Journal of Education and Learning Technology (JELT)
ISSN 2720-7730
Volume 6 Issue 4 April 2025 pp 203 - 218
Available online at: https://noyam.org/journals/jelt/
DOI: https://doi.org/10.38159/jelt.2025646

Evaluating the Impact of Staff Cybersecurity Culture on Cyber Resilience in Colleges of Education: Insights from 12 Colleges of Education in Ghana

Daniel Paa Korsah[1]

[1] Department of Mathematics and ICT, Komenda College, Ghana

ABSTRACT

Tertiary educational institutions have become increasingly reliant on computers and network technologies for their operations in the last few decades and this comes with a significant increase in cyber threats. Ghanaian Colleges of Education (CoEs), which are responsible for training teachers for basic schools, also face these cybersecurity challenges. A key solution to mitigating these challenges is the development of a robust cybersecurity culture among academic and non-academic staff. This study aimed to assess the impact of the Cybersecurity Act 2020 (Act 1038) on staff perceptions of the importance of cybersecurity, the effectiveness of technical measures against cyber threats and the perceived cyber resilience of the colleges. The study employed a mixed-method approach, using a descriptive cross-sectional survey design with a sample of 298 academic and non-academic staff from 12 colleges. A questionnaire and an interview guide were used to collect both quantitative and qualitative data. The findings revealed that awareness of the Cybersecurity Act 2020 was low among CoE staff, limiting its impact on their perception of cybersecurity importance. Despite low awareness of the Act, staff demonstrated a strong commitment to personal cybersecurity practices, indicating a need for structured institutional cybersecurity policies and training. The study emphasizes the need for targeted cybersecurity awareness programs for CoE staff and stronger collaboration between CoEs, the Ministry of Education and other stakeholders to establish a proactive cybersecurity culture. Empirical data on how staff in Ghanaian CoEs perceive and practice cybersecurity is presented, contributing to the expanding research on cybersecurity culture in educational institutions.

Correspondence
Daniel Paa Korsah
Email: danielpaakorsah@komendacollege.edu.gh

Publication History
Received: 6th January, 2025
Accepted: 3rd April, 2025.
Published: 17th April, 2025.

Keywords: *Cybersecurity Culture, Cyber Resilience, Staff Perceptions, Tertiary Education.*

INTRODUCTION

Information technology infrastructure has seen expanded growth in educational institutions in the last two decades. This transformation is driven by the need to integrate innovative teaching methods, enhanced communication among students and staff and the quest to achieve administrative efficiency. This increase, however, has also exposed institutions to a growing number of cyber threats, including cross-site scripting, malware injection, phishing scams and insider threats. As colleges generate and store large amounts of information, including students' personal records, administrative communications, accreditation and compliance information as well as alumni records, the consequences of cybersecurity breaches can be severe, leading to financial losses, reputational damage

and legal suits.[1] The concept of cybersecurity has thus emerged as a critical factor in protecting the IT infrastructure of these institutions and the individuals therein. Cybersecurity culture covers the attitudes of staff and students, technical knowledge, infrastructure and knowledge regarding cyber protection.[2] This is directed by organisational policies, training programs and the overall commitment of leadership to ensure cyber protection.

Research shows that an organisations' ability to recover from cyber attacks and respond to cyber incidents is a result of a robust cyber security culture.[3] Organisational cyber security culture involves identifying key cyber security behaviors, establishing a cyber security champion network, building a cyber security hub and aligning security awareness activities with internal and external campaigns.[4] Colleges of Education (CoEs) face unique challenges in cultivating a robust cybersecurity culture. This is partly due to the absence of policy frameworks and diverse backgrounds and varying levels of technical expertise among staff.[5] Moreover, in as much as the culture of openness and collaboration is beneficial for learning in educational environments, it can inadvertently undermine security measures in campus cyberspace if not managed properly. Given this complexity, it is crucial to examine how staff perceptions and behaviors shape the cyber resilience of these institutions. The Cybersecurity Act 2020 (Act 1038) passed in November 2020 serves as a framework for enhancing cybersecurity practices in organisations, including educational institutions.

The Act requires that organisations implement comprehensive strategies to protect sensitive information and mitigate risks.[6] Despite this regulatory framework, there is still limited understanding of how the cybersecurity culture among staff influences cyber resilience in CoEs in Ghana. Ensuring compliance with cyber protection policies requires not only technical controls but also a strong cyber protection culture among personnel. However, the extent to which the Cybersecurity Act 2020 has shaped staff perceptions, behaviors and institutional resilience remains unclear. Cybersecurity culture, which encompasses the attitudes, behaviors, knowledge and awareness of personnel regarding cyber risks, plays a critical role in protecting an institution's information assets. In educational institutions, where digital infrastructures are increasingly relied upon for administrative and instructional activities, staff perceptions of cybersecurity and their adherence to best practices are pivotal in maintaining a secure cyber environment. A weak cybersecurity culture among academic and non-academic staff may expose CoEs to cyber threats, undermining the effectiveness of cybersecurity policies and technical safeguards. Existing studies on cybersecurity have primarily focused on technical vulnerabilities, policy implementation, and the development of cyberculture, with little emphasis on how institutional cybersecurity policy affects cyber resilience.[7] Furthermore, there is limited empirical evidence on the extent to which CoEs in Ghana have integrated awareness and practices in response to the Cybersecurity Act 2020.

This study seeks to bridge this gap by evaluating the impact of staff cybersecurity culture on cyber resilience in 12 CoEs in Ghana. To explore the relationship between cybersecurity policies,

---

[1] Steven Furnell and Jayesh Navin Shah, "Home Working and Cyber Security – an Outbreak of Unpreparedness?," *Computer Fraud & Security* 2020, no. 8 (January 2020): 6–12, https://doi.org/10.1016/S1361-3723(20)30084-1.

[2] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," February 26, 2024, https://doi.org/10.6028/NIST.CSWP.29.

[3] Muhammad Fakhrul Safitra, Muharman Lubis, and Hanif Fakhrurroja, "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity," *Sustainability* 15, no. 18 (September 6, 2023): 1–32, https://doi.org/10.3390/su151813369.

[4] Moneer Alshaikh, "Developing Cybersecurity Culture to Influence Employee Behavior: A Practice Perspective," *Computers & Security* 98 (November 2020): 1–20, https://doi.org/10.1016/j.cose.2020.102003.

[5] Yan Chen et al., "Understanding Inconsistent Employee Compliance with Information Security Policies Through the Lens of the Extended Parallel Process Model," *Information Systems Research* 32, no. 3 (September 2021): 1043–65, https://doi.org/10.1287/isre.2021.1014.

[6] Ministry of Communications and Digitalisation. 2024. *National Cybersecurity Awareness Month Launched to Educate Public on Digital Safey.* September 2, accessed December 4, 2024. https://moi.gov.gh/newsroom/2024/09/national-cybersecurity-awareness-month-launched-to-educate-public-on-digital-safey/.

