



Cyber Security in Indonesian Higher Education Institutions: Lessons Learned from Recent Cyber Attacks

Jonathan Nahum Marpaung

Fakultas Ekonomi Bisnis, Universitas Indonesia, Indonesia

Email: jonathan.nahum@office.ui.ac.id

Abstract

Cyber security is paramount to the sustainability of higher education institutions as more institutions move their information system to the cloud and allow stakeholders to access their information technology services from on-campus WIFI and mobile devices. This study aims to understand Indonesian higher education's current cyber security landscape by analyzing recent cyber-attacks that hit all sectors, notably higher education. Recent news articles and government reports related to cyber-security were analyzed using document analysis. This study found that data theft attacks were the number one cyber threat that higher education institutions faced, followed by attacks on institutional websites, social media pages, and personal mobile devices. This study found that the nature of recent cyber-attacks was consistent with the assessment posed by previous literature that stakeholders' recent level of ability in cyber-security is not where it is supposed to be. The potential impact of future cyber-attacks on institutions and stakeholders is significant, underscoring the importance of this new understanding, which can help institutions prepare their stakeholders better to mitigate such threats.

Keywords: *Network security; Cyber-attacks; Higher education; Data assurance; Information security competency*

1. INTRODUCTION

Indonesia experienced more than eleven million cyber-attacks in the year 2022, and gigabytes of personal information was stolen, which was then distributed illegally online for others to exploit [1][2]. Indeed, cyber-attacks have steadily risen as organizations move their storage and computing to cloud systems that can only be accessed online. Higher education institutions have also followed the trend and moved their services and data to the cloud, hoping stakeholders could understand the possible cyber threats and how to secure their valuable assets properly [3]. The promise of having a more robust and secure system has to be reevaluated as hackers have adapted to the current condition and continued their attacks.

The continued cyber-attack is a wake-up call for information technology professionals to secure critical data and infrastructure in all areas, including higher education. One recent example of a cyber-attack in Indonesian higher education is the attack on the Diponegoro University system, which resulted in the data breach of more than 125,000 students [4]. It is imperative to assume that the trend will continue without good cyber security in place for all institutions, including higher education. Cyber-security itself is defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets [5].

Previous literature on cybersecurity in higher education institutions has focused on specific topics, such as student behavior with cybersecurity [6] and the effect of distance learning on cybersecurity [7]. There are also efforts to study broader areas of cybersecurity, such as institutional strategies for cybersecurity [8], aspects of cyber-security in higher education institutions [9], and emerging issues for cybersecurity in higher education institutions [10]. The aforementioned studies used a literature review to answer the research questions, similar to what this study used to answer the question: How is the Indonesian higher education's current cyber security landscape in regards to the types, frequencies, and mitigations of cyber-attacks? As the data analyzed are publicly accessible data ranging from 2020 to 2024, the study and findings are limited by the data used.

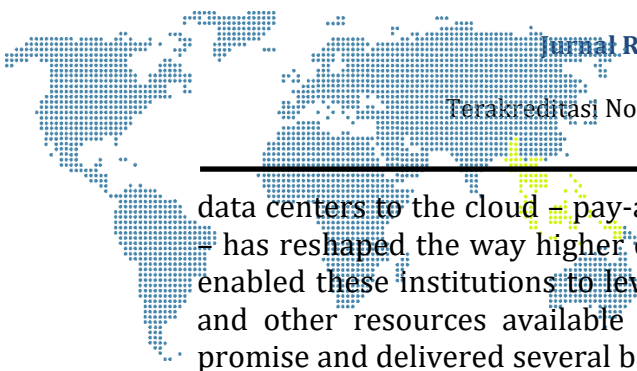
2. RESEARCH METHODOLOGY

Network technology has evolved from the original conception of the World Wide Web by connecting just two devices to the present day, where all devices can be connected to the World Wide Web through the Internet of Things (IoT) framework. The evolution of networking technology created a new ecosystem known as cyberspace, an interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers [11]. In the domain of cyberspace itself, cyber-security is present and needed to secure valuable assets, both software and hardware.

Cyber-security, as presented in the previous section, is a collection of several different things, such as tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies, to protect an organization against security risks in the cyber environment (International Telecommunication Union, 2008). From the description, Cybersecurity is not just one or two items working in tandem but a concoction of stakeholders, software, hardware, policy, and actions working harmoniously. Indeed, the components above are essential to create a robust cyber-security system that can mitigate critical threats that can threaten both the organization's and the organization's assets.

