

THE INFLUENCE OF CYBERSECURITY AND TECHNICAL SKILLS ON EMPLOYEES' WORK MOTIVATION AT BSI KCP JATIBARANG, INDRAMAYU REGENCY

Dewi Fatmasari¹, Diani Nurwahyuni², Rita Kusumadewi³, Dikdik Harjadi⁴, Muhamad Fikri bin Aziz⁵

¹⁻³ Faculty of Islamic Economics and Business, Islamic Banking, Universitas Islam Negeri Siber Syekh Nurjati Cirebon

⁴ Faculty of Economics and Business, Universitas Kuningan

⁵ Islam Business School, Universiti Utara Malaysia

Email corresponding author: dewifatmasari@syekhnurjati.ac.id

ABSTRACT

As technology and communication have advanced, so too has banking in Indonesia, which has aided in the emergence of mobile banking—a service provided by banks to conduct online transactions. Nonetheless, banking has seen the highest number of online anomalies; in 2023, 966,533 ransomware anomalies were identified out of 160 million malware anomalies. Then, cybercrime attacks affected about 50% of Indonesia's banking sector. Banks can successfully combat cybercrime assaults by having workers with technical expertise. Developing technological expertise is the primary means of creating security protection that works. Bank employees can compete in the digital world by strengthening their internal systems with the help of individuals with excellent technological capabilities.. The purpose of this study is to ascertain how technical skills and cybersecurity affect the work motivation of Bank Syariah Indonesia (BSI) employees. This study employs a quantitative methodology with a descriptive model, gathering data via questionnaire distribution and observation. We employ f tests, t tests, multiple linear regression testing, validity and reliability tests, and traditional assumption tests. The findings: (1) Employee work motivation at Indonesian Islamic banks is positively and significantly impacted by cybersecurity factors by 17.05%. (2) With a value of 11.17%, technical ability variables significantly and favorably affect employee job motivation in Indonesian Islamic banks. (3) Cybersecurity and technical ability variables can influence employee job motivation by 94.7% and have a favorable and significant effect at the same time.

Keywords: Cybersecurity, Technical skill, Work motivation

INTRODUCTIONS

The development of information technology has brought about very significant changes to the business strategies of the business world, including banking, by placing information technology as the main element in the production process or service provision. Judging from the competition in product quality, the services offered, and conducting large-scale promotions, companies compete to provide the best service and provide satisfaction to attract customers. Banking in Indonesia has now followed the development of technology and communication, thus encouraging the formation of mobile banking, which is a service from banks to carry out transactions that can be accessed online. Facilities in mobile banking include fund transfers, balance information, account mutations, electricity payments, credit top-

ups, and others, which make mobile banking important and often used in daily activities. (Zulfahmi et al, 2023).

The Indonesian government has issued 60 laws regulating the digital economy. Regarding the security of the system used, the government formed a cyber team or *Badan Siber dan Sandi Negara (BSSN)* in Presidential Decree Number 53 of 2017 concerning the National Cyber and Crypto Agency which is tasked with carrying out cyber security tasks effectively and efficiently by utilizing, developing, and consolidating all elements related to cyber security (Edy et al, 2022).

Although there is a Law on the Protection of Digital Banking Transactions, it does not guarantee that cybercrime will not occur. According to Nurma (2023), it is explained that a cybercrime attack also occurred on the digital services of Bank Syariah Indonesia (BSI) which was disrupted for 2 weeks. This case is a hacking that is suspected to be a ransomware attack that attacks BSI's digital system or technology which results in customers being unable to access and transact via mobile banking, ATMs, and tellers.

According to Alcianno (2019), in overcoming cybercrime attacks, banks can achieve success by linking technical skills to employees. Basically, technical skills are technical abilities needed to carry out certain tasks. These skills include a person's ability to perform or complete technical tasks, such as IT management skills. Technical skills are also skills or expertise (Djien, 2021). Technical skills are skills or expertise possessed by an employee to carry out and complete the tasks assigned to them (Djien, 2021). Improving technical skills is the main key to building an effective cybersecurity defense. Through Certified Information System Security Professional (CISSP) or Certified Ethical Hacker (CEH) certification training and continuous development, bank employees are empowered with in-depth knowledge of cybersecurity, including attack identification, prevention, and rapid response. These points are the dimensions for measuring technical skills this time. Banks can form an internal security team consisting of individuals with strong technical skills, ensuring that monitoring suspicious activity and handling incidents can be carried out effectively. The implementation of the latest and high-quality security system is the basis for protecting digital assets.

