Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic

Hendro Wijayanto[1]*, Iwan Ady Prabowo[2]
Informatics Program STMIK Sinar Nusantar Surakarta [1], [2]
hw.wijayanto@gmail.com[1], iwanadyp@gmail.com[1]

***Abstract*— The penetration of Indonesian internet users in first quarter of 2020 has increased by 17 percent compared to 2019. Based on Google Consumer Barometer in 2018, many 79% of Internet users in Indonesia use the internet on a daily basis. During the Covid-19 Pandemic, universities had to do Study From Home and Work From Home. This resulted, use of information technology and computers also increasing. This increase will have an impact on the level of cybercrime vulnerability. The scale of cyber vulnerability is needed to measure level of cybersecurity in universities, especially in data managers. The Risk Cybersecurity Behavior Scale (RScB) is the result of input from digital forensic investigators and law enforcement. Developed further and adapted to the conditions of college or universities in Indonesia. From this, the cyber vulnerability scale is formed. There are five scales, Very Safe, Safe, Vulnerable, Very Vulnerable, and Dangerous. Where the scale is used in negative and positive statements. From the measurement of the questionnaire based on the Risky Cybersecurity Behavior Scale model, the Cronbach Alpha value is 0.721 or has a reliable status. The results show an average value of 3.3 or a vulnerable scale. Total average value of negative statements is 2.53 or scale close to vulnerability. So it is necessary to socialize the importance of cybersecurity to minimize occurrence of cybercrime.**

Keywords*— *Cybersecurity, RScB, Vulnerability Scale, Cybercrime, Covid-19

I. INTRODUCTION

The penetration of internet users in Indonesia has always increased every year. Research released by Hotsuite and We Are Social in January 2020 states that the number of internet users in Indonesia has reached 175.4 million people. Meanwhile, total population of Indonesia is around 272.1 million. This number has increased by 17 percent compared to 2019, or around 27 million users [1]. From the same source, it is stated that the largest internet usage dominates on smartphones and social media devices. Based on the Google Consumer Barometer in 2018, 79% of Internet users in Indonesia use the internet on a daily basis [2].

At the end of 2019 the world was shocked by the emergence of the Coronavirus Disease 19 or Covid-19 pandemic which caused several regions in Indonesia forced to lockdown starting April 2020. Some activities outside the home must be stopped and replaced with Work From Home (WFH). Even the education sector, it was also affected, forcing them to Study From Home (SFW).

Of course, the existence of Work From Home (WFH) and Study From Home (SFH) causes an increase in Indonesia internet uses for the first quarter of 2020. The increasing use of internet will cause an increase in cybercrime. Changes in work practices and socializing make many people spend their time online. Apart from that, the unemployment rate has also increased, which means it is likely that some of these people will turn cybercrime to keep earning income [3] [4].

Many important data stored as educational transactions in the college. Starting from the identity of lecturers, students and lecture activities. Of course, college database manager, an administrator must understand the importance of data and information security in using computer devices. If not, it will result in the inability of the agency to deal with cybercrime. Especially during the Covid-19 pandemic, the use of information technology and computers has increased. So that the need for vigilance from data managers.

Risky Cybersecurity Behaviors Scale (RScB) is a method for calculating the risk level of potential cybercrimes by assessing the linkert scale. Where in items related to computer use, internet, social media, use of online storage and exchanging information. With the existence of cybersecurity behavior assessment, it can be a reference for increasing cyberattack awareness in College. With the existence of cyber crime vulnerability assessment in the education sector, later it can provide referrals as suggestions or references in providing cyber crime mitigation policies in higher education.

