ISSN : 2350-0743

www.ijramr.com

International Journal of Recent Advances in Multidisciplinary Research
Vol. 10, Issue 10, pp.8959-8965, October, 2023

RESEARCH ARTICLE

UNDERSTANDING AND ADDRESSING CYBERSECURITY CHALLENGES IN ACADEMIC INSTITUTIONS: A COMPREHENSIVE ASSESSMENT

*** Dr. Kehinde Kenny Onayemi**

IT instructor at the Southern Alberta Institute of Technology School of Advanced Digital, The Southern Alberta Institute of Technology, Alberta, Canada

ARTICLE INFO

Article History:
Received 08th July, 2023
Received in revised form
20th August, 2023
Accepted 16th September, 2023
Published online 30th October, 2023

Key Words:

Cybersecurity Challenges, Phishing Attacks, Cybersecurity Awareness, Network Vulnerability Assessment, Incident Response Strategies.

ABSTRACT

The study's objective was to identify and assess unique cybersecurity challenges in academic institutions, including vulnerabilities in interconnected networks and the diverse user base. This study targeted students, faculty members, administration, and IT staff. The study showed that 68% expressed a high or concerned level of cybersecurity worry. The key challenges highlighted were phishing attacks (68%), lack of awareness and training (63%), unauthorized access (61%), weak passwords (59%), malware/ransomware (39%), lack of resources (37%), and inadequate network protection (34%). Cybersecurity measures were deemed ineffective (39%), moderately effective (22%), or highly effective (14.6%). Notable vulnerabilities within interconnected networks included outdated software/systems (58.5%), insider threats (56.1%), weak encryption (56.1%), third-party vulnerabilities (41.5%), and misconfigured devices (31.7%). Network vulnerability assessments were infrequent (65.4%). The major obstacles to the implementation of effective cybersecurity measures were lack of budget/resources (65.9%), limited awareness (63.4%), insufficient staff expertise (53.7%), and resistance to new tech (51.2%). The study revealed reported cybersecurity incidents or breaches (48.8%), underscoring the importance of preventive measures and incident response strategies to safeguard sensitive data and institutional integrity. The study recommended the Implementation of mandatory annual cybersecurity training and establishment of clear incident response protocols; Conducting of regular network vulnerability assessments and promote collaboration and ongoing training and lastly; Launch cybersecurity awareness campaigns and encourage two-factor authentication for academic accounts.

INTRODUCTION

The evolving cybersecurity landscape in higher education is a vital concern as institutions must safeguard extensive volumes of sensitive data. In response, institutions must allocate appropriate resources and adopt adaptable practices, given the dynamic nature of cybersecurity threats (Brooks, 2023). Over the last decade, the prominence of cybersecurity has grown significantly, fueled by recurring reports of breaches, data loss, politically motivated attacks, and rising awareness of the associated costs and hazards (Brooks, 2023). Higher education leadership is now keenly engaged, motivated both by institutional challenges and escalating insurance expenses, resulting in a unique intersection of education and cybersecurity considerations. The intricate tapestry of a university campus, while offering diverse experiences, introduces distinct challenges in cybersecurity. Campuses host visitors for numerous events, researchers collaborate worldwide, students pursue personal experiences, and faculty work from diverse locations, magnifying vulnerabilities (Brooks, 2023).

Corresponding author:** ***Dr. Kehinde Kenny Onayemi,
IT instructor at the Southern Alberta Institute of Technology School of Advanced Digital, The Southern Alberta Institute of Technology, Alberta, Canada

Such complexity is underscored by the University of Wisconsin—Madison's global presence and diverse activities, reflecting the broader challenges faced by higher education institutions (Brooks, 2023). The necessity to secure private information, coupled with the potential repercussions of data breaches, further emphasizes the urgency for a robust cybersecurity framework (Brooks, 2023). Data breaches entail substantial costs, not only due to potential downtime but also in restoring compromised services and mitigating reputational damage (Brooks, 2023). An evolving threat landscape necessitates leaders' awareness of dynamic cybercriminal motivations, as attackers target data for various reasons including financial gain and political agendas (Brooks, 2023). Alarming statistics reveal the extent of vulnerabilities, with a study indicating that 79% of educational institutions reported at least one successful cyberattack within the past year (Brooks, 2023). While the multifaceted nature of cybersecurity challenges may pose barriers, leaders' commitment to continuous vigilance and investment remains pivotal to mitigating risks (Brooks, 2023). Establishing a culture of security, addressing individual behaviors, and embracing security-conscious practices constitute vital steps towards a cyber-resilient higher education environment (Brooks, 2023).

