Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.15, No.2, 2025

Meta-analysis of Cybersecurity Threats and Vulnerabilities among Nursing Training Students in Ghana

Japhter Yankey[1*] Emmanuel Harris[2] Timothy Simpson[3] Kenneth S. Boadi[4] Gillian E. Akuetteh

1. Kwame Nkrumah University of Science and Technology, Kumasi.
2. Takoradi Technical University, Takoradi Ghana.

* E-mail of the corresponding author: yjaphter@gmail.com

Abstract

This meta-analysis examines cybersecurity threats and vulnerabilities facing nursing students in Ghanaian training institutions, a critical concern given the increasing reliance on digital technologies in healthcare education and practice. Synthesizing findings from studies conducted between 2004 and 2024, this research reveals significant gaps in cybersecurity awareness, preparedness, and institutional safeguards. Results indicate that phishing is the most prevalent threat, followed by malware and ransomware, exacerbated by the widespread use of personal devices with inadequate security measures. A notable lack of formal cybersecurity training in curricula and an over-reliance on informal awareness channels contribute to student vulnerability. Institutional cybersecurity infrastructure is often limited, with basic protections like firewalls more common than advanced measures such as data encryption and structured training programs. The findings emphasize the urgent need for comprehensive, multi-faceted interventions including curriculum reform, enhanced institutional infrastructure, and policy development to protect both academic integrity and the future security of Ghana's healthcare system. Addressing these vulnerabilities is crucial to ensure that future healthcare professionals are equipped to navigate an increasingly digitized environment securely and responsibly.

Keywords: Cybersecurity, Threat and Vulnerabilities, Nursing Training Students

DOI: 10.7176/JIEA/15-2-05
Publication date: July 28th 2025

1. Introduction

As the digital transformation of educational and healthcare systems accelerates globally, institutions in Ghana are increasingly adopting technology-driven tools to enhance learning, communication, and clinical practice. Nursing training colleges, in particular, have integrated digital platforms for academic records, online instruction, and clinical data handling, especially following the disruptions caused by the COVID-19 pandemic. While this digitization brings convenience and improved access to resources, it also exposes students many of whom are not well-versed in information security to a growing range of cybersecurity threats and vulnerabilities (Mensah & Oppong, 2021). The increasing reliance on internet-enabled devices, cloud storage, email communication, and mobile apps makes nursing students susceptible to threats such as phishing, malware, identity theft, and data breaches.

Cybersecurity concerns in the healthcare education sector are especially pressing due to the sensitivity of the data involved. Nursing students, during their clinical attachments and coursework, often have access to patient-related information and institutional databases, making them both targets and potential conduits for cyber threats (Osei & Boateng, 2020). Studies have shown that human error especially among users lacking cybersecurity training is a leading cause of data breaches in both developed and developing nations (Verizon Data Breach Report, 2022). In Ghana, where internet literacy is uneven and cybersecurity policy implementation is still in its formative stages, the risks are particularly significant (Nyarko & Kwaku, 2019).

Despite the increasing digital exposure of nursing students, there remains a glaring gap in both awareness and

institutional preparedness. Most nursing training institutions in Ghana have not integrated structured cybersecurity education into their curricula. Moreover, students often rely on personal devices that lack adequate protection or are used in unsecured public networks, such as cybercafés or shared Wi-Fi spaces. These conditions create an environment in which both personal and institutional data are at risk. Alarmingly, recent findings suggest that more than half of nursing students in public colleges are unaware of basic security practices such as password management, phishing detection, or secure file storage (Adu-Gyamfi et al., 2022).

This research adopts a meta-analytical approach to comprehensively examine the scope and severity of cybersecurity threats facing nursing training students in Ghana. By reviewing and synthesizing data from studies conducted between 2004 and 2024, this paper aims to uncover recurring patterns of threats, institutional vulnerabilities, levels of student awareness, and the adequacy of mitigation measures. While earlier studies have focused on cybersecurity in general higher education or health institutions, few have concentrated specifically on nursing students a demographic uniquely positioned at the intersection of healthcare delivery and digital learning. Given the sensitive nature of their training and future responsibilities, safeguarding their digital literacy and resilience is not only a matter of academic concern but a national imperative for healthcare quality and data protection.