Paradigm shift is critical to the effectiveness of cybersecurity techniques and practices. Since most cyber incidents are human-caused, this shift requires research that extends to unexplored areas such as aspects of cybersecurity behavior. It is more important to focus on social and behavioral problems to improve the current situation. This paper is an attempt to provide an overview of relevant theories and principles, and provides insights including an interdisciplinary framework that incorporates behavioral cybersecurity.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v9i3.1021, Copyright ©2020
Submitted : 27 Oktober 2020, Revised : -, Accepted : 27 Oktober 2020, Published : 2 November 2020

II. LITERATURE REVIEW

Covid-19 pandemic has tremendous effects in all aspects of life. Drastic changes occurred both on the social and economic side. The results of the analysis of cybercrime during the Covid-19 Pandemic show that the increased of information technology and the internet will have implications for an increase in cybercrime. Changes in work patterns, lack of public vigilance in utilizing technology, increasing unemployment are important reasons for cyberattacks. The recommendation is the government, media and institutions should be aware of this and it is necessary to carry out a campaign on the importance of information security during the Pandemic [3, 5]. There are so many threats of cybercrime that can occur during the Covid-19 Pandemic. Here are 10 deadly cybersecurity threats is DDoS Attack, Malicious Domains, Malicious Websites, Malware, Ransomeware, Spam Email, Malicious Social Media Messaging, Business Email Compromise, Mobile Apps, and Browsing Apps [6] [7].

Measurement of information security awareness and data privacy on Android Smartphone users has also been carried out with an information security awareness level of 71% and 76% privacy. In its measurement, it uses the dimensions of Attitude, Knowledge and Behavior towards Smartphone use [8]. Information security awareness also attacks users of smartphones and other mobile devices. It is proven that many smartphone users have banking applications in it. In addition, the fraudulent model still occurs via SMS, telephone or Financial Technology [9].

In the behavior theory and cybersecurity rules mentioned by DNV-GL Cybersecurity, one of the core cybersecurity concepts is people. First, it is important for all stakeholders in college to be aware of their role in preventing and reducing cyber threats, be it understanding sensitive data, or understanding phishing e-mails. Second, in the case of specialized technical security staff, updating their skills and qualifications to ensure that appropriate controls, technology and practices are in place to prevent cyber threats is critical to an organization's ability to prevent cyberattacks [10].

A. College or University Data Center

Based on Presidential Decree number 11 of 2020 concerning Determination of COVID-19 public health emergencies in Indonesia, which requires countermeasures in accordance with statutory provisions, the Directorate General of College has implemented various strategies to carry out these efforts. To avoid the spread and spread of the Covid-19 Pandemic, a policy of work, worship and study from home has been issued. Face-to-face learning is transformed into online learning [9].

The College Data Center is the main data which contains data on students, lecturers and teaching and learning activities. Important data is stored starting from personal data, name of birth, mother, place of birth date, address and contact information.

B. Risky Cybersecurity Behaviors Scale (RScB)

Risk Cybersecurity Behaviors Scale (RCsB) refers to the Security Behavior Intentions Scale (SeBIS). This scale was created with input from Digital Forensic investigators and Law Enforcement Risky Cybersecurity Behaviors Scale (RScB) sebagain merujuk pada Security Behavior Intentions Scale (SeBIS).[10].

The questionnaire asks participants to rate themselves regarding their behavior in using computer technology by selecting a scale of 0-5 (where 0 = Never and 5 = Very Often). The final scale includes 20 items with possible scores ranging from 0-150. A higher RScB score indicates an individual at risk of engaging in cybersecurity behavior. In this study, all 20 items have a mean value of 27.72, standard deviation of 14.81 and Cronbach α of 0.823 which indicates that the questionnaire items are very reliable [11]. The complete list of items for the Risky Cybersecurity Behaviors Scale (RScB) is shown in Table I.

TABLE I. ITEM OF RISKY CYBERSECURITY BEHAVIORS SCALE (RSCB)

No	Item
1	Sharing passwords with friends and colleagues.
2	Using or creating passwords that are not very complicated (e.g. family name and date of birth).
3	Using the same password for multiple websites.
4	Using online storage systems to exchange and keep personal or sensitive information.
5	Entering payment information on websites that have no clear security information/certification
6	Using free-to-access public Wi-Fi
7	Relying on a trusted friend or colleague to advise you on aspects of online-security.
8	Downloading free anti-virus software from an unknown source.
9	Disabling the anti-virus on my work computer so that I can download information from websites.
10	Bringing in my own USB to work in order to transfer data onto it.
11*	Checking that software for your smartphone/tablet/laptop/PC is up-to-date.
12	Downloading digital media (music, films, games) from unlicensed sources
13	Sharing my current location on social media.
14	Accepting friend requests on social media because you recognise the photo.
15	Clicking on links contained in unsolicited emails from an unknown source.
16	Sending personal information to strangers over the Internet.
17	Clicking on links contained in an email from a trusted friend or work colleague.
18*	Checking for updates to any anti-virus software you have installed.
19	Downloading data and material from websites on my work computer without checking its authenticity.
20	Storing company information on my personal electronic device (e.g. smartphone/tablet/laptop)

