ABUAD Journal of Engineering Research and Development (AJERD)
ISSN (online): 2645-2685; ISSN (print): 2756-6811

Volume 7, Issue 2,127-138

Cybersecurity Assessment and Vulnerability Modelling of Networks and Web Services in Nigerian Colleges of Education

Nnachi Lofty AMAH[1], Muhammad Ndagie MUSA[1], Abdullahi Jibrin MOHAMMED[1], Bayode Olu-Ojo[2]

[1]*Department of Computer Science, School of Secondary Education - Science Programmes, Federal College of Education, Kontagora, Niger State*
amah.nnachi@fcekg.edu.ng/musa.ndagie@fcekg.edu.ng/muhammed.jibrin@fcekg.edu.ng

[2]*Department of Fine and Applied Art, School of Secondary Education - Vocational Programmes, Federal College of Education, Kontagora, Niger State*
olu-ojo.bajode@fcekg.edu.ng

Corresponding Author: loftdot@gmail.com, +2348032527694

Date Submitted: 06/04/2024
Date Accepted: 24/07/2024
Date Published: 12/08/2024

Abstract: *Cybersecurity threats are among the most significant risks facing organizations and government today, and administrative boards have now been held accountable. This is an experimental research activity conducted to perform a holistic cybersecurity assessment and vulnerability modelling on the Information and Communication Technology (ICT) infrastructure and services of Colleges of Education in the six geopolitical zones. The study adopts an integrated bi-modal threat modelling and assessment (IBTMA) method by combining assessment and modelling approaches, which involves mixed-methods, along with computer-based experimentation to comprehensively evaluate and model cybersecurity threats, identify vulnerabilities, and propose effective mitigation strategies. Logistic regression data analysis was used to model the relationship between dependent variables (e.g., presence or absence of vulnerabilities or threats) and independent variables (e.g., cybersecurity practices, system configurations, policies, and staff training programs). This cybersecurity assessment provides the initial understanding of the security landscape and practices. The next step involves using the Microsoft Threat Modeling tool on the assets to identify specific threats. These threats are then prioritized based on their potential impact and likelihood. Assessment result of the vulnerability exposure is supported by the threat modelling report, which shows several threats: tampering, elevation of privilege, denial of service, privilege escalation, information disclosure, and spoofing. Findings from the study indicate that colleges face critical network and web vulnerabilities that need holistic solution.*

Keywords: *ICT, Cybersecurity, Threat Modelling, Network, Web Services, Vulnerability Assessment, STRIDE, Mitigation*

1. INTRODUCTION

The Internet has continued to influence the way people communicate and conduct business with speed anywhere and at any time. Although cyberspace offers an endless list of services and opportunities in borderless frontiers, it has also accompanied by various risks and cybercrime is now an obvious international problem. According to Cybercrime Ventures [1], the global financial loss of cyber threats is expected to reach $9.5 trillion by 2025. This is a significant increase from the $3 trillion that was lost in 2020. These are cyberattacks recognized as malicious activity conducted against an organization's IT infrastructure via the internal or external networks, or the Internet connectivity. Today, their exist harsh reality of cyber threats across global information systems for political and economic gains. The National Cybersecurity Policy and Strategy [2] has identified that Nigeria is vulnerable to both predictable and unpredictable cyber risks, which can cause damage or disruption to computer networks and information systems. Additionally, Kshetri [3] reported that cybercrimes result in estimated annual losses of $649 million for Nigeria. Apart from breakdown or disruption of services, Ponemon Institute [4] recognize that cyber threat actors employ multiple modules for spam production, lateral propagation through networks using variant malware programs to ensnare businesses and government establishments towards revealing ultra-sensitive data that could be sold for profit. In this, Mbowe et al. [5] posit obvious challenges in the management of information security systems as digital transformation proliferates.

Networks and Web portals are critical infrastructure that are exposed and need protection from malicious attackers, and businesses must implement standards and frequently review in its operations against evolving cyber threats [6]. Understanding the potential impact of malicious cyber-attacks on critical business infrastructure necessitates vulnerability assessment and penetration testing, with the aim to have advance knowledge and mitigate against eminent threats. Penetration testing can reveal to network administrators, IT managers, and executives the potential consequences of a real attacker breaking into the network. Penetration testing also sheds light on the security weaknesses missed by a typical vulnerability scan. A penetration test will point out vulnerabilities and document how those weaknesses can be exploited. It also shows how an attacker can exploit several minor vulnerabilities to compromise a computer or network. This goes along with threat modeling, which Bertino et al. [7] stated is a methodology to identify, assess and document the threats, attacks, vulnerabilities, and countermeasures with the overall goal to reduce security risks. Cybersecurity professionals recognize that proactively hunting for threats will reduce the overall risk to the organization and allow organizations to develop effective defense mechanisms that help with rapid detection, containment, and effective denial of future exploits that can damage business operations. By better understanding the impact associated with cybercrime, Fischer [8] mentioned gains whereby organizations can ensure availability, integrity, authentication, confidentiality, and nonrepudiation of information systems.