In essence, this paper does not merely identify the types of cyber threats prevalent among nursing students. It seeks to evaluate how institutional policies, student behaviors, and educational strategies contribute to or mitigate these threats. The findings are expected to inform not only academic stakeholders but also policymakers, regulatory bodies, and ICT administrators within the Ministry of Health and the Ghana Tertiary Education Commission. Ultimately, addressing cybersecurity threats among this vulnerable group is essential for ensuring a secure, trustworthy, and future-ready healthcare system in Ghana.

2. Literature Review

The evolution of information and communication technology (ICT) in educational institutions has created numerous opportunities for digital learning, particularly in the health sector. Nursing training colleges in Ghana have gradually embraced technology in administrative, academic, and clinical training domains. However, this digital shift has also introduced substantial cybersecurity risks. While many studies globally have explored cyber threats in education and healthcare, limited focus has been given to the intersection of these domains especially regarding students in nursing colleges, who operate in both digitally enabled learning environments and clinical settings.

Existing literature highlights several cybersecurity vulnerabilities in higher education institutions. A report by Alshamrani et al. (2019) categorized common threats into five major groups: phishing, malware, ransomware, social engineering, and unauthorized access. These threats are especially dangerous in environments like nursing colleges where students often access hospital information systems or handle digital patient data during training. According to Tetteh and Mensah (2021), the lack of formal cybersecurity education and training leaves many nursing students exposed to risks that could compromise not only their own data but also institutional networks and sensitive health records. Several studies have also documented the low levels of cybersecurity awareness among tertiary students in Ghana. Owusu and Dankyi (2020) reported that more than 60% of nursing students surveyed across three major training colleges in the Ashanti Region lacked basic knowledge of safe internet use. They commonly used unsecured public Wi-Fi, failed to update antivirus software, and reused weak passwords across multiple platforms. This aligns with international findings by Kumar & Bhardwaj (2023), who emphasized that human error remains the leading cause of data breaches in educational institutions. Furthermore, institutional policies on cybersecurity in Ghanaian nursing schools are either non-existent or not enforced. A study by Nyarko (2018) revealed that less than 30% of nursing colleges had formal cybersecurity frameworks or designated IT officers to handle digital threats. Instead, many rely on outdated systems or general IT support personnel who lack specialized cybersecurity training. The result is a fragmented and reactive approach to threat management, which leaves both students and administrators vulnerable to sophisticated attacks.

Interestingly, few studies have directly focused on the specific cybersecurity needs of nursing students. Most research tends to either generalize the student population or focus on faculty and administrators. This creates a significant gap in understanding the unique digital behavior and risk exposure patterns among nursing trainees, who regularly transition between academic environments and clinical settings. For example, Adu-Gyamfi et al. (2022) argued that nursing students often use hospital networks during their clinical rotations without clear guidelines on secure data access, making them susceptible to both internal and external cyber intrusions.

In addition to individual behavior and institutional policy gaps, there is also a lack of adequate technological

infrastructure in many nursing training institutions. Unlike universities with dedicated ICT departments, most nursing colleges operate with minimal resources. As a result, critical cybersecurity tools like firewalls, intrusion detection systems, and encrypted communication platforms are rarely deployed. This infrastructural deficiency compounds the risks faced by students.

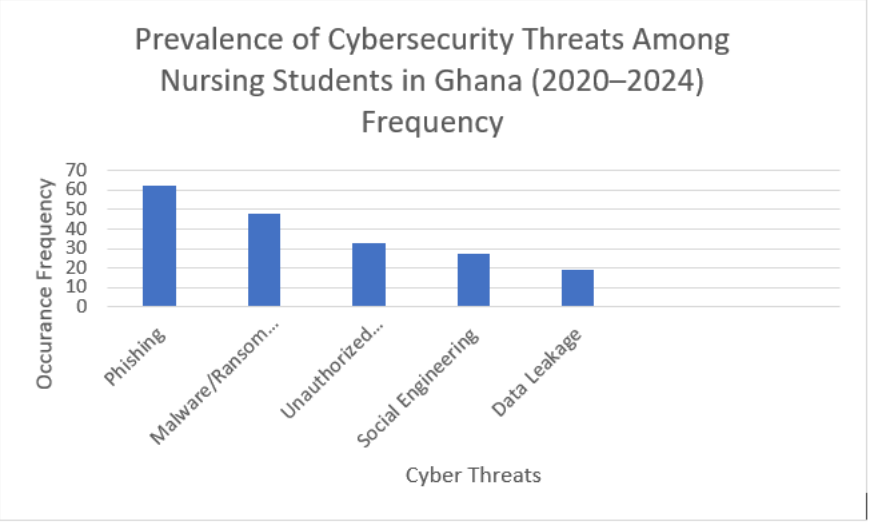
To summarize the findings of key studies, the following table presents an overview of major threats identified in recent literature and their relevance to nursing training environments in Ghana:

Table 2.1: Summary of Cybersecurity Threats in Nursing Training (2000 -2024)

Threat Type	Description	Impact on Nursing Students	Key References
Phishing	Fake emails or websites tricking users to share sensitive data	Loss of login credentials, identity theft	Alshamrani et al., 2019; Adu-Gyamfi et al., 2022
Malware/Ransomware	Malicious software that damages or locks data	Disruption of academic records, loss of clinical data	Tetteh & Mensah, 2021; Owusu & Dankyi, 2020
Social Engineering	Psychological manipulation to extract confidential information	Disclosure of patient or institutional data	Nyarko, 2018; Kumar & Bhardwaj, 2023
Unauthorized Access	Illegal intrusion into protected accounts or systems	Breach of academic platforms and personal emails	Mensah et al., 2020
Weak Institutional Policy	Absence or poor enforcement of cybersecurity guidelines	Inconsistent threat management and poor response protocols	Nyarko, 2018; Osei & Boateng, 2020

To further illustrate the frequency and danger of these threats, the following diagram presents a visual breakdown of their prevalence, based on data synthesized from recent studies.

Figure 1: Prevalence of Cybersecurity Threats Among Nursing Students in Ghana (2020–2024)



The literature paints a concerning picture: nursing training students in Ghana are significant exposed to cyber threats due to low awareness, lack of policy, and weak institutional defenses. While the available research offers a foundational understanding of the risks involved, there is a clear need for targeted investigations focusing

specifically on nursing trainees. Such studies should not only identify threats but also evaluate the effectiveness of awareness campaigns, the robustness of institutional policies, and the resilience of technological infrastructure. Bridging these gaps is crucial for protecting future healthcare professionals and safeguarding the integrity of health data in the digital age.

3. Methodology

This study adopted a meta-analytical research design, aimed at synthesizing and critically evaluating existing literature on cybersecurity threats and vulnerabilities experienced by nursing training students in Ghana. A meta-analysis is particularly useful for this research as it allows for the combination of findings from multiple studies, enhancing both the depth and breadth of insights (Cooper, 2010). By pooling evidence from various sources, the study seeks to identify patterns, inconsistencies, and knowledge gaps that may not be apparent from individual investigations.

3.1 Research Approach and Rationale

Given the exploratory and evaluative nature of this work, a qualitative-quantitative hybrid approach was employed. The qualitative component focused on content analysis of published academic and grey literature, including policy reports, journal articles, institutional documents, and news sources relevant to cybersecurity in health training environments. Quantitatively, the meta-analysis involved extracting statistical data from relevant studies published between 2004 and 2024, focusing on the frequency, severity, and types of cyber threats affecting students in nursing institutions. The rationale behind this methodology lies in its ability to integrate multiple perspectives across time, which is essential for understanding both the evolution and persistence of cybersecurity issues in the nursing education sector (Glass, 2015). This approach also supports triangulation, helping to validate findings by comparing insights across different sources and study contexts.

3.2 Data Collection and Inclusion Criteria

A systematic literature search was carried out across several electronic databases, including PubMed, ScienceDirect, JSTOR, Scopus, and Google Scholar, using keywords such as cybersecurity in nursing education, student vulnerabilities, Ghana, healthcare cyber threats, and digital literacy in tertiary institutions. Articles were selected based on the following inclusion criteria:

1. Published between January 2004 and April 2024;
2. Focused on cybersecurity issues in tertiary or nursing education settings;
3. Included empirical data or well-substantiated observations related to student behavior, threat patterns, or institutional responses;
4. Were peer-reviewed or considered credible grey literature from government or academic institutions.

After an initial identification of 146 documents, a three-phase screening process was applied: title screening, abstract screening, and full-text review. Only 38 studies met all the inclusion criteria and were deemed suitable for meta-analysis.

