https://doi.org/10.37075/BJIEP.2024.2.07
Bulgarian Journal of International Economics and Politics, 2024, Vol. 4, Issue 2, pp. 110-126

Cybersecurity in Higher Education: Challenges and Measures for Information Storage

Elena Angelova[1]

Received: 20.08.2024
Available online: 20.12.2024

Abstract

In the modern digital age, cyber security has emerged as an issue of extreme importance, impacting various sectors and industries worldwide. Notably, higher education institutions have become prime targets for cyber-attacks and other security breaches due to their possession of a vast array of valuable and sensitive information. These institutions store a wealth of personal, financial and research data, making them attractive to malicious actors seeking to exploit vulnerabilities in their information systems. The consequences of such threats can be severe, including reputational damage, financial loss and even legal consequences. Additionally, the disruptive nature of these attacks could significantly disrupt the academic and administrative operations of these institutions, adversely affecting students, faculty and staff. The purpose of this paper is to undertake a comprehensive examination of the issue of cyber security in higher education and to propose practical solutions to address these challenges. This review will look at the different types of cyber threats these institutions face, with a particular focus on identifying the associated problems and presenting effective solutions. It is imperative that higher education institutions should undertake proactive measures to address these concerns as this will protect their position, strengthen the confidence of their stakeholders and ensure the continued pursuit of their educational goals.

Keywords: higher education, cyber threats, cybersecurity, users, internet security
JEL: I23, I29, K24, L86

[1] Doctoral student at the Department of National and Regional Security, University of National and World Economy; e-mail address: leniangel@unwe.bg

Introduction

Every day, users engage in various activities that involve the use of their personal information on the Internet. These activities cover a wide range of areas including, but not limited to, online banking, educational services, healthcare and online commerce. The higher education sector stands as one of the industries facing significant risks (Najiyah and Putriani, 2024). Cases of cyber-attacks leading to data breaches have been documented in educational institutions. Users in higher education institutions rely heavily on devices that provide them with significant flexibility. This allows them to seamlessly adapt to using the Internet and access it when it's convenient for them, regardless of the device they use. However, the task of ensuring cyber security in higher education is a huge challenge.

In the current era where computer systems and the Internet play an increasingly important role, a comprehensive understanding of cyber security is of utmost importance. Institutions of higher education, which store a wealth of valuable research data, personal information, and academic materials, have become prime targets for cybercriminals (Rohan et al., 2023). The consequences of these violations can be severe, including loss of intellectual property, reputational damage, financial burdens, and disruption of educational activities. Chabrow and Ross (2015) highlight the vulnerability of higher education institutions due to their inadequate cybersecurity measures, with the abundance of academic research making them an attractive target for cybercriminals. The potential disruption of academic operations as a result of hacking is a serious concern in the higher education industry. Hackers use the information obtained from these institutions and profitably sell the data as it has become a valuable asset. Online systems of educational institutions are particularly susceptible to cyber security threats, given that almost all activities in higher education rely heavily on computer technology and Internet connectivity. It is critical to recognize the close interrelationship between higher education systems and the online realm. However, the domain of cyberspace is fraught with dangers that arise primarily from theft and illegal activities, raising concerns about cybersecurity. Cybersecurity functions as a protective shield for computerized systems encompassing hardware, software, and digital information, protecting them from malicious actions such as theft, sabotage, disruption, or fraud (Najiyah and Putriani, 2024).

Methodology

The aim of this article is to offer a brief overview of the existing scholarly works related to cyber security in higher education, with special emphasis on both the problematic situation and the corresponding solution. A thorough investigation was undertaken to determine the root cause of the problem as well as to identify the most effective course of action to protect information security. Weak security system policies in large organizations such as schools and universities can be exacerbated by untrained workers and employees, leading to direct access attacks (Liluashvili, 2021). A significant challenge in cybersecurity for higher education institutions is the presence of insufficient security system policies, which affect overall cybersecurity. According to a study by BitSight, a firm focused on cyber risk management, the higher education sector encounters a greater frequency of ransomware attacks than other industries examined. Such attacks frequently result in major financial losses and breaches of data (Fouad, 2021). Another threat is phishing attacks, which involve criminals targeting victims' confidential information via email, social media, or text messages (Alkhalil et al., 2021). An analysis, entitled "Why Cyber Security Should Be a Priority for the Education Sector," highlights that over 80% of cyber incidents are the result of human error (Swivel Secure, 2021). Research circles within the higher education community and various discussion forums were consulted to gain a deeper understanding of the current circumstances facing students.

Findings

Cybersecurity issues in higher education

Digital transformation has been accelerated by the security-changing COVID-19 pandemic. Due to the spread of the virus around the world, many higher education institutions and research organizations have switched to remote work, using various devices to connect to university systems, applications and work files (Pavlova, 2022). A significant challenge is ensuring secure access to these resources. According to a report from the Microsoft Security Center (Microsoft Security, 2020), the education sector accounted for 61% of the 7.7 million malware threats identified in 2020. They examined the cyber risks facing universities and the key measures in security needed in the digital environment.