Problem statement: The ever-evolving landscape of cybersecurity presents a pressing challenge for academic institutions, characterized by diverse user demographics, interconnected networks, and a host of vulnerabilities. Amidst this complexity, the lack of comprehensive cybersecurity measures threatens the integrity of sensitive data, educational continuity, and the reputation of these institutions. This study seeks to address the critical problem of cybersecurity in academic settings by identifying the unique challenges faced by various stakeholders, evaluating the effectiveness of existing measures, and highlighting the key obstacles that hinder the implementation of robust cybersecurity strategies.

Purpose of the study: The main of this study is to identify and assess the unique cybersecurity challenges faced by academic institutions, including the vulnerabilities inherent in their interconnected networks and diverse user base.

LITERATURE REVIEW

A study by Triplett (2022) addresses the cybersecurity challenges in education, particularly in the context of online and remote learning. The study focuses on strategies that educational institutions can employ to enhance students' cybersecurity awareness and encourage them to consider pursuing a career in cybersecurity. The research conducted a systematic review of ten studies and found that game-based strategies were effective in achieving these objectives. The abstract concludes by suggesting that game designers and developers should consider creating advanced games that assess students' cybersecurity skills and their ability to respond to aggressive cyberattacks, in addition to enhancing their knowledge of cybersecurity. In the realm of primary and secondary education, as well as government training programs, concerns arise regarding the ability to cultivate individuals capable of mitigating escalating cyberattack and cybercrime risks in K–12 online education (Domeij, 2019). While technology integration in educational settings enhances remote learning, it exacerbates cybersecurity threats faced by schools and students alike, escalating vulnerabilities (Hasib, 2018). This predicament is exacerbated by the COVID-19 pandemic's impact, as cybersecurity leadership and government initiatives struggle to cope with the evolving landscape (Wright, 2016). The failure to standardize cybersecurity professionalization and address talent scarcity amplifies existing shortcomings (Wright, 2016). The shift to remote learning and work schedules further intensifies cybersecurity challenges, emphasizing the urgency to address the scarcity of cybersecurity professionals (Wright, 2016).

Amid the rapid growth of cybersecurity as a crucial domain in information technology (Dunn & Merkle, 2018), a concerning shortage of cybersecurity specialists has emerged, raising alarms (Filipczuk et al., 2019; Hart et al., 2020; Mountrouidou et al., 2019). This shortage is compounded by the rising frequency and sophistication of cyberattacks, with notable correlations between attack rates and the number of available cybersecurity specialists (Hart et al., 2020; Mountrouidou et al., 2019). Consequences are evident: companies with cybersecurity staff vacancies face heightened cyberattack risks (Mountrouidou et al., 2019). The scarcity's global scale is pronounced, with estimates of over 3 million cybersecurity professionals professionals (Choudhury, 2022), leaving institutions, businesses, and individuals susceptible to cyberthreats.

The shortage's multifaceted causes extend to inadequate educational programs and mentorship (Armstrong et al., 2018; Hodhod et al., 2019). A dearth of mentors, particularly women role models, dissuades female students from joining the cybersecurity field (Pinchot et al., 2020). Scarcity also hampers the development of robust cybersecurity curricula in schools and contributes to the disconnection between education and industry requirements (Armstrong et al., 2018). The need for mitigation strategies is evident; hackers exploit resource shortages to target sensitive information from educational institution servers (Filipczuk et al., 2019; Oyedotun, 2020). Consequently, the inadequacies of resources, funding, and proper cybersecurity education give rise to critical concerns about the cybersecurity status of K–12 schools (Coleman & Reeder, 2018).

