Borneo International Journal eISSN 2636-9826; Vol. 7 (4); 2024; 22-27
Published by *Majmuah Enterprise*
www.majmuah.com

An Awareness of Cybersecurity Risk Assessment and Management Among Students

AHMAD ARIF HAKIMI. MOHAMAD FADLI ZOLKIPLI

School of Computing, College of Arts and Sciences, Universiti Utara Malaysia (UUM), 06010 Changlun, Kedah, MALAYSIA
Email: ahmad_arif_hakimi@soc.uum.edu.my | Tel: +60109216136 | m.fadli.zolkipli@uum.edu.my

Received: November 18, 2024
Accepted: November 22, 2024
Online Published: December 01, 2024

Abstract

The present study aims to measure the level of cybersecurity awareness among university students and their practice level in terms of risk assessment and management. In the modern age, universities tend to rely much on digital platforms. For this reason, students are exposed to many types of cyber threats compromising personal data security and institutional security, such as phishing, malware, and identity theft. It focuses on the desperate need in institutes of higher learning for cybersecurity education on safe browsing behavior, risk reduction, and preparation of the computerized workforce. This study justifies the introduction of the cybersecurity module in university curricula that can facilitate students with pragmatic skills in the identification and effective response against cyber threats. The present study will contribute to such a goal of a safer academic environment by finally offering targeted cybersecurity training that fosters a culture of digital responsibility.

Keywords: cybersecurity, digital awareness, risk management, higher education, phishing, malware

1. Introduction

With everything turning digitally, cybersecurity is the foremost worry for all individuals and organizations. These digital technologies, while making life so easy, expose their users to almost all kinds of cybersecurity threats, including data breaches, phishing attacks, and identity theft (Schatz, Bashroush, & Wall, 2017). These risks drive the need for cybersecurity awareness management strategies, among young adults who are considered heavy internet users devoid of the requisite awareness to navigate through these dangers safely (Katsumata, Hemenway, & Gavins, 2010). Students in universities are just like most other university students around the world which are they depend so much on digital platforms either for educational or personal purposes and perhaps bring themselves within the crosshairs of cyber threats. Hence, awareness and understanding of cybersecurity risks are among those issues of huge significance both for their personal safety and for maintaining standards of information security at university (Khader, Karam, & Fares, 2021). The research show that the low level of cybersecurity risk management - such as recognition of a probable threat and proactive measures of security may drastically reduce these risks (Tissir, Kafhali, & Aboutabit, 2020).

This present study aims to find out the level of awareness of students regarding cybersecurity issues and their perceived knowledge regarding risk assessment and management. The research study also attempts to undertake a voyage of enlightenment to the developing body of literature in cybersecurity education, with a specific interest in higher education, where students go into professional settings that are increasingly digital (Jalil et al., 2024; Scala et al., 2019). Understanding these factors may help develop targeted educational programs that better prepare students to protect their data and navigate cyber threats effectively.

2. Literature Review

As digital technology has permeated nearly every aspect of life, cybersecurity should be ensured because most of our personal and professional activities are being carried out using the internet. In other words, cybersecurity is a mechanism that protects Internet-connected systems, including hardware, software, and data, against cyberattacks. Most of these attacks generally aim at accessing, degrading, disrupting, distorting, or gaining unauthorized use of the asset service or information (Schatz et al., 2017). These kinds of attacks are becoming increasingly frequent, sophisticated, and destructive in nature. Thus, good cybersecurity practice should be implemented, especially within an academic environment. Since universities must process a sea of sensitive information, it is more likely that they fall prey in cyberattacks, ranging from sensitive students' personal details to research data.

However, with the sudden overnight expansion of e-learning and distant working, universities depend on cybersecurity more than ever. It is not just protection against data breaches that it is concerned with, but it also involves educating students and staff for the best practices that could help in preventing security breaches. A cybersecurity aware environment would be shared a responsibility in which every entity of the institution, starting from staff to faculty to students, would be involved with one another in maintaining digital safety.