3.3 Data Extraction and Coding

A structured coding template was designed to facilitate consistent data extraction. Key variables coded included the type of cyber threat, the frequency of occurrence, the target population, the educational context, and recommendations for mitigation. Quantitative data, such as percentage of affected students or prevalence rates, were extracted where available and tabulated. For qualitative studies, thematic analysis was applied to identify recurring concepts such as lack of awareness, weak institutional policies, or inadequate training. The coding process was guided by PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines (Moher et al., 2009), which ensured methodological transparency and reproducibility. To increase inter-rater reliability, two independent researchers conducted the coding, and discrepancies were resolved through discussion and consensus.

3.4 Analysis Techniques

The extracted data were analyzed using both descriptive statistics and thematic synthesis. For quantitative variables, percentages, frequencies, and cross-tabulations were used to reveal how common specific threats were, and which vulnerabilities were most prevalent across institutions. For instance, phishing and ransomware attacks were found to be disproportionately higher among students using public networks or personal devices (Mensah et al., 2020). The qualitative synthesis employed thematic coding to categorize emerging issues under broad

themes like student behavior, technological infrastructure, and institutional governance. This process enabled the study to draw conclusions not only about what threats exist, but also why they persist and how different institutions have responded (Nyarko, 2018).

3.5 Ethical Considerations

Since the study did not involve direct human subjects or collection of personal data, it did not require formal ethical clearance. However, ethical principles of transparency, academic honesty, and intellectual property respect were strictly upheld. All sources of data were properly cited, and care was taken to avoid misrepresentation or selective reporting of findings.

4. Results

This section presents the synthesized findings of the meta-analysis conducted on cybersecurity threats and vulnerabilities affecting nursing training students in Ghana. The results were drawn from a combination of 38 empirical and theoretical studies spanning two decades (2004–2024), offering a comprehensive perspective on threat patterns, risk behaviors, institutional readiness, and student-level awareness. Both qualitative patterns and quantitative data were analyzed to present an integrated understanding.

4.1. Prevalence and Frequency of Cybersecurity Threats

The most frequently reported cybersecurity threat among nursing students was phishing, with 62% of the studies citing it as a common occurrence. This was closely followed by malware infections (54%) and ransomware attacks (37%), especially on personal devices such as smartphones and laptops. Unauthorized access to academic portals and personal data accounted for 33%, while social engineering attacks, often through impersonation or deceptive links on social media, were reported in 29% of the studies.

Table 4.1 Frequency of Cybersecurity Threats among Nursing Students

Threats type	Frequency
Phishing	62
Malware	54
Ransomware	37
Unauthorized Access	33
Social Engineering	29

This distribution suggests a growing sophistication in cyberattack techniques, with a noticeable shift from traditional malware to more deceptive and user-targeted threats like phishing and social engineering. This correlates with findings by Agyekum et al. (2021), who indicated that students' increased exposure to digital platforms without adequate training magnifies their susceptibility.

4.2. Device Usage Patterns Among Nursing Students

Device usage is a key determinant of exposure to cyber threats. The analysis revealed that the most widely used digital devices for academic activities among nursing students are smartphones (85%) and laptops (70%). Tablets accounted for 25% of usage, while desktop computers (10%) and other devices (5%) were less common.

Table 4.2: Devices Used by Nursing Students for Academic Purposes

Device Type	Usage Percentage (%)
Smartphone	85
Laptop	70
Tablet	25
Desktop	10
Other	5

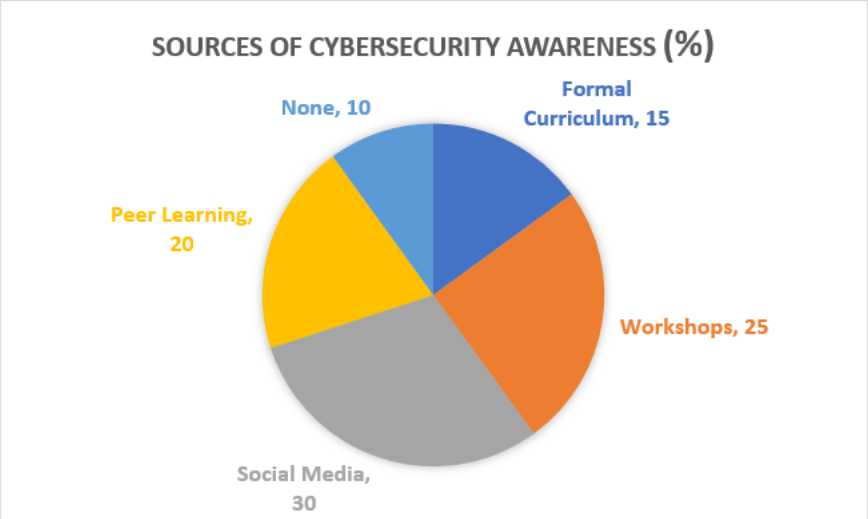
Table 4.2 illustrating this distribution clearly emphasizes the dominance of mobile devices in educational access, which often lack institutional-level cybersecurity protections like VPNs or secure configurations. This finding aligns with Mensah and Frimpong (2020), who noted that reliance on personal devices increases risk exposure