METHODOLOGY

The methodology employed in this study utilizes a mixed-methods approach to comprehensively examine the cybersecurity challenges faced by academic institutions and their potential impact. Quantitative data was collected through an online survey distributed to a diverse sample of participants, including students, faculty members/administration, and IT staff. This survey gathered responses regarding the level of cybersecurity concern, perceptions of key challenges, and effectiveness of current cybersecurity measures. The quantitative data was analyzed using descriptive statistics, providing insights into the prevalence and distribution of cybersecurity concerns and challenges. Furthermore, qualitative data was obtained through open-ended survey questions to delve deeper into participants' experiences and perceptions of cybersecurity issues. The combination of quantitative and qualitative data allows for a holistic understanding of the multifaceted cybersecurity landscape in academic institutions. The study involved 41 participants, ensuring a representative sample from different roles within these institutions, including faculty, administration, and IT professionals.

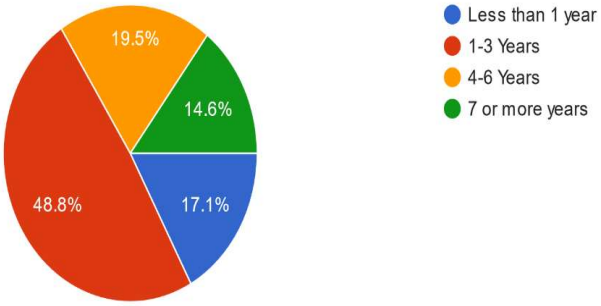
RUSTLES

The findings in this study are detailed in this work below:

Demography: In this section, we present key demographic information gathered from respondents representing various roles within academic institutions and their respective lengths of association with these institutions. This foundational data provides insights into the diverse perspectives and experiences contributing to our comprehensive analysis of cybersecurity challenges in academic settings.

Respondent's Role in the Academic Institution: This section focuses on the roles of respondents within their academic institutions, including students, faculty members, IT staff, administration, and an option to specify "Other" roles. Understanding the distribution of roles provides context for how different stakeholders perceive and interact with cybersecurity challenges. From the study, it was revealed that majority of the respondents, 57% were students followed by 29% who were faculty members and 10% from the administration department and the minority group was that from the IT department since they are never so many in the institution. This implies that the major dimensions of an academic institution were represented in this study.

Length of Time in Association with the Academic Institution: In this part, respondents are asked about the length of their association with the academic institution, with options ranging from less than 1 year to 7 or more years. This information helps gauge the level of experience and familiarity respondents have with the institution, which can influence their perspectives on cybersecurity challenges and solutions.

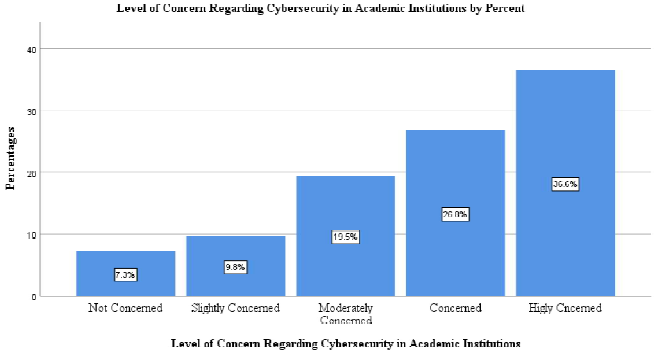


From that data collected, the study shows that the majority, 49% of the respondents had associated with the academic institution 1-3 years and 20% had associated with the academic institution for 4-6 years. 17% and 15% of the respondents had associated with the academic institution for either less than 1 year and 7 or more years respectively. This implies that the respondents had reliable experience in the institution to comment on the items investigated.

Section Two

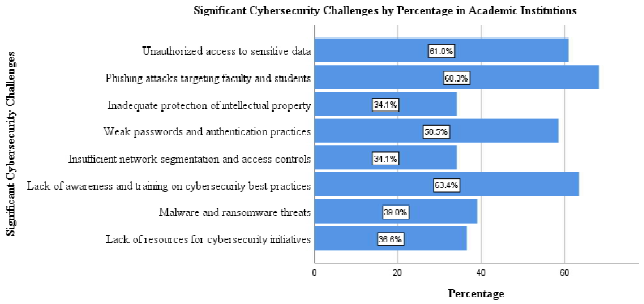
Cybersecurity Challenges in academic Institutions: This section delves into the cybersecurity landscape of academic institutions, as perceived by the individuals directly involved. It begins by assessing the level of concern regarding cybersecurity, followed by an exploration of the specific challenges deemed significant within academic environments. The effectiveness of existing cybersecurity measures and the types of vulnerabilities observed within interconnected networks are examined. Furthermore, the frequency of network vulnerability assessments and penetration testing is considered, along with the identified obstacles hindering effective cybersecurity implementation. Finally, respondents are asked about any recent cybersecurity incidents or breaches and given an opportunity to provide additional insights, offering a comprehensive view of cybersecurity challenges in academic institutions.