With the increasing number of attacks (cybercrime) in the banking world, cybersecurity is needed, which is an effort to ensure that the security attributes of the organization and its use are guaranteed. Cybersecurity is defined by Munawarah et al (2022) as the practice of protecting systems, networks, programs, data and information from digital threats or attacks. The following are some key elements of cybersecurity according to Munawarah (2021), namely privacy policy documents, information infrastructure, perimeter defense, network monitoring system, information system and event management, network security assessment, human resource and security awareness.

There are other factors that support employee performance, namely ability. Work ability is the ability of employees to perform certain tasks in the right way. If employee talents are developed and used properly, it can affect the progress of the company (Arini, 2020). Apart from ability, there is motivation and work enthusiasm, which can channel and support employee behavior to try harder and achieve better results (Tsauri, 2021).

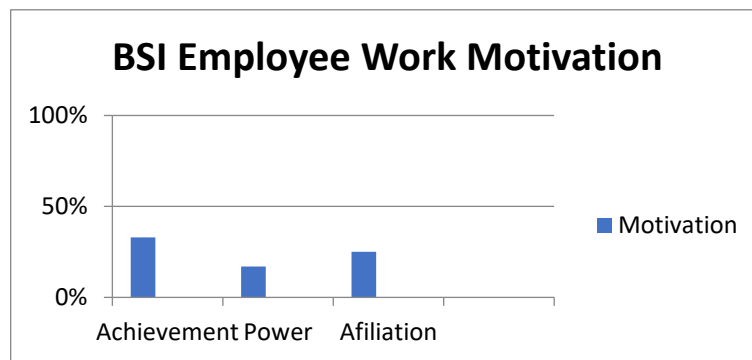


Diagram 1.2. Employee Work Motivation

As can be seen from diagram 1.2 above, employees are more motivated by personal achievement and high performance standards than by the need to be accepted by colleagues or to hold positions of influence and control. They are more focused on achieving goals and succeeding in challenging tasks. This will lead to higher productivity, innovation, and significant contributions to the progress of the organization. However, in reality, power is the biggest influence because in some work environments, the power structure determines who succeeds and who does not. to get recognition, promotion, or opportunity. The data was obtained through observation by distributing google forms whose contents are related to indicator statements, namely the need for achievement, the need for power and the need for affiliation. The results of each of these indicators obtained the results of the need for achievement of 30%, the need for power of 10%, and the need for affiliation of 20%.

Along with this, employees who have high technical skills can strengthen the internal system of BSI bank employees so that they can compete in the digital world, effective management of cybersecurity will involve proactive planning, implementation of strict security policies, and continuous training, continuous operational smoothness is a natural result of this combination. with improved technical skills, employees can better adapt to technological changes and respond efficiently to cyber attacks. Effective management creates a solid framework to maintain smooth operations, minimize the risk of disruption, and optimize technical skills. (Hasibuan, 2020).

Based on the description above, to achieve maximum results, an employee must work hard by providing the abilities they have and supported by existing facilities and infrastructure. where a person's ability can be measured from the level of IT skills management or expertise (skills) and knowledge possessed in carrying out the tasks that have been given. Based on the description of the background, the author is interested in conducting further research related to the impact of cybersecurity on the banking sector, with a focus on how the level of technical skills of Indonesian Islamic Bank (BSI) employees can affect employee work motivation entitled "THE INFLUENCE OF CYBERSECURITY AND TECHNICAL SKILLS ON THE WORK MOTIVATION OF BSI EMPLOYEES KCP JATIBARANG INDRAMAYU.

LITERATURE REVIEW

According to Munawarah et al (2022) and Triwahyuni et al (2022). Cybersecurity is the practice of protecting systems, networks, programs, data and information from digital threats or attacks. Meanwhile, according to Ayuni (2021) Cybersecurity is an effort to protect a system from unauthorized attacks carried out by irresponsible individuals or groups, cybersecurity actions are specifically designed to ward off threats to all connected systems, both in relation to networks, applications and data transfer. Several studies related to this have also been conducted, including research by Alcianno (2019) which concluded that employee technical skills are needed in this case to be able to reduce the risk of Cybersecurity crimes, such as in-depth knowledge of cyber security, attack identification, prevention and