Several cyber-security threats that organizations should build their defense around are man-in-the-middle attacks – interference between two communication ends, brute-force attacks – repeated attempts to gain access until the correct key is acquired, distributed denial of service (DDoS) attacks – flooding a host server with attacks until service is not available, social engineering or phishing attacks – gain unauthorized access to critical information through human interaction, and malware attacks – malicious software used to gain access to confidential information [12]. While man-in-the-middle attacks may not pose as much threat as before because of the mass implementation of encryption, brute force attacks, DDoS, phishing, and malware still pose a significant threat to institutions.

Indeed, cyber threats persist in all different types of institutions. Higher education institutions are possible targets for cyber-attacks as more institutions adopt the practice of off-loading their services to the cloud. Moving services and



data centers to the cloud – pay-as-you-go service, computing, and storage services – has reshaped the way higher education institution do their core businesses and enabled these institutions to leverage processing, storage, database management, and other resources available on the cloud [13][14]. Moving to the cloud did promise and delivered several benefits such as mobility – the capacity to distribute materials and host classes online so that students can utilize their mobile devices, new services – allow institutions and lecturers to offer innovative teaching methods, storage – the ability to expand storage capabilities, and efficiency – deliver new ways to make their organizations more efficient [15]. Despite its benefits, cloud computing is not without its issues.

Several complications can occur when higher education institutions' services and data are moved to the cloud. Some of these concerns are security, privacy, vendor lock-in, network performance, reliability, trust and management, licensing and pricing, acceptance and adoption, and sustainability and post-adoption concerns [16]. Like any other information system, security is still one of the top issues to solve before a full-scale implementation. There has been much progress made in cloud computing security since it has gone mainstream, and vendors continue to develop and implement security improvements to safeguard better the data of their customers [17], [18], [19]. One interesting observation that [20] discussed regarding concerns regarding moving services to the cloud is that studies frequently focus on the usefulness of the technology and are inclined to exclude human aspects – such as adoption and diffusion. Indeed, a system made by humans and used primarily by humans cannot escape from the nature of humans, be it the good and bad aspects of being a human.

Cloud computing is just one part of a modern infrastructure that higher education institutions demand from the stakeholders. The increased usage of on-campus WIFI service, social media, and smartphones by users sanctioned by the institutions opens up new possible cyber-attacks. Possible cyber-attacks that institutions can experience are social media/website defacing, social media hostile takeover/account hijacking, smartphone trojan/spyware, embedded system malware, denial-of-service attacks, man-in-the-middle attack, phishing, and data breach [21], [22], [23], [24].

Following the trend and moving their services and data to the cloud, in addition to more vulnerability points, higher education hopes those involved can keep up with the changes, understand possible cyber threats, and secure their valuable assets properly (Al-Shqeerat et al., 2017). The reality, however, is that stakeholders' recent aptitude is not where it is supposed to be and can pose a severe threat if not addressed correctly [25], [26]. Indeed, the interaction between humans and technology, particularly in cyberspace, is not an easy task to develop and maintain, much less to be consistently secure all the time. There are several factors that institutions can implement or consider in reducing the amount of human error that can compromise an institution's integrity, such as planning for the worst, ambiguity, data security, training/education, policy, and security culture [27], [28]. The threats created by accidental insiders caused by ignorance, lack of



attention, or human error are rapidly becoming an increasing distress to security professionals, and there has been a lack of progress in remedying this matter [24].

This study utilized a document analysis approach to understand Indonesian higher education's current cyber security landscape, particularly concerning cyber threats that higher education institutions have to prepare for. Based on grounded theory, a document analysis study differs from a literature review study. While literature review is primarily used to do meta-analysis and find future direction for a topic or field, document analysis seeks to discover and understand phenomena in society by analyzing and synthesizing documents on a specific topic [29], [30], [31], [32]. Document analysis is also suitable for this exploratory study as the media analyzed are written, contrary to content analysis that can analyze information from different types of media [33], [34].

The study analyzed two types of documents: news articles and government reports/documentation. Selected news articles in the last five years on cyber-attacks on institutions in Indonesia, including higher education, were analyzed for this study. Selected government reports on cyber-attacks issued in the last five years were also analyzed for this study. In addition to the documents above, scholarly works on cybersecurity and seminal and recent articles were selected for this study to form a comprehensive lens for analyzing the selected news article and government report. Twenty news articles and nine government agency reports were analyzed to understand further the current cyber-security landscape in Indonesia's higher education.