Level of Concern Regarding Cybersecurity in Academic Institutions: In this section, we delve into the perceptions and concerns of individuals within academic institutions regarding cybersecurity. Respondents are asked to rate their levels of concern on a scale from 1 to 5, providing insights into the overall awareness of cybersecurity issues. The findings are shown below:



The participants' level of concern regarding cybersecurity in academic institutions was assessed. The responses indicated a range of concerns, with varying degrees of intensity. The majority of respondents expressed a high level of concern (36.6%), followed by those who reported being concerned (26.8%). A substantial portion of participants indicated being moderately concerned (19.5%), while a smaller proportion indicated being slightly concerned (9.8%). A minority of respondents reported not being concerned (7.3%). The findings reflect a diverse spectrum of cybersecurity concerns within academic institutions. The diverse range of concern levels signifies the critical importance of addressing cybersecurity comprehensively within academic institutions to align with varying degrees of apprehension.

Significant Cybersecurity Challenges: The study identify specific challenges they consider significant within the academic environment, such as unauthorized data access, phishing attacks, weak authentication practices, and more. These findings offer a valuable glimpse into the key cybersecurity priorities and worries within academic institutions, paving the way for a deeper understanding of the challenges and potential solutions in the subsequent sections. The findings are shown below:



In response to inquiries about the prominent cybersecurity challenges within the institution, the majority of respondents, totaling 68%, identified phishing attacks targeting faculty and students as a significant concern. Following this, 63% of participants highlighted the lack of awareness and training regarding cybersecurity best practices, while 61% recognized unauthorized access to sensitive data as a noteworthy challenge. Notably, a substantial 59% of respondents acknowledged weak passwords and authentication practices as a pronounced cybersecurity issue. Additionally, 39% and 37% of participants considered malware and ransomware threats, as well as the lack of resources for cybersecurity initiatives, to be significant threats, respectively.Furthermore, the study unveiled that 34% of respondents perceived inadequate protection of intellectual property and insufficient network segmentation and access controls as noteworthy cybersecurity challenges. Interestingly, only a marginal 5% reported encountering other distinct challenges, such as the need for a seamless transition, in their assessment. These findings show the array of cybersecurity challenges faced by academic institutions, ranging from social engineering threats to deficiencies in awareness, training, and resource allocation, underscoring the multifaceted nature of the cybersecurity landscape.

The identified cybersecurity challenges underscore the imperative for the institution to focus on targeted awareness campaigns, comprehensive training initiatives, and resource allocation. Addressing the prevalent issues of phishing attacks, inadequate awareness, and weak authentication practices

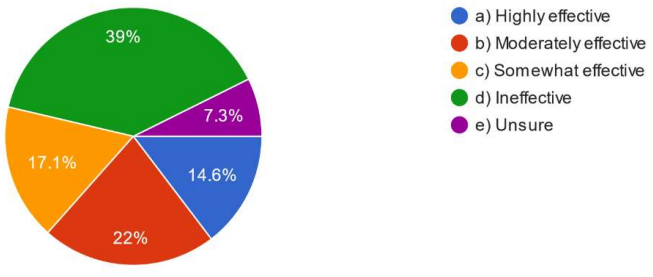
demands tailored educational interventions to enhance users' vigilance. Prioritizing cybersecurity resources and bolstering defenses against malware and ransomware threats is essential to safeguard critical data. Furthermore, proactive measures to bolster intellectual property protection and enhance network segmentation can enhance overall cybersecurity resilience. This underscores the urgency of fostering a culture of cybersecurity awareness and investing in robust defenses to mitigate the identified vulnerabilities. Respondents when asked an item to express their opinion on the challenges faced the main theme from the thematic analysis revealed was Increased Cybersecurity Threats. The corresponding responses include:

> *"I was given a link, and my Windows firewall didn't trust it, so I got nervous…." "There may be a significant number of fake users accessing the campus network with malicious intent, which poses a considerable threat." "Cybercriminals often target academic institutions through phishing emails and social engineering tactics." "With the rise of online learning, schools are now more vulnerable than ever to cyberattacks, which can have serious consequences for both students and staff."*

These statements shed light on the pervasive vulnerability of academic institutions to cyber threats. The experience of a mistrusted link triggering anxiety underscores the heightened sense of caution required in the digital landscape. The notion of fake users infiltrating the campus network for malicious purposes points to a concerning security gap. The acknowledgment of cybercriminals targeting academic institutions through phishing and social engineering tactics highlights the need for proactive defense measures.