Allowing personal devices to work both on and off campus offers a variety of benefits, including increased employee satisfaction, greater productivity and cost savings. However, the main concern is that this practice undermines robust security protocols. Employees often use personal smartphones, laptops, tablets, external devices and wireless routers, which often lack the necessary internal network security software. This situation leads to numerous security challenges. Higher education institutions must consistently assess their cyber resilience and their ability to facilitate learning processes through a combination of human resources and information technology.

Many universities worldwide have created and released guidelines regarding the use of personal devices. St. John's University applies this policy (Policy 911, 2019) to its community, which includes "faculty, administrators, staff, students, graduate/technical assistants, alumni, interns, guests, outsiders, and organizations that have access to the network university services, as well as other authorized users." The University of Edinburgh (Information Security, 2022) recognizes the benefits of using personal devices for work and outlines the basic requirements that these devices must meet. According to the University of Sheffield policy (The University of Sheffield, 2021), the institution endorses a "bring your own device" approach, ensuring that staff maintain control over the data they manage, regardless of ownership of the device used to connect to the university network. In the section entitled “Monitoring of User-Owned Devices” it is stated that “[T]he University will not monitor the contents of personal devices, but reserves the right to monitor and log data traffic transferred between the device and University systems.

Educational institutions worldwide suffer significant financial losses as they try to recover from such personnel incidents. There is a pressing need for robust cybersecurity training programs. The foundation of an effective cybersecurity culture relies solely on employee understanding of the underlying processes.

One of the cybersecurity challenges facing higher education institutions is having an inadequate security system policy that has implications for cybersecurity. A study conducted by BitSight, a company specializing in cyber risk management, revealed that the higher education sector experiences the highest incidence of ransomware attacks compared to other industries surveyed. These attacks often lead to significant financial losses and data breaches (Fouad, 2021). Ransomware is a type of virus or malware that gives the attacker access to all the data on the victim’s laptop while preventing the victim from accessing their own data until the requested ransom is paid. This vulnerability is often exploited by individuals with access to IT networks or systems, including employees and vendors (Kundy and Lyimo, 2019: 2). In particular, suppliers may introduce unsafe products to the market, thereby increasing the risks associated with them. This issue is commonly referred to as “technical collateral debt”. If these products are widely used by higher education institutions, the risk of cyber threats would escalate (Hogg, 2015). In addition, the lack of attention to software and operating system updates among those responsible for information system management in higher education institutions is a cause for concern. By ignoring the update process, these institutions leave themselves vulnerable to potential risks and compromise their security posture (Mena-Guacas et al., 2024). Regular updates are crucial to reducing the high risk of virus attacks. It is worth noting that hackers have been exploiting known vulnerabilities since 2002, which account for almost 90% of reported cases (Harrison and Pagliery, 2015).

Figure 1 illustrates that various educational institutions are more inclined to detect breaches or attacks compared to the typical business drawing from data from the United Kingdom. The comparison in 2023 marks a shift from 2022, when primary schools and UK businesses showed similar levels of identification. The main Statistical Release delves into this phenomenon, highlighting that the incidence of cyber security breaches and attacks has decreased among businesses this year, dropping from 39% in 2022 to 32% in 2023, largely due to a reduction in incidents among micro businesses. In comparison, there are no noticeable differences in the results for all four categories of educational institutions from the previous year. Although the figures for secondary schools, colleges, and higher education institutions have decreased compared to last year, these variations lack statistical significance. The long-term trend since 2020 (back then educational institutions were first part of the survey) does not indicate any reliable upward or downward movement for any of the four groups. Primary schools continue to be the least prone to breaches or attacks among the four educational categories, while further and higher education institutions are, together, the most vulnerable. This trend has persisted since 2020, reflecting a consistent pattern over the years.

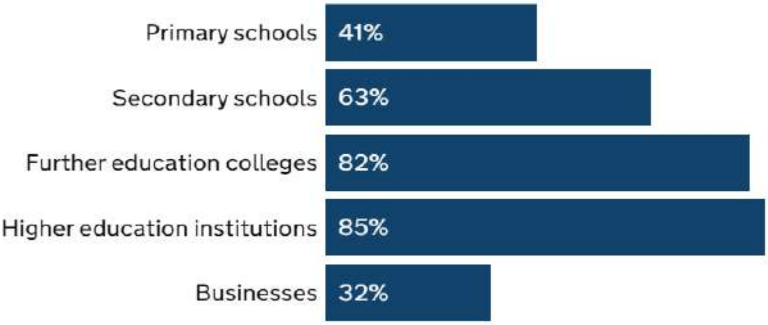

Figure 1. Organisations in the UK identifying breaches or attacks in the last 12 months
Source: Department for Science, Innovation & Technology (2023)