rapid response. This specific knowledge concerns the use or operation of various existing installations, both applicable software and hardware. Another study was also conducted by McClelland (2022) whose results explain that this work motivation can determine what employees need to maintain work motivation for Loyalty in an organization or company such as, the need for achievement, the need for power and the need for affiliation. Other studies also state that Cybersecurity has a significant effect on the work motivation of Indonesian Islamic bank employees in the study (Endang Naryono, 2021, Ayu Nuraeni, 2022 and Dwi Astuti, 2021) which shows the results of the study that cyber security has a positive effect on employee work motivation. A positive organizational culture can increase employees' sense of security and comfort in working, thereby increasing their motivation. Good cyber security can also increase employee trust in the bank, so that they feel more motivated to work well.

METHODS

This study uses quantitative research methods. The source of data collection is primary using a questionnaire. The distribution of questionnaires was carried out by 40 BSI KCP Jatibarang Indramayu Regency employees. Determination of the number of samples using the Census Sampling formula or Saturated sampling, the model used is Multiple Linear Regression Analysis. The first test was carried out by means of descriptive variable analysis, then the questionnaire data quality test was carried out, namely the validity and reliability test, then continued by conducting a classical assumption test including the normality test, multicollinearity test, and heteroscedasticity test. And data processing using the IBM SPSS version 23 application. Testing was carried out by looking at the results of the t test (partial), F test (simultaneous), and determination coefficient test R^2 .

RESULT AND DISCUSSION

Data Quality Test Results

a. Validity Test

Based on the validity test, it shows that the Cybersecurity and Technical Skill variables on Employee Work Motivation have an R_{table} value of 0.304 and the R_{count} value of each statement is greater than the R_{table} . So all statement items on each variable in the questionnaire are valid.

b. Reliability Test

Table 3.2 Reliability Test Results

Variable	Cronbach's Alpha	Accuracy	Keterangan
Cybersecurity	0,967	0,6	Reliabel
Technical skill	0,958	0,6	Reliabel
Motivation	0,940	0,6	Reliabel

Source: IBM SPSS data processing version 23

Based on Table 3.2 above, it explains that the output results show that the Alpha coefficient values of the variables studied show various results. The Cronbach's alpha value on the Cybersecurity variable is 0.967. Then the Cronbach's alpha value on the Technical skill variable is 0.958 and the Cronbach's alpha value on the Work Motivation variable is 0.940. All research variables have a Cronbach's alpha value of more than 0.6. Thus, it can be concluded that all variables used in this study are reliable.

Multiple Linear Regression Analysis

Table 3.3 Multiple Linear Regression Test Results

Model		Unstandardized Coefficients		Standardized Coefficients		Sig.	Correlations		
		B	Std. Error	Beta	T		Zero-order	Partial	Part
1	(Constant)	2.550	3.251		.784	.438			
	Cybersecurity	-.151	.064	-.205	-2.372	.023	.832	-.363	-.090
	Technical skill	1.092	.082	1.153	13.374	.000	.969	.910	.505

Source: IBM SPSS data processing version 23

Based on table 3.3, the multiple linear regression analysis obtained a constant value (α) of 2,550, the regression coefficient value of the Cybersecurity variable (β_1) of -0,151, the regression coefficient value of the Technical Skill variable (β_2) of 1,092. So it can be formulated

$$Y = \alpha + \beta_1 X_1 + \beta_2 X_2 + e = 2,550 + -0,151 + 1.092 + e.$$

From the equation above, it can be explained the results of the analysis of the discussion, namely the constant value (α) of 2,550. This means that if the Cybersecurity variables (X_1) and *Technical skill* (X_2) re considered constant, then the level of Work Motivation is 2,550. The regression coefficient value of the Cybersecurity variable (β_1) in the linear regression is -0.151, meaning that if the Cybersecurity variable increases by one unit, Work Motivation will increase by -0.151. The regression coefficient value of the Technical skill variable (β_2) in the linear regression is 1.092. This means that if the Technical skill variable increases by one unit, Employee Work Motivation increases by 1, 092. From table 3.3 above, it can be seen that the results of the individual influence test (%) of the variables X_1 on Y and X_2 on Y are as follows :

$$R X_1 = -0,205 \times 0,832 = 0,17056 = 17,05\%$$

$$R X_2 = 1,153 \times 0,969 = 1,117257 = 11,17\%$$

Based on the calculation results above, it can be seen that the results of the test of the individual influence of variable X_1 (*cybersecurity*) on employee work motivation are 17.05%, while the results of the test of the individual influence of variable X_2 (*technical skill*) on employee work motivation are 11.17%.