These come in the form of various types of vulnerabilities that are exploited across systems and among a lot of different types of users. Some of the most common types of attacks include phishing, malware, ransomware, and DDoS (distributed denial-of-service) attacks. People commonly fall prey to giving away personal information through fraudulent emails or messages in phishing; these appear to be legitimate. he particularly unsettling issue in the university environment is how easily phishing can be perpetrated due to open networks and dissemination practices (Cherdantseva et al., 2015). Malware and ransomware-all of which are all equally damaging: malware compromises system functionality, and ransomware holds data "hostage" until a ransom is paid. The consequences of these kinds of threats could be grave: financially, universities stand to lose much owing to demands for ransomware or resources required to recover in the wake of such attacks. It is reputation and trust, though, that will be the long-term casualties if either student data or research is compromised. DDoS-essentially working to overwhelm the networks with traffic-can impact basic services, delaying academic and research work (Katsumata et al., 2010). Not to mention the psychological effect that such breaches have on students and staff: the outcome of a data breach is that people feel violated and less secure. Because of this, universities need not just technical robust defenses but also a culture of cybersecurity awareness that will allow students and staff to understand how to identify and respond to the threats (Tissir et al., 2020).

In other words, a cyber threat can be viewed as the probability that a risk could occur along with the consequences or impact it may realize. The university setting makes cybersecurity risks very complex because there are diverse users of shared digital resources: students, faculty, and staff. Each of these persons has different levels of awareness of cybersecurity; therefore, vulnerabilities could be present (Yang et al., 2020). Management of cybersecurity risk is less about technology but, rather, learning what the possible threats may be, estimating the probability of occurrence, and building up strategies that might help mitigate the effect when a cyber-attack occurs. Many universities are using a structured approach for risk assessment; these do tend to assist them in identifying the most significant risks they may use resources. These methods serve well in prioritizing security efforts and go a long way toward enabling universities to protect their operations and resources, according to Aksu et al.. (2017), Besides the institutional data, good cybersecurity practices protect the personal information of students, thus creating a much safer and more secure academic environment.

The major components of cybersecurity include awareness among students. Students' knowledge on cybersecurity varies a lot, mainly depending on the level of digitization and formal training in this aspect (Sarathchandra et al., 2016). For example, students who are much engaged on digital platforms without security awareness will easily be affected by these threats, such as phishing or malware. Khader et al. (2021) determined that even as students apparently seem to understand the basics of cyber threats, the lack of specific practices that they could use to their advantage has partly been missing. Perhaps it is the lack of this sort of practical knowledge that is causing students unconsciously to involve themselves and their institutions in certain kinds of risks. The result of focused training and awareness, according to Larionova et al. (2023), would be increasing the number of students who can develop good skills in online protection. In essence, this would include practical workshops, test phishing, and instructions on working with security tools which in aggregate allow responsibility and readiness. Those universities that include cybersecurity awareness in the curriculum have higher success rates because the students themselves will protect not only their information but contribute to a safe campus. A proactive approach helps everyone involved by instilling a shared responsibility culture in cybersecurity.

Universities bear a special responsibility in teaching students the ways of digital space safely. According to available studies, embedding cybersecurity into curricula makes much difference in equipping students with relevant identification and response skills against cyber threats (Perälä & Lehto, 2024). Workshops on this, or integration of such modules into relevant courses, will provide students with basic knowledge on how to protect themselves and their digital environments. Practical exercises in the form of cybersecurity simulations will be of immense help. Indeed, Mukherjee et al. (2024) established that practical exercises raise awareness and at the same time enhance the critical thinking and problem-solving ability of students in the domain of cybersecurity. Further, such programs go toward the broader vision of building a more digitally aware and responsible society where students who know about issues in cybersecurity can be better prepared to protect themselves and the eventual work environment. Therefore, by giving due importance to cybersecurity education, universities protect not only their data and network but also ensure that students take away lifelong knowledge of how to stay safe digitally. This proactive approach will both contribute to the

culture of cybersecurity that looks after the whole academic community and prepare them for the security challenges awaiting them upon graduation.

