ICIC Express Letters
Volume **17**, Number **10**, October **2023**

ICIC International ©2023 ISSN 1881-803X
pp. 1151–1158

ASSESSING CYBERSECURITY READINESS AMONG HIGHER EDUCATION INSTITUTIONS IN INDONESIA USING MANAGEMENT PERSPECTIVES

Nashrul Hakiem[1,*], Sarika Afrizal[2], Imam Marzuki Shofi[1]
Luh Kesuma Wardhani[1], Nenny Anggraini[1], Sonny Zulhuda[3]
and Yudi Setiadi[4]

[1]Department of Informatics
Faculty of Science and Technology
[4]Internal Audit Unit
Universitas Islam Negeri Syarif Hidayatullah Jakarta
Jl. Ir. H. Juanda No. 95, Jakarta 15412, Indonesia
{ imam; luhkesuma; nenny.anggraini; yudi.setiadi }@uinjkt.ac.id
*Corresponding author: hakiem@uinjkt.ac.id

[2]Department of Information Systems
Faculty of Computer Science
Universitas Pembangunan Nasional Veteran Jakarta
Jalan RS. Fatmawati, Jakarta 12450, Indonesia
sarika.afrizal@upnvj.ac.id

[3]Department of Civil Law, Ahmad Ibrahim Kulliyyah of Laws
International Islamic University Malaysia
Jln Gombak, P.O. Box 10, Kuala Lumpur 50728, Malaysia
sonny@iium.edu.my

Received October 2022; accepted January 2023

Abstract. *The COVID-19 pandemic is a disruptive era for the academic emerging technologies as a result of implementation of e-learning through an integrated higher education information system. Currently, the scientific literature to address the cybersecurity readiness level of higher education from the sociotechnical aspect is still little known. For this reason, the objective of this research is to determine the level of cybersecurity readiness of higher education institutions in Indonesia based on the user and management perspective and factors associated with cybersecurity readiness. An online survey was conducted amongst respondents who both manage and use information systems. Three aspects of the assessment were carried out based on the Sociotechnical System-Cybersecurity Framework (STS-CF) which assessed the infrastructure (hardware and software) readiness and organizational support. The survey results emphasized that social and technical readiness is significantly found related to cybersecurity readiness in higher education. In conclusion, most higher education institutions are ready to implement cybersecurity; however, several factors are needed to improve such as access to the infrastructure, cybersecurity policies, and standardized procedures for data security.*

Keywords: Cybersecurity framework, Cybersecurity readiness, Islamic higher education, Sociotechnical system, Management perspective

1. Introduction.

Nowadays, the Indonesian Ministry of Education urges the use of digitalized learning techniques. Integrated learning systems in higher education are making more use of digital technology and slowly replacing the face-to-face or traditional learning processes. Electronic learning systems such as the use of social media for education, online classes, online quizzes, etc. have increased Internet access in the institution [1]. Digital

DOI: 10.24507/icicel.17.10.1151

learning may also increase accessibility to academic materials, availability of institution data, and promote the integration of the academic process into a system [2].

Access to the academic system through the Internet has increased data exchange amongst the institutions which may create harm to information security [3,4]. The misuse of devices such as computers, handphones, or tablets causes damage or corrupts the system in order to take advantage of personal data. Based on Indonesian regulations, the protection of user data is one of the most important factors that must be provided by the system operator. This regulation also strengthens the requirement that the electronic system must meet the security aspects through the information security of the internal network system [5].

Previous research concluded that the rapid development of Information and Communication Technology (ICT) in an organization will increase information security vulnerabilities from cyber threats [6]. Based on data from the Indonesian Security Incident Response Team on Internet Infrastructure (Id-SIRTII) by end of 2021, there were 573 hacking cases dominated by the academic sector as targets. It is also known that the highest cyber threat activities occurred on 25 November 2021, which resulted in 75 cases [7]. Based on previous studies, the posture of digital learning systems such as establishing security policies across the enterprise is important to achieve an optimal readiness to fight against threats posed by the attacker as well as the insider [8]. Another study also mentioned that user awareness of the cybersecurity process is needed since they often fail to recognize and have less knowledge to protect their computing devices [9].