Lack of training among staff and workers is an issue that needs to be addressed, as it can significantly increase the risk of cyber threats. Additionally, lack of support and awareness from senior management and staff regarding cybersecurity can contribute to the vulnerability of the existing system (Alfawaz et al., 2015). Higher education institutions often overlook weaknesses in their security systems, which can lead to various cyber threats. One such threat is phishing attacks, which involve criminals targeting victims' confidential information via email, social media, or text messages. Phishing activities aim to trick people into unknowingly providing personal information for criminal purposes. In addition, weak security system also exposes higher education institutions to malware attacks. According to Cheng and Wang (2022), malware refers to malicious software that has the ability to disrupt or manipulate the normal functioning of digital devices. It is worth noting that malware can exist on a system for extended periods of time without the knowledge of the system owner. These attacks often occur as a result of human error or lack of vigilance. The consequences of such attacks can have various detrimental effects on an institution. One notable impact is the damage it does to a company's reputation. In addition, if the information system is compromised or damaged, this not only makes it difficult to function, but also requires its replacement. Therefore, the company's reputation suffers as a result of this situation. In cases where a system fails in a high-risk group, almost half of the system becomes inoperable, further exacerbating the impact on the information system. Thus, the reputation of the company is significantly affected by these circumstances.

Cyber threats caused by the human factor

Institutions of higher education face a major pitfall and ongoing problem in their efforts to advance human knowledge and protect society from technical attacks. Despite the presence of modern cyber security measures and trained personnel, hacking activities continue to flourish, targeting higher education institutions with the intention of stealing critical and sensitive information. Additionally, various factors such as environmental, social, political, constitutional, organizational, economic, and personal influences affect an individual's ability to detect and mitigate identified threats. Research suggests that employees susceptible to hacking should be categorized based on an analysis of the challenges posed by both traditional and modern tools, followed by the development of training programs aimed at preventing successful hacking attempts. Additionally, effectively addressing the cybersecurity risks posed by students in higher education requires raising the general level of information security awareness among all employees, as eliminating social engineering breaches is proving to be a difficult task. According to the researchers, despite the availability of many modern communication applications, a person's email address remains a permanent online identity. The purpose of the study is to identify email security vulnerabilities that malicious actors use to engage in phishing via phishing emails. The persistent shortage of cybersecurity experts remains a huge obstacle facing higher education institutions (ISACA, 2020). Unfortunately, little progress has been made in this regard, as evidenced by recent studies conducted by Burrell and Kelly (2021) and Crumpler and Lewis (2019). ISACA's Global State of Cybersecurity Survey provides extensive research involving more than 2,000 cybersecurity experts across 17 different industries. The use of the term "global" indicates that the study included participants from around the world and was not limited to those in the United States. The research therefore has an international dimension.

Because of its global scope, the results of the study can be more confidently applied beyond the United States to include universities in Europe and Asia. This is particularly important because the challenges identified, including the understaffing of cybersecurity teams and the lack of practical experience of recent graduates, are not limited to one nation, but represent problems from around the world.

The findings of the ISACA's Global State of Cybersecurity Survey reveal the following picture. The broader problem of a persistent shortage of security professionals in both government and industry globally is highlighted by the finding that 62% of respondents reported that their cybersecurity teams were understaffed. Likewise, continued recruitment and retention challenges within cybersecurity teams, which have seen minimal improvement over the years, are a widespread concern.

The survey also shows that 70% of respondents believe that less than half of security candidates have the necessary network security skills, while 73% of recent graduates have no practical experience. These problems highlight a global deficit in cybersecurity education, affecting not only institutions in the United States, but also those in Europe and Asia. The lack of skilled cybersecurity professionals is a widespread problem, as evidenced by 59% of cybersecurity leaders who say their teams are understaffed.

Therefore, ISACA's Global State of Cybersecurity Survey offers important insights that serve a global audience that includes universities in Europe and Asia. The international scope of the study ensures that its findings are relevant and can guide strategies and improvements in cybersecurity education and workforce development worldwide.

The discussion by Yuchong and Qinghui (2021) also delves into potential career paths in cybersecurity. A key aspect of creating and maintaining a profitable cybersecurity program is the ability to identify and meet workforce requirements. Previous research in cybersecurity education has primarily focused on two main areas: the use of specialized labs, platforms, and technologies in cybersecurity courses, and the delivery of cybersecurity education courses and textbooks. It is worth noting that cybersecurity covers a wide range of topics, making it challenging to cover all aspects within a single semester or degree program. To address this issue, each program is tasked with defining and designing the specific topics and methodologies to be covered. Over the past two decades, the US federal government has implemented various initiatives aimed at developing higher education security policies, standards, and regulations, such as the National Telecommunications Security Policy. The NIST Cybersecurity Framework, as well as the National Cybersecurity Education Strategic Framework Initiative (NIST, 2018), the National INFOSEC Education and Training Program, and the National Information Systems Security Education Conference, are integral components of this endeavor. Its primary goal is to provide comprehensive training to college and university students in preparation for careers in information security. However, there is a notable lack of research that delves into the theoretical underpinnings needed to create instructional cybersecurity programs that are aligned with the specific requirements of higher education institutions.