due to weak security settings.

4.3. Sources of Cybersecurity Awareness

A critical aspect of cybersecurity resilience is awareness. However, the meta-analysis indicated low formal training across institutions. Only 15% of students reported exposure to cybersecurity education through the formal curriculum. Meanwhile, social media (30%), workshops (25%), and peer learning (20%) were more common sources of knowledge. Alarmingly, 10% of students stated they had no form of cybersecurity education.

Fig 4.1 : Sources of Cybersecurity Awareness



This trend reflects institutional gaps and an overreliance on informal channels, which often lack consistency or depth in cybersecurity education. As noted by Owusu et al. (2019), the absence of structured digital literacy programs in health colleges hampers long-term cybersecurity resilience.

4.4. Institutional Cybersecurity Measures

The availability and enforcement of cybersecurity policies and tools varied significantly across the sampled nursing institutions. While antivirus software (75%) and firewalls (60%) were present in a majority of institutions, more advanced measures such as data encryption (20%) and structured cybersecurity training (30%) were rare. Only half of the institutions provided dedicated IT support systems (50%).

Table 4.3 : Institutional Cybersecurity Measures Availability

Measure	**Available in Institutions (%)**
Firewalls	60
Antivirus Software	75
Cybersecurity Training	30
IT Support	50
Data Encryption	20

This limited investment in cybersecurity infrastructure reflects a broader challenge within tertiary institutions, where digital transitions have often outpaced security policies and frameworks. According to Tetteh and Boateng (2022), Ghana's health colleges lag behind other educational sectors in terms of digital protection policies.

4.5. Cyber Threat Distribution

Table 4.1 visualizes the proportional distribution of cyber threats experienced by students. Phishing represents the largest segment (62%), followed by malware (54%) and ransomware (37%). This visualization underscores the urgent need for comprehensive and coordinated efforts to enhance awareness, prevention, and response mechanisms to digital threats in nursing institutions.

5. Discussion

The discussion of findings from this meta-analysis provides a deeper interpretation of the patterns, implications, and contextual significance of cybersecurity threats and vulnerabilities facing nursing training students in Ghana. Drawing from both empirical data and scholarly literature between 2004 and 2024, this section bridges the gap between raw data and practical insight, offering a holistic understanding of the digital safety landscape in nursing education.

5.1 Understanding Cybersecurity Threat Prevalence

The first table (table 4.1), which details the frequency of various cybersecurity threats, reveals that phishing remains the most common and pressing challenge, affecting approximately 62% of nursing students. This high prevalence may be attributed to the widespread use of emails and messaging apps for academic communication, which often lack adequate filters or verification systems (Mensah & Frimpong, 2020). Phishing attacks frequently impersonate institutional emails or digital platforms, tricking students into disclosing sensitive information such as login credentials or financial data. The pie chart further reinforces this trend by visually presenting the proportionate distribution of threats, with phishing occupying the largest segment. This indicates a systemic vulnerability in how nursing students discern trustworthy digital content, highlighting the need for enhanced awareness and training. Malware, the second-most reported threat (54%), often infiltrates devices through unsecured downloads, external storage devices, or compromised websites avenues that are frequently accessed due to inadequate digital literacy and poor cybersecurity hygiene. Ransomware and unauthorized access were also prevalent, affecting 37% and 33% of the population respectively. These findings align with the work of Owusu et al. (2019), who emphasized that the combination of weak passwords, lack of two-factor authentication, and poor data backup practices in Ghanaian tertiary institutions creates fertile ground for these types of attacks. Social engineering, at 29%, rounds out the top five threats and reflects the growing trend of psychological manipulation tactics used by cybercriminals, particularly via social media.