[7] Rifel Jeene Celeste and Nimfa Osias, "Challenges and Implementation of Technology Integration: Basis for Enhanced Instructional Program," *American Journal of Arts and Human Science* 3, no. 2 (June 4, 2024): 106–30, https://doi.org/10.54536/ajahs.v3i2.2656; Lawrence A Gordon, Martin P Loeb, and Lei Zhou, "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?," *Journal of Computer Security* 19, no. 1 (2011): 33–56; Betsy Uchendu et al., "Developing a Cyber Security Culture: Current Practices and Future Needs," *Computers & Security* 109 (October 2021): 102387, https://doi.org/10.1016/j.cose.2021.102387.

institutional practices and staff perceptions, this study seeks to address the following research questions:

1. What is the impact of the Cybersecurity Act 2020 (Act 1038) on staff perception of the importance of cybersecurity in CoEs in Ghana?
2. How effective are the technical measures implemented by CoEs in protecting against cybersecurity threats, according to staff perceptions?
3. What is the perception of CoE teachers with respect to the cyber resilience of their colleges?

By identifying these vulnerabilities, the institutions can tighten targeted measures aimed at improving their cyber resilience. The findings of this research will also offer valuable insights for IT staff, college administrators and policymakers. By examining the influence of staff attitudes and practices on cyber resilience, the findings of this research can guide the creation of effective policies and training programs specifically designed to protect personal and organisational data. This is intended to increase cyber resilience, creating a safer cyberspace for the colleges. Furthermore, this research contributes to the expanding literature on cybersecurity in educational institutions with specific reference to CoEs. By concentrating on the colleges, the study addresses a knowledge gap that provides insights that can be applied to other educational settings, thereby pushing the frontiers of knowledge on cybersecurity in academia. The study is structured into key sections, including the Introduction, which outlines the background, problem statement and research questions. The Literature Review examines cybersecurity culture in educational institutions, while the Methodology explains the survey approach and sampling methods. The Findings and Discussion analyze staff perceptions and institutional cybersecurity measures. Finally, the Conclusion and Recommendations highlight key insights and propose strategies to strengthen cybersecurity culture and resilience in colleges.

LITERATURE REVIEW

Cybersecurity Culture in Educational Institutions

Cybersecurity culture encompasses the collective attitudes, values and practices regarding cybersecurity within an organization.[8] In the context of educational institutions, a strong cybersecurity culture is important for ensuring that both staff and students are aware of the potential threats and are prepared to respond to them accordingly. It is evident that a robust cybersecurity culture can significantly improve an institution's cyber resilience.[9] Developing a strong cybersecurity culture in educational institutions presents unique challenges. Diverse student and staff backgrounds, varying technical proficiency and the dynamic nature of educational settings can hinder effective cybersecurity implementation.[10] Moreover, many educators may underestimate the significance of cybersecurity, perceiving it as a technical issue rather than a fundamental aspect of their roles.[11] To nurture an effective cybersecurity culture in educational environments, comprehensive training and awareness programs are essential. It must be noted that well-structured cybersecurity awareness initiatives can considerably affect staff behaviors and attitudes, leading to enhanced security practices.[12] Additionally, promoting open dialogue about cybersecurity concerns can promote a proactive culture of identifying and mitigating risks.[13] The Cybersecurity Act 2020 (Act 1038) passed by the parliament of Ghana serves as a significant framework aimed at improving cybersecurity practices across multiple sectors, including higher education. The law highlights the importance of institutions adopting

[8] Anagha Anilkumar, Filip Dimitrov, and Anup Narayanan, "The Differences and Relationship Between Awareness, Behavior, and Cyber Security Culture," November 29, 2023, https://securityquotient.io/the-differences-and-relationship-between-awareness-behavior-and-culture-in-cyber-security/.

[9] Celeste and Osias, "Challenges and Implementation of Technology Integration: Basis for Enhanced Instructional Program."

[10] Madhav Mukherjee et al., "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes," *Information* 15, no. 2 (February 18, 2024): 1–23, https://doi.org/10.3390/info15020117.

[11] N. A. A Rahman et al., "The Importance of Cybersecurity Education in School," *International Journal of Information and Education Technology* 10, no. 5 (2020): 378–82, https://doi.org/10.18178/ijiet.2020.10.5.1393.

[12] Sunil Chaudhary, Vasileios Gkioulos, and Sokratis Katsikas, "Developing Metrics to Assess the Effectiveness of Cybersecurity Awareness Program," *Journal of Cybersecurity* 8, no. 1 (January 28, 2022): 1, https://doi.org/10.1093/cybsec/tyac006.

[13] Sivaraju Kuraku et al., "Cultivating Proactive Cybersecurity Culture among IT Professional to Combat Evolving Threats," *International Journal of Electrical, Electronics and Computers* 8, no. 6 (2023): 01–07, https://doi.org/10.22161/eec.86.1.

proactive measures for cybersecurity, thereby shaping staff perceptions of its importance.[14] It also seeks to regulate cybersecurity activities, protect critical information infrastructure and promote the development of a secure cyberspace in various institutions in Ghana. Examining this framework and its impact on cybersecurity culture is crucial for assessing cybersecurity practices in CoEs.

The Importance of Cybersecurity Measures in Protecting Data

The implementation of robust cybersecurity measures is important for safeguarding sensitive data and also preserving the integrity of the systems. Technical measures encompass the tools and systems deployed to protect information systems from cyber-attacks. In the Ghanaian tertiary education context, these measures are integral to establishing a secure environment that supports teaching and learning. Universities and colleges typically implement several technical measures, including access controls, intrusion detection systems, malware solutions, internet content filtering, firewalls and data encryption. Firewalls act as gateways between internal networks and external risks, regulating data traffic, providing access control and preventing unauthorized access based on predetermined security rules.[15] Intrusion detection systems track network traffic for any suspicious activities and can notify network administrators of potential security breaches, allowing swift intervention.[16] Firewalls and content filtering play a crucial role in securing institutional networks by regulating data traffic and blocking access to malicious or inappropriate content.

However, their effectiveness heavily depends on staff and student compliance with security protocols. If users attempt to bypass firewalls using VPNs or proxy servers, or if they disregard safe browsing practices, these security measures may become ineffective. Additionally, content filtering relies on users adhering to acceptable use policies; otherwise, unauthorized access to restricted sites or downloading harmful files can expose the system to cyber threats. Therefore, fostering a strong cybersecurity culture among staff and students is essential for ensuring the success of these technical safeguards. If staff and students disregard security procedures, even the most sophisticated technical solutions may be ineffective.[17] Therefore, making sure that these technological safeguards are used appropriately requires cultivating a healthy cybersecurity culture.