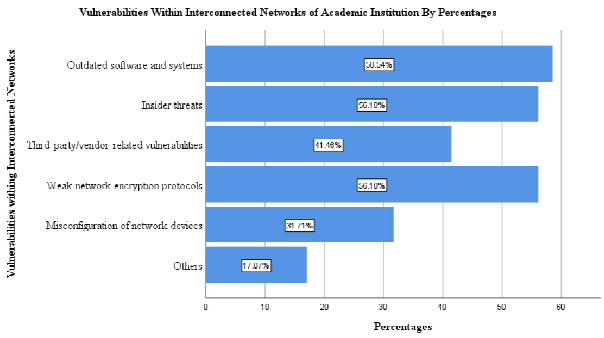
The assertion that online learning has intensified institutions' vulnerability underscores the urgency of bolstering cybersecurity protocols. Collectively, these statements underscore the critical need for comprehensive cybersecurity strategies to safeguard academic networks, both to protect the valuable data within and to ensure the safety of students and staff.

Effectiveness of the Current Cyber Security Measures in the Academic Institutions: This section investigates the perceived effectiveness of existing cybersecurity measures within academic institutions. Respondents are prompted to evaluate these measures as highly effective, moderately effective, somewhat effective, ineffective, or express uncertainty. Their responses shed light on the overall confidence in the current security infrastructure and inform discussions about areas in need of improvement as shown below:



When respondents were asked to rate the effectiveness of the current cyber security measures in the academic institutions, the majority of the respondents, 39% of them reported that it was ineffective followed by 22% of them who reported that it was moderately effective. Only 14.6% of the respondents reported that it was highly effective, while 17% reported that it was somewhat effective and only 7.3% reported that they were unsure. These findings imply that there is need for more efforts to be employed in the institutions to improve on the effectiveness of the current cyber security measuresthat are in place.

Types of Vulnerabilities Observed Within the Interconnected Networks of the Academic Institutions: Here, we explore the vulnerabilities observed within interconnected networks of academic institutions. Respondents are presented with various vulnerability types and asked to select those they have encountered, including outdated software, insider threats, third-party/vendor-related vulnerabilities, weak network encryption, misconfigured network devices, and more. These insights provide a comprehensive picture of the security challenges faced by academic institutions as shown below:



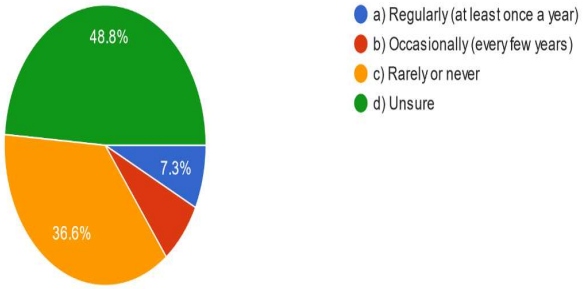
During the study respondents were asked on which types of vulnerabilities have been observed within the interconnected networks of the academic institutions. Outdated software and systems scored highly with 58.5%, followed with insider threats and weak network encryption protocols which recorded 56.1% underscoring the urgency of enhancing internal security measures and encryption practices. Furthermore, the presence of third-party/vendor-related vulnerabilities (41.5%) and misconfigurations of network devices (31.7%) signifies the complexity of safeguarding networks against external and internal risks. The reported "other vulnerabilities" at 7.2% encompass additional critical issues, including the lack of access to essential security software such as VPN and Malware, as well as instances of SAIT Server compromise. Qualitative data showed a theme on
Unique Academic Environment Challenges as shown by the responses shown:

> *"Academic institutions often have an open and collaborative environment, which can create difficulties in enforcing strict security measures."* And another respondent reported that *"academic institutions deal with a diverse range of devices owned by students, faculty, and staff. This brings the challenge of managing security across various operating systems, hardware, and software configurations."*

Collectively, these findings emphasize the multifaceted nature of network vulnerabilities and highlight the necessity of a comprehensive, layered approach to network security within academic institutions.