Previous research concluded that the readiness for cybersecurity implementation has various influencing factors such as from the individual aspect such as human resources [10], the technical aspect such as the use of new technology [11], and the social aspect such as intersectoral coordination [12]. The sociotechnical characteristics suggest the need for engagement of social and technical aspects of the individual and the organization as a whole [13]. However, research regarding cybersecurity readiness using the socio-technical framework in higher education institutions is a complex issue due to the disseminated function of IT management in the institutions and numerous departments involved. Hence, user readiness to utilize cybersecurity measures using the STF framework is still less known.

A comprehensive evaluation of the factors associated with cybersecurity readiness in higher education institutions is needed to address the relative insufficiency of research in this area. Thus, this study is aimed at evaluating cybersecurity readiness in higher education based on the user perspective using a sociotechnical framework and to measure the association of related factors to cybersecurity readiness. The results of this study will have implications for increasing knowledge of cybersecurity and to facilitate the implementation of electronic system security strategic plans in higher education institutions.

The paper is organized as follows. The methodology is given in Section 2 including research participants, research instruments and data analysis. The result and discussions are detailed in Section 3. Conclusions are given in Section 4.

2. **Methodology.** A purposive sampling technique was applied using an online survey among lecturers, administration staff, and IT coordinators from Islamic higher-education institutions in Indonesia. The questionnaire was developed to measure the level of readiness of higher education institutions related to cybersecurity implementation which was divided into 3 aspects: software availability, hardware readiness, and organizational support. The research was conducted between May to August 2021.

2.1. **Research participants.** The population of the study was chosen through convenience sampling from the relevant department which consists of the Head of the IT Division, lecturers, and administration staff. There are 52 colleges known as Islamic higher-education institutions in Indonesia which are classified into three institutions based on their capacity, namely UIN, IAIN, and STAIN. First institution, STAIN or *Sekolah Tinggi Agama Islam Negeri*, is an Islamic academic institution that conducts a single academic programme. The second institution, IAIN *or Institut Agama Islam Negeri*, has several academic programmes for Islamic studies. The third institution, UIN or *Universitas Islam Negeri*, runs academic programmes in several disciplines including Islamic studies and general studies.

2.2. **Research instruments.** To deliver a theoretical framework, a research instrument was developed using several questions aimed to evaluate the level of readiness for cybersecurity implementation. To develop the questions, we collected questions from previous studies and classified them into three aspects: hardware readiness, software availability, and organizational support. After deleting redundant questions and modifying based on validity measurement, the questionnaire was delivered to the respondents.

The study used a Likert-type scale (e.g., 1. Strongly disagree to 5. Strongly agree) and was divided into four sections, namely Section A as the demographic data, Section B for the hardware readiness, Section C for the software availability, and Section D for the organizational support. The survey instrument was developed using the Sociotechnical System-Cybersecurity Framework (STS-CF).

The analysis suggested that the questionnaire items remaining constituted an acceptable version of the readiness aspects. The estimates of reliability were generally acceptable. Specifically, coefficient alphas were 0.87 for hardware readiness, 0.87 for software readiness and 0.88 for organizational support.

2.3. **Data analysis.** Descriptive statistics using STATA 15th version were used to analyze the collected data whereas the regression analysis was conducted to determine factors affecting cybersecurity readiness. The USA National Institute of Standards and Technology (NIST) maturity of readiness was used in determining the expected level of cybersecurity readiness.

Overall, the sample included 72 subjects who participated in the survey and were working in different types of institutions. The following table provides the characteristics of the respondents where 36 respondents were IT coordinators, 20 respondents were lecturers and 16 respondents were administrative staff.

Table 1. Characteristics of respondents

Position at the institution	**Number of respondents (N)**	**Type of institution**		
		UIN	**IAIN**	**STAIN**
IT Coordinator	36 (50%)	14	20	2
Lecturer	20 (27.8%)	8	12	–
Administrative staff	16 (22.2%)	7	7	2
Total	72 (100%)	29	39	4

3. **Result and Discussions.** The results of this study review the main findings by comparing them with the results of previous studies and explanations of previous theories that are appropriate or support the results of this study.