External entities trick users into providing their personal information

In the realm of higher education, the cybersecurity problem can manifest itself when outside entities use deceptive tactics to coerce users into revealing their personal information. Those external actors who do not have a primary role in interactions or transactions between different parties, but may still have a vested interest or concern, pose a significant threat. To protect their systems from unauthorized access, most organizations rely on passwords. However, system security breaches, data theft, and system exploitation often occur as a result of “cracking” a user’s login credentials or obtaining them through hacking. It is critical to include human factors in the conceptualization of security processes because security measures are designed, implemented, and breached by individuals. Surprisingly, human considerations have become more relevant to hackers than to cybersecurity professionals. Social manipulation techniques, such as password fabrication and manipulation, exploit users who are unfamiliar with security protocols (Adams et al., 1999). These cybercriminals use open source applications to make sure that the people clicking on their ads are really people. Educational institutions, in particular, store vast amounts of data relating to their students as well as their academic and non-academic staff. This data includes information such as residential addresses, dates of birth and full names. While this information may not seem as important as bank details or identification numbers, it can prove valuable to cybercriminals. Phishing attacks pretending to be close relatives or friends are possible. Cybercriminals can also use this information to pretend to be students or employees for a profit.

According to Lötter and Futcher (2014), email clients offer sufficient security measures. However, it is important to note that emails can also serve as a valuable tool for hackers planning phishing scams. The credibility and trustworthiness of an email greatly increases its value in the event of a security breach. By gaining unauthorized access to an institution's email account, fraudsters can take advantage of the institution's reputation by sending phishing emails. In addition, ".edu" email addresses belonging to students and faculty members are often publicly exposed, making it easier for attackers to identify and target potential victims. Also, cybercriminals can easily get an educational domain email address for themselves. Therefore, email attacks serve as a starting point for theft in higher education. Higher education institutions, especially their employees, face a higher risk of falling victim to phishing attempts. It is critical to recognize that it only takes the error of one employee for the entire university system to be compromised by this threat.

Solutions

The National Initiative for Cybersecurity Education (NICE)

Before deploying technology solutions, it is critical that users have a comprehensive understanding of identifying and responding to suspicious phishing emails. This study outlines the key components of a comprehensive program aimed at testing, training, measuring, and improving an organization's cybersecurity measures to effectively reduce the risk of phishing attacks. The development and implementation of this program is based on practical experience in designing training programs and following the guidelines provided by the National Institute of Standards and Technology (NIST). Improving overall cybersecurity measures can significantly reduce vulnerability to phishing cyberthreats. As the demand for cybersecurity professionals continues to grow, it is recommended that NIST initiate a NICE project on the cybersecurity framework. The NICE Framework offers valuable recommendations and guidance to educators in developing cyber security training programs that equip graduates with the necessary skills to meet the cyber security requirements of higher education institutions. This framework enables educators to create a rigorous cybersecurity curriculum that is aligned with the standards set by higher education institutions (NIST, 2018). The NICE framework plays a crucial role in establishing a link between cyber security education and the requirements of higher education institutions. By improving communication between cybersecurity educators, trainers, certifiers, employers and employees, the NICE framework facilitates more effective information exchange. In addition, the primary analysis process identifies the essential tasks that people must perform in order to perform their job duties effectively. A skills analysis further delineates specific job roles and related tasks. The NICE framework covers different categories, areas of expertise and posts. These organizational components are structured in the framework. Recognizing the need to bridge the industry gap, the National Institute of Standards and Technology (NIST) recommends that educational institutions align their training courses with the NICE framework.

Originally designed as a resource aimed at a national audience, the NICE (National Cyber Security Training Initiative) framework remains highly relevant and illustrative in contexts outside the United States, thanks to its thorough and organized method of defining and structuring cybersecurity roles. Its compatibility extends to non-US environments:

1. Standardization and common language. The NICE Framework creates a shared terminology that articulates the tasks related to cybersecurity, as well as the knowledge and skills required to perform those tasks. This shared language is advantageous on a global scale because it offers a uniform method of delineating roles and responsibilities in cybersecurity. Educational institutions and industries around the world can apply this framework to ensure consistency and clarity in cybersecurity training and job positions.

2. Training and qualification requirements. The framework outlines the required training and qualification criteria to cultivate essential knowledge, skills and abilities (KSA) to perform cybersecurity tasks. This comprehensive approach to KSA ensures that cybersecurity professionals can be effectively trained to meet industry standards regardless of their geographic location.

3. Curriculum development. The NICE Framework provides important guidance and recommendations for educators charged with creating cyber security training programs that equip graduates with the essential skills to meet the cyber security requirements of higher education institutions. This ensures that the curriculum remains robust and in line with industry standards, a need recognized by educational institutions around the world.

Application in contexts outside the United States

1. Industrial requirements and educational research. A recent study conducted by Armstrong et al. (2020) used the NICE framework to assess the knowledge, skills and competencies required to meet industrial cyber security requirements. This shows that the principles of the framework can be successfully used to recognize and address the requirements of non-US industry.

2. Improved communication. This framework promotes better communication between cybersecurity educators, trainers, certifiers, employers and employees, resulting in more effective information exchange. Such a need is universal as the global cybersecurity industry faces comparable challenges related to skills shortages and workforce development.

3. Task and skills analysis. The core analytical process of the NICE Framework defines key tasks while detailing specific job roles and their associated responsibilities. This methodical strategy for defining job roles and tasks is proving useful in any nation as it establishes a clear path for developing cybersecurity careers and workforce planning.