Frequency of Academic Institutions in Conducting Network Vulnerability Assessments and Penetration Testing: This section examines the frequency with which

academic institutions conduct network vulnerability assessments and penetration testing. Respondents choose from options like regular assessments (at least once a year), occasional assessments (every few years), rare or no assessments, or express uncertainty. This data highlights the institution's proactive stance toward network security and opportunities for enhancing their security practices as expressed in the findings below:

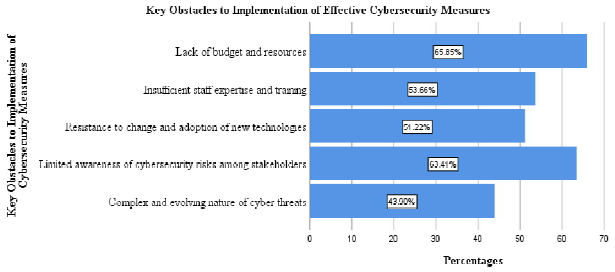


When respondents were asked how frequently the academic institution conducts the network vulnerability assessments and penetration testing, 48.8% of the respondents were unsure, whereas 36.6% reported rarely or never. 7.3% of the respondents only showed that their institutions regularly did so at least once a year or occasionally did so (every few years). The uncertainty and infrequent implementation of network vulnerability assessments and penetration testing (65.4% either unsure or rarely/never conducting them) highlights the need for academic institutions to establish regular and systematic assessment practices. One of the themes from thematic analysis was Crisis Response and Incident Management which shows need for preparedness regarding such incidences as shown by one of the informants:

> *"Academic institutions need to be prepared for cybersecurity incidents, including ransomware attacks, data breaches, and DDoS attacks. Crisis response planning and incident management become critical."*

By prioritizing consistent assessments, institutions can proactively identify and address potential vulnerabilities, enhancing their overall cybersecurity resilience.

The Key Obstacles to Implementing Effective Cybersecurity Measures in the Academic Institutions: In this segment, respondents are asked to identify the key obstacles hindering the implementation of effective cybersecurity measures within academic institutions. They could select from a list of potential barriers, including budget constraints, staff expertise and training limitations, resistance to adopting new technologies, limited awareness of cybersecurity risks among stakeholders, and the evolving nature of cyber threats. This data identifies critical challenges that must be addressed to bolster cybersecurity efforts as illustrated in the findings below:



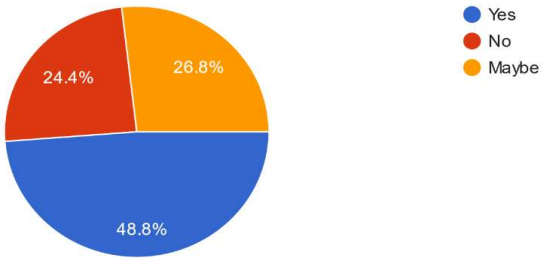
Respondents were also asked about their opinion on what are the key obstacles to implementing effective cybersecurity measures in the academic institutions, the findings underscore the pressing need for academic institutions to address critical barriers in their pursuit of effective cybersecurity. A significant majority, 65.9%, highlighted the lack of budget and resources as a major hurdle, indicating the urgency of allocating adequate funding to bolster cybersecurity efforts. Equally concerning is the revelation that 63.4% identified limited awareness of cybersecurity risks among stakeholders, emphasizing the importance of comprehensive awareness campaigns and education initiatives. Moreover, the substantial percentages (53.7% and 51.2%) expressing concerns about insufficient staff expertise and training, as well as resistance to embracing new technologies, underline the imperative to invest in personnel development and cultivate a culture of innovation. The complex and evolving nature of cyber threats, cited by 43.9%, accentuates the need for institutions to stay vigilant and adaptable, constantly evolving their strategies to counter emerging challenges. Collectively, these implications emphasize the multifaceted approach required to fortify academic institutions' cybersecurity posture and create a resilient environment against cyber threats. When respondents were asked to provide any additional comments or insights regarding the unique cybersecurity challenges faced by the academic institution, the responses were derived thematically and the critical them that came up the most was Insufficient funding and resources as shown below:

> "*More funding from the government is needed to combat cybersecurity.*"; "*Possibly not enough budgeted towards the IT/Cybersecurity departments nationwide? Possibly not enough manpower?*"; "*Maybe this campus should upgrade its Computing equipment, software, and hardware.*"; "*I believe due to the financial restraints, cybersecurity is not prioritized as it should be.*"; "*The department is understaffed, and their leadership position is unfilled.*";and"*Budget limitations can hinder the implementation of robust cybersecurity infrastructure and hiring of skilled personnel.*"

The interviewee statements above underscore the critical issue of inadequate funding and resources in the realm of cybersecurity. The consistent emphasis on insufficient budgets, manpower, and equipment across government and educational institutions points to a pressing need for increased financial support. These statements highlight a potential lack of prioritization for cybersecurity due to financial restraints, resulting in departments being understaffed and leadership positions remaining vacant. The overarching implication is that limited budgets hinder the establishment of robust cybersecurity infrastructure and the recruitment of skilled personnel, ultimately compromising the ability to effectively combat evolving cyber threats.

Significant Cybersecurity Incidents: Here, respondents are questioned about the occurrence of significant cybersecurity incidents or breaches within their academic institution over the past year. Their responses indicate the prevalence of security breaches and emphasize the importance of proactive security measures and incident response strategies in safeguarding sensitive data and institutional integrity. When respondents were asked whether there has been any significant cybersecurity incidents or breaches withing the academic

institution in the past year, 48.8% of the respondents agreed that yes, it has happened and 24.4% of them negated it while



26.8% of the respondents were not sure about that incident in their institution. These findings are in alignment with those from the thematic analysis called Academic Institutions as Targets as shown below:

"Higher education is a major target for cyberattacks. The education and research sectors were the top targets for cyberattacks in 2021, with an average of 1,605 attacks per organization per week, a 75% increase over 2020 according to recent publications"

The prevalence of reported cybersecurity incidents and breaches within academic institutions, with nearly half of respondents confirming their occurrence, underscores the need for heightened vigilance, preventive measures, and incident response strategies to safeguard sensitive data and maintain institutional integrity.

Discussion of Literature

The findings of this study align with and extend upon several key themes highlighted in the provided literature. Triplett's study (2022) on cybersecurity challenges in education resonates with the current research's emphasis on enhancing cybersecurity awareness and knowledge among students. The study's focus on game-based strategies mirrors the significance of tailored educational interventions suggested in our findings. While Triplett emphasizes game-based learning, our study highlights the multifaceted nature of challenges, ranging from phishing attacks to weak authentication practices, underscoring the need for a comprehensive approach that includes awareness campaigns, training initiatives, and resource allocation (Triplett, 2022). The issues surrounding cybersecurity in primary and secondary education, as noted by Domeij (2019), Hasib (2018), and Wright (2016), are echoed in our findings. The shift to remote learning due to the COVID-19 pandemic has intensified cybersecurity vulnerabilities, aligning with our observation of the challenges academic institutions face in adapting to the evolving landscape (Domeij, 2019; Hasib, 2018; Wright, 2016). Additionally, the shortage of cybersecurity specialists mentioned by Filipczuk et al. (2019), Hart et al. (2020), and Mountrouidou et al. (2019) resonates with our study's findings on inadequate staff expertise and training as a major challenge (Filipczuk et al., 2019; Hart et al., 2020; Mountrouidou et al., 2019). The shortage of cybersecurity professionals, as outlined by Choudhury (2022), compounds the challenges academic institutions face in implementing effective cybersecurity measures. Our findings on the lack of resources and budget as significant obstacles align with the broader issue of resource shortages in the field, leaving institutions susceptible to cyber threats (Choudhury, 2022).

Furthermore, the literature's focus on inadequate educational programs and mentorship (Armstrong et al., 2018; Hodhod et al., 2019) corresponds with our study's implications regarding the need for tailored training initiatives and educational interventions (Armstrong et al., 2018; Hodhod et al., 2019). The literature's call for robust cybersecurity curricula and the disconnection between education and industry requirements mirrors our findings on the lack of awareness and training (Coleman & Reeder, 2018).