3.1. **Readiness level.** The result showed that more than half of the respondents agreed that the cybersecurity readiness in their institution was at the level of proactive (38.89%) and progressive (38.89%), while only 12.50% of respondents were classified in the reactive level of readiness and 9.72% in the passive level (see Table 2).

Table 2. Cybersecurity readiness level

Readiness level	Freq.	Percent	Cum.
Passive	7	9.72	9.72
Reactive	9	12.50	22.22
Proactive	28	38.89	61.11
Progressive	28	38.89	100.00
Total	72	100.00	

3.2. **Findings of hardware readiness.** The hardware readiness variable was developed with respect to clarifying the implementation of asset inventory and access to the hardware. Linear regression analysis was performed to measure the relationship of hardware support to cybersecurity readiness and determine factors associated with cybersecurity readiness. The results showed that several aspects which build hardware readiness such as secure access (0.000), safety procedure ($p = 0.007$), licensed hardware ($p = 0.029$), IT design (0.037), and periodic assessment (0.001) were related to cybersecurity readiness.

Table 3. Linear regression result for hardware readiness

Cybersecurity readiness	Coef.	Std. Err.	t	$P > \|t\|$	[95% Conf.	Interval]
Secure access	.4383326	.0836167	5.24	0.000	.2711307	.6055346
Safety procedure	−.2115158	.075382	−2.81	0.007	−.3622513	−.0607802
Well-maintained assets	.1111371	.060098	1.85	0.069	−.0090363	.2313105
Licensed ICT	−.1181725	.0527532	−2.24	0.029	−.2236591	−.0126859
Infrastructure capability	−.0016467	.0518567	−0.03	0.975	−.1053407	.1020472
ICT design	.1593221	.0745566	2.14	0.037	.010237	.3084072
Asset inventory	.0428524	.1006783	0.43	0.672	−.1584664	.2441711
Update maintenance	.0182648	.0838658	0.22	0.828	−.1494353	.1859649
Security framework	.033695	.0786677	0.43	0.670	−.1236108	.1910008
Periodic assessment	.345979	.0988344	3.50	0.001	.1483474	.5436106
_cons	.4365812	.3628093	1.20	0.233	−.2889008	1.162063

3.3. **Findings of software readiness.** The emphasis on secure software development has steadily increased throughout the software development life cycle. Building secure software requires security awareness during the requirements engineering stage of software development. One of the major challenges confronting the software industry is that many organizations embark on secure software development initiatives without knowing whether they are fully prepared to do so. The findings indicated that several factors contribute to software readiness, such as software license ($p = 0.000$), web firewall ($p = 0.000$), and software policy ($p = 0.009$).

3.4. **Findings of organizational support.** Organizations that are prepared to face cyber-attacks and secure organizational resources are those that can effectively manage organizational values, beliefs, and behaviours related to improving organizational cybersecurity. Organizations can improve organizational culture by providing support for activities and collaboration across groups, as well as encouraging team members to contribute to cybersecurity. The findings show that several factors contribute to organizational support, including security policy (0.014), regular monitoring ($p = 0.001$), and standardized security process (0.000).

TABLE 4. Linear regression result for software readiness

Cybersecurity readiness	Coef.	Std. Err.	t	$P > \|t\|$	[95% Conf.	Interval]
Security assessment	.0768571	.051536	1.49	0.141	−.0261955	.1799097
Software access	−.028421	.0569125	−0.50	0.619	−.1422246	.0853826
Network access	.0271866	.0417769	0.65	0.518	−.0563515	.1107247
Software license	.2092688	.0476633	4.39	0.000	.1139602	.3045774
Malware software	.0795034	.0598771	1.33	0.189	−.0402284	.1992352
Software update	.0743926	.0759708	0.98	0.331	−.0775204	.2263055
Network protection	−.0265097	.0544813	−0.49	0.628	−.1354518	.0824325
Web firewall	.2948262	.0389888	7.56	0.000	.2168632	.3727892
Software policy	.1546566	.0568789	2.72	0.009	.0409202	.2683931
Individual access	−.0096541	.0503652	−0.19	0.849	−.1103656	.0910574
_cons	.6161241	.2359329	2.61	0.011	.1443471	1.087901