3. Discussion

1. Risk Assessment Methodologies

It is one of the basic building blocks in gaining and understanding the threats of cybersecurity: risk assessment. Many different methodologies exist, all with various strengths and limits. For example, qualitative risk assessment methods rely on expert judgment to categorize risks with respect to their potential impact and likelihood. This type of approach is particularly useful within the academic environment when risks vary significantly in type and are quite hard to quantify. On the other hand, quantitative approaches are used for rating in numerical form with the purpose of evaluating the seriousness of possible vulnerabilities (Aksu et al., 2017). The Common Vulnerability Scoring System issues the severity of evaluation. Though the quantitative analyses can be much more detailed, yet they do essentially require very specialized knowledge and certain tools to implement, which may not always be at one's disposal in a non-technical university setting. Combining elements of both qualitative and quantitative methodologies achieves a judicious balance. For example, universities could use a multitiered risk assessment system that identifies the most important assets using expert judgment and then assesses vulnerability through quantitative scoring. In this case, the institutions are in a position where they can effectively invest resources in which high-risk areas are attended to with a wider view on other less important potential threats. It needs to be continuous-the process of risk assessment must be updated periodically to achieve the emergence of new cyber threats and technologies.

2. Effective Risk Management Strategies

Management of cybersecurity-related risks refers to the set of practices aimed at reducing either the probability or consequences a cyber threat may have. As such, efficient cybersecurity strategies vary tremendously-from basic controls like firewalls, antivirus software, and timely software updating to more advanced ones, including network segmentation and access control. A reasonable approach to risk management in this academic environment would probably involve a combination of technical, administrative, and educative controls. This generally tends to be the most effective strategy. Sounding administrative controls will benefit the universities enormously. However, in helping to protect institutional data and preparing the university for when breaches do occur, it involves assistance from policies like requirements for secure login, encryption of data, and incident response planning. But their success depends totally on how well they are communicated to and enforced amongst students and staff. Such training programs allow all users to be informed and observe the policies that minimize human error that may lead to the compromising of institutional security. Beyond this, collaborative cybersecurity-partnership with cybersecurity companies or government agencies-allows university awareness of current threats and defenses. Integrating such information within cybersecurity policy will ensure that the university's approach remains current and impenetrable to all emerging cyber threats.

3. The Role of Technology in Enhancing Cybersecurity

Technology does so much in enhancing cybersecurity in educational organizations. Such software, like intrusion detection systems, endpoint protection, and network monitoring, can identify potential threats and report them automatically, or even take the neutralization of such upon themselves before they spread. For instance, IDS might monitor the flow of network traffic for suspicious activity, warning IT staff such that, in essence, an early warning system is provided, which allows timely response in the case of a potential breach (Cherdantseva et al., 2015). With Artificial Intelligence and Machine Learning, cybersecurity benefits a lot because the system can be taught to learn from the pattern in data and hence mark any deviation-an anomaly-which might pose a security risk. In academic circles, this will also cushion large networks and intricate databases from continuous manual monitoring, which is virtually impossible. Advanced technology tools do not come without their own challenges in the form of high purchase costs and skilled personnel to run and maintain such a suite of systems. This is the very reason an institution should consider weighing up the costs against the benefits and choose only those tools which best match its risk profile and resource availability.

Another consideration is the cloud-based solutions, which, on one hand, scale and make things flexible; on the other hand, special risks come in security. Each university should confirm that every cloud service provider follows the high standards of security and will use such cloud services together with strong internal controls. With proper management, technology would go a long way in reducing the risks of cybersecurity while meeting the objectives of the digital transformation of the academic institution.