Search engines such as Google.com and Bing.com were utilized to find the articles, in addition to news agency internal search engines. Keywords used to find articles on cyber-attacks on higher education institutions were: bobol, bocor, data, diretas, hacker, diserang, bajak, universitas, website, kampus, lemah, dijual, dan situs. Articles analyzed by this study are listed in Table 1. Similar to the method of finding the articles, search engines were also used to find relevant government agency reports. The three relevant agencies were Indonesia's National Computer Security Incident Response Team (CSIRT), Interpol, and ASEAN. Six relevant reports were retrieved from the National CSIRT of Indonesia, two cyber threat assessment reports from Interpol, and one cybersecurity strategy from ASEAN.

Table 1. Title, year of publication, and origin of news articles analyzed

Title	Year	Origin
4 Penyebab PDNS Bisa Diserang Hacker, Pakar UM Surabaya: Kurangnya Literasi Digital	2024	Detik
Data Mahasiswa Kalteng Tersebar di Situs Gelap	2024	Palangka Express
Data Mahasiswa UPI Diduga Bocor, Apa Langkah Pihak Kampus?	2022	Detik
Data Pribadi Bocor, Mahasiswa Muhammadiyah Ramai – Ramai Surati Presiden RI	2022	Muhammadiyah
Data Universitas Tanjungpura diduga bocor, 3 halaman exemple jadi bukti	2024	Topik
Fakta-fakta Pusat Data Nasional Diobok-obok Hacker Ransomware: 210 Instansi Terdampak	2024	Tempo
Gawat, Data 125.000 Mahasiswa Undip Bobol!	2021	Gatra



Title	Year	Origin
Hacker Bobol Data Alumni Universitas Brawijaya Malang	2022	Suara Malang
Hacker Sebar Data yang Disebut Milik Mahasiswa dan Alumni UB Angkatan 2020	2022	Detik
Medsos Pengurus BEM UI Diretas Usai Sebut Jokowi 'King of Lip Service'	2021	Detik
Pemuda Ini Bobol Website Untad, Hasil Kejahatan Mencapai Miliaran Rupiah	2021	Kumparan
Penjelasan Undip Usai Pengumuman Ujian Mandiriya Diserang Hacker	2024	Detik
Puluhan Juta Data Matahari.com dan Kampus Prasetya Mulya Diduga Bocor	2024	CNN Indonesia
Ribuan Data Milik Untan Diduga Bocor	2024	RRI
Sempat Pulih, WA Rektor UNS Jamal Wiwoho Dibajak Lagi!	2023	Detik
Situs FIB UGM Diretas, Hacker Tulis Pesan soal Jual Beli Konten Seks Mahasiswa	2022	Detik
Teguh Aprianto, Hacker yang Bongkar Lemahnya Situs Pemerintah	2021	CNN Indonesia
Universitas Brawijaya Akui Diserang Hacker, Kevalidan Data Masih Diselidiki	2022	Detik
Untan Pontianak Klaim 52.000 Data yang Diretas dan Dijual Bukan Data Sensitif	2024	Kompas
Website Universitas Muria Kudus Bobol, Data 12.000 Mahasiswa UMK Beredar di Situs Jual Data Bjorka	2022	Tribun Muria

Selected news articles and reports were analyzed by synthesizing topics and ideas related to cybersecurity. The attacks on higher education institutions were first categorized according to previous literature [20], [23], [24]. Then, these attacks were analyzed to find possible remedies according to seminal works in the field. Finally, these attacks were cross-referenced to the reports released by government agencies to find meaningful patterns

3. RESULTS AND DISCUSSION

The analysis of the news articles resulted in four major types of attacks. Data breach and theft are the most reported cyber-attacks by Indonesian news agencies, with 12 reported attacks. This is followed by website defacing (3 instance), social media attacks (1 instance), and smartphone (WhatsApp) attacks (1 instance). The finding is consistent with the reports released by agencies concerning the attacks targeting valuable data using malware or other trojan-like methods that have been prevalent in recent years [35], [36]. While attacks on websites, social media, and smartphone communication apps may not be as crucial as data theft attacks, institutions need to be aware of and mitigate them, as they can ruin an institutional reputation. In the case of the Faculty of Humanities at Gadjah Mada University, the hacker defaced their website and posted content that was sexual in nature [37].