TABLE 5. Linear regression result for organizational support

Cybersecurity readiness	Coef.	Std. Err.	t	$P > \|t\|$	[95% Conf.	Interval]
Security policy	.121237	.0476293	2.55	0.014	.0259309	.2165431
Assessment tool	.0002508	.0475998	0.01	0.996	−.0949961	.0954977
Adequate budget	−.0355234	.0500203	−0.71	0.480	−.1356138	.064567
Certified training	.0129363	.0517084	0.25	0.803	−.090532	.1164045
Regular monitoring	.2236695	.0633828	3.53	0.001	.0968408	.3504983
Standardized security process	.3685736	.0683994	5.39	0.000	.2317067	.5054405
Commitment	−.0155953	.0491341	−0.32	0.752	−.1139124	.0827218
Risk management	.0094603	.0510802	0.19	0.854	−.092751	.1116716
Cyber team response	.0681222	.0613628	1.11	0.271	−.0546644	.1909089
Control ability	−.0425656	.0595352	−0.71	0.477	−.1616953	.0765642
Awareness	.0778945	.0547668	1.42	0.160	−.0316936	.1874826
_cons	.9517772	.2221117	4.29	0.000	.5073328	1.396222

3.5. **Scatter plots.** A scatter plot as depicted in Figure 1 was generated for hardware readiness, software readiness, and organizational support to provide a visual examination of the positive linearity of cybersecurity readiness. The result implied that hardware readiness is associated with cybersecurity readiness concerning secure access, safety procedures, licensed hardware, IT design, and periodic assessment. While software readiness was linked to cybersecurity readiness in terms of the software license, web firewall, and software policy. Organizational support was linked to cybersecurity readiness in terms of security policy, regular monitoring, and standardized security processes.

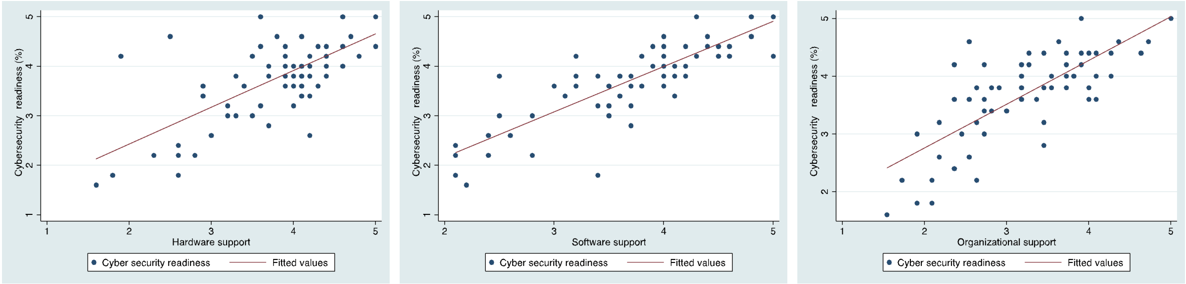

FIGURE 1. Scatter plot of hardware readiness, software readiness and organizational support

3.6. **Discussion.** The findings of this study show that a greater number of respondents have positive perceptions of cybersecurity implementation in Islamic higher institutions. The university members have the ability to effectively evaluate the security initiatives. Most of the respondents claim that the readiness level of the organization is at the proactive and progressive level where the organizational management would be responsible for establishing, managing, and reviewing the security state of data held by actively employing advanced security technology as a measure to reduce (or eliminate) the possibility of and to prevent hackers. The proactive level recognizes the importance of IT security and has basic protection to avoid ingress by hackers, despite the fact that they are still not using technology to reduce cyber threats. To classify the readiness level of an organization as supported by previous research which explains that the case organization has put some measures in place, but there is still a need to investigate their functionality within the organizational structure [11].