The Impact of Staff Perception on Cybersecurity Practices in Educational Institutions

Staff perception regarding the effectiveness of technical measures usually put in place by IT staff greatly influences their willingness to incorporate cybersecurity practices into their daily routines. Research by Sigurosson indicates that if staff find cybersecurity measures cumbersome or ineffective, their compliance may diminish, increasing the risk of vulnerabilities.[18] Therefore, it is important for colleges not only to focus on implementing technical measures but also involve staff in assessing and improving upon the security measures put in place.[19] By aligning cybersecurity practices with national legislation, CoEs can enhance their overall security posture and ensure compliance with legal standards. Staff training and awareness initiatives are crucial for fostering a strong cybersecurity culture within CoEs. These programs equip staff with the necessary knowledge and skills to identify, prevent and respond effectively to cyber threats. Given that human behavior is frequently seen as the

[14] Ministry of Communications and Digitalisation, "National Cybersecurity Awareness Month Launched to Educate Public on Digital Safety," September 2, 2024, https://moi.gov.gh/newsroom/2024/09/national-cybersecurity-awareness-month-launched-to-educate-public-on-digital-safey.

[15] Raed Alsaqour, Ahmed Motmi, and Maha Abdelhaq, "A Systematic Study of Network Firewall and Its Implementation," *International Journal of Computer Science & Network Security* 21, no. 4 (2021): 199–208.

[16] Catherine Chipeta, "What Is an Intrusion Detection System (IDS)? + Best IDS Tools," , November 18, 2024, https://www.upguard.com/blog/intrusion-detection-system.

[17] Kuraku et al., "Cultivating Proactive Cybersecurity Culture among IT Professional to Combat Evolving Threats."

[18] Ragnar Sigurðsson, " The Human Element: A Crucial Aspect of Cyber Risk Assessment Services and 8 Ways to Address It," July 27, 2023, https://awarego.com/the-human-element-in-cyber-risk-assessment-services/.

[19] Dawit Tolossa, "Importance of Cybersecurity Awareness Training for Employees in Business," *VIDYA - A JOURNAL OF GUJARAT UNIVERSITY* 2, no. 2 (August 8, 2023): 104–7, https://doi.org/10.47413/vidya.v2i2.206.

weakest link in cybersecurity, improving staff awareness is vital for enhancing overall cyber resilience.[20]

Challenges in Implementing Effective Cybersecurity Training in Colleges

Despite the numerous benefits, many colleges face obstacles when implementing effective training and awareness programs, they include budget limitations, time constraints and a lack of expertise. These can impede the development and execution of comprehensive training initiatives.[21] In addition, staff attrition can disrupt continuous training efforts, which in turn complicates the maintenance of consistent levels of awareness and compliance throughout the institution. The success of training programs often depends on their relevance and engagement. Programs that are excessively technical or not tailored to the specific needs of educational staff may struggle to capture interest and encourage lasting behavioral change.[22] It is imperative for colleges to create training programs that are informative, interactive and pertinent to the day-to-day responsibilities of staff.

Cyber Resilience in Educational Institutions

Cyber resilience refers to an organisation's capacity to prepare for, respond to and recover from cyber incidents while maintaining confidentiality, availability and integrity of sensitive data.[23] In educational institutions, fostering a culture of cyber resilience is particularly important due to the increased reliance on digital technologies for teaching and learning as well as for administrative duties. Due to the diverse users and technological skill levels in CoEs, fostering cybersecurity awareness is essential for safety. Educational institutions are frequently targeted by cyberattacks due to their rich stores of sensitive data including students' personal and academic records as well as research data. The ramifications of a cyber incident can be significant, resulting in data breaches, operational interruptions and reputational harm.[24] It is therefore important to develop effective cyber resilience strategies to ensure that teaching and learning continue in the face of cyberattacks while safeguarding the integrity of institutional data.

Building Cyber Resilience: Key Strategies for Educational Institutions

Key components of cyber resilience include risk assessment and management, incident response planning, ongoing training and awareness, collaboration and information sharing. Regular risk assessments enable institutions to pinpoint vulnerabilities and prioritize their cybersecurity efforts. A well-structured incident response plan is essential for mitigating the consequences of cyber incidents, detailing roles and responsibilities, communication protocols and recovery procedures to ensure prompt reactions to security breaches.[25] Continuous training and awareness initiatives improve staff comprehension of cybersecurity risks and best practices. Staff who are engaged and informed are more inclined to adopt secure behaviors, thus bolstering the institution's overall resilience.[26] Collaborating with other educational institutions, government entities and cybersecurity organisations further enhances cyber resilience. Sharing information about threats and best practices promotes a collective defense approach, improving the resilience of the entire educational sector.[27]

---

[20] Zheng Yan et al., "Finding the Weakest Links in the Weakest Link: How Well Do Undergraduate Students Make Cybersecurity Judgment?," *Computers in Human Behavior* 84 (2018): 375–82.
[21] Mukherjee et al., "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes," 4.
[22] Kuraku et al., "Cultivating Proactive Cybersecurity Culture among IT Professional to Combat Evolving Threats."
[23] Tolossa, "Importance of Cybersecurity Awareness Training for Employees in Business."
[24] Yan et al., "Finding the Weakest Links in the Weakest Link: How Well Do Undergraduate Students Make Cybersecurity Judgment?"
[25] Nur Aqilah Zaffan Farok and Mohamad Fadli Zolkipli, "Incident Response Planning and Procedures," *Borneo International Journal EISSN 2636-9826* 7, no. 2 (2024): 69–76.
[26] Misael Sousa de Araujo, Bruna Aparecida Souza Machado, and Francisco Uchoa Passos, "Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance," *Applied Sciences* 14, no. 5 (March 4, 2024): 1–16, https://doi.org/10.3390/app14052116.
[27] Kuraku et al., "Cultivating Proactive Cybersecurity Culture among IT Professional to Combat Evolving Threats."

Challenges to Cyber Resilience and Role of Stakeholders

Despite the critical need for cyber resilience, CoEs encounter various challenges in their implementation. Limited budgets can constrain investments in necessary technologies and training initiatives.[28] Furthermore, the rapid rate of technological change can often exceed institutions' capacity to update their defenses, leaving them vulnerable to emerging threats. Additionally, the diverse character of educational environments, which frequently encompasses varying levels of technical ability among staff and students, complicates the establishment of consistent security practices. Institutions must navigate these challenges while promoting a security culture that emphasizes the shared responsibility of all stakeholders in protecting digital assets. IT staff, faculty members, students and administrators all play a unique role in strengthening cybersecurity culture within educational institutions.