** Positive Value*

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v9i3.1021, Copyright ©2020
Submitted : 27 Oktober 2020, Revised : -, Accepted : 27 Oktober 2020, Published : 2 November 2020

In processing the questionnaire data, there are several steps that must be passed. Starting from data entry into the computer, normalization, validity and reliability testing, descriptive analysis to hypothesis testing. Descriptive statistics are useful for describing the summary of research data such as mean, standard deviation, variance, mode, minimum, maximum and total number [12] [13].

III. RESULT AND DISCUSSION

Data collection was carried out with vulnerability during April - June 2020 or peak of the Covid-19 Pandemic. Where several regions are implementing lockdowns and are currently Worfk From Home (WFH). The respondents were the managers or administrators of the Database College in LLDIKTI 6 Central Java Region, without any educational level restrictions.

In this questionnaire model, additional variables are carried out based on the Risk Cybersecurity Behavior Scale (RScB) or in Table 1, to further clarify the behavior of Internet and computer users. The addition this variable is by looking at the activities of using information technology and computers during the Covid-19 Pandemic. Five (5) groups will be formed, namely, behavior using passwords, data and information access behavior, device and internet or network usage behavior, social media behavior and behavior using smartphone devices. The total number of question items (Q) is 33, it can be shown in Table II

TABLE II. CYBERSECURITY BEHAVIOR QUESTIONNAIRE ITEMS

A. Behavior of Using Password	
Variable	**Items**
Q1.1 b)	Sharing passwords with friends and colleagues.
Q1.2 b)	Using or creating passwords that are not very complicated (e.g. family name and date of birth).
Q1.3 b)	Using the same password for multiple account.
Q1.4 a)	Using two-step password verification (OTP, SMS, Authenticator)
Q1.5 a)	Log out the account after use
Q1.6	Save Passwords in the web browser
B. Behavior of Data and Information Access	
Variable	**Items**
Q2.1 b)	Using online storage systems to exchange and keep personal or sensitive information.
Q2.2	Storing important data / files without password in online storage
Q2.3 b)	Entering payment information on websites that have no clear security information/certification
Q2.4 b)	Clicking on links contained in unsolicited emails from an unknown source.
Q2.5	Download data / files / materials from the website without checking their authenticity
Q2.6 b)	Bringing in my own USB to work in order to transfer data onto it.
Q2.7	Opens a file regardless of the file extension / type
C. Behavior of Device and Internet / Network Usage	
Variable	**Items**
Q3.1 b)	Using free-to-access public Wi-Fi
Q3.2 b)	Downloading free anti-virus software from an unknown source.
Q3.3 b)	Downloading digital media (music, films, games) from unlicensed sources
Q3.4	Using illegal / pirated applications / software
Q3.5	Sharing folders / files between computers
Q3.6	Clicking on the popup Ads On the website
Q3.7	Using a Virtual Private Network (VPN)
D. Behavior of Social Media	
Variable	**Items**
Q4.1 b)	Accepting friend requests on social media because you recognise the photo.
Q4.2 b)	Sharing my current location on social media.
Q4.3	Displays personal information on social media profiles
Q4.4	Provide posts to social media regularly every day
Q4.5	Repost (repost) without confirmation of correctness
Q4.6	Using more than one social media
Q4.7	Using social media for business / selling
E. Behavior of Using Smartphone Devices	
Variable	**Items**
Q5.1	Using a smartphone with the Android operating system
Q5.2	Unlock system access rights (ROOT / JAILBRAKE) Smartphone
Q5.3 a)	Use a PIN / Password combination to unlock a smartphone device
Q5.4	Activating Smartphone GPS
Q5.5	Enable Smartphone Auto Syncronization
Q5.6	Lend a smartphone to a friend