The current findings show that the cybersecurity readiness of the system is associated with socio-technical aspects. A good IT infrastructure can encourage organizations to become more prepared for cyber-attacks [14]. In this study, hardware readiness as one of the technical aspects is associated with cybersecurity readiness with respect to secure access, safety procedure, licensed hardware, IT design, and periodic assessment. Secure access to the hardware such as memory, RAM using code and protection schemes, and other verification mechanisms can be used to ensure the integrity of memory access [15]. Furthermore, a previous study also found that periodic measurement of ICT security in terms of infrastructure as well as risk management can help organizations achieve a cybersecurity level of readiness [11]. The use of hardware equipment in the process of managing information systems strongly supports the implementation of cybersecurity which aims to protect software from attacks, disruptions, or other threats [16].

Another technical aspect of cybersecurity is software readiness. Security issues are highly dependent on technology that determines security weaknesses and vulnerabilities driven by the availability of software and network systems [13]. The current result shows that software readiness is linked to cybersecurity readiness in terms of the software license, web firewall, and software policy. According to a previous study, technical security controls including software security have a positive effect on cybersecurity readiness. The majority of respondents agreed that software controls have contributed significantly to a reduction in cybersecurity incidents. As a result, this study concluded that technical aspects are important factors that influence cybersecurity readiness.

The other aspect of cybersecurity readiness is the social aspect which is categorized as organizational readiness. Based on the current result, organizational support is linked to cybersecurity readiness with respect to security policy, regular monitoring, and a standardized security process. A previous study concluded that organizations that can effectively manage organizational values, beliefs, and behaviours related to improving organizational cybersecurity are better prepared to face cyber-attacks and have secure organizational resources [17]. Organizations can improve cybersecurity awareness by promoting activities and cross-group collaboration, as well as encouraging team members to contribute to cybersecurity implementation [18].

Based on the current result, the majority of respondents agree that many activities are being carried out at present to maintain data security within the institutions. Several aspects that might drive the implementation of cybersecurity in higher education institutions such as the availability of cybersecurity policy, standardized security procedures, and control with respect to periodic monitoring and access. A previous study suggested that if more emphasis is placed on improving cybersecurity values and beliefs within organizations, they would be more prepared to secure the cyberinfrastructure and services to avoid cyber-attacks [18]. Furthermore, endorsing activity coordination and collaboration across different groups to improve cybersecurity and solve security issues can help to improve organizational culture [10]. Thus, using the socio-technical framework of the cybersecurity, a socio-technical model could assist leaders of higher education institutions in understanding the structure and characteristics of the existing infrastructure to improve cybersecurity implementation in an organization.

3.7. **Research implication.** The cybersecurity readiness framework that is based on the socio-technical theory is used to measure expectations of cybersecurity implementation from the academic perspective. The contribution of the current research is that it provides empirical data concerning the socio and technical aspects of readiness in Islamic higher education institutions. This information is important to elaborate on factors related to readiness to initiate actions and tools for future cybersecurity directions.

4. **Conclusion.** In general, from the technical aspect, in terms of hardware readiness and software availability, most Islamic higher education institutions are ready to implement cybersecurity. However, in terms of organizational support, several factors need to improve such as access to the infrastructure, cybersecurity policies, the availability of standard operating procedures for data security, as well as training to increase cybersecurity knowledge. The limitation of this study is the possibility of bias in the research because it is based on user perceptions. Therefore, some hardware and software security tools may be used to test the systems, as well as gaining confirmation from the experts using in-depth interviews that may be performed to explore further information obtained from the instrument. Since the study explores only Islamic higher education institutions in Indonesia, further advice is required to test the instrument on other higher education institutions and other organizations such as health organizations and government institutions.

REFERENCES

[1] M. M. N. H. Ja'ashan, The challenges and prospects of using e-learning among EFL students in Bisha University, *Arab World English J.*, vol.11, no.1, pp.124-137, DOI: 10.24093/awej/vol11no1.11, 2020.

