	66	22.5	71.2
Employee (non-IT)	36	12.2	83.4
Government Official	49	16.7	100
Total	294	100	

Source: Field Data, 2024.

The occupation of respondents provides insights into the diversity of stakeholders involved in cybersecurity resilience efforts in Edo State. The presence of students, IT professionals, business owners, employees (non-IT), and government officials highlights the multi-stakeholder nature of cybersecurity governance and underscores the importance of collaboration across sectors for effective cybersecurity management.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 04 Apr. 2024, pp: 904-913 www.ijaem.net ISSN: 2395-5252

Table 4: Cybersecurity Awareness and Knowledge

How would you rate your overall knowledge of cybersecurity?	Frequency	Percentage	Cumulative Percentage
Very low	19	6.5	6.5
Low	23	7.8	14.3
Moderate	168	57.1	71.4
High	63	21.4	92.8
Very High	21	7.1	100
Total	294	100	
How often do you update your knowledge of cybersecurity best practices?	Frequency	Percentage	Cumulative Percentage
Daily	40	13.6	13.6
Weekly	21	7.1	20.7
Monthly	23	7.8	28.5
Rarely	168	57.1	85.6
Never	42	14.3	100
Total	294	100	
Have you received any formal training or education in cybersecurity?	Frequency	Percentage	Cumulative Percentage
Yes	105	35.7	35.7
No	189	64.3	100
Total	294	100	

Source: Field Data, 2024.

The analysis of cybersecurity awareness and knowledge among respondents reveals a mixed background of understanding and practices. When asked to rate their overall knowledge of cybersecurity, the majority of respondents (57.1%) reported a moderate level of awareness, followed by 21.4% with a high level and 7.1% with a very high level. However, notable proportions also reported low to very low levels of knowledge (14.3%). Regarding the frequency of updating cybersecurity knowledge, a significant portion (57.1%) indicated rare updates or no updates at all, with only 13.6% reporting daily updates. This suggests potential gaps in staying abreast of evolving cyber threats and best practices. Furthermore, while 35.7% of respondents reported receiving formal training or education in cybersecurity, a majority (64.3%) indicated no such training, indicating a need for enhanced educational initiatives to improve cybersecurity literacy among the populace. Overall, the findings underscore the importance of continuous education and awareness initiatives to bridge knowledge gaps and promote proactive cybersecurity practices in Edo State.

Table 5: Cyber Hygiene Practices

Do you regularly update your software and operating systems to protect against vulnerabilities?	Frequency	Percentage	Cumulative Percentage
Always	20	6.8	6.8
Often	85	28.9	35.7
Sometimes	104	35.4	71.1
Rarely	85	28.9	100
Total	294	100	
Do you use strong, unique passwords for your online accounts?	Frequency	Percentage	Cumulative Percentage
Always	209	71.1	71.1
Often	22	7.5	78.6
Sometimes	21	7.1	85.7
Rarely	23	7.8	7.8

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 04 Apr. 2024, pp: 904-913 www.ijaem.net ISSN: 2395-5252

Never	19	6.5	100
Total	294	100	
Do you use public Wi-Fi networks without taking additional security precautions?	Frequency	Percentage	Cumulative Percentage
Always	Nil	0.0	0.0
Sometimes	Nil	0.0	0.0
Rarely	103	35	35
Never	191	65	100
Total	294	100	
Have you enabled two-factor authentication (2FA) where available?	Frequency	Percentage	Cumulative Percentage
Yes, for all accounts	231	78.6	78.6
Yes, for some accounts	44	15	93.6
No	19	6.5	100
Total	294	100	

Source: Field Data, 2024.