The Role of Stakeholders Enhancing Cyber Resilience in CoEs

In every educational institution, cybersecurity leaders play a pivotal role in setting the cybersecurity agenda. Their dedication to championing cybersecurity influences cybersecurity initiatives and the allocation of resources to protect virtual infrastructure. Effective administrative leadership promotes a culture that recognizes cybersecurity as an essential component of the safety of the educational ecosystem.[29] Administrative and technology leaders are also responsible for ensuring compliance with relevant regulations, such as the Cybersecurity Act 2020, which requires institutions to implement appropriate measures to safeguard sensitive information.[30] IT staff are the first line of defense against cyberattacks. They are responsible for executing and managing technical security measures, conducting regular assessments and responding to security threats and incidences.[31] One key function of IT staff is to educate other stakeholders about cybersecurity best practices and ensure adherence to security protocols across the school environment. Additionally, they play a critical role in facilitating ongoing training and awareness initiatives tailored to the unique needs of different categories of staff, usually with diverse backgrounds.[32] Academic staff significantly influence the cybersecurity culture within CoEs. Their interactions with students allow them to inculcate cybersecurity awareness into their teaching and encourage safe online practices among students.[33] By being models of secure behaviours and stressing its importance in their teaching, they can help create a security culture that goes beyond the classroom.

Students are both contributors to and beneficiaries of a strong cybersecurity environment. Their awareness level, attitudes and behaviour toward cybersecurity can impact the overall safety of the institution. Involving students' initiatives such as awareness campaigns, webinars and peer-led training can instill a sense of ownership and responsibility in them.[34] As students become educated about cybersecurity threats and best practices, they are more likely to adopt secure behaviours which increases the overall cyber resilience of the organisations. External stakeholders, such as technology vendors, cybersecurity consultants and government agencies, private sector companies and regulatory agencies also play a role in fortifying cybersecurity efforts in educational institutions. Collaborating with these partners can provide access to valuable expertise, resources and best practices that can strengthen the institution's cybersecurity framework. In addition, participating in information-sharing networks can enable institutions to stay current about vulnerabilities and emerging threats.[35] The efforts of all stakeholders are essential for ensuring a strong cybersecurity culture in CoEs. By ensuring collaboration and continuous engagement among all parties involved, educational institutions can

[28] Mukherjee et al., "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes."
[29] Mukherjee et al., "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes."
[30] Tolossa, "Importance of Cybersecurity Awareness Training for Employees in Business."
[31] Farok and Zolkipli, "Incident Response Planning and Procedures."
[32] Yan et al., "Finding the Weakest Links in the Weakest Link: How Well Do Undergraduate Students Make Cybersecurity Judgment?"
[33] Rahman et al., "The Importance of Cybersecurity Education in School."
[34] Kuraku et al., "Cultivating Proactive Cybersecurity Culture among IT Professional to Combat Evolving Threats."
[35] Deborah Housen-Couriel, "Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace," in *Cyber Peace* (Cambridge University Press, 2022), 39–63, https://doi.org/10.1017/9781108954341.003.

enhance their cybersecurity culture and improve their capacity to effectively mitigate and respond to current and emerging cyber threats.

THEORETICAL FRAMEWORK

This study adopted the Protection Motivation Theory (PMT) as the guiding framework to evaluate the impact of staff cybersecurity culture on cyber resilience in CoEs in Ghana. Developed by Rogers,[36] PMT provides a psychological perspective on how individuals assess threats and adopt protective behaviors in response to perceived risks. It is widely applied in cybersecurity research to understand compliance with security policies and best practices. PMT comprises two key cognitive processes: threat appraisal and coping appraisal. Threat appraisal involves evaluating the severity of cybersecurity threats and one's vulnerability to them, influencing staff perceptions of risks such as phishing, malware and data breaches.[37] Coping appraisal, on the other hand, assesses the effectiveness of protective actions (e.g., strong passwords, multi-factor authentication) and the confidence of staff in implementing these measures. The balance between these two processes determines the likelihood of adopting security-conscious behaviors. By applying PMT, this study examines how staff perceptions of cybersecurity threats and their ability to mitigate risks influence institutional cyber resilience. Understanding these dynamics can help develop targeted interventions, such as awareness training and policy enforcement, to foster a strong cybersecurity culture within CoEs.

METHODOLOGY

This study employed a mixed-method approach, using descriptive cross-sectional survey to collect both quantitative and qualitative data. The population of the study was made up of academic and non-academic staff from 12 CoEs in Ghana. Multi-stage sampling was used to select respondents. This sampling method was employed to enhance representativeness, feasibility and efficiency in selecting participants. Given the large and geographically dispersed population, a direct random sampling of individual participants across all CoEs would have been impractical. The use of multistage sampling allowed for a structured and systematic selection process while maintaining randomness at different stages. By adopting this sampling approach, the study balanced statistical rigor, logistical feasibility and inclusivity, making it a robust method for investigating cybersecurity awareness and resilience in CoEs. First, simple random sampling was used to select 12 colleges to participate in the study. There were 1,248 staff in the 12 colleges. Secondly, stratified random sampling was used to select 298 staff in the colleges for the study. The selected staff included teachers, administrative staff, IT support staff, finance and accounting staff and library staff. To ensure fair representation of staff across the selected 12 colleges a proportional allocation method was used to distribute the 298 sampled staff members. Given the total population of 1,248 staff, each college's sample size was determined based on its relative staff strength. Within each college, staff members were further stratified into teachers, administrative staff, IT support staff, finance and accounting staff and library staff. Proportional allocation was used to ensure that all staff categories were adequately represented. For example, in College A, where the total staff population was 108, a sample of 28 staff members was selected, consisting of 12 teachers, 6 administrative staff, 3 IT support staff, 5 finance and accounting staff and 2 library staff. Similarly, other colleges had their sample sizes determined based on their staff strength, ensuring equitable representation. This multi-stage sampling approach, combining random selection of colleges and stratified sampling of staff, ensured a representative and unbiased selection of participants to respond to the questionnaire.

A purposeful sub-sample of 35 participants was selected from the larger group to obtain richer qualitative insights that complemented the quantitative survey data. Building on the multi-stage sampling that initially yielded 298 staff members from 12 CoEs, the interviewees were chosen by first

[36] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," **Journal of Psychology** 91, no. 1 (1975): 93–114.

[37] Jian Mou et al., "A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach," **Journal of the Association for Information Systems** 23, no. 1 (2022): 196–236, https://doi.org/10.17705/1jais.00723.

identifying a diverse subset from the survey sample that included representatives from all staff categories; teachers, administrative staff, IT support staff, finance and accounting staff, and library staff, ensuring that the qualitative phase captured the distinctions and context behind the survey responses. The selection criteria emphasized including individuals with varying roles and lengths of service, thus incorporating insights from both academic and non-academic personnel and reflecting the multifaceted nature of cybersecurity challenges within the CoEs. In addition, participants who exhibited a strong interest in discussing cybersecurity awareness and resilience through their survey responses or follow-up expressions of interest were prioritized, ensuring that the interviewees were knowledgeable and engaged with the topic. The final number of 35 interviewees was determined based on data saturation, with the research team observing that no substantially new insights were generated after this number of interviews, thereby balancing comprehensive exploration of the subject matter with efficiency.