4. Challenges Among Students in Cybersecurity

While the challenge is different at a university level largely because of the varied levels of awareness, inconsistent online behavior, and the wide use of personal devices on campus networks, even very highly digitally literate students retain limited knowledge of cybersecurity, perhaps limited to the use of antivirus software or the recognition of suspicious emails. Gaps in knowledge and experience are the reasons they are highly vulnerable to most common cyber threats, such as phishing, malware, and social engineering attacks (Khader et al., 2021). The most serious risks revolve around the undesired awareness of risk related to disclosure online. Students very often use social media and other kinds of digital platforms, whereby accident they disclose private information that may be used by the attackers. For example, sharing with social media information about academic schedules, birthdays, and even hobbies provide cybercriminals with just the kind of information they need to provide targeted phishing attempts. This habit of over-sharing online, coupled with a minimum knowledge of privacy settings, puts them at higher risks for identity theft and fraud.

The second problem is weak passwords that students use, along with poor password management practices. Most students use the same password for different platforms or keep it based on some general information, like birthdays or some easily guessed words, which could make access easier for an attacker. What is more, public Wi-Fi, which is widely used by students in libraries or cafes, makes them even more exposed. Students usually have no idea how unsafe it is to use unsecured networks, where they get into "man-in-the-middle" attacks by cybercriminals who steal critical information. The other important device security-related aspect that the student usually doesn't pay much attention to: With the rapid growth in accessing university networks with personal devices-laptops, tablets, or smartphones-the settings may be unsatisfactory in terms of their security. The device may not be updated with a software that has various security features installed or may never have been set up to conduct so-called recommended security practices in terms of updating software regularly. This could lead to wider university network vulnerabilities, because an unsecured personal device can be an entry point for cyber threats (Yang et al., 2020).

Last but not least, there is a general misconception among students of the implications of cyber incidents. Because most of the students think that they are not targeted, or huge organizations are basically those which have to worry about cyber threats, which may make them less careful. The latter may also allow a few more hazardous behaviors: downloading software from unknown sources, or even completely disregarding cybersecurity training programs at universities. These issues could be overcome only by tailored programs of sensitization which must include training in safe habits of working with digital content and personal responsibility regarding the security of the academic environment.

4. Conclusions

The increased use of digital technologies in higher education means that the need for cybersecurity awareness is increasingly growing. This paper underlines, for instance, that students are particularly vulnerable to a variety of cybersecurity threats resulting from their ignorance and unawareness of the risks involved. This may lead to such devastating consequences as data and identity breaches, which signifies the inclusion of strong cybersecurity training within the curriculum at educational institutions. The literature illustrates that comprehensive cybersecurity education, including practical workshops and real-world simulations, further combined with ongoing methodologies for risk assessments, significantly enhances the levels of students' competence in mitigating cyber threats. This proactive approach will protect institutional data, but it will also equally importantly prepare students with responsible digital behaviors that will protect personal information.

In this respect, consultation with cybersecurity experts and integration into the curriculum would not be merely important strategies for helping to instill the culture of cybersecurity awareness on campus but necessary ones. Therefore, each university is supposed to enhance the creation of awareness among students through proper training to empower them in battling emerging cyber threats. The inconsistent behaviour online, poor password management, and perceptions of not being targets will be approached through tailored sensitization programs and endorsement of safe digital practice. After all, cybersecurity awareness development is not a technical issue but a very important competence in the process of training students for responsible behavior within the framework of the increasingly connected digital world. By giving more emphasis to the education of cybersecurity, campuses will be able to provide students with the experience not only of recognizing risks but also being prepared with knowledge and skills for self-security and active contribution toward a secure academic environment.

Acknowledgments

The authors would like to thank all members of the School of Computing who participated in this study. This study was carried out as part of the System and Network Security Project. This work was supported by Universiti Utara Malaysia.