The analysis of cyber hygiene practices among respondents reveals a varied approach to safeguarding online security. While a majority (71.1%) reported using strong, unique passwords for their online accounts, indicating a positive adherence to a fundamental security measure, there are notable disparities in other areas. Regarding software updates, a significant portion of respondents (35.4%) reported only updating their software and operating systems sometimes, suggesting a potential gap in proactive vulnerability management. Additionally, a substantial proportion (65%) indicated never using public Wi-Fi networks, signifying a cautious approach to avoiding potential security risks associated with these networks. Also, a positive trend emerged with the adoption of two-factor authentication (2FA), with 78.6% enabling it for all accounts, indicating a proactive approach to enhancing account security. Overall, while there are strengths in certain practices, such as password management and 2FA adoption, there is a need for improved awareness and adherence to best practices, particularly in areas such as software updates, to mitigate cyber threats effectively.

Table 6: Cyber Threats and Incidents

Have you or your organization experienced any cyber threats or incidents in the past year?	Frequency	Percentage	Cumulative Percentage
Yes	85	28.9	28.9
No	209	71.1	100
Total	294	100	

Source: Field Data, 2024.

The analysis of cyber threats and incidents among respondents indicates a significant presence of such incidents within the past years, with 28.9% of respondents reporting experiences. This finding outlines the persistent nature of cyber threats in Edo State and highlights the importance of strengthening cybersecurity measures to mitigate risks and enhance resilience. The prevalence of cyber threats emphasizes the need for proactive strategies and robust defenses to safeguard against potential attacks and mitigate their impact on individuals and organizations.

Table 7: Public Awareness Campaigns and Initiatives

Are you aware of any public awareness campaigns or initiatives related to cybersecurity in Edo State?	Frequency	Percentage	Cumulative Percentage
Yes	62	21.1	21.1

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 04 Apr. 2024, pp: 904-913 www.ijaem.net ISSN: 2395-5252

No	232	78.9	100
Total	294	100	

Source: Field Data, 2024.

The knowledge of public awareness campaigns or initiatives related to cybersecurity appears relatively low among respondents, with only 21.1% indicating awareness. This finding suggests potential gaps in communication and outreach efforts, indicating the need for increased efforts to raise awareness about cybersecurity issues and promote educational initiatives in Edo State. Improving public awareness and understanding of cybersecurity risks and best practices is crucial for empowering individuals and organizations to protect themselves against cyber threats effectively. Enhanced awareness campaigns and initiatives can play a vital role in building a cyber-resilient community and fostering a culture of cybersecurity awareness and vigilance.

b. Qualitative Analysis

The qualitative data obtained from in-depth interviews with 20 respondents was analyzed using thematic analysis techniques. Transcripts of the interviews were categorized to identify key themes, issues, and challenges related to cybersecurity resilience and cyber hygiene practices in Edo State. These thematic categories were then systematically analyzed to uncover patterns, discrepancies, and insights that emerged from the qualitative data.

Interview Questions and Responses

1. Question: How would you define cybersecurity in your own words? The responses from all 20 respondents highlighted a common understanding of cybersecurity as the protection of digital assets and information from various cyber threats. Key themes included the proactive nature of cybersecurity, the importance of safeguarding sensitive information, and the role of technology and awareness in maintaining security.
2. Question: Can you share any experiences or encounters with cyber threats in your personal or professional life? Respondents shared a range of experiences with cyber threats, including phishing scams, malware infections, and ransomware attacks. These firsthand accounts underscored the prevalence and impact of cyber threats on individuals and organizations in Edo State, emphasizing the need for robust cybersecurity measures.
3. Question: What do you think are the most significant cybersecurity challenges faced by organizations in Edo State?

Summary of Responses:

- There's a significant lack of awareness among employees regarding cybersecurity risks. Many individuals are not fully aware of the potential threats they may encounter and how to mitigate them effectively.
- The rapid pace of technological advancements poses a challenge for cybersecurity in Edo State. With new technologies emerging constantly, it's challenging for organizations to keep up and ensure their systems remain secure.
- The evolving nature of cyber threats presents a major challenge. Cybercriminals are constantly developing new techniques and tactics, making it difficult for organizations to anticipate and defend against these threats."
- There's a lack of skilled cybersecurity professionals in the state. Many organizations struggle to find qualified individuals who can effectively manage cybersecurity risks and protect their systems.
- Limited resources and budget constraints hinder efforts to implement robust cybersecurity measures. Many organizations in Edo State may not have the necessary funds to invest in advanced security solutions and training programs.