4. Recommendations from NIST. The National Institute of Standards and Technology (NIST) advises educational institutions to synchronize their training programs with the NICE framework. Although NIST operates in the United States, its guidelines are based on internationally recognized best practices in cybersecurity education and workforce development.

Many cases of international adoption can be observed in regions such as Europe and Asia. Various European nations, with the support of organizations such as ENISA (European

Union Agency for Cybersecurity), have expressed interest in similar to NICE frameworks to standardize cybersecurity training and develop their workforce. In addition, countries including Singapore and Japan, are considering adopting NICE-inspired frameworks to improve their national cybersecurity strategies and education initiatives.

Although the NICE framework originated in the United States, its principles and organized methodology for cybersecurity training and workforce development have significant relevance to contexts outside the US. Its standardized language, training prerequisites, and task analysis demonstrate global applicability, making it an essential resource for addressing the global cybersecurity skills shortage.

Creating an effective cyber risk management strategy

Cyberattacks are widespread in higher education not because of deficiencies in IT infrastructure, but rather because of the vastness, complexity, and use of multiple system programs and software within these institutions. The widespread use of tablets and smartphones, allowing users to connect to the Internet, further complicates the implementation of robust security measures. Institutions of higher education employ various strategies to mitigate cyber risks, such as upgrading software and hardware to effectively manage Internet access, traffic, and intrusion detection systems. As highlighted by Liluashvili (2021), the development of a comprehensive cyber risk management plan stands as a paramount element in an organization's cyber security framework. In the face of cybersecurity threats, there are specific methods that institutions can use to protect themselves. It takes a collective effort across the organization to effectively combat cyber attacks. Scientific researchers and institutes store invaluable research data that must be protected from the clutches of cybercriminals. In order to ensure the privacy of such data, researchers must cooperate tactically with the system authorities. Higher education institutions can create collaborative teams that include department heads, researchers, and key security personnel. It is of the utmost importance to maintain constant vigilance and implement appropriate safeguards to protect both confidential personal information and valuable research data. To ensure the effectiveness of IT operations, it is imperative that individuals using technology receive appropriate access credentials based on their level of risk exposure. According to Liluashvili (2021), implementing a Privileged Access Management (PAM) solution is necessary to automate the administration of credentials and regulate restricted access. An alternative approach is to control user access through a tiered system, where higher-level privileges grant greater access to required resources while restricting access to a select group of users. Given that hackers often target administrator credentials to gain unauthorized access to valuable data and exploit vulnerable systems, regular monitoring of each individual account is critical. It is also essential to have secure protocols for resetting identities, such as passwords, tokens, and tickers. To maintain a high level of cybersecurity in any organization, it is imperative to separate user credentials and login access for individual employees. By taking this approach, the impact of a potential breach will be minimal, as the malicious actor's restricted access features will prevent widespread damage. Educational institutions that have adopted this system have had fewer incidents of system outages.

Data security requires effective password management. Password strength is critical to protecting both personal and business information and protecting privacy. Password policies are extremely important to users, whether regular or remote. Establishing a secure password involves following several guidelines (Vu et al., 2007). One such guideline is the length requirement. Passwords must be at least eight characters long. The complexity of a password is directly related to its resistance against hacking attempts. Additionally, users should refrain from using generic models. It is recommended to avoid using capital letters at the beginning or including non-traditional symbols and numbers at the end. While simple patterns help with memorization, they also make passwords more susceptible to guessing.

Improving the security system in higher education institutions

Advances in technology have led to the popularity of Artificial Intelligence (AI) and the Internet of Things (IoT). Consequently, there has been an increase in cyber security threats in recent years. The increasing interconnectedness of the Internet and the evolving nature of attacks have led to a significant increase in cyber attacks (Cheng and Wang, 2022). Therefore, it is imperative that corrective measures are taken to address this issue. One potential solution to this problem is the improvement of the security system in higher education institutions. Mayieka Jared Maranga and Dr. Masese Nelson suggest that higher education institutions should invest in state-of-the-art research laboratories and prioritize individual and collaborative cybersecurity research and development. In addition, senior management must allocate sufficient financial resources to cyber security. Substantial funds are needed to provide the necessary facilities and infrastructure, including the latest technologies, to digitize security systems in national educational institutions. It is therefore imperative that the government takes a vital role in allocating funds within the budget to facilitate the improvement of security systems in higher education institutions. Governments should consider implementing measures to protect against cyber threats. By implementing cybersecurity measures, computers, networks, key systems, software applications and data in higher education institutions can be protected from potential digital risks. Implementing these cybersecurity safeguards is critical for higher education institutions to maintain the trust of their customers (Maranga and Nelson, 2019).