a) Positive Value
b) Items From RScB Scale

Scale is needed to determine the measurement value. Each item variable uses a linkert scale to measure individual behavior by responding for 5 choice points, namely 1) Very Never, 2) Never, 3) Never, 4) Often and 5) Very Often. The results of the scale of each variable will relate to the level of cybersecurity vulnerability. In behavior with positive value on very frequent scale, it will indicate cybersecurity vulnerability is very safe of cyberattack. Meanwhile, behavior with a negative value on a very frequent scale will indicate dangerous cyber vulnerability. As shown in Table III

TABLE III. CYBERSECURITY VULNERABILITY BEHAVIOR SCALE

Scale		**(Q) Negative**	**(Q) Positive**
1	Very Never	Very safe	Dangerous
2	Never	Secure	Very Vulnerable
3	Ever	Vulnerable	Vulnerable
4	Often	Very Vulnerable	Secure
5	Very often	Dangerous	Very Secure

Reliability test is needed to measure the accuracy of measurement results. This is very important so that the questionnaire (Table II) used as a data collection tool is truly reliable.

TABLE IV. RELIABILITY STATISTIC

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.721	.721	33

Based on Table IV, the results of the Cronbach α are 0,721. Where entered into a scale of 0.6 - 0.79 or accepted reliability category. This means that if the questionnaire is used for re-

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v9i3.1021, Copyright ©2020
Submitted : 27 Oktober 2020, Revised : -, Accepted : 27 Oktober 2020, Published : 2 November 2020

measurement on a different object, it will produce constant results.

TABLE V. FREQUENCY STATISTICS OF RESPONDENTS ANSWER

	N		Mean	Median	Mode	Std. Deviation	Min	Max	Sum
	Valid	Missing							
Q1.1	34	0	1.65	1.50	1	.849	1	5	56
Q1.2	34	0	2.79	3.00	2	1.175	1	5	95
Q1.3	34	0	3.88	4.00	4	.946	2	5	132
Q1.4	34	0	3.71	4.00	5	1.194	1	5	126
Q1.5	34	0	3.85	4.00	5	1.209	1	5	131
Q1.6	34	0	2.79	3.00	3	1.321	1	5	95
Q2.1	34	0	3.56	4.00	3	1.106	1	5	121
Q2.2	34	0	2.59	3.00	3	1.209	1	5	88
Q2.3	34	0	2.26	2.00	2	1.263	1	5	77
Q2.4	34	0	1.50	1.00	1	.826	1	4	51
Q2.5	34	0	2.41	2.00	3	.957	1	5	82
Q2.6	34	0	2.76	2.00	2	1.281	1	5	94
Q2.7	34	0	2.15	2.00	2	.925	1	4	73
Q3.1	34	0	2.50	3.00	3	1.237	1	5	85
Q3.2	34	0	3.68	4.00	4	1.065	1	5	125
Q3.3	34	0	3.00	3.00	3	1.044	1	5	102
Q3.4	34	0	3.12	3.00	3	1.008	1	5	106
Q3.5	34	0	2.91	3.00	3	1.190	1	5	99
Q3.6	34	0	1.76	1.00	1	1.017	1	5	60
Q3.7	34	0	2.82	3.00	2	1.141	1	5	96
Q4.1	34	0	1.76	2.00	2	.699	1	4	60
Q4.2	34	0	2.56	2.50	1	1.260	1	5	87
Q4.3	34	0	2.74	3.00	3	1.189	1	5	93
Q4.4	34	0	2.50	2.00	2	.961	1	5	85
Q4.5	34	0	1.82	2.00	1	.869	1	4	62
Q4.6	34	0	3.47	3.50	3	1.051	1	5	118
Q4.7	34	0	2.88	3.00	3	1.343	1	5	98
Q5.1	34	0	4.74	5.00	5	.511	3	5	161
Q5.2	34	0	2.35	2.50	1	1.203	1	5	80
Q5.3	34	0	4.15	4.50	5	1.158	1	5	141
Q5.4	34	0	3.82	4.00	5	1.141	1	5	130
Q5.5	34	0	3.44	4.00	4	1.160	1	5	117
Q5.6	34	0	1.85	2.00	1	.857	1	4	63

On Table V, the mode value for each variable will be analyzed. The Mode is value that most often appears in the results of the questionnaire answers. The purpose this analysis is to determine the level of cybercrime vulnerability in each behavior group.