Instruments and Data Collection Procedure

The instruments for the study were developed by the researcher in accordance with the stated research objectives and literature review. The questionnaire was made up of 4 sections. Questions in Section One focused on collecting demographic information from the participants. Questions from Section Two were on eliciting information from participants on "Education and Awareness of Cybersecurity" in the CoEs. Section Three examined staff perceptions of the effectiveness of technical measures protecting CoEs against cybersecurity threats while Section Four focused on the perceptions of staff members with regards to cyber resilience in CoEs. The questionnaire was reviewed by experts in cybersecurity in education to establish its content validity. Face validity was also established by pre-testing the instrument at a college of education with similar characteristics as the colleges that participated in the study. The pre-testing was done to assess the instrument's dependability. The Cronbach's alpha coefficient was employed to assess the internal reliability and was found to be 0.79. This suggests that all the elements comprising the individual questionnaire items on the questionnaire have acceptable and good reliability.[38] Letters were presented to the principals of the selected colleges to seek permission for data collection before the study commenced. The questionnaires were administered online over a five-week period with participation being entirely voluntary. The interview guide consisted of open-ended questions designed to elicit detailed responses on the impact of the Cybersecurity Act 2020 on staff perceptions of cybersecurity, the effectiveness of technical measures in place and teachers' views on the cyber resilience of their institutions. The questions were refined through pilot testing with a small group of participants to ensure clarity, relevance, and the ability to probe deeper into the issues. Interviews were conducted via virtual platforms, recorded with consent, and later transcribed for thematic analysis, ensuring that the qualitative data provided a rich complement to the quantitative findings of the study.

DATA ANALYSIS

Linear regression analysis was conducted to examine the impact of staff knowledge of the Cybersecurity Act (2020) on their perceptions of cybersecurity culture (Research Question 1). Descriptive statistics, including means and standard deviations were used to analyze staff perceptions of the effectiveness of technical cybersecurity measures implemented by IT staff (Research Question 2) and the cyber resilience of the participating colleges (Research Question 3). In addition, the qualitative interview responses were transcribed, coded and thematically analyzed to identify recurring patterns and insights related to staff attitudes and experiences, thereby complementing the quantitative findings and enriching the overall interpretation of the results.

[38] Darren George and Paul Mallery, *IBM SPSS Statistics 26 Step by Step: A Simple Guide and Reference* (New York: Routledge, 2020), https://doi.org/10.4324/9780429056765.

PRESENTATION OF RESULTS

This section presents the analysis of the data collected, organized thematically based on the three research questions formulated for the study.

Research Question 1: What is the impact of the Cybersecurity Act 2020 (Act 1038) on staff perception of the importance of cybersecurity in CoEs in Ghana?

Table 1: Impact of Cyber Security Act 2020 (Act 1038) Awareness on Staff Perception of Cybersecurity

Variables	Std Beta	t-value	sig
CS	.677	13.589	.000
R square	.459		
Adjusted R square F-value	.456 184.673		

The results in Table 1 indicate that awareness of the Cybersecurity Act 2020 (Act 1038) has a moderate impact on staff members' perceptions of the importance of cybersecurity, as evidenced by an adjusted R-square value of 0.456. This implies that the Act accounts for 45.6% of the variance in staff perceptions, while the remaining variance is influenced by other factors not included in the model.

Additionally, the model's regression slope is significantly different from zero ($F = 184.673$, $p < .001$), confirming that the model is statistically significant. The standardized regression estimate ($\beta = 0.677$, $p < .001$) further indicates a moderate positive influence of cybersecurity awareness on staff perception.

Research Question 2: How effective are the technical measures implemented by CoEs in protecting against cybersecurity threats, according to staff perceptions?

Table 2: Effectiveness of Technical Measures Implemented by CoEs to Protect Against Threats

Item	N	Mean	Std. Deviation
I find the cybersecurity technical measures effectively implemented in my college e.g., firewalls, antivirus software, encryption	298	2.16	1.088
The technical measures and technical support provided by my college influenced my attitude toward compliance with cybersecurity policies.	298	3.11	0.998
The availability of technical support affected my confidence in handling potential cybersecurity incidents or breaches.	298	2.30	1.091
The technical measures and support services increased my awareness of cybersecurity threats and the importance of preventive measures.	298	2.28	0.965
The technical measures and support provided by my college positively influenced my perception of the institution's commitment to cybersecurity.	298	2.11	1.077
Overall Mean	**298**	**2.39**	**1.043**

The findings from Table 2 suggest that staff members perceive the effectiveness of technical measures in CoEs as low (Overall Mean = 2.39, SD = 1.04). Staff do not feel adequately supported by existing cybersecurity measures, including firewalls, antivirus software and encryption. The lowest mean score (Mean = 2.11) corresponds to the perception of institutional commitment to cybersecurity, indicating a lack of confidence among staff regarding their colleges' proactive stance on cybersecurity

threats. However, some staff acknowledged that technical support positively influenced their compliance with cybersecurity policies (Mean = 3.11). These findings highlight gaps in the implementation and communication of cybersecurity measures, emphasizing the need for improved infrastructure and awareness programs to enhance staff engagement and confidence in cybersecurity strategies.

Research Question 3: What is the perception of CoEs teachers with respect to cyber resilience in their colleges?

Table 3: Perception of Teachers Regarding Cyber Resilience in CoEs

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
I am vigilant in recognizing and reporting phishing emails or other suspicious communications.	298	1	5	2.79	1.270
I regularly ensure that my work devices and software are updated with the latest security patches	298	1	4	3.08	.804
I frequently use secure networks (e.g., VPNs recommended by my institution) when accessing remote resources that require me to type in my credentials to browsers	298	1	4	2.64	1.062
I am diligent in protecting sensitive data (e.g., using encryption)	298	1	5	2.89	1.151
I am committed to adhering to and promoting robust cybersecurity practices to ensure the integrity, confidentiality, and availability of digital assets and information systems.	298	1	4	2.75	1.074
I find the communication regarding cybersecurity policies and updates within my college effective.	298	1	4	2.36	.943
I am confident in the cybersecurity measures and protocols established by my college to protect against cyber threats.	298	1	4	2.40	.948
I believe my college is responsive in addressing and managing cybersecurity incidents and breaches.	298	1	4	2.43	1.143
I often integrate cybersecurity best practices into my daily work activities.	298	1	5	2.50	1.071
Overall Mean	**298**			**2.65**	**1.052**

The results in Table 3 reveal that while staff perception of cyber resilience (Overall Mean = 2.65, SD = 1.052) is slightly higher than their perception of technical measures (Mean = 2.39), they have little confidence in the cyber resilience of their colleges. Staff members lack confidence in cybersecurity measures and protocols (Mean = 2.40) and do not find communication regarding cybersecurity policies effective (Mean = 2.36). The highest mean score (Mean = 3.08) was related to keeping devices and software updated, suggesting that some staff members follow basic cybersecurity practices. However, low scores across other indicators suggest a need for more proactive cybersecurity strategies to enhance cyber resilience in CoEs. These findings highlight the importance of improving

cybersecurity training, communication and infrastructure to foster a stronger cybersecurity culture among CoEs staff.