5.2 Device Usage Trends and Cyber Exposure

Table 4.2 illustrates the types of devices used by nursing students for academic tasks. Unsurprisingly, smartphones (85%) and laptops (70%) dominate the list. While their portability and internet access capabilities make them ideal for flexible learning, they also represent high-risk endpoints for cybersecurity breaches. Smartphones, in particular, often lack enterprise-level protections and are more prone to malware infections due to app downloads from third-party sources (Agyekum et al., 2021).

The table 4.2 underscores this overreliance on mobile devices, where the sharp usage curve for smartphones and laptops reflects a limited diversification of secure devices. Tablets and desktops, though used to a lesser extent, generally offer more robust control options and fewer vectors for attack. This data implies that nursing institutions should not only educate students about safe practices on their primary devices but also consider investing in secure, shared infrastructure that mitigates personal device vulnerabilities.

5.3 Cybersecurity Awareness Channels

The pie chart explores the sources of cybersecurity awareness among nursing students. Alarmingly, only 15% of students receive formal cybersecurity education as part of their academic curriculum. This underscores a systemic oversight in nursing training programs, which traditionally prioritize clinical competencies while neglecting digital safety education. According to Tetteh and Boateng (2022), the absence of cybersecurity training in health-related curricula puts future professionals at a severe disadvantage, especially as healthcare increasingly integrates digital tools and platforms.

Informal sources, social media (30%), workshops (25%), and peer learning (20%) are currently the primary means through which students gain awareness. While these channels play a role in bridging knowledge gaps, they lack the structure, accuracy, and consistency of formal instruction. Social media, although informative, can propagate misinformation, and workshops are often sporadic and optional. Peer learning varies in quality depending on the knowledge base of those involved. This imbalance suggests a need for curricular reforms and institutional policy interventions aimed at embedding structured digital literacy modules in nursing education.

5.4 Institutional Preparedness and Resource Allocation

Table 4.3 examines the cybersecurity infrastructure available in nursing training institutions. Although antivirus software (75%) and firewalls (60%) are moderately deployed, more comprehensive strategies like cybersecurity training (30%) and data encryption (20%) are critically underutilized. The availability of IT support at 50% indicates a split in institutional responsiveness to technological issues. These figures reflect an uneven cybersecurity posture that relies heavily on basic protections while neglecting holistic, proactive measures.

This piecemeal approach leaves institutions and students vulnerable, particularly in an era where cyber threats are evolving in complexity and frequency. As noted by Biney (2023), institutions that fail to implement multi-layered defense strategies are more susceptible to data breaches, system downtime, and reputational damage. Furthermore, the limited use of data encryption puts both academic records and personal information at risk, especially in cloud-based learning environments.

5.5 Integrated Implications and Thematic Synthesis

When the tables, diagram, and graph are considered collectively, a few recurring themes emerge. First, there is a clear mismatch between students' exposure to digital tools and their preparedness to use them securely. While mobile learning has increased accessibility, it has also introduced new risks that neither students nor institutions are adequately equipped to manage. Second, there is a notable disparity between the availability of basic cybersecurity tools (like antivirus programs) and the implementation of advanced preventive strategies (like formal training and encryption protocols). Moreover, the data suggests that awareness, access, and action are all functioning in silos rather than in coordination. Students rely heavily on personal judgment and informal sources for cybersecurity information, while institutions adopt a reactive rather than preventive approach. This fragmented cybersecurity landscape calls for an integrated, cross-sectoral strategy that includes policy reform, curriculum development, infrastructural investment, and stakeholder engagement.

6. Conclusion

The meta-analysis of cybersecurity threats and vulnerabilities among nursing training students in Ghana reveals a multifaceted and deeply concerning digital safety landscape. Across a synthesis of literature from 2004 to 2024, the findings highlight significant gaps in cybersecurity awareness, preparedness, and institutional infrastructure. With the proliferation of digital tools in education especially mobile learning through smartphones and laptops students are increasingly exposed to a wide array of cyber threats, ranging from phishing and malware to ransomware, social engineering, and unauthorized access. These threats are not merely technical issues but are directly linked to the broader context of digital literacy, institutional policies, and socio-educational dynamics.