A. Analysis of Using Password Behavior

There are 6 (six) questionnaire statements in the behavior of using passwords. There are 2 (two) positive statements and 4 (four) negative statements. For positive statements, Q1.4 (using two-step verification) and Q1.5 (log out account after use) have a mode value of 5 (Very often). Statements to pay attention to are the Q1.3 statement (using the same password for multiple accounts) with a value of 4 (Often) and Q1.6 (saving passwords in the browser) with a value of 3 (ever).

Based on the scale of vulnerability in Table III, respondents are in the vulnerable category of cyber attacks in terms using passwords for several accounts and the confidentiality passwords stored in a web browser.

B. Analysis of Data and Information Access Behavior

In data and information access behavior with a statement of 7 (seven), there is an indication of cybersecurity vulnerabilities in statements Q2.1 (using an online storage system to exchange and store information), Q2.2 (storing important data without passwords in online storage) and Q2.5 (downloading data / files from the site without checking authenticity).

C. Analysis of Using Internet Devices / Network Access Behavior

The results of internet usage behavior show Q3.1 (using free wifi to access important information), Q3.3 (downloading data / files from illegal sources), Q3.4 (using illegal / pirated applications / software) and Q3.5 (sharing folders / files between computers) are vulnerable to cyber attacks. In addition, in Q3.2 (using free antivirus) it is in the very vulnerable category for users to experience cyber attacks..

D. Analysis of Social Media Behavior

Social media behavior shows vulnerable level in Q4.3 (displaying personal information on social media profiles), Q4.6 (using more than one social media) and Q4.7 (using social media for business / selling).

E. Analysis of Using Smartphone Behavior

Smartphone physical device security with PIN / Password (Q5.3) entered at a very secure level. Respondents' results show very often (5) in using PIN / Password on their smartphone. This statement is a positive statement.

The negative statement results in Q5.4 (activating the Smartphone GPS) shows a dangerous level with a value of 5 (five). Whereas in the negative statement Q5.5 (activating autosynconization) shows that the level is very vulnerable with a value of 4 (four).

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v9i3.1021, Copyright ©2020
Submitted : 27 Oktober 2020, Revised : -, Accepted : 27 Oktober 2020, Published : 2 November 2020

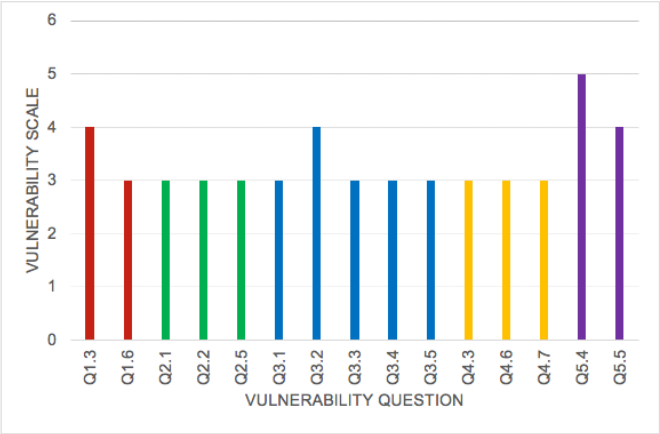

Fig. 1. Cybersecurity Behavior Vulnerability Diagram in College

In Figure 1, you can see the distribution of statements with levels from vulnerable to dangerous. Where the average value is 3,3 or categorized as vulnerable to cyberattacks. Meanwhile, the average value of all negative statements in Table 1 is 2,53 or falls into the near vulnerable category.