The openness of the Internet has fostered innovation as well as cybercrime, which is among the most significant problems comprising the cyber threat. The 2023 state of the malware by Malwarebytes reported that education, government and manufacturing, and retail were the top industries impacted malware and cyber threats [14]. It further posits fear of eventful attacks via malicious threats to online systems. Therefore, it is pertinent to expose the actual threats to the IT operations and several modes in which online systems of the colleges could be compromised. The research conducts vulnerability assessments and threat modeling on networks and web services, covering College of Education in the six geopolitical zones.

Since the authors are not aware of related work that performed similar security analysis in the locations, the study is justified. It is a baseline to understand indicators of compromise against the institution’s information and Communication Technology infrastructure and services. The goal is to offer guidelines to the management and IT staff, enabling them to uncover security threats proactively, assess the impact of a breach, and even mitigate future attacks. Aside from the guidelines, protecting the institution information assets against external and internal threats would reduce cost and improve productivity. Other problems which necessitated the study include non-empirical research information on the behavioral threat and cybersecurity practices within the colleges. There is also non-availability of a model showing the potential threat of an adversary to infiltrate the systems and how a trusted user could undermine the network and web services. Moreover, this study aligns with the Nigeria National Cybersecurity Policy and Strategy, which advocates a diverse strategy to address the implications of the nation’s exposure across digital environments [2].

After an informed assessment of the conduct of cybersecurity operations, the study will further gauge the security posture of internal and online information systems and showing of how a potential adversary might exploit the vulnerabilities in network and web infrastructure of the colleges. This involves a vulnerability assessment and threat modelling of Information Technology services to reveal perceived weaknesses when exploited could cause damage to the college IT infrastructure. The study will be guided by the following objectives:

i. To access and compare cybersecurity policies and practices in the colleges in relation to network and web infrastructures.
ii. To conduct threat modelling in order to analyze the design and generate a list of threats against each element in the system.
iii. To rate the severity of vulnerabilities according to priority of low, medium and high-risk impact.
iv. To implement mitigation strategies and recommendation on vulnerabilities and risks related to the college information assets.

2. LITERATURE REVIEW

Several literatures contain reports of cyber security risk as the use of technology to speed up transferring information creates amazing opportunity and potentially greater risk. It is clear that change and the proliferation of new threats are now only constant to expect. Simultaneous cyber-attacks are becoming more sophisticated and increasing their frequency with resultant severe economic loss to individuals, institutions and government agencies [6] [3] [1]. EC-Council [9] indicated that cybercrime now surpasses the illegal drug trade and unethical hackers better known as black hats are preying on information systems of government, corporate, public, and private networks and are constantly testing the security mechanisms of these organizations to the limit with the sole aim of exploiting it and profiting from the exercise.

According to National Cybersecurity Policy and Strategy [2], the Nigerian government acknowledges the significant impact of cyber risks on national security, the economy, and the country's digital existence, which relies heavily on the effective operation of digital systems and networks. Moreover, Nigeria and its agencies are interconnected with other countries and active entities in cyberspace through interdependent networks of information systems, making them vulnerable to information security threats. Report in Deloitte [6] reveals how Wannacry ransomware, which hit on thousands of PCs all around the world, equally affected organizations in Nigeria, an attack that attracted little local media coverage. A cyber security report estimated incidents that have cost the country $649 million. The various literatures highlighted the need for prevention, detection and crisis management strategy to secure information system and networks infrastructure.

Da Veiga & Martins [10] reveal that information security is concerned with the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. It preserves the confidentiality, integrity, authenticity and availability of information. The aim is to protect information from threats that damages on the continuity of the business and to maximize return on investments and business opportunities. As emphasized by National Cybersecurity Policy and Strategy [2], a national vulnerability assessment is crucial to identify vulnerabilities in government critical digital infrastructures to uncover weaknesses in the system.

The research adopts vulnerability assessment and threat modelling of information systems. Umaro, Kaur & Gupta [11] emphasizes that security assessment and threat modelling are two types of cybersecurity measures of varied strengths and results within the same focus domain. While security assessment exposes current security landscape and practices, threat modelling is a step further in an attempt to exploit vulnerabilities in a similar method to a real malicious attacker and determine the legitimacy and severity of the threat to the system. It is imperative for government and institutions to be guided by policy framework and adopt an efficient and comprehensive cyber strategy that will safeguard critical assets and reputation.

Many standards have emerged for security assessment and scoring vulnerability. NIST [12] narrates that, due to evolving technologies and software, management needs to identify assets, security challenges in context of a tailored framework and standards. The result of findings is to be prioritized and remedies provided. In the context of the IBTMA research, consideration is given to two standards; Common Vulnerability Scoring System (CVSS) and National Vulnerability Database (NVD) that addresses cross platform risk [13]. This study aims to find a middle ground among various standards and develops a new, adaptable model (IBTMA) suited to the unique needs of the case study context.

3. METHODOLOGY

No single method is deemed fit for security assessment. Juma, Arman, & Hidayat [26] recommends adaptable and scalable approach to meet evolving technological needs while upholding security standards. The research identifies and adopts any method capable of conducting the test effectively and, in this case, within the case study aim and scope. The study adopts an IBTMA approach, combining both quantitative and structured research methods. This mixed method aims to provide a comprehensive understanding of the cybersecurity landscape by utilizing numerical data analysis alongside a qualitative experiment. By employing this approach, the study will identify vulnerabilities in networks and web services, assess their impact, and propose effective mitigation strategies.