DISCUSSION

The findings of the analysis of the questionnaire provide valuable insights into the relationship between awareness of cybersecurity legislation and staff perceptions of cybersecurity in CoEs. Awareness of the Cyber Security Act 2020 (Act 1038) was found to have a moderate impact on staff perceptions, with an adjusted R^2 value of 0.456. This percentage suggests that legal frameworks play a vital role in shaping the cybersecurity culture within educational institutions, reinforcing the importance of integrating policy awareness in cybersecurity training, especially during professional development sessions in CoEs.[39] The statistical significance of the model, supported by an F-value of 184.673 ($p<0.001$), confirms that this relationship is not due to random chance. This finding is consistent with previous research that emphasizes the role of regulatory frameworks in enhancing cybersecurity culture in educational institutions.[40]

Furthermore, standardized regression estimates indicate a strong positive influence of awareness on staff perceptions ($\beta = 0.677$, $p<0.001$). This finding suggests that as staff members become more aware of the Cyber Security Act 2020, their perceptions of cybersecurity and its importance within their institutions improve moderately. This aligns with the assertion by Li et al. that increased awareness and understanding of cybersecurity policies can enhance compliance and engagement among staff.[41] Given these findings, CoEs should prioritize initiatives to improve awareness through regular training sessions, workshops and informational resources that contextualize the Act within daily institutional operations. By fostering an environment where staff are well-informed about cybersecurity legislation, institutions can cultivate a culture of vigilance and proactive engagement with cybersecurity practices.[42] A well-informed staff is crucial in fostering a proactive cybersecurity culture.

The study also highlights concerns regarding the effectiveness of technical cybersecurity measures. The overall mean score of staff members' perception of technical safeguards such as firewalls, antivirus software protection, and encryption was notably low (Mean = 2.39, SD = 0.91), indicating a perceived inadequacy of these measures. This perception is troubling as it suggests a lack of confidence among staff in the institution's ability to protect against cyber threats, which is essential for fostering a secure educational environment.[43] Similarly, the mean score for staff perceptions of institutional commitment to cybersecurity was particularly low (Mean = 2.11), suggesting a significant gap in staff confidence regarding the proactive measures taken by their institutions. Research indicates that a lack of perceived institutional commitment can lead to decreased compliance with security policies and practices.[44] Thus, CoEs must not only enhance their technical defenses but also actively communicate their cybersecurity strategies to staff, reinforcing institutional commitment to cybersecurity.

Although some technical measures positively influenced attitudes towards cybersecurity policy compliance (Mean = 3.11), the overall lack of confidence in these measures raises concerns about institutional cyber resilience. Staff perceptions of cyber resilience were moderately low (Mean = 2.65, SD = 1.052), suggesting that while there is some awareness of cybersecurity issues, significant deficiencies remain. One critical concern is the low confidence in existing cybersecurity protocols

[39] Candour Legal, " Comprehending the Nuances of Cybersecurity Legal Frameworks Across the Globe," May 24, 2024, https://candourlegal.com/comprehending-the-nuances-of-cybersecurity-legal-frameworks-across-the-globe/.
[40] Abby Dellapina et al., " The Crucial Role of Regulatory Frameworks in Ensuring Robust Cyber Security," July 16, 2014, https://cyberprotection-magazine.com/our-authors.
[41] Ling Li et al., "Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior," *International Journal of Information Management* 45, no. 7 (April 2019): 13–24, https://doi.org/10.1016/j.ijinfomgt.2018.10.017.
[42] Peter Hall, " Building a Resilient Cybersecurity Culture in Educational Institutions," February 12, 2024, https://secarma.com/building-a-resilient-cybersecurity-culture-in-educational-institutions.
[43] Khando Khando et al., "Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review," *Computers & Security* 106 (July 2021): 1–22, https://doi.org/10.1016/j.cose.2021.102267.
[44] Martin Karlsson et al., "The Effect of Perceived Organizational Culture on Employees' Information Security Compliance," *Information & Computer Security* 30, no. 3 (2021): 382–401.

(Mean = 2.40). This finding aligns with previous research that emphasizes the critical role of staff confidence in the effectiveness of cybersecurity measures.[45] When faculty members and non-academic staff lack confidence in the protocols designed to protect their institutions, it can lead to complacency and reduced adherence to security policies, ultimately increasing vulnerability to cyber threats.[46] Another notable issue is the perception that communication regarding cybersecurity policies is ineffective (Mean = 2.36). In order to understand their roles in creating a secure environment, there should be effective communication to ensure that staff members are not only aware of existing policies but also understand their roles and responsibilities in this regard.[47] Colleges must prioritize clear and consistent communication to improve staff engagement and compliance with cybersecurity policies. Furthermore, there should be consistent efforts to clearly communicate policies and procedures.[48] Training should not only cover technical aspects of emerging threats but also emphasize the importance of vigilance and proactive engagement with cybersecurity practices.

Interview Responses on Cybersecurity Awareness and Institutional Resilience

To gain a deeper understanding of staff perceptions of cybersecurity and the institutional efforts toward cyber resilience, semi-structured interviews were conducted with 35 purposively selected staff members from the 298 who participated in the quantitative phase of the study. The selected respondents represented a cross-section of roles; academic staff, administrative personnel, IT support, finance and accounting staff and library staff, drawn from all 12 Colleges of Education (CoEs) involved in the study. This diversity allowed the findings to capture a wide range of experiences with cybersecurity practices, institutional support mechanisms, and awareness of the Cybersecurity Act 2020 (Act 1038). The responses complemented and contextualized the quantitative results, particularly the findings on low institutional awareness of the Act and the relatively strong personal cybersecurity practices among staff. Many participants indicated that they had little to no knowledge of the Cybersecurity Act 2020 and only a few were vaguely familiar with it through informal channels such as social media or casual discussions. One IT staff member explained: *"I have heard about the Act, but I don't know what it actually says or how it's supposed to be implemented in our college."* A teacher added: *"We've not had any official communication or training about the Act. Most of us are just trying to stay safe online based on personal understanding."* Despite this limited awareness, respondents generally agreed that cybersecurity is critical to their daily work, particularly in light of increasing digitization of records, teaching materials and administrative processes. A finance officer noted: *"We handle sensitive information, so if someone gains unauthorized access, it could affect both staff and students. Even though we are not formally trained, we try our best to be cautious."* Similarly, a library staff member shared: *"We use email and online resources regularly, so basic safety practices like not clicking unknown links or sharing passwords are part of what we do every day."*