It is within the scope of the institution’s authorities to initiate training and awareness initiatives that aim to improve computer users’ understanding of the importance of cyber security (Aldawood and Skinner, 2019). The importance of cyber security awareness cannot be overstated as it serves as a safeguard against becoming a victim of cyber crime. This awareness should spread to all segments of society, paying special attention to students who are most vulnerable to cybercrime due to their age and cognitive development. Therefore, imparting cyber security knowledge and skills to students becomes imperative to protect them from becoming targets of cyber crimes. In response to the increasing prevalence of social engineering attacks, educational institutions have developed education and awareness programs (Ibidem.). Additionally, installing firewalls in educational institutions can significantly improve cyber security. The deployment of real-time firewalls and anti-virus programs serves as a proactive measure (Cheng and Wang, 2022). By configuring firewalls and using up-to-date operating systems, users can effectively disable remote access, thereby thwarting hackers' attempts to take over their computers. By strengthening their cybersecurity systems, higher education institutions indirectly contribute to protecting their systems from being compromised by malicious individuals.

Discussion

The explicit need for cybersecurity in Higher Education Institutions is multifaceted and increasingly crucial in today's digital age. As these institutions continue to integrate technology into their educational frameworks, they become more susceptible to cyber threats, making robust cybersecurity measures essential.

Firstly, Higher Education Institutions handle a vast amount of sensitive data, including personal information of students and staff, financial records, and intellectual property. This data is highly attractive to cybercriminals, who may target institutions to steal this information for financial gain or other malicious purposes. Secondly, the academic environment often encourages open access to information and collaboration, which, while beneficial for research and learning, can create vulnerabilities in IT systems. This open-access culture requires a delicate balance between accessibility and security to ensure that research and educational activities can proceed without compromising sensitive data.

Moreover, with the increasing reliance on digital platforms for distance learning and administrative functions, any disruption caused by cyber-attacks can severely impact educational delivery. For instance, a ransomware attack could lock administrators out of critical systems, delaying academic operations and causing significant inconvenience to students and faculty. The demand for cybersecurity skills is also rising within the Information Systems field, highlighting the importance of preparing graduates who can address these challenges (Towhidi and Pridmore, 2023). This demand underscores the necessity for Higher Education Institutions to integrate cybersecurity into their curricula, equipping students with the skills needed to protect against cyber threats.

The weak security system policy mentioned earlier can have a significant impact on cyber security. The evidence presented shows that the person responsible for managing the systems at the Higher Education Institution neglected to update the software, leaving the operating system vulnerable. This lack of sensitivity to their responsibilities results in many parties bearing the consequences. Systems that are not regularly updated are more susceptible to virus threats than devices that receive regular maintenance and updates. To improve cyber security, those responsible should consider implementing firewalls in educational institutions. Firewalls can indirectly block certain cyber threats. In addition, dangerous and low-quality products are often placed on the market, which pose a risk. These dangerous products are often sold at lower prices, attracting unscrupulous Higher Education Institutions looking for cost-cutting measures. This serves as a major cause of ineffective security systems. Therefore, the government must play a crucial role in providing additional funds to enable Higher Education Institutions to improve their security systems. Institutions with greater financial resources have the ability to acquire higher quality products. Additionally, within large organizations such as schools and universities, the presence of untrained workers can lead to direct access attacks. Errors are more common among untrained workers, which can further exacerbate cyber threats. In addition, untrained employees are more susceptible to attack by hackers. Therefore, it is the institution's responsibility to implement training and awareness programs that aim to increase the awareness of computer users. Having such programs indirectly cultivates a sense of responsibility among employees to protect user data. Employees will make more efforts to acquire proper knowledge to use the system and prioritize safety measures. Finally, a lack of support from senior management contributes to the vulnerability of cyber systems.

If higher authorities refuse to allocate additional funds to strengthen the system, higher education institutions will face many challenges. Managers must recognize their responsibility to strengthen their institution's security systems to prevent information leakage. Therefore, senior officials should invest in modern research labs and place greater emphasis on individual and collective cybersecurity research and development. This is a necessary action. In order to increase the security levels of higher education institutions, it is imperative to establish a robust security system. Research in information systems education highlights the need to shape IS courses in line with the current demands of industries and businesses, ensuring that IS graduates are well prepared for their future careers. Several initiatives have been developed to support this endeavour, including the NIST Cybersecurity Framework, the Cybersecurity Education Role Framework, the National Cybersecurity Education Strategic Plan Initiative (NIST, 2018), the National INFOSEC Education and Training Program and the National Security Information Systems Conference. However, previous studies have failed to address the conceptual framework for developing a cybersecurity program that aligns with industry needs. A significant finding from this study underscores the importance of implementing a comprehensive phishing education program alongside email security technologies. The NICE project, in collaboration with the National Institute of Standards and Technology (NIST), has been instrumental in meeting the growing demand for cybersecurity professionals. The project framework provides recommendations and guidance for educators in designing cybersecurity training programs that equip graduates with the necessary skills to meet industry demands. The framework highlights the need for educators to develop a rigorous cyber security program that meets market demands (NIST, 2018).