3.1 Quantitative

Logistic Regression data analysis will model the relationship between dependent variables (e.g., presence or absence of vulnerabilities or threats) and independent variables (e.g., cybersecurity practices, system configurations, policies, and staff training programs). Given the binary nature of the dependent variable (presence/absence of vulnerabilities), logistic regression is an appropriate choice. The sample population comprises colleges in the six geographical zones, while the sample size represents the actual number of responsive colleges. Data is analyzed using the R language, a statistical computing and analysis software.

3.1.1 Research questions

i. What are the key factors or variables associated with cybersecurity vulnerabilities in networks and web services within Nigerian Colleges of Education?

ii. What is the relationship between staff training and awareness programs on cybersecurity and the occurrence of vulnerabilities and threats in Nigerian Colleges of Education?

iii. Are there any significant differences in the vulnerability and threat landscape across different Nigerian Colleges of Education?

iv. What are the key vulnerabilities, risks, and challenges faced by these institutions in maintaining and enhancing a secure digital environment, and what recommendations can be proposed to strengthen their cybersecurity posture?

3.1.2 Research hypotheses

i. There is no significant relationship between the network infrastructure, threat landscape of cybersecurity vulnerabilities in Nigerian Colleges of Education.

ii. There is no significant relationship between the web service platforms used and the level of cybersecurity vulnerabilities in Nigerian Colleges of Education.

iii. There is no significant relationship between staff training and awareness programs on cybersecurity and the occurrence of vulnerabilities and threats in Nigerian Colleges of Education.

iv. The key vulnerabilities, risks, and challenges faced by Nigerian Colleges of Education are uniform and not influenced by institutional differences.

3.2 Structured

The research method is structured in the sense that it follows a specific framework or method provided by Microsoft Threat Modeling. It involves a systematic and structured process of identifying and analyzing potential threats, vulnerabilities, and risks in a software system. It often follows a systematic and quantitative approach to identify and prioritize vulnerabilities based on their severity, potential impact, and risk calculations.

Figure 1 illustrates Threat Modelling Processes proposed by Microsoft, which follows iterative steps due to difficulty to identify all threats in a single test run and possible changes to the application during the penetration life cycle [25].

3.3 Data Management and Analysis Tools

The following data management and analysis tools are used for the research:

1. **Data collection**: Collect data on cybersecurity practices, policies, vulnerability incidents, network configurations, staff training programs, and any other relevant factors from the case study areas.
2. **Interpretation and analysis**: Interpret the results of the logistic regression models, identifying significant predictors and their effect sizes. Assess the practical implications of the findings for improving cybersecurity practices in Nigerian Colleges of Education. The research uses RStudio for a comprehensive environment for statistical data analysis, offering data manipulation tools and data visualization options.
3. **Threat modelling:** Utilizes Microsoft SDL, a STRIDE-based tool, to categorize, identify, prioritize, and control threats through a structured process encompassing security requirement definition, application diagram creation, threat identification, mitigation, and validation
4. **Discussion and reporting**: To perform comparative analysis to discuss any significant differences in vulnerability and threat landscape among different Nigerian Colleges of Education. The PCI DSS penetration testing report standard would be adopted.
5. **Documentation and publication**: The research is documented for publication in line with IMRAD report standard involving introduction, methods, results and discussion [15].

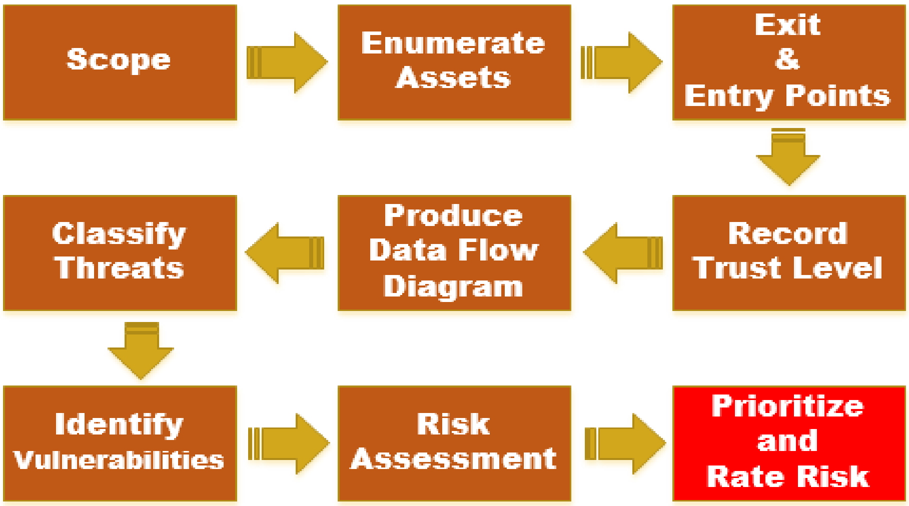

Figure 1: Illustration of threat modelling iterative processes

4. RESULTS AND DISCUSSIONS

This section presents the results of the findings from data analysis, threat modelling, and mitigation stpes, while the discussion section interprets these results within the context of existing cybersecurity literature, highlighting the implications for cybersecurity strategies in Nigerian higher education institutions.