Overall, the responses highlight the multifaceted nature of cybersecurity challenges facing Edo State, including issues related to awareness, technology, threat landscape, workforce, and resource constraints. Addressing these challenges will require a comprehensive and coordinated approach involving education, technology adoption, capacity building, and resource allocation.

4. Do you regularly update your software and operating systems to protect against vulnerabilities?

Summary of Responses

- Yes, I make sure to regularly update my software and operating systems to ensure they are protected against vulnerabilities. I understand the importance of staying up-to-

International Journal of Advances in Engineering and Management (IJAEM)
Volume 6, Issue 04 Apr. 2024, pp: 904-913 www.ijaem.net ISSN: 2395-5252

date with security patches and fixes to prevent potential cyber attacks.

- ❖ I try to update my software and operating systems whenever I can, but it's not always consistent. Sometimes I may forget or delay updates due to other priorities or concerns.
- ❖ I update my software and operating systems occasionally, but not as frequently as I should. It can be challenging to keep track of all the updates, especially with multiple devices and applications to manage.
- ❖ No, I rarely update my software and operating systems. I prefer to stick with what works and avoid the hassle of updating unless absolutely necessary.

The responses to the question regarding the regular updating of software and operating systems reflect varying levels of diligence in cybersecurity practices among respondents. While some individuals prioritize regular updates as a proactive measure to protect against vulnerabilities, others exhibit a more lax approach, citing challenges such as forgetfulness or inconvenience. It is evident that maintaining a consistent update regimen presents challenges for some individuals, highlighting the importance of awareness and education initiatives to emphasize the critical role of software updates in cybersecurity hygiene. Additionally, strategies to streamline the update process and enhance user convenience may be beneficial in encouraging more widespread adoption of regular update practices. Overall, the findings underscore the need for continued efforts to promote and facilitate cybersecurity best practices, including regular software updates, to mitigate the risk of security breaches and vulnerabilities in Edo State.

5. What improvements or initiatives would you recommend to enhance cybersecurity resilience in the state?

Summary of Responses

- ❖ Establishment of a Cybersecurity Council:

A dedicated council to oversee cybersecurity efforts and ensure coordination among government agencies, private sector organizations, and law enforcement.

- ❖ Cybersecurity Awareness and Education:

Implementation of public awareness campaigns, training programs, and workshops to educate citizens, businesses, and government employees on cybersecurity best practices and the latest threats.

- ❖ Incident Response Plan:

Development and regular updating of a comprehensive incident response plan to quickly respond to and contain cyber threats.

- ❖ Cybersecurity Framework Adoption:

Adoption of a widely recognized cybersecurity framework (e.g., NIST Cybersecurity Framework) to guide cybersecurity practices and risk management.

- ❖ Investment in Workforce Development and Infrastructure:

Investment in training and developing a skilled cybersecurity workforce to meet the state's cybersecurity needs. Also, improvement in technology infrastructure to support cybersecurity efforts.

The recommendations provided by respondents underscore the importance of a multifaceted approach to enhancing cybersecurity resilience in Edo State. Establishing a dedicated Cybersecurity Council would ensure effective coordination and collaboration among various stakeholders, facilitating the development and implementation of cohesive cybersecurity strategies. Additionally, robust awareness campaigns and educational initiatives are crucial for empowering individuals and organizations with the knowledge and skills necessary to mitigate cybersecurity risks effectively. The development of a comprehensive incident response plan and adoption of recognized cybersecurity frameworks are essential for proactive threat management and adherence to industry standards. Moreover, investments in workforce development and infrastructure improvements are imperative to build a strong cybersecurity ecosystem capable of addressing evolving threats. Overall, the recommendations highlight the need for concerted efforts from government, businesses, academia, and the community to fortify cybersecurity defenses and safeguard against cyber threats in Edo State.

c. Gap Analysis

The gap analysis conducted in this study aimed to assess the current state of cybersecurity practices in Edo State, define an ideal state based on established cybersecurity standards and best practices, and identify the gaps between the two states.