While individual commitment to cybersecurity was evident, institutional support appeared inconsistent and in many cases, insufficient. Respondents reported a lack of formal policies, structured training, or regular communication from management on cybersecurity protocols. An administrative officer remarked: *"Our college has not provided any formal guidelines or workshops on cybersecurity. Whatever we do is based on personal experience or help from the IT unit."* An IT support staff member echoed this concern: *"We are doing our best with limited resources, but there's no comprehensive strategy for managing cyber threats."* Most respondents called for structured, mandatory training sessions, frequent updates on national cybersecurity initiatives, and the development of clear institutional policies. A tutor recommended: *"Workshops should be organized to educate all staff on cybersecurity threats and how to protect our systems. It should not be left to the IT department alone."*

[45] Li et al., "Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior."
[46] Juan Hernadez, "Cybersecurity Challenges in Education," June 10, 2024, https://preyproject.com/blog/cybersecurity-challenges-in-education.
[47] Michael Mncedisi Willie, "The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture," *Journal of Research, Innovation and Technologies (JoRIT)* 2, no. 16 (September 2023): 180, https://doi.org/10.57017/jorit.v2.2(4).05.
[48] Puhakainen and Siponen, "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," *MIS Quarterly* 34, no. 4 (2010): 757–78, https://doi.org/10.2307/25750704.

Overall, the interviews reinforced the survey's findings that there is a notable gap between staff members' awareness of national cybersecurity legislation and the actual cybersecurity practices at the institutional level. Nonetheless, the strong individual efforts by staff members to protect themselves digitally highlight an untapped potential for building a more resilient cybersecurity culture within the CoEs. The insights gathered from these interviews underscore the need for targeted training programs, stronger leadership involvement and cross-sector collaboration to improve institutional cyber resilience in Ghana's Colleges of Education.

RECOMMENDATIONS

Based on the study's findings, Colleges of Education (CoEs) should implement structured and ongoing cybersecurity training focused on the Cyber Security Act 2020 (Act 1038) and its implications for staff roles and responsibilities. These sessions should be conducted at least bi-annually, covering current cybersecurity threats, best practices, and the technical measures in place to safeguard institutional networks. Practical simulations should be integrated to enhance staff engagement and preparedness. In addition to training, CoEs must foster a culture where cybersecurity is a shared responsibility among staff and students. Awareness campaigns, clear institutional policies and incentives for compliance should be incorporated to encourage proactive engagement with cybersecurity practices. A well-defined strategy that integrates cybersecurity expectations into institutional guidelines will help reinforce this culture. Furthermore, management should create platforms for open communication, allowing stakeholders to express cybersecurity concerns without fear of victimization. Establishing regular cybersecurity forums or feedback mechanisms will facilitate transparent discussions, ensuring that staff and students feel empowered to contribute to institutional security efforts. By prioritizing these initiatives, CoEs can strengthen their cybersecurity culture, reduce vulnerabilities and foster a safer institutional cyberspace. Immediate action is essential to mitigate cyber threats and enhance institutional resilience in an increasingly digital academic environment.

CONCLUSION

This study provides critical insights into the cybersecurity landscape within Colleges of Education (CoEs) in Ghana, particularly the influence of staff awareness of the Cybersecurity Act 2020 on cyber resilience. The findings indicate that awareness of this legal framework significantly impacts staff perceptions of cybersecurity, explaining approximately 46% of the variance. This highlights the need to integrate cybersecurity policy awareness into training programs to ensure staff understand their roles in maintaining a secure institutional environment. However, the study revealed that staff members have low confidence in the technical measures implemented by IT personnel and perceive their colleges' cyber resilience as only moderate. The overall mean scores suggest that, while some awareness exists, institutions must strengthen both their technical infrastructure and communication strategies. A lack of perceived institutional commitment to cybersecurity can lead to reduced compliance and increased vulnerability to threats, making it crucial for CoEs to foster a strong cybersecurity culture. To enhance cyber resilience, CoEs should urgently implement regular cybersecurity training, improve communication of policies and create an environment that encourages open dialogue on security concerns. Failure to address these issues could expose institutions to greater cyber risks. Therefore, policymakers, administrators and IT personnel must collaborate to develop proactive security measures and ensure their consistent enforcement.

LIMITATIONS AND SUGGESTIONS FOR FURTHER STUDIES

Despite the valuable insights provided by this study, several limitations must be acknowledged. First, the study employed a descriptive cross-sectional survey design, which captures data at a single point in time. This limits the ability to analyze changes in cybersecurity culture and resilience over time. A longitudinal study could provide a more comprehensive understanding of trends and improvements in cybersecurity practices within CoEs. Second, the study relied on self-reported data from staff members, which may be subject to response bias. Participants may have overestimated their cybersecurity awareness or practices due to social desirability bias. Future studies could complement self-reported

data with observational methods or system log analyses to obtain more objective measures of cybersecurity practices. Additionally, while the study covered 12 CoEs in Ghana, findings may not be entirely generalizable to all CoEs or other higher education institutions in the country. Expanding the study to include a larger sample of institutions across different regions would enhance the generalizability of the findings. Finally, the study focused primarily on academic and non-academic staff, without directly incorporating student perspectives. Since students are also key users of institutional IT systems, future research could explore their role in strengthening cybersecurity culture and resilience. Building on the current research, future studies should adopt a longitudinal approach to track changes in cybersecurity culture and resilience over time. Such studies could use case studies to provide deeper insights into cybersecurity challenges and best practices, examine student perceptions of cybersecurity and their role in enhancing institutional cyber resilience, compare cybersecurity culture across different types of tertiary institutions (e.g., public vs. private universities) to assess variations in cybersecurity awareness and practices, and investigate the effectiveness of specific cybersecurity training programs in improving staff compliance with security protocols.

BIBLIOGRAPHY

Alsaqour, Raed, Ahmed Motmi, and Maha Abdelhaq. "A Systematic Study of Network Firewall and Its Implementation." *International Journal of Computer Science & Network Security* 21, no. 4 (2021): 199–208.

Alshaikh, Moneer. "Developing Cybersecurity Culture to Influence Employee Behavior: A Practice Perspective." *Computers & Security* 98 (November 2020): 1–20. https://doi.org/10.1016/j.cose.2020.102003.

Anilkumar, Anagha, Filip Dimitrov, and Anup Narayanan. "The Differences and Relationship Between Awareness, Behavior, and Cyber Security Culture," November 29, 2023. https://securityquotient.io/the-differences-and-relationship-between-awareness-behavior-and-culture-in-cyber-security/.

Araujo, Misael Sousa de, Bruna Aparecida Souza Machado, and Francisco Uchoa Passos. "Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance." *Applied Sciences* 14, no. 5 (March 4, 2024): 1–16. https://doi.org/10.3390/app14052116.

Candour Legal. " Comprehending the Nuances of Cybersecurity Legal Frameworks Across the Globe," May 24, 2024. https://candourlegal.com/comprehending-the-nuances-of-cybersecurity-legal-frameworks-across-the-globe/.