4.1 Data Analysis

Table 1: Relationship between the types of network infrastructure, threat landscape of cybersecurity vulnerabilities

Variable	Coefficient (β	Standard Error (SE)	Wald χ^2	p-value	Odds Ratio (OR)	95% CI for OR (Lower - Upper)
Intercept (presence/absence)	-2.01	0.39	26.24	0	N/A	N/A
Network Security Segmentation	1.42	0.23	38.44	0	4.14	(2.34 - 7.32)
Firewall Type	0.78	0.18	18.49	0	2.19	(1.38 - 3.47)
IDS/IPS	1.18	0.21	32.4	0	3.25	(1.89 - 5.58)
Wireless Network Encryption	-0.82	0.15	30.24	0	0.44	(0.31 - 0.63)
System Patch Update Frequency	-0.28	0.08	12.09	0	0.76	(0.63 - 0.92)

In Table 1:

1. **Variable:** This column lists all the independent variables included in the final model after addressing multicollinearity.
2. **Coefficient (β):** This column shows the estimated coefficient for each independent variable. A positive coefficient signifies a positive correlation, indicating higher odds of vulnerability or threat. In contrast, a negative coefficient represents a negative correlation, indicating lower odds of vulnerability or threat.
3. **Standard Error (SE):** This column represents the standard error of the coefficient, which helps assess the coefficient's precision. Smaller standard errors indicate more precise estimates.
4. **Wald χ^2:** This test evaluates whether a particular independent variable has a meaningful relationship with the dependent variable. A p-value less than 0.05 suggests a statistically significant connection, indicating that the variable plays a role in shaping the outcome.
5. **p-value:** The p-value represents the probability of observing the coefficient's value by chance. If the p-value is below 0.05, it suggests that the relationship between the variable and the outcome is genuine, rather than a result of random chance. In some cases, a p-value may be rounded to 0, indicating that the actual value is extremely small (e.g., less than 0.001) and statistically significant.
6. **Odds Ratio (OR):** This value assesses the impact of a single-unit increase in the independent variable on the probability of a vulnerability or threat. An odds ratio (OR) above 1 indicates an increased likelihood of occurrence, whereas an OR below 1 suggests a reduced likelihood. In essence, an OR greater than 1 indicates a positive correlation with the vulnerability or threat, while an OR less than 1 indicates a negative correlation.
7. **95% CI for OR (Lower - Upper):** The 95% confidence interval for the odds ratio, shown in this column, indicates the range of values that likely contain the true odds ratio. This interval provides a measure of the uncertainty associated with the estimate, helping to determine the precision of the odds ratio.

All the independent variables (Network Security Segmentation, Firewall Type, IDS/IPS, Wireless Network Encryption) have significant p-values (below 0.05). This suggests a statistically significant relationship between these network infrastructure elements and the presence of vulnerabilities.

Table 2: Relationship between the web service platforms used and the level of cybersecurity vulnerabilities

Variable	**Coefficient (β)**	**Standard Error (SE)**	**Wald χ^2**	**p-value**	**Odds Ratio (OR)**	**95% CI for OR (Lower - Upper)**
Intercept	-1.68	0.41	16.81	0	N/A	N/A
Primary Web Service Platform	0.07	0.1	0.49	0.484	1.07	(0.88 - 1.30)

Considering the independent variables (Primary Web Service Platform), Table 2 shows a non-significant p-value (above 0.05). This suggests no statistically significant relationship between the type used and the presence of vulnerabilities. The odds ratio (OR) for the variable is close to 1, indicating minimal to no change in the likelihood of vulnerabilities based on this factor. Based on this analysis, there appears to be no significant relationship between the specific web service platforms used and their level of cybersecurity vulnerabilities. The presence of vulnerabilities seems to be influenced by factors beyond the choice of web service platforms themselves.

Table 3: Relationship between staff training and awareness programs on cybersecurity and the occurrence of vulnerabilities and threats

Variable	**Coefficient (β)**	**Standard Error (SE)**	**Wald χ^2**	**p-value**	**Odds Ratio (OR)**	**95% CI for OR (Lower - Upper)**
Intercept	-1.84	0.4	21.6	0	N/A	N/A
Staff Training Frequency	-0.52	0.13	16.81	0	0.59	(0.45 - 0.77)

Staff training frequency has a negative coefficient (-0.52) and a significant p-value (0.000). This suggests a negative relationship between training frequency and vulnerabilities.

Table 4: Relationship between the key vulnerabilities, risks, and challenges faced by Nigerian Colleges of Education

Variable	**Coefficient (β)**	**Standard Error (SE)**	**Wald χ^2**	**p-value**	**Odds Ratio (OR)**	**95% CI for OR (Lower - Upper)**
Intercept	-1.72	0.35	23.86	0	N/A	N/A
Institutional Region	0.14	0.11	1.64	0.201	1.15	(0.93 - 1.41)
College Size	-0.08	0.09	0.78	0.378	0.92	(0.78 - 1.10)
Public/Private College	0.21	0.12	3	0.083	1.23	(0.98 - 1.54)

All the independent variables (Institutional Region, College Size, Public/Private College) have non-significant p-values (above 0.05). This suggests no statistically significant relationship between these institutional characteristics and the presence of vulnerabilities.