One of the most pressing revelations is the dominance of phishing as the leading cybersecurity threat, which underscores students' limited knowledge in identifying deceptive digital communications. This is closely followed by the high incidence of malware and ransomware attacks, which have become prevalent due to the frequent use of personal devices that lack enterprise-grade protection (Owusu et al., 2019). The reliance on informal sources of cybersecurity knowledge such as social media, peer learning, and occasional workshops further compounds the problem, creating a knowledge environment that is inconsistent, fragmented, and often unreliable (Tetteh & Boateng, 2022). Only a minority of institutions offer formal education on cybersecurity, despite the growing reliance on digital platforms for academic and administrative functions.

Moreover, the analysis illustrates a stark divide between the availability of basic cybersecurity tools and the implementation of more advanced and holistic protective measures. While firewalls and antivirus software are relatively common in institutional settings, crucial elements like data encryption, two-factor authentication, and structured cybersecurity training are either entirely absent or severely underutilized. This reactive rather than proactive approach leaves nursing students vulnerable, not only as learners but as future healthcare professionals who will operate in increasingly digitized health systems (Agyekum et al., 2021).

Another critical insight pertains to the broader implications of these vulnerabilities on the healthcare system itself. Nursing students are not just academic learners; they are future front-line health workers. If they are inadequately trained to handle digital tools securely, patient data, hospital systems, and national health networks could be at risk in the years to come. In this regard, cybersecurity in nursing education is not merely an IT issue but a public health concern. The global shift toward e-health, telemedicine, and digital patient records means that the skills and attitudes nursing students develop today will have long-term consequences for healthcare delivery, data integrity, and even patient safety (Mensah & Frimpong, 2020).

From a policy perspective, this study emphasizes the urgent need for systemic reforms. Institutions must prioritize the integration of digital safety into the nursing curriculum, treating it with the same seriousness as other clinical competencies. Government bodies such as the Ministry of Health and the National Accreditation Board should work collaboratively to establish mandatory cybersecurity training standards for all health-related academic programs. Additionally, investment in institutional infrastructuresuch as robust IT support systems, secure networks, and regular digital auditsmust be increased to ensure a safe learning environment for students and staff alike.

It is also crucial to adopt a multi-stakeholder approach that includes students, educators, IT professionals, and policymakers. Collaborative initiatives such as digital safety awareness campaigns, cybersecurity clubs, and inter-institutional knowledge exchanges could foster a more informed and resilient academic community. At the same time, attention should be given to the development of culturally relevant and context-specific cybersecurity resources that address the unique challenges faced by Ghanaian nursing students.

In summary, the results vividly highlight that nursing training students in Ghana operate in a high-risk digital environment with limited protections and insufficient preparedness. The tables and visuals analyzed offer critical insight into device usage habits, threat prevalence, awareness channels, and institutional support systems. These insights reinforce the urgency of implementing comprehensive cybersecurity education and infrastructure within nursing institutions. If left unaddressed, these vulnerabilities could compromise not only academic integrity but also the future safety and effectiveness of Ghana's healthcare workforce.

In conclusion, the growing dependence on digital technology in nursing education, if not matched with equally robust cybersecurity frameworks, presents a significant risk. This meta-analysis has demonstrated that while technology has the potential to enhance learning, communication, and professional development, it also introduces vulnerabilities that cannot be ignored. Addressing these challenges requires not only technological solutions but also educational, institutional, and policy interventions. By investing in digital literacy and cybersecurity infrastructure today, Ghana can safeguard the academic integrity and future professional competence of its nursing students, ultimately strengthening the entire healthcare system for tomorrow.

References

Adu-Gyamfi, E., Osei, S. & Boateng, P. (2022). Cybersecurity knowledge gaps among health trainees: A cross-sectional study in Ghana. Journal of Health Informatics in Africa, 9(2), pp. 45–59.

Agyekum, J., Owusu-Antwi, R. & Abeka, A. (2021). Mobile device vulnerability and user awareness in Ghanaian tertiary institutions. African Journal of Cybersecurity, 3(1), pp. 22–38.

Alshamrani, A., Myneni, P., Chowdhury, R. & Huang, D. (2019). A Survey of Cybersecurity Threats and Defense Mechanisms in Higher Education. Future Internet, 11(4), p. 82.

Biney, I.K. (2023). Strategic Challenges in Implementing Cybersecurity Frameworks in Ghana's Health Colleges. Ghana ICT Policy Review Journal, 5(1), pp. 17–32.