References

Aksu, M. U., Dilek, M. H., Tatlı, E. İ., Bicakci, K., Dirik, H. İ., Demirezen, M. U., & Aykır, T. (2017, October 1). *A quantitative CVSS-based cyber security risk assessment methodology for IT systems*. IEEE Xplore. https://doi.org/10.1109/CCST.2017.8167819

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*(56), 1–27. https://doi.org/10.1016/j.cose.2015.09.009

Hussain, A., Mohamed, A., & Razali, S. (2020). A Review on Cybersecurity. *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, *28*. https://doi.org/10.1145/3386723.3387847

Jalil, M., Ali, N. H., Yunus, F., Zaki, F. A. M., Hsiung, L. H., & Almaayah, M. A. (2024). Cybersecurity Awareness among Secondary School Students Post Covid-19 Pandemic. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *37*(1), 115–127. https://doi.org/10.37934/araset.37.1.115127

Katsumata, P., Hemenway, J., & Gavins, W. (2010). Cybersecurity risk management. *2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE*. https://doi.org/10.1109/milcom.2010.5680181

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity Awareness Framework for Academia. *Information*, *12*(10), 417. https://doi.org/10.3390/info12100417

Kozieł, G., Dziuba-Kozieł, M., & Łukasik, E. (2024). CYBERSECURITY AWARENESS AMONG YOUNG LEARNERS – A CASE STUDY. *INTED Proceedings*, *1*, 1508–1513. https://doi.org/10.21125/inted.2024.0439

Larionova, A. V., Olesya Yu. Gorchakova, & Fakhretdinova, A. P. (2023). Cybersecurity: Young People's Awareness and Risk Management. *Lecture Notes in Networks and Systems*, 649–657. https://doi.org/10.1007/978-3-031-23856-7_57

László Bognár, & László Bottyán. (2024). Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students. *Education Sciences*, *14*(6), 588–588. https://doi.org/10.3390/educsci14060588

Lemieux, F. (2018). Cyber Threats, Intelligence Operations, and Mass Surveillance. *Intelligence and State Surveillance in Modern Societies*, 139–163. https://doi.org/10.1108/978-1-78769-171-120181007

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Mukherjee, M., Ngoc Thuy Le, Chow, Y.-W., & Susilo, W. (2024). Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information*, *15*(2), 117–117. https://doi.org/10.3390/info15020117

Neha Chhabra Roy, & Sreeleakha P. (2024). Proactive cyber fraud response: a comprehensive framework from detection to mitigation in banks. *Digital Policy, Regulation and Governance*. https://doi.org/10.1108/dprg-02-2024-0029

Nwobodo, L. K., Nwaimo, C. S., Adegbola, A. E., Nwobodo, L. K., Nwaimo, C. S., & Adegbola, A. E. (2024). Enhancing cybersecurity protocols in the era of big data and advanced analytics. *GSC Advanced Research and Reviews*, *19*(3), 203–214. https://doi.org/10.30574/gscarr.2024.19.3.0211

Piia Perälä, & Lehto, M. (2024). Educating Cybersecurity Experts: Analysis of Cybersecurity Education in Finnish Universities. *Proceedings of the ... European Conference on Information Warfare and Security*, *23*(1), 371–378. https://doi.org/10.34190/eccws.23.1.2256

Sarathchandra, D., Haltinner, K., & Lichtenberg, N. (2016, April 1). *College Students' Cybersecurity Risk Perceptions, Awareness, and Practices*. IEEE Xplore. https://doi.org/10.1109/CYBERSEC.2016.018

Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the Five Hard Problems of Cybersecurity. *Risk Analysis*, *39*(10), 2119–2126. https://doi.org/10.1111/risa.13309

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*, *12*(2). https://doi.org/10.15394/jdfsl.2017.1476

Tissir, N., El Kafhali, S., & Aboutabit, N. (2020). Cybersecurity management in cloud computing: Semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments*, *7*, 69–84. https://doi.org/10.1007/s40860-020-00115-0

Yang, L., Lau, L., & Gan, H. (2020). Investors' perceptions of the cybersecurity risk management reporting framework. *International Journal of Accounting & Information Management*, *28*(1), 167–183. https://doi.org/10.1108/ijaim-02-2019-0022