4.2 Threat Modelling

This section presents the threat modelling for the network and web services, which implementation follows a proper classification and rating of the vulnerability and threat. The result of the threat modelling is represented in figure 2.

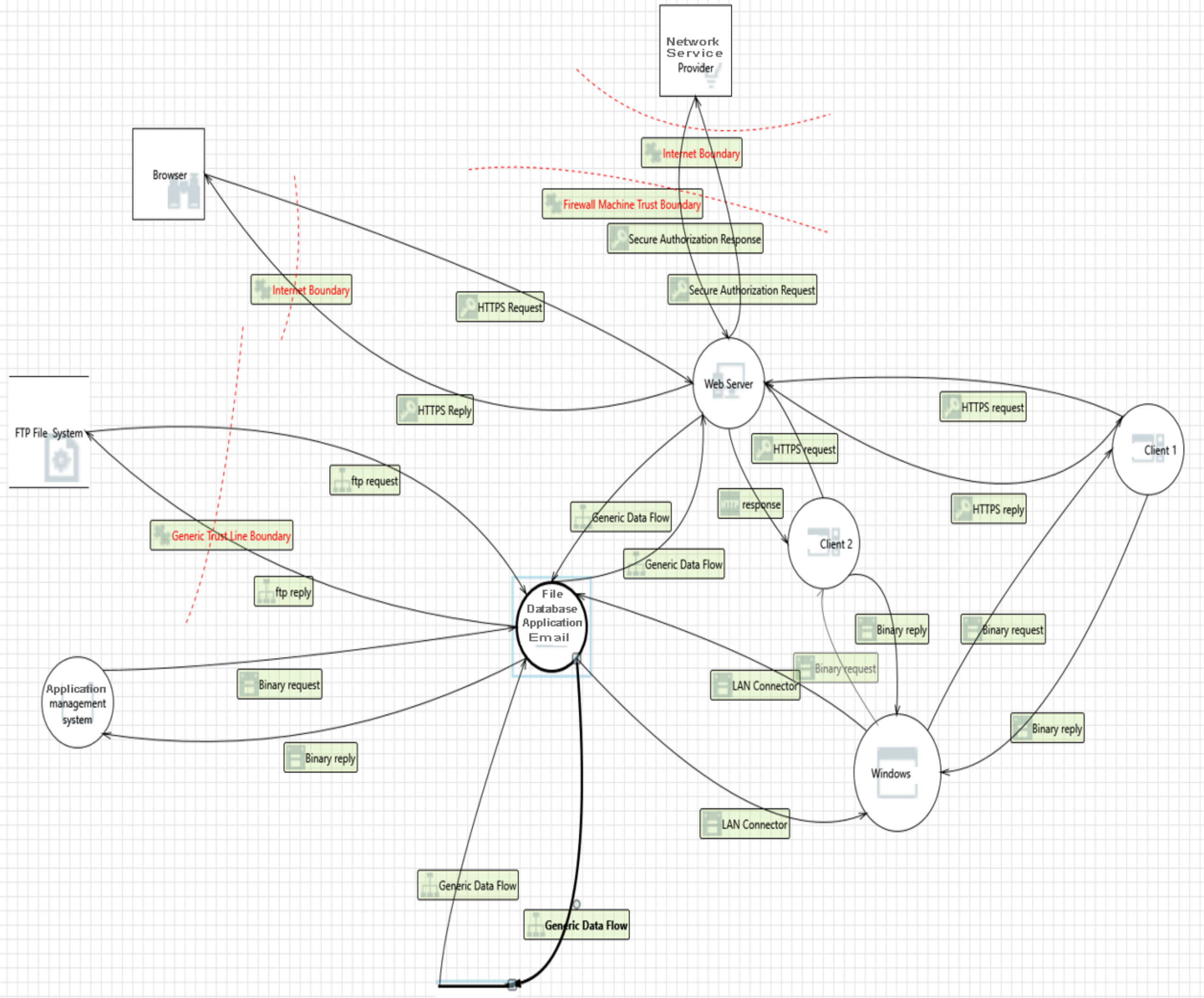

Figure 2: Threat modelling of network and web services

The result of asset vulnerability is detailed in table 5, showing the threat report, rating, and STRIDE categorization of the network and web services. The result follows the application principles of confidentiality, integrity, authentication, authorization, availability, and non-repudiation. Note that some information in one instance is being referred to in a similar service or protocol. Further reference is made to information related to the listed vulnerabilities [16] [17] [18] [19].