IV. CONCLUSION

The questionnaire variable formed based on the Risk Cybersecurity Behaviors Scale (RCsB) have Cronbach α is 0.721 or the reliability is accepted.

The increasing level information technology and computer use during the Covid-19 Pandemic will affect the scale of cybercrime vulnerability behavior. There are 33 cybersecurity behavior statements with 30 negative statements and 3 positive statements. Of the 30 negative statements, 15 statements resulted in values from vulnerable to very vulnerable (Figure 1). The average value of cybersecurity is 3,3 or in the vulnerable category. While the average value of negative statements is 2,53 with the category approaching vulnerable. This assessment is based on the answers of 34 respondents from the LLDIKTI 6 Central Java Region.

Future research needs to analyze the relationship between categories. In addition, respondents are not limited to administrators only, but also to all components of college. Information about cybersecurity also needed to minimize the cybercrime.

ACKNOWLEDGMENT

All research activities are funded by the Ministry of Education and Culture of the Republic of Indonesia in 2020 for the Beginner Lecturer Research scheme with the title "Analysis of Higher Education Readiness Levels in Facing Cyber Crime Attacks (Case Study of Higher Education in the Central Java Region)".

REFERENCES

[1] Hootsuite, We Are Social, "Digital 2020. Indonesia," Hootsuite, United State, 2020.

[2] A. Darmayani, Siberpedia Panduan Pintar Keamanan Siber, Yogyakarta: Center for Digital Society (CfDS), 2019.

[3] L. A. S. R. C. N. E. E. Harjinder Singh Lallie, "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic," University of Strathclyde Glasgow, United Kingdom, 2020.

[4] P. Mahadevan, "Cybercrime Threats during the COVID-19 pandemic," Global Initiative Against Transnational Organized Crime, Switzerland, 2020.

[5] J. Wiggen, "The impact of COVID-19 on cyber crime and state-sponsored cyber activities," Konrad-Adenauer-Stiftung, German, 2020.

[6] S. N. B. Z. Navid Ali Khan, "Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic," 2020.

[7] S. N. B. J. Navid Ali Khan, "UAV's Applications, Architecture, Security Issues and Attack Scenarios: A Survey," *1st International Conference on Technology Innovation and Data Sciences (ICTIDS)*, vol. 1, no. 1, 2019.

[8] C. Y. P. Robbi Akramana, "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia," *Jurnal Sistem Informasi Bisnis*, vol. 8, no. 2, pp. 115-122, 2018.

[9] A. H. M. D. H. Hendro Wijayanto, "Analisis Penyalahgunaan Data Pribadi Dalam Aplikasi Fintech Ilegal Dengan Metode Hibrid," *Jurnal Ilmiah Sinus*, vol. 1, no. 18, pp. 1-10, 2020.

[10] A. R. a. A. Services, "Behavioral Theories in Security Compliance – Defining the People Problem," 19 February 2019. [Online]. Available: https://www.astrit9.com/behavioral-theories-in-security-compliance-defining-the-people-problem/. [Accessed 11 October 2020].

[11] D. J. P. Tinggi, Panduan Penyelenggaraan Pembelajaran Semester Gasal 2020/2021 di Perguruan Tinggi, Jakarta: Direktorat Jenderal Pendidikan Tinggi Kemdikbud RI, 2020.

[12] E. P. Serge Egelman, "Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)," *ACM Conference on Human Factors in Computing System*, pp. 2873-2882, 2015.

[13] L. Hadlington, "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon*, p. e00346, 2017.

[14] V. Herlina, Panduan Praktis Mengolah Data Kuesioner Menggunakan SPSS, Jakarta: Elex Media Komputindo, 2019.

[15] L. R. U. Wiratna Sujarweni, The Master Book of SPSS. Pintar Mengolah Data Statistik untuk Segala Keperluan Secara Otodidak, Yogyakarta: Start Up, 2019.

p-ISSN 2301-7988, e-ISSN 2581-0588
DOI : 10.32736/sisfokom.v9i3.1021, Copyright ©2020
Submitted : 27 Oktober 2020, Revised : -, Accepted : 27 Oktober 2020, Published : 2 November 2020