This study found four significant server-based cyber-attacks in analyzing selected news articles relevant to this study's goal. The first cyber-attack occurred at Universitas Diponegoro, which resulted in more than 125,000 student data being breached and distributed online by the perpetrators. Universitas Diponegoro

student data was hosted on a server accessible from the World Wide Web. Experts from within and outside the university have not located where the breach originated and suspected that one or more administrator credentials have been compromised. The university faced criticism from outside experts for their lack of encryption efforts as sensitive data were saved in plain text, as shown by the leaked data.

The second cyber-attack occurred at Universitas Prasetya Mulya, which targeted all student academic data for 2021. The stolen data resides on a server and can be accessed from the World Wide Web. The university has not found where the data breach originated but suspected that one or more administrator's devices might have been compromised. The third cyber-attack occurred at Universitas Pendidikan Indonesia, where 14 gigabytes of data were breached. The university claimed that its system was not compromised and that the data came from the Kartu Indonesia Pintar Kuliah government program. Still, the server-based data that Universitas Pendidikan Indonesia maintains was compromised and used illegally by other perpetrators to apply for online loans and exploitative actions. There has not been any conclusive answer on how the data was breached. The university suspected the breach came from someone who has access to the government system, intentionally or unintentionally.

The final cyber-attach occurred at Universitas Brawijaya, where private and sensitive information from the alumni of the agricultural department was breached and distributed only by hackers. In this particular case, the data was stored on a server, and the university was able to determine that the perpetrators had been trying to get into the server by using a brute-force attack. The university determined the attack by looking at the access logs and reports. The four cyber-attacks above are summarized by diagram 1 below. All analyzed cyber-attacks involved server-based systems where data is stored on a server accessible through the World Wide Web. Three of the cyber-attacks stole student data, while one breached alumni data. In terms of the means of attacks, three were due to human error caused by compromised credentials or devices, and one was due to an insecure system that enabled the perpetrators to use brute force attacks.

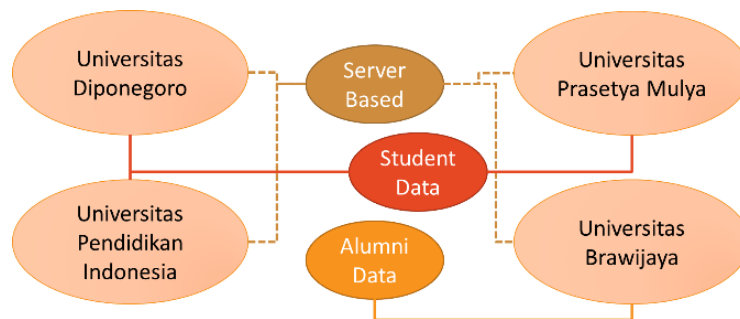


Figure 1. Analyzed cyber-attacks that compromised institutional data

Government reports and documentation provided valuable information on the number of cyber-attacks and the types of attacks in Indonesia. The Indonesian

Cyber and Sign Agency (BSSN) gathered its data by providing critical stakeholders with systems that can monitor and record different types of attacks. On the other hand, the INTERPOL reports gathered the data through INTERPOL's member countries and private partners, and the ASEAN desk conducted research. Analysis and synthesis of the documents above enabled this study to discover the latest trend in cyber-attacks that happened in Indonesia.

The data gathered by BSSN suggested that the number of cyber-attacks is consistent from 2020 to 2022, which hovers around three hundred million attacks. Curiously, the source of the most attacks has changed throughout the years, with India taking the number one spot in 2020 and Indonesia in 2022. Of all the different cyber-attacks, malware attacks are consistently the most used method by hackers. The top two malware used between 2020 and 2022 are Win32/Small and Win32/ZombieBoy.A!.bit, with Win32/Ymacco.AA6F is taking third place in 2022. From 2020 to 2022, hackers mostly targeted port 445, which is used by the samba (SMB) service to host and serve files, with port 22, which is used for secure shell (SSH), and port 80, used for Hypertext Transfer Protocol (HTTP) as the second and third most attacked port.

INTERPOL [31] suggested that social engineering/phishing is still prevalent in ASEAN countries, and Indonesia has been the leading target, particularly for small and medium businesses (SMBs). Indeed, the number of phishing sites has increased over the years, and many have adopted a secure socket layer (SSL) in order to look and feel like real websites/web services. Software as a service (Saas) and webmail are still the most targeted system by phishing, followed by financial institutions, payment system, social media, and E-commerce/retail business. INTERPOL [36] speculated that the availability of phishing software for purchase has enabled even amateurs to do this kind of cyber-attack and thus increased the number of attacks.