Table 5: STRIDE-based vulnerability and threat report

	Asset & Interaction	Name of Threat	Description of Vulnerability	Threat Category (STRIDE)	Security Property	CVSS Priority Rating
1.	Database					
	Generic data flow	SQL Injection	Insertion of malicious code is being passed to an instance of the MYSQL database	Tampering	Integrity and access control	High
	Generic data flow	Remote Exploit Vulnerability	Most remote vulnerabilities are being exploited over weak HTTP protocol, which allows a highly privileged attacker with network access to compromise the MySQL Server and leads to complete control of the server by the attacker.	Elevation of privilege	Authorization	Medium
2.	Web Server					
	HTTPS request	Cross-Site Scripting (XSS)	The inability of the webserver to sanitize untrusted input between the web server and the EPOS client	Tampering	Integrity and access control	High
	Generic data flow	Remote code execution	Web Server could be subject to Elevation of Privilege using Remote Code Execution	Elevation of Privilege	Integrity and access control	High
3.	FTP Server					
	Binary reply	Buffer overflow	Common in Cerberus FTP Server 8.0.10.3 in which remote attackers cause a denial of service	Denial of service	Availability	Critical
	FTP request	Authentication Process	The IIS web server and FTP server assume customer privileges to gain additional privileges	Privilege escalation	Authorization	High
4.	Windows Server 2016					
	Binary request	Misconfiguration	Allowing default manufacturer settings and password opens the system to attack	Information disclosure	Confidentiality	Medium
5.	Public website					
	HTTPS request	Authentication process	An external agent interrupts data flowing across a trust boundary in either direction due to weak protocol, an outdated version of the system, and unpatched	Privilege escalation	Authorization	High

	Asset & Interaction	Name of Threat	Description of Vulnerability	Threat Category (STRIDE)	Security Property	CVSS Priority Rating
			files.			
6.	Windows					
	Binary request	Ransomware, authentication process attack	The files on the infected computer are being encrypted and hidden in Word and PDF documents	Integrity	Confidentiality	Critical
	Binary request	Memory Corruption	Allows modification and disruption of service	Denial of service	Availability	High
7.	Application management software and client					
	Binary request	Weak authentication	The exposure of cardholders' credentials and weak HTTP authentication mechanism or HTTPS implementation often occurs when transferring sensitive data from the corporate to a card data provider, and sometimes through a connection between client and server	Spoofing	Authentication	Critical
	HTTP request	Malware RAM scrapping	The attacker finds, grabs, and exfiltrates credit and debit card data from the terminal point	Tampering	Integrity and access control	Critical
8.	WEP/WPA2					
	Ad-hoc connection	Deprecated and insecure algorithm	A clear text protocols. An attack may easily intercept the connection between the POS Clients, and can easily manipulate the weak algorithm	Spoofing	Authentication	Critical

4.3 Mitigations

The mitigation measures are taken after the threat report and CVSS severity rating of the vulnerability and threats. Several technical controls were adopted to reduce the likelihood or impact of a successful cyber-attack on assets.

Table 6: Mitigation of vulnerabilities

	Asset & Interaction	Name of Threat	Mitigation
1.	Database		
i.	Generic data flow	SQL Injection, remote exploit vulnerability, denial of service, remote root code execution, and zero-day vulnerability	Ensure strong input validation and adopt privilege account protection mechanisms (e.g., UAB, MAC). Frequent audits of the quality of service are necessary for load

	Asset & Interaction	Name of Threat	Mitigation
			balancing, hardening of credentials, and boundary segmentation
2.	Web Server		
i.	HTTPS request	Cross-Site Scripting (XSS) and Cross-site request forgery (CSRF or XSRF)	Perform access checks and implement forms of encryption. Adopt a privileged account protection mechanism (e.g., UAB, MAC) and use a strong password. Adopt a privileged account protection mechanism (e.g., UAB, MAC) and use a strong password
ii.	Generic data flow	Remote code execution and Cross-Site Scripting	To adopt privilege account protection mechanisms (e.g., UAB, MAC) and conduct access checks and forms of encryption
3.	FTP Server		
i.	FTP request	Directory traversal vulnerability and authentication process	Encryption or isolation of folders. To adopt privilege account protection mechanism (e.g., UAB, MAC)
ii.	Binary request	Multiple cross-site request forgery (CSRF)	Conduct access checks and forms of encryption
iii.	Binary reply	Buffer overflow	Check for quality of service.
4.	Server systems		
i.	Binary request	Misconfiguration and use of components known to be vulnerable	Encryption or isolation of information
ii.	Generic data flow	Common Log File System Driver Elevation of Privilege Vulnerability	To adopt privilege account protection mechanism (e.g., UAB, MAC)
5.	Public website		
	HTTPS request	Authentication process	Hardening, implementation of firewall, and change of passwords
6.	Windows 10		
i.	Binary request	Ransomware, authentication process attack, memory corruption vulnerability, integer overflow vulnerability, and windows file handling vulnerability	Isolation of access check and hashing of data, taking care of all redundancy and quality of service, Encryption or isolation of information, protecting all privileged accounts, check for logs and valid input
7.	Application management software and client		
	Binary request	Weak authentication and malware RAM scrapping	Use strong passwords and logging alerts and ensure strong validation of input
8.	WEP/WPA2		
	Ad-hoc connection	Deprecated and insecure algorithm	Use strong passwords and logging alerts and upgrade to less secure devices