Hypothesis Test Result

1. T-Test (Parsial)

Table 3.4 Results of t-Test (Partial)

Model		Unstandardized Coefficients		Standardized Coefficients		Sig.	Collinearity Statistics	
		B	Std. Error	Beta	T		Tolerance	VIF
1	(Constant)	2.550	3.251		.784	.438		
	Cybersecurity	-.151	.064	-.205	-2.372	.023	.192	5.207
	Technical skill	1.092	.082	1.153	13.374	.000	.192	5.207

Source: IBM SPSS data processing version 23

The T-test tests whether the independent variables (cybersecurity and technical skills) individually affect the dependent variable (work motivation) known T_{tabel} value at a significance level of 0,05 and $df = n - k - 1$ atau $df = 40 - 3 = 37$. (df = degrees of freedom, n = number of respondents, k = number of independent variables), so T_{tabel} is 1.687. Based on the SPSS output results in table 3.4, we can see that the cybersecurity variable (X_1) has a value of $t_{hitung} > t_{tabel}$, which is $2.372 > 1,687$ and has a significance value of $0,023 < 0,05$ so we can conclude that H_{01} is rejected and H_{a1} is accepted, meaning

that the cybersecurity variable (X_1) has a positive and significant influence on the work motivation of Bank Syariah Indonesia employees (Y). For the technical skill variable (X_2) has a $t_{hitung} > t_{tabel}$ namely $13.374 > 1.687$ and has a significance value of $0.002 < 0.05$ so we can conclude that H_0 is rejected and H_a is accepted, which means that the technical skill variable (X_2) as a positive and significant influence on the work motivation of Bank Syariah Indonesia employees (Y).

2. F-Test (Simultan)

Table 3.5 Result of F-Test (Simultan)

Model	Sum of Squares	Df	Mean Square	F	Sig.
1 Regression	5453.062	2	2726.531	331.806	.000 ^b
Residual	304.038	37	8.217		
Total	5757.100	39			

Source: IBM SPSS data processing version 23

Table 3.5 above shows that the $F_{count} > F_{table}$ ($331.806 > 3.25$) and significance < 0.05 ($0.000 < 0.05$) then H_0 is rejected and H_{a3} is accepted, so it can be concluded that cybersecurity and technical skills together or simultaneously have a positive and significant effect on the work motivation of Bank Syariah Indonesia employees..

3. Analysis of Determination Coefficient (R^2)

Table 3.6 Analysis of Determination Coefficient (R^2)

Model	R	R Square	Adjusted Square	R Std. Error of the Estimate
1	.973 ^a	.947	.944	2.86657

Source: IBM SPSS data processing version 23

Based on the SPSS output table "model summary" above, it can be seen that the coefficient of determination or R square 0,947. his R square value is from the square of the correlation coefficient value or R, which is $0.973 \times 0.973 = 0.946$. The value of R^2 is 0,947 or 94,7%. This value means that the cybersecurity variable (X_1), and technical skill (X_2) by 94,7% influence employee work motivation. and the remaining 5,3% is influenced by other variables outside the variables studied.

DISCUSSION

1. The Influence of Cybersecurity (X_1) on the Work Motivation of Bank Syariah Indonesia Employees (Y)

Based on the results explained above, it can be concluded that the dimensions of cybersecurity such as privacy policy documents, information infrastructure, defense primers, network monitoring systems, information systems and cyber security ranking event management and human resource and security awareness. Do not affect the work motivation of Bank Syariah Indonesia employees by 4.75. The indicator with the highest average value is the confidentiality of customer personal data "this shows that when a banking employee is able to maintain customer personal data and is responsible for the leakage of customer personal data, for example customer identity data such as name, NIK, address, date of birth and financial data such as account number and balance. Maintaining is the first step to avoid risks that may occur. So if there is an employee who is able to maintain and be responsible for customer personal data, it needs to be appreciated properly. This can contribute significantly to the success of Islamic banks in implementing sharia principles such as the principle of maintaining justice (adl), the principle of maintaining trust (amanah) and building trust from both clients and the general public..