CONCLUSION

In conclusion, the provided literature and the findings from our study collectively underscore the urgent need for comprehensive cybersecurity measures in academic institutions. The challenges highlighted in both the literature and our research emphasize the multifaceted nature of cybersecurity vulnerabilities, the significance of tailored education and training initiatives, and the imperative for resource allocation to address the scarcity of cybersecurity professionals. This intersection underscores the critical importance of fostering a culture of cybersecurity awareness, education, and innovation to effectively navigate the evolving cybersecurity landscape in academic institutions.

RECOMMENDATIONS

Faculty and Administration: Mandatory Cybersecurity Training: Implement mandatory annual cybersecurity training sessions for all faculty and administration members. This training should cover essential topics such as identifying phishing attempts, secure password management, and recognizing potential threats. Regular training will enhance their cybersecurity awareness and preparedness. Establish Clear Incident Response Protocols: Develop and communicate clear incident response protocols that outline the steps to take in case of a cybersecurity breach. This includes reporting procedures, containment measures, and communication guidelines. By having a well-defined plan in place, faculty and administration can respond swiftly and effectively to mitigate potential damage.

IT Staff: Regular Network Vulnerability Assessments: Conduct regular network vulnerability assessments and penetration testing to identify potential weaknesses in the institution's systems. These assessments should be performed at least annually and after any significant system changes. Addressing vulnerabilities promptly will bolster the institution's overall cybersecurity posture. Collaboration and Training: Foster collaboration between IT staff and other departments to ensure a cohesive approach to cybersecurity. Provide ongoing training for IT professionals to stay updated on the latest cybersecurity threats and trends. This will enable them to implement proactive measures and respond effectively to emerging challenges.

Students: Cybersecurity Awareness Campaigns: Launch engaging and informative cybersecurity awareness campaigns targeting students. These campaigns can include workshops, webinars, and interactive sessions that educate students on topics such as safe online behavior, recognizing phishing attempts, and protecting personal information. Encourage Two-Factor Authentication: Encourage students to enable two-factor authentication (2FA) for their academic accounts. This additional layer of security significantly reduces the risk of

unauthorized access, as it requires a second verification step beyond just a password.

REFERENCES

Triplett, W. J. 2022. Addressing Cybersecurity Challenges in Education. International Journal of STEM Education for Sustainability, Vol.3, No.1, 2023, pp. 47-67 e-ISSN 2798-5091. DOI. 10.52889/ijses.v3i1.132

Choudhury, S. R. 2022. Addressing the global cybersecurity workforce shortage. Information Systems Management, 39(1), 7-17.

Domeij, R. 2019. Cybersecurity threats in primary and secondary education: Swedish teachers' perceptions and strategies. Education and Information Technologies, 24(4), 2603-2619.

Dunn, J. W., & Merkle, J. C. 2018. Assessing perceptions of the cybersecurity workforce and career preference. International Journal of Information Security, 17(6), 693-701.

Filipczuk, P., Hernandez-Castro, J. C., & Li, J. 2019. A comprehensive review of attacks and countermeasures in cyber-physical systems. Information Fusion, 51, 145-167.

Hasib, M. M. (2018). The impact of cybersecurity on the growth of online learning. Journal of Education and Learning, 7(4), 40-51.

Hart, L. C., Peterson, R. C., & Caputo, D. D. 2020. Cybersecurity professionals: Leadership, ethics, and compliance. Journal of Leadership, Accountability and Ethics, 17(1), 1-13.

Mountrouidou, V., Raisi, N., & Delavar, G. 2019. Examining the relationship between e-government and digital divide in cybersecurity. Government Information Quarterly, 36(2), 364-374.

Oyedotun, T. D. 2020. Examining challenges in online education systems for primary and secondary schools in developing countries: A study in Nigeria. Educational Technology Research and Development, 68(6), 2975-2997.

Wright, D. 2016. Lessons learned from cybersecurity challenges. International Journal of Management & Information Systems (Online), 20(3), 219-222.

Brooks, L. 2023. Navigating the Changing Cybersecurity Landscape in Higher Education. Educause Review. Retrieved from https://evolllution.com/technology/tech-tools-and-resources/navigating-the-changing-cybersecurity-landscape-in-higher-education/ as at 16th august 2023

****