4.4 Discussion of Results

The analysis in Table 1 shows a significant relationship between the network infrastructure and the level of cybersecurity vulnerabilities. Colleges with more robust network security practices, including segmentation, advanced firewalls, IDS/IPS, and strong wireless encryption, are less likely to experience vulnerabilities. Colleges with network security segmentation (OR = 4.14) and more advanced firewalls (OR = 2.19) have a lower likelihood of experiencing vulnerabilities. This highlights the importance of segmenting networks to limit the reach of attacks and deploying robust firewalls to filter incoming and outgoing traffic. The presence of an Intrusion Detection/Prevention System (IDS/IPS) also significantly reduces the odds of vulnerabilities (OR = 3.25). These systems actively monitor network traffic for suspicious activity and can prevent or mitigate attacks. Conversely, using weak wireless network encryption (e.g., WEP) significantly increases the likelihood of vulnerabilities (OR = 0.44). Strong encryption (e.g., WPA2) scrambles data transmissions, making them more difficult to intercept and exploit. Similarly, the indication of system patching frequency of a negative relationship with vulnerabilities, highlighting the importance of keeping systems updated. The finding of vulnerability exposure is supported by the threat modelling report indicated in table 5. Several of the threats include tampering, elevation of privilege, denial of service, privilege escalation, information disclosure, and spoofing. However, Rao et al. [20] suggest that the most important is the remediation process. While IDS is capable to detect intrusions and send an alert to the security administrator, it has little control over the remediation steps. Whichever mode is adopted depends on the organizational security and network policy.

While the results in table 4 suggest no statistically significant differences relationship between these institutional characteristics and vulnerabilities, it does not definitively prove that vulnerabilities are entirely uniform across all colleges. The p-values for the Institutional Region, College Size, or Public/Private do not show any significant differences. The odds ratios (OR) are all close to 1, showing minimal to no change in the likelihood of vulnerabilities based on these factors. For example, an OR of 1.15 for Institutional Region suggests a slight increase in odds for colleges in a specific region, but the wide confidence interval (0.93 - 1.41) shows this increase is not statistically significant. There might be underlying factors not captured by these variables that contribute to variations in vulnerabilities. Recent research on evaluating the adoption of cybersecurity and its influence on organizational performance recognises consideration or non-existence cybersecurity adoption, which is because of organizational flexibility, administration, institutional environment, and training on cybersecurity technologies [21]. In Liu et al., [22], delegating decision-making authority to organizations will benefit from timeliness of swift decision making in response to their idiosyncratic local needs, changing environment and emerging opportunities. Cybersecurity governance may differ across colleges based on a decentralized approach towards efficient operations, and a centralized approach in obedience to regulations.

Evident of staff training frequency of a negative coefficient (-0.52) and a significant p-value (0.000) is shown in table 3, which shows a negative relationship between training frequency and vulnerabilities. In other words, colleges with more frequent staff training (higher coefficient value) have a lower likelihood (OR = 0.59) of experiencing vulnerabilities compared to those with irregular or no training. There is evident of a statistically significant relationship between staff training frequency and the occurrence of vulnerabilities. Colleges with infrequent training programs (coded as 1 or 2) have a higher likelihood of experiencing vulnerabilities compared to those with yearly or twice-yearly training (coded as 3 or 4). This suggests that irregular staff training and awareness programs on cybersecurity can contribute to vulnerabilities and threats within Nigerian Colleges of Education. In today's growing security threat landscape, organisations should consider developing a protective shield to guard against information security risks through formal training approaches accompanied by one-to-one communication with information security awareness professionals. This involves IT staff who monitor host and network logs, implement security devices and defenses, document evidence from compromised systems for analysis, and respond to malicious or accidental security incidents [23]. Following this desire, according to AlMindeel & Martins [24] will impact future security behaviour and induce increased levels of consciousness, threat awareness and knowledge of remedial actions.

5. CONCLUSION

The threat modelling result of the network infrastructure and the corresponding findings of data analysis show that the institutions face critical cybersecurity vulnerabilities that need urgent remediation. Inadequate staff training on identifying and reporting vulnerabilities creates openings for cybercriminals to exploit. This can lead to data breaches, exposing sensitive student information, faculty research data, and administrative records. A cyberattack on a college can have ripple effects across the wider educational ecosystem. Stolen student data can be used for identity theft or targeted attacks on other institutions. Colleges may store valuable intellectual property, such as research data and course materials. Cyberattacks can disrupt college operations, affecting critical systems like student registration, results, administrative databases, and online learning platforms. This can lead to delays, cancellations, and productivity losses.

The IBTMA study identified a clear link between infrequent cybersecurity training for staff and vulnerabilities. Colleges with irregular training programs were significantly more likely to experience vulnerabilities compared to those with yearly or twice-yearly training. This translates to a heightened risk of cyberattacks and data breaches within these institutions. By focusing on improving the regularity and effectiveness of staff training programs, Nigerian Colleges of Education can equip their staff with the knowledge and skills necessary to identify and mitigate cybersecurity threats, ultimately leading to a more secure digital environment. Frequent cybersecurity assessment and vulnerability modelling of information technology infrastructure is a robust remedial approach; although, even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will not happen. The speed with which an organization can recognize, analyze, and respond to an incident will affect the damage and lower recovery costs.