In addition to phishing, malware is a leading method of breaching the system and extracting valuable data. In their latest report, Indonesia led the number of ransomware attacks amongst other countries in ASEAN with 1,308,371 attacks in 2020. Industries affected the most by ransomware are manufacturing, retail, government agencies, healthcare, and construction. Being a victim of ransomware is not cheap, as the average ransomware payouts have increased from USD 10,000 in 2018 to USD 178,000 in 2020, according to the INTERPOL report. Indeed, the amount of ransom paid is attributed to the two tactics used to distribute ransomware. The first is the spray-and-pray tactic, which sends malware through spam mail or fake malicious advertisements with the hope that some unfortunate users will take the bait. The second tactic, the targeted tactic, is when the hackers scout potential targets before actively finding a way to infiltrate and map the victim's network. The latter tactic requires more effort and yields more ransom amounts.

Recent successful cyber-attacks that targeted organizations in Indonesia, notably higher education institutions, are more likely caused by human aspects rather than security holes in the operating system, web services, and devices connected to the World Wide Web. This is consistent with previous literature that

suggested stakeholders' recent level of aptitude towards safe cloud computing, particularly in cyber-security, is not up to par and can cause a severe threat to their organization and personal information if not addressed correctly by them and security professionals [21]; [26], [27]. This study wants to highlight ransomware and phishing attacks as they continue to rise in higher education institutions and exploit the low level of aptitude amongst the stakeholders.

Ransomware used to be a cyber-attack that targets individuals marked as highly valuable target. The paradigm has changed as hackers have viewed any individuals as an entry point to higher value targets, such as banks, hospitals, and higher education institutions [36]. As illustrated in diagram 2, devices can be infected with malware and used by hackers to identify high-value targets and entry points. Once they have determined their target and potential entry point, they can penetrate the system, most likely not hosted on a cloud computing platform, and retrieve valuable assets, be it a program or personal data. This ransomware scheme might explain what happened to Universitas Diponegoro, Universitas Prasetya Mulya, and Universitas Pendidikan Indonesia.

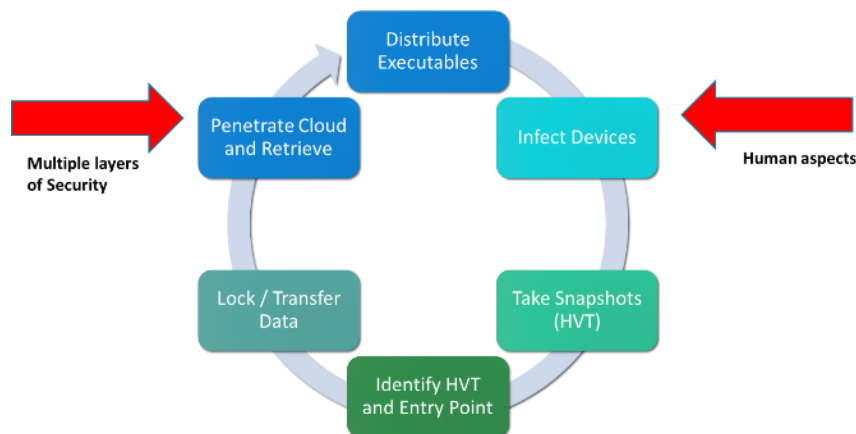


Figure 2. Process flow of the new ransomware scheme

While vendors have made tremendous efforts to secure the security of their cloud computing platforms, the human aspect is still in play when users of these secure platforms can still be compromised – both their credentials and devices [18], [19]. Carlin and Curran [17] suggest that vendors fully educate their customers on different cloud computing platforms and how human aspects can affect the security and integrity of the customer’s services and data. The study, as mentioned earlier, even suggests that customers acquire third-party auditors to help ensure the safety of their system.