- ❖ Identifying and Defining the Current State

The current state of cybersecurity practices in Edo State was evaluated through surveys, interviews, and documentary analysis.

Key findings revealed varying levels of cybersecurity awareness and practices among individuals and organizations. While some respondents demonstrated a moderate to high level of awareness and adherence to cybersecurity measures, others exhibited gaps in knowledge and implementation of best practices. Concerns were raised regarding awareness gaps, inconsistent software updates, and limited resources for cybersecurity initiatives.

❖ Defining an Ideal State Based on Established Standards

The ideal state of cybersecurity resilience was defined based on established standards and best practices, such as those outlined in recognized frameworks like the NIST Cybersecurity Framework. This ideal state encompasses a comprehensive approach to cybersecurity, including robust awareness and education programs, regular software updates and vulnerability assessments, effective incident response mechanisms, and a skilled cybersecurity workforce. Additionally, it emphasizes proactive measures to mitigate emerging cyber threats and adherence to industry standards and regulations.

❖ Identifying the Gaps

A comparison between the current state and the ideal state revealed several gaps in cybersecurity practices in Edo State. These gaps include:

1. Inadequate cybersecurity awareness and education initiatives, leading to knowledge gaps and ineffective cybersecurity practices.
2. Insufficient resources and infrastructure for conducting regular vulnerability assessments and implementing proactive cybersecurity measures.
3. Lack of a comprehensive incident response plan and coordination mechanism to address cyber threats promptly and effectively.
4. Shortage of skilled cybersecurity professionals and limited investment in workforce development programs.
5. In consistencies in software updates and patch management, leaving systems vulnerable to exploitation.

V. CONCLUSION

This research emphasizes the imperative of strengthening cybersecurity resilience in Edo State through targeted interventions and strategic initiatives. The findings revealed a diverse understanding of the current state of cybersecurity practices, highlighting areas of strengths and opportunities for improvement. By conducting comprehensive surveys, interviews, and documentary analyses, the study explains the multifaceted nature of cybersecurity challenges facing individuals and organizations in the state. The gap analysis identifies critical disparities between the current state and the ideal state of cybersecurity resilience, emphasizing the need for concerted efforts to bridge these gaps and align practices with established standards and best practices.

VI. RECOMMENDATIONS

Based on the findings and conclusions of the study, the following recommendations are proposed to enhance cybersecurity resilience in Edo State:

1. Strengthen Cybersecurity Awareness and Education Initiatives: Implement comprehensive public awareness campaigns, training programs, and workshops to educate citizens, businesses, and government employees on cybersecurity best practices and the latest threats. This should include raising awareness about the importance of regular software updates, strong password management, and safe internet usage practices.
2. Formulate a dedicated Cybersecurity Council comprising representatives from government agencies, private sector organizations, academia, and law enforcement to oversee cybersecurity efforts, develop strategies, and ensure coordination and collaboration among stakeholders.
3. Develop and regularly update a comprehensive incident response plan to effectively respond to and contain cyber threats. This should include clear procedures for incident detection, analysis, containment, eradication, and recovery, as well as mechanisms for communication and coordination during a cybersecurity incident.
4. Adopt Recognized Cybersecurity Frameworks: Implement widely recognized cybersecurity frameworks such as the NIST Cybersecurity Framework to guide cybersecurity practices and risk management. This will provide a structured approach for organizations to assess their cybersecurity posture, identify areas for improvement, and align their practices with industry standards.
5. Invest in Workforce Development: Allocate resources for training and developing a skilled cybersecurity workforce to meet the state's cybersecurity needs. This should include initiatives to recruit and retain cybersecurity professionals, as well as opportunities for

ongoing training and professional development in cybersecurity-related fields.