A recent study (Armstrong et al., 2020) used the NICE framework to highlight the importance of understanding, skills and capabilities to address the cybersecurity needs of industry. The framework serves as a valuable tool that effectively aligns cybersecurity education with industry requirements. To bridge industry gaps, educational institutions are advised by the NIST to align their programs with the NICE framework. Cyber-attacks are becoming more common in all sectors, especially targeting government institutions and critical infrastructure. This has sparked increased interest in cybersecurity measures and legislation. To protect the personal and sensitive information of students and staff, higher education networks must implement a sophisticated combination of accessible platforms and robust security measures. Unfortunately, hackers have identified educational institutions as prime targets for data theft, as these institutions store vast amounts of valuable information. In addition, many colleges have adopted a more transparent approach, allowing quick and efficient access to their websites for students and parents. Unfortunately, this inadvertently exposes vulnerabilities that cybercriminals exploit, often using email phishing as an easy method to break into university and college systems. Academics and higher education workers can easily accept and eventually join this fraudulent hacking scenario if only a trusted domain name like ".edu" or ".org" is used. This security problem can be reduced by implementing Privileged Access Management (PAM). This is because PAM software can provide secure remote access to individuals without providing external domain identification, limiting access to only necessary sources and reducing the likelihood of unauthorized access to sensitive information. It can also ensure that all external activities are tracked and documented.

Conclusion

The issue of cyber security is no longer a secret knowledge only for hackers; it has now become a major issue for higher education institutions due to the increase in the use of the Internet. The vulnerability of these institutions to cyberattacks is exacerbated by a weak governance environment. Our observations show that hackers can exploit security holes in the system to steal data from anyone associated with an institution of higher education, be it students, instructors, or staff. As higher education institutions move from traditional paper-based data storage to digital systems, it is imperative that they prioritize and pay close attention to cybersecurity when it comes to storing, accessing and retrieving critical information. In today's era, information and data protection is a prerequisite for most Higher Education Institutions around the world, as unauthorized access to such assets can lead to significant problems in the future. While it is impossible to completely eliminate cybercrime, Higher Education Institutions must remain vigilant while using the Internet, ensuring that all online transactions are conducted securely and without data leakage. It is critical for these institutions to collaborate and maintain unwavering focus and attention to maintain information security. In addition, the implementation of appropriate security controls is essential to prevent unauthorized disclosure of information.

References

Adams, A., Sasse, M.A. and Lunt, P. (1997). “Making passwords secure and usable.” In: Thimbleby, H., O’Conaill, B., Thomas, P.J. (eds) *People and Computers XII*. Springer, London, pp. 1–19. DOI: https://doi.org/10.1007/978-1-4471-3601-9_1

Aldawood, H. and Skinner, G. (2019). “Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues.” In: *Future Internet*, Vol. 11, Issue 3, 73. DOI: https://doi.org/10.3390/fi11030073

AlFawaz S., Plagnol, V., Wong, F.S.L. and Kelsell, D.P. (2015). “A novel frameshift *MSX1* mutation in a Saudi family with autosomal dominant premolar and third molar agenesis.” In: *Archives of Oral Biology*, Vol. 60, Issue 7, pp. 982-988. DOI: https://doi.org/10.1016/j.archoralbio.2015.02.023

Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I. (2021). “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy.” In: *Frontiers in Computer Sciences*, Vol. 3. DOI: https://doi.org/10.3389/fcomp.2021.563060

Armstrong, M., Jones, K.S., Namin, A.S. and Newton, D.C. (2020). “Knowledge, Skills, and Abilities for Specialized Curricula in Cyber Defense: Results from Interviews with Cyber Professionals.” In: ACM Transactions on Computing Education, Vol. 20, Issue 4, pp. 1-29. DOI: https://doi.org/10.1145/3421254

Burrell, R. and Kelly, C. (2021). “The COVID-19 Pandemic and the Challenge for Innovation Policy.” In: *Northern Ireland Legal Quarterly*, COVID-19 Supplement Vol. 72, No. S1, pp. 212-219. DOI: https://doi.org/10.53386/nilq.v72iS1.955

Chabrow, E. and Ross, R. (2015). China blamed for Penn State Breach. DataBreachToday. May 15 http://www.databreachtoday.com/china-blamed-for-penn-state-breach-a-8230.

Cheng, E.C., and Wang, T. (2022). “Institutional strategies for cybersecurity in higher education institutions.” In: *Information*, Vol. 13, Issue 4, 192. Special Issue Information Technologies in Education, Research and Innovation. DOI: https://doi.org/10.3390/info13040192.

Crumpler, W. and Lewis, J. (2019). “The Cybersecurity Workforce Gap.” Center for Strategic and International Studies, Washington DC. [Online]. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf. (last visited June, 2024).

Department for Science, Innovation & Technology (2023). “Cyber security breaches survey 2023: education institutions annex.” Official Statistics. Published April 19, 2023. [Online]. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex#appendix-a-further-information (last visited May, 2024).

Fouad, N.S. (2021). “Securing higher education against cyberthreats: from an institutional risk to a national policy challenge.” In: *Journal of Cyber Policy*, Vol. 6, Issue 2, pp. 137–154. DOI: https://doi.org/10.1080/23738871.2021.1973526

Harrison, V. and Pagliery, J. (2015). “Nearly 1 million new malware threats released every day.” In: *CNN Business*, April 14, 2015. [Online]. Available at: https://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/index.html (last visited June, 2024).