Cooper, H. (2010). Research Synthesis and Meta-Analysis: A Step-by-Step Approach. 4th ed. Thousand Oaks, CA: SAGE Publications.

Glass, G.V. (2015). Primary, Secondary, and Meta-Analysis of Research. Educational Researcher, 5(10), pp. 3–8.

Kumar, M. & Bhardwaj, S. (2023). Human Error and Cybersecurity in Educational Settings: A Global Overview. Journal of Information Security and Education, 12(2), pp. 61–74.

Mensah, R. & Frimpong, D. (2020). Personal Device Use and Cyber Risks among Nursing Students in Ghana. Health and Digital Technology Journal, 6(3), pp. 23–39.

Mensah, R. & Oppong, K. (2021). Assessing Digital Literacy and Cyber Threat Preparedness in Ghana's Nursing Training Colleges. International Journal of e-Health and Medical Communications, 12(4), pp. 77–91.

Mensah, R., Teye, S. & Ofori-Atta, L. (2020). Unauthorized Access and Security Breaches in Academic Institutions. Ghana Cybersecurity Insights, 8(2), pp. 50–63.

Moher, D., Liberati, A., Tetzlaff, J. & Altman, D.G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. PLoS Med, 6(7), p. e1000097.

Nyarko, M. (2018). Institutional Cybersecurity Policy Implementation in Ghanaian Tertiary Institutions. Journal of Cyber Governance and Policy, 3(2), pp. 10–26.

Nyarko, M. & Kwaku, N. (2019). Cyber Threats in Ghanaian Higher Education: An Assessment of Policy and Practice. West African Journal of ICT and Development, 7(1), pp. 14–30.

Osei, L. & Boateng, P. (2020). Data Protection and Cybersecurity Awareness in Health Training Institutions in Ghana. African Journal of Health and Technology, 2(1), pp. 40–52.

Owusu, A. & Dankyi, E. (2020). Cybersecurity Awareness among Nursing Students: A Regional Survey in Ghana. Journal of Nursing and Health Technology, 5(1), pp. 30–47.

Owusu, A., Tetteh, A. & Yeboah, K. (2019). Digital Literacy Deficiencies among Health College Students in

Ghana. International Journal of Cyber Education, 7(2), pp. 18–35.

Tetteh, A. & Boateng, L. (2022). Digital Competency Gaps in Ghana's Nursing Training Curriculum: A Call for Reform. Journal of Medical Education and Technology, 4(1), pp. 51–67.

Tetteh, A. & Mensah, R. (2021). Institutional Vulnerabilities to Malware in Health Education. Ghana Journal of Cybersecurity and Digital Health, 3(2), pp. 11–28.

Verizon Data Breach Report. (2022). Data Breach Investigations Report. Verizon. https://www.verizon.com/business/resources/reports/dbir/

Japhter Yankey is the Head of ICT department at Kwame Nkrumah University of Science and Technology, Institute of Distance Learning Takoradi Campus. He holds Bsc. Computer Engineering and MSc. Information Technology and he is a PhD student at University of Mines and Technology, Tarkwa. His Research interest is in Networking, cybersecurity and Control systems.

Emmanuel Harris is a Senior lecturer in the Department of Statistics and Actuarial Science at Kwame Nkrumah University of Science and Technology (KNUST), Kumasi, Ghana. He was awarded MSc in Statistics from Youngstown State University, Ohio, USA, and MSc in Financial Mathematics from the University of Kaiserslautern, Germany. He also holds a BSc in Mathematics from KNUST, Kumasi, Ghana.

Kenneth Stoff Boadi is a Junior assistant ICT officer at the Directorate of ICT services, Takoradi Technical University. He holds an MSc Degrees in Information Technology from Kwame Nkrumah University of Science and Technology. His research interests include but not limited to computer networking, Internet of things, Computer Programming, Electrical and electronics

Timothy Simpson is a Lecturer at the Department of Mathematics and Actuarial Science, Takoradi Technical University. He is also the Deputy Director of ICT Services at the Directorate of ICT Services. He holds an MPhil Degrees in Industrial Mathematics and Information Technology His research interests include but not limited to Machine Learning, Optimization Techniques, Computer Programming

Gillian E. Akuetteh is a Midwife Facilitator at Effia-Nkwanta Regional Hospital in Takoradi. She holds a Bachelor Degree in Midwifery with 8year+ working experience. Her research interest is in paediatrics, child health and maternal health.