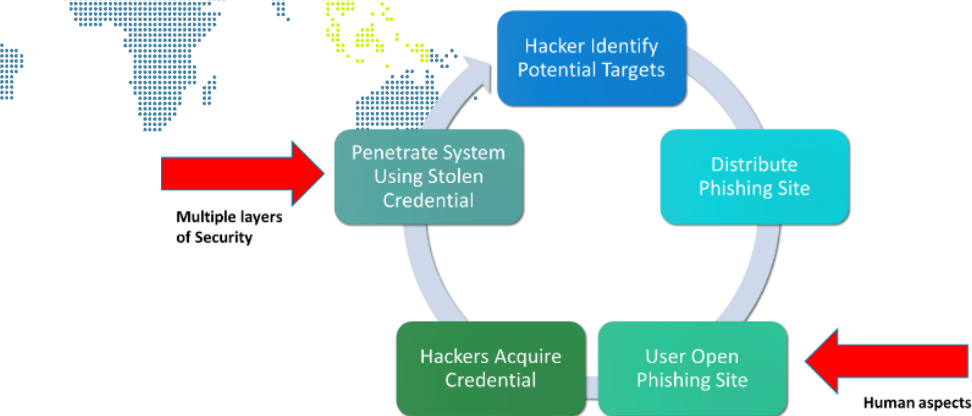


Figure 3. Process flow of the new phishing scheme

Phishing attacks are not new but still prevalent in today's cyber-security world. Much like ransomware, phishing attacks have evolved to attack not just individual assets but also higher-value targets. The human aspects come into play when users who are ignorant or not adept in spotting phishing engage with the phishing site and give up their legitimate credentials, as shown in diagram 3. Again, while vendors have fortified their cloud computing platform with multiple layers of security, all of that becomes a moot point as hackers can gain access with a legitimate credential. This new scheme of phishing attacks might be able to answer what happened to Universitas Brawijaya.

The rising trend of cyber-attacks in Indonesia, particularly attacks that exploit human ignorance and errors, will put more pressure on Indonesian higher education institutions to increase the level of security knowledge and awareness of the stakeholders. Data has shown that the trend will continue and higher education institutions are more vulnerable compared to other industries [36]. While the situation looks like a hopeless case, there are measures that institutions can take to remedy this situation or at least prevent it from spiraling out of control.

Indonesia's higher education institutions cannot afford not to increase their level of aptitude because the consequences will be very damaging for the institutions and the country. Fortunately, there are steps that institutions can take to help themselves in preventing cyber-attacks caused by human factors. Measures that institutions can perform to increase the level of aptitude regarding cyber-security among their stakeholders are creating a secure culture, ensuring continuous training, creating a better cyber-security policy, and planning for the worst [25], [27], [28]. For the immediate future, vendors, such as Microsoft, suggest institutions adopt these minimum standards for greater resiliency to the rising level of threats in the digital ecosystem: enable multifactor authentication, apply zero trust principles by not trusting anything that comes from outside of the organization, use modern anti-malware software, keep systems up to date, and protect data by following best practices in data assurance [22].

4. CONCLUSION

This study aims to understand the current cyber-security landscape in Indonesia's higher education system and the types, frequencies, and mitigations of cyber-attacks. Through analysis of documents related to cyber-attacks published by news and government agencies, this study finds that Indonesian higher education institutions have been hit by attacks that exploit weaknesses in the system that can be caused by low-level knowledge and ignorance of safe practices in the cloud computing era. While the findings suggest most of the attacks targeted valuable data, hackers exploited other attacks to deface institutional websites, social media pages, and critical stakeholder mobile devices. This study finds that the nature of recent cyber-attacks is consistent with the assessment posed by previous literature that stakeholders' recent level of ability in cyber-security is not where it is supposed to be. The rising trend of these attacks is concerning, and institutions should prepare their stakeholders better to protect their assets.

Previous literature suggests that there needs to be more effort to study the human aspects of cyber-security, as most studies concentrate on the technical side of things, such as technology and policies that can ensure better cybersecurity. This study hopes to contribute to the area that previous literature criticizes and help launch the effort to analyze the interplay between cyber security and human factors. The author hopes to continue this effort by investigating the current level of aptitude of the stakeholders in Indonesian higher education institutions and bring humanity to the forefront of the security issue. The nature of the data limited the scope of the research to attacks exposed by the news agencies in the last five years. A more comprehensive investigation and data can shape a more holistic view of the cyber-security landscape in Indonesian higher education. This new understanding can inform institutions on how to protect their valuable data and their reputation as premier higher education institutions.