Celeste, Rifel Jeene, and Nimfa Osias. "Challenges and Implementation of Technology Integration: Basis for Enhanced Instructional Program." *American Journal of Arts and Human Science* 3, no. 2 (June 4, 2024): 106–30. https://doi.org/10.54536/ajahs.v3i2.2656.

Chaudhary, Sunil, Vasileios Gkioulos, and Sokratis Katsikas. "Developing Metrics to Assess the Effectiveness of Cybersecurity Awareness Program." *Journal of Cybersecurity* 8, no. 1 (January 28, 2022): 1. https://doi.org/10.1093/cybsec/tyac006.

Chen, Yan, Dennis F. Galletta, Paul Benjamin Lowry, Xin (Robert) Luo, Gregory D. Moody, and Robert Willison. "Understanding Inconsistent Employee Compliance with Information Security Policies Through the Lens of the Extended Parallel Process Model." *Information Systems Research* 32, no. 3 (September 2021): 1043–65. https://doi.org/10.1287/isre.2021.1014.

Chipeta, Catherine. "What Is an Intrusion Detection System (IDS)? + Best IDS Tools." , November 18, 2024. https://www.upguard.com/blog/intrusion-detection-system.

Dellapina, Abby, Abhishek Kumar Singh, Adam Benson, and Adam Glick. " The Crucial Role of Regulatory Frameworks in Ensuring Robust Cyber Security," July 16, 2014. https://cyberprotection-magazine.com/our-authors.

Farok, Nur Aqilah Zaffan, and Mohamad Fadli Zolkipli. "Incident Response Planning and Procedures." *Borneo International Journal EISSN 2636-9826* 7, no. 2 (2024): 69–76.

Furnell, Steven, and Jayesh Navin Shah. "Home Working and Cyber Security – an Outbreak of Unpreparedness?" *Computer Fraud & Security* 2020, no. 8 (January 2020): 6–12.

https://doi.org/10.1016/S1361-3723(20)30084-1.

Gordon, Lawrence A, Martin P Loeb, and Lei Zhou. "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?" *Journal of Computer Security* 19, no. 1 (2011): 33–56.

Hall, Peter. " Building a Resilient Cybersecurity Culture in Educational Institutions," February 12, 2024. https://secarma.com/building-a-resilient-cybersecurity-culture-in-educational-institutions.

Hernadez, Juan. "Cybersecurity Challenges in Education," June 10, 2024. https://preyproject.com/blog/cybersecurity-challenges-in-education.

Housen-Couriel, Deborah. "Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace." In *Cyber Peace*, 39–63. Cambridge University Press, 2022. https://doi.org/10.1017/9781108954341.003.

Karlsson, Martin, Fredrik Karlsson, Joachim Åström, and Thomas Denk. "The Effect of Perceived Organizational Culture on Employees' Information Security Compliance." *Information & Computer Security* 30, no. 3 (2021): 382–401.

Khando, Khando, Shang Gao, Sirajul M. Islam, and Ali Salman. "Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review." *Computers & Security* 106 (July 2021): 1–22. https://doi.org/10.1016/j.cose.2021.102267.

Kuraku, Sivaraju, Dinesh Kalla, Fnu Samaah, and Nathan Smith. "Cultivating Proactive Cybersecurity Culture among IT Professional to Combat Evolving Threats." *International Journal of Electrical, Electronics and Computers* 8, no. 6 (2023): 01–07. https://doi.org/10.22161/eec.86.1.

Li, Ling, Wu He, Li Xu, Ivan Ash, Mohd Anwar, and Xiaohong Yuan. "Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior." *International Journal of Information Management* 45, no. 7 (April 2019): 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017.

Ministry of Communications and Digitalisation. "National Cybersecurity Awareness Month Launched to Educate Public on Digital Safety," September 2, 2024. https://moi.gov.gh/newsroom/2024/09/national-cybersecurity-awareness-month-launched-to-educate-public-on-digital-safey.

Mukherjee, Madhav, Ngoc Thuy Le, Yang-Wai Chow, and Willy Susilo. "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes." *Information* 15, no. 2 (February 18, 2024): 1–23. https://doi.org/10.3390/info15020117.

National Institute of Standards and Technology. "The NIST Cybersecurity Framework (CSF) 2.0," February 26, 2024. https://doi.org/10.6028/NIST.CSWP.29.

Puhakainen, and Siponen. "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study." *MIS Quarterly* 34, no. 4 (2010): 757–78. https://doi.org/10.2307/25750704.

Rahman, N. A. A, I. H. Sairi, N. A. M. Zizi, and F. Khalid. "The Importance of Cybersecurity Education in School." *International Journal of Information and Education Technology* 10, no. 5 (2020): 378–82. https://doi.org/10.18178/ijiet.2020.10.5.1393.

Safitra, Muhammad Fakhrul, Muharman Lubis, and Hanif Fakhrurroja. "Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity." *Sustainability* 15, no. 18 (September 6, 2023): 1–32. https://doi.org/10.3390/su151813369.

Sigurðsson, Ragnar. " The Human Element: A Crucial Aspect of Cyber Risk Assessment Services and 8 Ways to Address It," July 27, 2023. https://awarego.com/the-human-element-in-cyber-risk-assessment-services/.

Tolossa, Dawit. "Importance of Cybersecurity Awareness Training for Employees in Business." *VIDYA - A JOURNAL OF GUJARAT UNIVERSITY* 2, no. 2 (August 8, 2023): 104–7. https://doi.org/10.47413/vidya.v2i2.206.

Uchendu, Betsy, Jason R.C. Nurse, Maria Bada, and Steven Furnell. "Developing a Cyber Security Culture: Current Practices and Future Needs." *Computers & Security* 109 (October 2021): 102387. https://doi.org/10.1016/j.cose.2021.102387.

Willie, Michael Mncedisi. "The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture." *Journal of Research, Innovation and Technologies (JoRIT)* 2, no. 16 (September 2023): 180. https://doi.org/10.57017/jorit.v2.2(4).05.

Yan, Zheng, Thomas Robertson, River Yan, Sung Yong Park, Samantha Bordoff, Quan Chen, and Ethan Sprissler. "Finding the Weakest Links in the Weakest Link: How Well Do Undergraduate Students Make Cybersecurity Judgment?" *Computers in Human Behavior* 84 (2018): 375–82.

ABOUT AUTHOR

Dr. Daniel Paa Korsah is an esteemed lecturer at Komenda College of Education in Ghana. Holding a PhD in Information and Communication Technology, Dr. Korsah is a dedicated educator with a profound academic background. He has earned both an M.Ed. in Information Technology and a B.Ed. in Computer Science. Driven by a passion for advancing educational practices, his primary research focus revolves around E-Learning, technology acceptance and cybersecurity. His interest in cybersecurity research explores its implications for education and digital safety. Dr. Korsah's wealth of knowledge and commitment to the field make him a valuable contributor to the discourse on the intersection of education, technology and cybersecurity.