Hogg, M.A. (2015). “To belong or not to belong: Some self-conceptual and behavioural consequences of identity uncertainty.” In: *International Journal of Social Psychology*, Vol. 30, Issue 3, pp. 586–613. DOI: https://doi.org/10.1080/02134748.2015.1065090

Information Security (2022). “Using BYOD or Self-Managed Devices.” The University of Edinburgh, October 27, 2022. [Online]. Available at: https://infosec.ed.ac.uk/information-protection-policies/guidance-how-to-conform-with-policy/using-byod-or-self-managed (last visited June, 2024).

ISACA (2020). *State of Cybersecurity 2020.* [Online]. Available at: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/infographics/state-of-cybersecurity_ifg_0220b.pdf (last visited June, 2024).

Kundy, E.D. and Lyimo, B.J. (2019). Cyber Security Threats in Higher Learning Institutions in Tanzania, A Case of University of Arusha and Tumaini University Makumira. Olva Academy – School of Researchers, Vol. 2, Issue 3.

Liluashvili, G.B. (2021). Cyber risk mitigation in higher education. Law and World, 7(2), 15–27. https://doi.org/10.36475/7.2.2.

Lötter, A. and Futcher, L. (2015). “A framework to assist email users in the identification of phishing attacks.” In: *Information and Computer Security*, Vol. 23, No 4, pp. 370–381. DOI: https://doi.org/10.1108/ics-10-2014-0070.

Maranga, M. J. and Nelson, M. (2019). “Emerging issues in cyber security for institutions of higher education.” In: *International Journal of Computer Science and Network*, Vol. 8, Issue 4, pp. 371-379. [Online]. Available at: http://ijcsn.org/IJCSN-2019/8-4/Emerging-Issues-in-Cyber-Security-for-Institutions-of-Higher-Education.pdf (last visited July, 2024).

Mena-Guacas, A.F., Meza-Morales, J.A., Fernández, E and López-Meneses, E. (2024). “Digital Collaboration in Higher Education: A Study of Digital Skills and Collaborative Attitudes in Students from Diverse Universities.” In: *Education Sciences*, Vol. 14, No. 1: 36. DOI: https://doi.org/10.3390/educsci14010036

Microsoft Security (2020). Security intelligence, Microsoft Security, available at: https://www.microsoft.com/security/blog/security-intelligence/.

Najiyah, N.L. and Putriani, R. (2024). “Transformation of Hadith Study in the Digital Era: an Effectiveness of Hadith Applications and Websites.” In: *Mashdar: Jurnal Studi Al-Qur’an dan Hadis*, Vol. 6, pp. 27-42. DOI: http://dx.doi.org/10.15548/mashdar.v6i1.7882

NIST (2018). NICE Spring 2018 eNewsletter. [Online]. Available at: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-spring-2018-enewsletter (last visited July, 2023).

Pavlova, E. (2022). “Predizvikatelstva za kibersigurnostta pri izpolzwaneto na lichni ustroistva v UNSS”, Issue/2022, pp. 137-147. DOI: https://doi.org/10.37075/RP.2022.3.08

Policy 911 (2019). “Bring Your Own Device (BYOD) Policy.” St John’s University. Effective date 5/1/2019. [Online]. Available at: https://www.stjohns.edu/my-st-johns/human-resources/policy-911-bring-your-own-device-byod-policy (last visited June, 2024).

Rohan, R., Funilkul, S., Chutimaskul, W., Kanthmanon, P., Papasratorn, B., and Pal, D. (2023). Information security awareness in higher education institutes: A WORK IN PROGRESS. 2023 15th International Conference on Knowledge and Smart Technology (KST). DOI: https://doi.org/10.1109/kst57286.2023.10086884

Swivel Secure (2021). Why Cybersecurity Needs To Be a Priority for The Education Sector. [Online]. Available at: https://swivelsecure.com/solutions/education/why-cybersecurity-needs-to-be-a-priority-for-the-education-sector/ (last visited June, 2024).

The University of Sheffield (2021). IT Code of Connection. [Online]. Available at: https://www.sheffield.ac.uk/it-services/code-practice/code-connection?utm_source=chatgpt.com (last visited May, 2024).

Towhidi, G. and Pridmore, J. (2023). “Aligning Cybersecurity in Higher Education with Industry Needs.” In: *Journal of Information Systems Education*, Vol. 34, Issue 1, pp. 70-83. [Online]. Available at: https://aisel.aisnet.org/jise/vol34/iss1/6 (last visited May, 2024).

Vu, K.-P., Proctor, R.W., Bhargav-Spantzel, A., Tai, B.-L. (Belin), Cook, J. and Schultz, E. (2007). “Improving password security and memorability to protect personal and organizational information.” In: *International Journal of Human-Computer Studies*, Vol. 65, Issue 8, pp. 744–757. DOI: https://doi.org/10.1016/j.ijhcs.2007.03.007

Yuchong, L. and Qinghui, L. (2021). “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments.” In: *Energy Reports*, Vol. 7, pp. 8176-8186. DOI: https://doi.org/10.1016/j.egyr.2021.08.126