[2] D. Rahardjo, Sumardjo, D. P. Lubis and S. Harijati, Internet access and usage in improving students' self-directed learning in Indonesia open university, *Turkish Online J. Distance Educ.*, vol.17, no.2, pp.30-41, DOI: 10.17718/tojde.90196, 2016.

[3] F. Z. Benjelloun and A. A. Lahcen, Big data security: Challenges, recommendations and solutions, *Handb. Res. Secur. Considerations Cloud Comput.*, pp.301-313, DOI: 10.4018/978-1-4666-8387-7.ch014, 2015.

[4] M. A. Naagas, E. L. Mique, T. D. Palaoag and J. S. D. Cruz, Defense-through-deception network security model: Securing university campus network from DOS/DDOS attack, *Bull. Electr. Eng. Informatics*, vol.7, no.4, pp.593-600, DOI: 10.11591/eei.v7i4.1349, 2018.

[5] Presiden RI, *Regulation of the Government of the Republic of Indonesia Number 71 of 2019 on Electronic System and Transcaction Operations*, https://jdih.kominfo.go.id/produk_hukum/view/id/695/t/peraturan+pemerintah+nomor+71+tahun+2019+tanggal+10+oktober+2019, 2019.

[6] J. Jang-Jaccard and S. Nepal, A survey of emerging threats in cybersecurity, *J. Comput. Syst. Sci.*, vol.80, no.5, pp.973-993, DOI: 10.1016/j.jcss.2014.02.005, 2014.

[7] Id-SIRTII/CC, *December 2021 Monthly Report of National Cybersecurity Monitoring Result, Indonesia Security Incident Response Team on Internet Infrastructure Coordination Center, National CSIRT of Indonesia*, https://cloud.bssn.go.id/s/r7aFeXcF3ddfFaF, 2021.

[8] C. Richmond, *Cybersecurity Readiness: How"At Risk" Is Your Organization*, no.5, 2017.

[9] A. Alzubaidi, Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia, *Heliyon*, vol.7, no.1, DOI: 10.1016/j.heliyon.2021.e06016, 2021.

[10] S. Hasan, M. Ali, S. Kurnia and R. Thurasamy, Evaluating the cyber security readiness of organizations and its influence on performance, *J. Inf. Secur. Appl.*, vol.58, 102726, DOI: 10.1016/j.jisa.2020.102726, 2021.

[11] M. H. Shah, R. Muhammad and N. Ameen, *Cybersecurity Readiness of E-Tail Organisations: A Technical Perspective*, Springer International Publishing, 2020.

[12] T. A. Chapman, *Factors Affecting Perceptions of Cybersecurity Readiness among Workgroup IT Managers*, Ph.D. Thesis, University of Missisipi, 2019.

[13] U. P. D. Ani, H. (Mary) He and A. Tiwari, Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective, *J. Cyber Secur. Technol.*, vol.1, no.1, pp.32-74, DOI: 10.1080/23742917.2016.1252211, 2017.

[14] Berlilana, T. Noparumpa, A. Ruangkanjanases, T. Hariguna and Sarmini, Organization benefit as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness, *Sustain.*, vol.13, no.24, DOI: 10.3390/su132413761, 2021.

[15] G. Bloom, E. Leontie, B. Narahari and R. Simha, Hardware and security: Vulnerabilities and solutions, *Handbook on Securing Cyber-Physical Critical Infrastructure*, Elsevier Inc., pp.305-331, 2012.

[16] M. J. Islami, Challenges in the implementation of Indonesia's national cybersecurity strategy in terms of a global assessment, *J. Masy. Telemat. dan Inf.*, vol.8, no.2, pp.137-144, 2017.

[17] T. Mose, Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives: A case study of Nairobi county, *Int. Acad. J. Inf. Syst. Technol.*, vol.2, no.1, pp.157-182, 2019.

[18] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin and H. N. Basim, Cyber security awareness, knowledge and behavior: A comparative study, *J. Comput. Inf. Syst.*, vol.62, no.1, pp.82-97, DOI: 10.1080/08874417.2020.1712269, 2022.