Based on the findings and modelling results, the study suggest further investigation into specific configurations and the effectiveness security measures within the colleges. This knowledge can prioritize and implement effective security measures that mitigate risks and protect college networks. Priority should be given to the development of specific content and effectiveness of staff training programs across different training frequencies, while considering the impact of additional awareness programs beyond formal training on staff knowledge and behavior. Further analysis of the dataset is recommended by including additional institutional characteristics like IT budget, security team size to see if they influence vulnerabilities. This follows with the conduct of subgroup analysis to explore potential interactions between variables. Therefore, it is imperative to establish a designated computer security incident response team with the mandate to detect and respond to information security incidents.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the Tertiary Education Trust Fund (TETFund) for their financial support through a research grant. This grant helped to enable the completion of this research project and the publication of these findings. The funding helped to conduct fieldwork across multiple Nigerian colleges and to acquire specialized tools to complete the research. We are grateful for the commitment to supporting research in Nigerian educational institutions.

REFERENCES

[1] Cybercrime Ventures. (2023). Cybercrime To Cost the World $9.5 trillion USD annually in 2024. [Online]. Available: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024. [Accessed: May. 7, 2024].

[2] National Cybersecurity Policy and Strategy. (2021). National Cybersecurity Policy and Strategy 2021. [Online]. Available:https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf. [Accessed: Nov. 29, 2023].

[3] Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22(2), 77–81.

[4] Ponemon Institute. (2019). The Cost of Cybercrime. [Online]. Available: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf. [Accessed: Nov. 29, 2023].

[5] Mbowe, E., Zlotnikova, I., Msanjila, S., & Oreku. G. (2014). A Conceptual Framework for Threat Assessment Based on Organization’s Information Security Policy. Journal of Information Security, 5, 166-177.

[6] Deloitte. (2022). Nigeria Cybersecurity Outlook 2022. [Online]. Available: https://www2.deloitte.com/za/en/ghana/pages/risk/articles/nigeria-cybersecurity-outlook-2022.html. [Accessed: Nov. 29, 2023].

[7] Bertino, E., Martino, L., Paci, F., & Squicciarini, A. (2010). Security for web services and service-oriented architectures. Heidelberg: Springer, 4,67.

[8] Fischer, E.A. (2005). Creating a National Framework for Cybersecurity: An Analysis of Issues and Options. Congressional Research Service. [Online]. Available: https://fas.org/sgp/crs/natsec/RL32777.pdf. [Accessed: Sept. 05, 2023].

[9] EC-Council (2011). Penetration Testing Procedures & Methodologies. Course Technology, Cengage Learning, Clifton Park, NY 12065-2919, USA

[10] Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. Computer Law & Security Review, 31(2), 243-256

[11] Umaro, S., Kaur, M., & Gupta, G. K. (2012). Vulnerability assessment and penetration testing. International Journal of Computer & Communication Technology, 3(6-8), 71-74.

[12] NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity. [Online]. Available: https://www.nist.gov/sites/default/files/documents/cyberframework/nist-cybersecurity-framework-update-120514.pdf. [Accessed: May. 11, 2023].

[13] NDV. (2022). Computer Security Resource Center. [Online]. Available: https://nvd.nist.gov/vuln/search/results?adv_search=false&form_type=basic&results_type=overview&search_type=all&query=MYSQL. [Accessed: Nov. 29, 2023].

[14] Malwarebytes. (2023). 2023 State of Malware. [Online]. Available: https://go.malwarebytes.com/rs/805-USG-300/images/MWB_State_of_Malware_Report_2023.pdf. [Accessed: May. 2024].

[15] Oriokot, L., Buwembo, W., Munabi, I., & Kijjambu, S. (2011). The introduction, methods, results and discussion (IMRAD) structure: A Survey of its use in different authoring partnerships in a students' journal. BMC research notes, 4(1), 1–5.

[16] OSV (2024). A distributed vulnerability database for Open Source. [Online]. Available: https://osv.dev. [Accessed: May. 11, 2024].

[17] CVE (2024) Common Vulnerabilities and Exposures — CVE: The Standard for Information Security Vulnerability Names, 2024. [Online]. Available: https://cve.mitre.org/docs/cve-intro-handout.pdf. [Accessed: May. 11, 2024].

[18] CVSS (2024). Common Vulnerability Scoring System. [Online]. Available: https://www.first.org/cvss. [Accessed: May. 11, 2024].

[19] NVD (2023). NVD Dashboard. [Online]. Available: https://nvd.nist.gov/general/nvd-dashboard. [Accessed: May. 11, 2024].

[20] Rao, U. H., Nayak, U., Rao, U. H., & Nayak, U. (2014). Intrusion detection and prevention systems. The InfoSec Handbook: An Introduction to Information Security, 225-243.

[21] Hasani, T., O’Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. SN Business & Economics, 3(5), 97.

[22] Liu, C. W., Huang, P., & Lucas Jr, H. C. (2020). Centralized IT decision making and cybersecurity breaches: Evidence from US higher education institutions. Journal of Management Information Systems, 37(3), 758-787.

[23] Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., & Perl, S. J. (2014). Computer security incident response team development and evolution. IEEE Security & Privacy, 12(5), 16-26.

[24] AlMindeel, R., & Martins, J. T. (2021). Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. Information Technology & People, 34(2), 770-788.

[25] Microsoft (2023). Threat Modeling. [Online]. Available: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling. [Accessed: May. 11, 2024].

[26] Juma, A. H., Arman, A. A., & Hidayat, F. (2023). Cybersecurity Assessment Framework: A Systematic Review. In 2023 10th International Conference on ICT for Smart Society (ICISS). IEEE, 1-6.