6. Conduct Regular Vulnerability Assessments and Penetration Testing: Establish a regular schedule for conducting security audits, vulnerability assessments, and penetration testing to identify and address vulnerabilities in systems and networks proactively. This will help organizations identify potential security weaknesses and take corrective actions to mitigate risks.
7. Foster Collaboration and Information Sharing: Encourage collaboration and information sharing among government agencies, private sector organizations, academic institutions, and cybersecurity experts to exchange threat intelligence, best practices, and lessons learned. This will enhance situational awareness and collective defense against cyber threats.
8. Promote Cyber Hygiene Practices: Emphasize the importance of cyber hygiene practices such as regular software updates, patch management, data backup, and use of strong, unique passwords. Provide guidance and resources to individuals and organizations to implement and maintain good cyber hygiene habits.
9. Invest in Technology Infrastructure: Allocate resources for upgrading and enhancing technology infrastructure to support cybersecurity efforts, including cybersecurity tools and technologies, secure network architectures, and data protection mechanisms.
10. Monitor and Evaluate Cybersecurity Resilience: Establish mechanisms for monitoring and evaluating the effectiveness of cybersecurity resilience efforts in Edo State. This should include metrics for measuring cybersecurity maturity, incident response effectiveness, and awareness levels, with regular assessments to track progress and identify areas for improvement.

ACKNOWDGMENT

The authors express their sincere gratitude to the leadership of the Tertiary Education Trust Fund (TetFund), as well as the National Institute of Construction Technology and Management (NICTM), Uromi, for their generous financial support in facilitating this research.

REFERENCES

[1]. Kaur, P., 2020. Cyber Connectivity, Cybercrime and Cyberspace Regulations. Auburn University at Montgomery , Alabama, USA, Book Chapter, pp. 299 – 315.

[2]. European Commission, 2015. The European Agenda on Security, Strasbourg; European Commission. Retrieved from http;//ec.europa.eu/dgs/homeaffairs/elibrary/documents/basicsdocuments/docs/eu_agenda_on_security_en.pdf

[3]. Europo, 2016. The relentless growth of cybercrime. Retrieved from https;//www.europolo.europa.eu/newsroom/news/relentless-growth-of-cybercrim

[4]. Agbeboaye, C., 2024. Investigative Analysis of Cybercrime in Nigeria: Using Theft Triangle. Journal of Electrical System, 20-4s, pp 1275 – 1282.

[5]. Ogbile, M. I., & Okorie, P. U., 2015. Review and evaluation of cybersecurity threats on communication networks. International Conference on Cyberspace Governance - CyberAbuja2015, pp. 82 – 85.

[6]. Bada, M., Sasse, A. M., & Nurse, J. R. C., 2020. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?

[7]. Singh, D., Mohanty, N. P., Swagatika, S., & Kumar, S., 2020. Cyber-hygiene: The key Concept for Cyber Security in Cyberspace. Test Engineering Management, Vol. 83, pp. 8145-8152.

[8]. Panda, S., Panaousis, E., Loukas, G., & Laoudias, C.. 2020. Optimizing Investments in Cyber Hygiene for Protecting Healthcare Users. Link Springer.

[9]. Akpan, E. E., 2020. A Critical Analysis of Cyber Security and Resilience in Nigeria. World Atlas Journal of Library and Information Science, Vol. 5, Issue 1. Pp. 10 – 22.

[10]. Adebayo, J. A., Suleiman, I., Ade, A. Y., Ganiyu, S. O., Alabi, I. O., & Ade, A. Y. (2015). Digital Forensic Analysis for Enhancing Information Security. In Proceedings of the 2015 International Conference on Cyberspace Governance - CyberAbuja2015, pp. 38 – 44.