REFERENCES

- [1] D. Ghifari, "I think Indonesia's cybersecurity is run by 14-year olds': Hackers," *Asian News*, 2022. Accessed: Jan. 07, 2025. [Online]. Available: <https://asianews.network/i-think-indonesias-cybersecurity-is-run-by-14-year-olds-hackers/>
- [2] CNN Indonesia, "Data Pedulilindungi Tak Dienkripsi? Pakar Sindir Beda UCAP Dan Fakta," *CNN*, 2022. Accessed: Jan. 07, 2025. [Online]. Available: <https://www.cnnindonesia.com/teknologi/20221116133010-192-874507/data-pedulilindungi-tak-dienkripsi-pakar-sindir-beda-ucap-dan-fakta>
- [3] K. H., F. M., M. R., and H. Fajraoui, "Cloud Computing Security Challenges in Higher Educational Institutions - A Survey," *Int. J. Comput. Appl.*, vol. 161, no. 6, pp. 22-29, Mar. 2017, doi: 10.5120/ijca2017913217.
- [4] Insetyonoto, "Gawat, data 125.000 Mahasiswa Undip Bobol!," *Gatra*, 2021. Accessed: Jan. 07, 2025. [Online]. Available: <https://www.gatra.com/news-500217-hukum-gawat-data-125000-mahasiswa-undip-bobol.html>
- [5] International Telecommunication Union, "International Telecommunication Union, ITU-T Rec. X.1205, Overview of cybersecurity," 2008. Accessed: Jan. 07, 2025. [Online]. Available: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items

- [6] L. Muniandy, B. Muniandy, and Z. Samsudin, "Cyber Security Behaviour among Higher Education Students in Malaysia," *J. Inf. Assur. Cybersecurity*, pp. 1–13, Feb. 2017. doi: 10.5171/2017.800299.
- [7] A. Arina and A. Anatolie, "Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning," *Int. J. Sci. Technol. Res.*, vol. 10, no. 3, pp. 128–133, Mar. 2021.
- [8] E. C. K. Cheng and T. Wang, "Institutional Strategies for Cybersecurity in Higher Education Institutions," *Information*, vol. 13, no. 4, p. 192, Apr. 2022, doi: 10.3390/info13040192.
- [9] A.-C. Cojocariu, I. Verzea, and R. Chaib, "Aspects of Cyber-Security in Higher Education Institutions," 2020, pp. 3–11. doi: 10.1007/978-3-030-44711-3_1.
- [10] M. J. Maranga and M. Nelson, "Emerging Issues in Cyber Security for Institutions of Higher Education," *Int. J. Comput. Sci. Netw.*, vol. 8, no. 4, pp. 371–379, Aug. 2019.
- [11] JOINT CHIEFS OF STAFF WASHINGTON DC, "Department of Defense Dictionary Of Military and Associated Terms," Dec. 2010. doi: 10.21236/ADA536504.
- [12] A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," *Procedia Econ. Financ.*, vol. 28, pp. 24–31, 2015, doi: 10.1016/S2212-5671(15)01077-1.
- [13] A. Alharthi, F. Yahya, R. J. Walters, and G. B. Wills, "An Overview of Cloud Services Adoption Challenges in Higher Education Institutions," in *Proceedings of the 2nd International Workshop on Emerging Software as a Service and Analytics*, SCITEPRESS - Science and and Technology Publications, 2015, pp. 102–109. doi: 10.5220/0005529701020109.
- [14] N. Sultan, "Cloud computing for education: A new dawn?," *Int. J. Inf. Manage.*, vol. 30, no. 2, pp. 109–116, Apr. 2010, doi: 10.1016/j.ijinfomgt.2009.09.004.
- [15] V. H. Pardeshi, "Cloud Computing for Higher Education Institutes: Architecture, Strategy and Recommendations for Effective Adaptation," *Procedia Econ. Financ.*, vol. 11, pp. 589–599, 2014, doi: 10.1016/S2212-5671(14)00224-X.
- [16] Y. A. M. Qasem, R. Abdullah, Y. Y. Jusoh, R. Atan, and S. Asadi, "Cloud Computing Adoption in Higher Education Institutions: A Systematic Review," *IEEE Access*, vol. 7, pp. 63722–63744, 2019, doi: 10.1109/ACCESS.2019.2916234.
- [17] S. Carlin and K. Curran, "Cloud Computing Security," in *Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments*, IGI Global, pp. 12–17. doi: 10.4018/978-1-4666-2041-4.ch002.
- [18] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," *IEEE Access*, vol. 9, pp. 57792–57807, 2021, doi: 10.1109/ACCESS.2021.3073203.
- [19] M. Almorsy, J. Grundy, and I. Müller, "An Analysis of the Cloud Computing Security Problem," Sep. 2016.
- [20] R. Al Nafea and M. Amin Almaiah, "Cyber Security Threats in Cloud: Literature Review," in *2021 International Conference on Information Technology (ICIT)*, IEEE, Jul. 2021, pp. 779–786. doi: 10.1109/ICIT52682.2021.9491638.
- [21] A. Garba, Maheyzah Binti Sirat, Siti Hajar, and Ibrahim Bukar Dauda, "Cyber Security Awareness Among University Students: A Case Study," *Sci. Proc. Ser.*, vol. 2, no. 1, pp. 82–86, Apr. 2020, doi: 10.31580/sps.v2i1.1320.
- [22] Microsoft, "Microsoft Digital Defense Report 2022," 2022. Accessed: Jan. 07, 2025. [Online]. Available: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us>

- [23] X. Liu *et al.*, "Cyber security threats: A never-ending challenge for e-commerce," *Front. Psychol.*, vol. 13, Oct. 2022, doi: 10.3389/fpsyg.2022.927398.
- [24] J. Jang, J. Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973-993, Aug. 2014, doi: 10.1016/j.jcss.2014.02.005.
- [25] J. Jeong, J. Mihelcic, G. Oliver, and C. Rudolph, "Towards an Improved Understanding of Human Factors in Cybersecurity," in *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, IEEE, Dec. 2019, pp. 338-345. doi: 10.1109/CIC48465.2019.00047.
- [26] F. Khalid, M. Daud, M. Rahman, and M. Nasir, "An investigation of university students' awareness on cyber security," *Int. J. Eng. Technol.*, vol. 7, no. 421, pp. 11-14, 2014.
- [27] L. Hadlington, "The 'Human Factor' in Cybersecurity," in *Research Anthology on Artificial Intelligence Applications in Security*, IGI Global, 2020, pp. 1960-1977. doi: 10.4018/978-1-7998-7705-9.ch087.
- [28] M. Richardson, P. Lemoine, W. Stephens, and R. Weller, "Planning for Cyber Security in Schools: The Human Factor," *Educ. Plan.*, vol. 27, no. 2, pp. 23-39, 2020.
- [29] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *J. Bus. Res.*, vol. 104, pp. 333-339, Nov. 2019, doi: 10.1016/j.jbusres.2019.07.039.
- [30] S. Shaw, J. Elston, and S. Abbott, "Comparative analysis of health policy implementation," *Policy Stud.*, vol. 25, no. 4, pp. 259-266, Dec. 2004, doi: 10.1080/0144287042000288451.
- [31] W. Goddard and S. Melville, *Research Methodology: An Introduction*. Juta and Company, 2004.
- [32] G. A. Bowen, "Document Analysis as a Qualitative Research Method," *Qual. Res. J.*, vol. 9, no. 2, pp. 27-40, Aug. 2009, doi: 10.3316/QRJ0902027.
- [33] M. Bengtsson, "How to plan and perform a qualitative study using content analysis," *NursingPlus Open*, vol. 2, pp. 8-14, 2016, doi: 10.1016/j.npls.2016.01.001.
- [34] R. Whitemore and K. Knafl, "The integrative review: updated methodology," *J. Adv. Nurs.*, vol. 52, no. 5, pp. 546-553, Dec. 2005, doi: 10.1111/j.1365-2648.2005.03621.x.
- [35] National CSIRT of Indonesia, "Lanskap Keamanan Siber Indonesia 2023," 2023. Accessed: Jan. 07, 2025. [Online]. Available: <https://csirt.kemenkeu.go.id/in/post/lanskap-keamanan-siber-indonesia-2023>
- [36] Interpol, "ASEAN cyberthreat assessment 2020," 2020. Accessed: Jan. 07, 2025. [Online]. Available: https://asean.org/wp-content/uploads/2021/01/ASEAN_CyberThreatAssessment_2020.pdf
- [37] DetikJateng, "Situs fib UGM diretas, hacker Tulis Pesan soal jual beli konten seks mahasiswa," *DetikJateng*, 2022. Accessed: Jan. 07, 2025. [Online]. Available: <https://www.detik.com/jateng/jogja/d-6365071/situs-fib-ugm-diretas-hacker-tulis-pesan-soal-jual-beli-konten-seks-mahasiswa>