The indicator with the lowest average value is being able to implement applicable laws with a value of 3.97. This fairly high value is because respondents can implement the law sufficiently. The ability of employees to implement applicable laws effectively can help prevent and investigate cyber security breaches, as well as protect sensitive organizational data and information. For example,

when respondents experienced a cybercrime attack on Bank Syariah Indonesia, respondents were only able to report the cybercrime attack and those who followed up were their superiors.

The results of this study are in line with the theory put forward by Munawarah (2022) which explains that cybersecurity can maintain the confidentiality, integrity and availability of cybersecurity which includes authenticity, accountability and reliability. Where cybersecurity is not only important to protect personal data and sensitive information, but also to maintain the smooth running of the banking business. Threats to cybersecurity continue to grow, so it is important to always update knowledge and implement best practices in cybersecurity. Each respondent has an important role in maintaining cybersecurity by following good security practices and reporting suspicious activity. In other words, if cybersecurity can be implemented properly by employees, it can increase employee work motivation, conversely if cybersecurity cannot be implemented properly, it will decrease the level of employee work motivation. Thus, the implementation of cybersecurity can be one of the keys to making employees able to maintain the security of Indonesian Islamic bank customers.

2. The Influence of Technical Skills (X_2) on the Work Motivation of Bank Syariah Indonesia Employees (Y)

Based on the results explained above, it can be concluded that the technical skill dimension such as in-depth knowledge of cyber security, attack identification, prevention, and rapid response, has an influence on the work motivation of Indonesian Islamic bank employees by 4.73. The indicator with the highest average value, namely being able to understand cyber risks and threats, shows that respondents have an understanding of the risks in cyber security and threats. When a cyber attack occurs, respondents quickly understand the risks that occur and are able to make improvements so that the cyber threat can be handled immediately. This reflects that respondents have a good understanding and dedication in preventing the risk of cyber attacks. By using sophisticated firewalls, antiviruses, and antimalware to protect bank systems and networks from cyber attacks and encrypting data to protect sensitive customer data, such as financial data and personal data. Thus, customers should always check with their bank for the latest information on their personal data protection policies. This will provide employee work motivation by increasing their understanding of cyber threats, with aspects that can help maintain employee work motivation such as attack identification, prevention and rapid response.

The indicator that obtained the lowest average value, namely being able to develop a cyber security strategy, obtained a value of 3.85. This shows that even with the lowest average value, it has a fairly high value, this shows that there is a lack of respondents in the ability to respond and resolve cyber attacks effectively so that they cannot provide solutions to this problem. This has implications for Vulnerability to Cyber Attacks such as blocking attacks, isolating infected systems, or recovering lost data. This ability is very important in dealing with cybersecurity attacks. which causes respondents to be able to develop an understanding of cyber security strategies. Developing an understanding of cyber security strategies in this case is the same as developing employee technical skills that can hone understanding of both risk prevention and attack identification. If all of the above understanding can be developed properly, it will result in good performance for employees which will affect employee work motivation..

The results of this study are in line with the theory put forward by Gibson (2021) which explains that technical skills or technical abilities are the abilities and knowledge needed to perform specific tasks related to technology and its applications. This shows the potential of people to carry out tasks or jobs. That ability may or may not be utilized. Meanwhile, according to David (2021), technical skills are the ability to perform certain tasks using the knowledge and skills that have been learned. These skills can be obtained through education, training, or work experience. Thus, ability is closely related to the physical and mental abilities that people have to carry out work and not what they want to do.

Technical skills are a person's expertise in developing the techniques they have, such as calculating accurately, operating a computer. These technical skills are specific competencies to carry out tasks or the ability to use techniques, tools, procedures and knowledge about specialized fields correctly and appropriately in carrying out their duties..

The results of this study are in line with previous studies which state that technical skills have a significant effect on the work motivation of Indonesian Islamic bank employees (Amalia et, al 2022, Alcinno et.al, 2019 and Adrian, 2022) which show the results of their research that technical skills have a positive influence that directly affects the work motivation of Indonesian Islamic bank employees..

3. The Influence of Cybersecurity (X_1) and Technical Skills (X_2) on the Work Motivation of Indonesian Islamic Bank Employees (Y)

Based on the results explained above, it can be concluded that the cybersecurity and technical skill variables simultaneously affect the Employee Work Motivation variable with a contribution of 94.7% influencing Employee Work Motivation and the remaining 5.3% influenced by other variables outside the variables studied. Based on the recapitulation table of respondents' statements, it shows that the indicator that obtained the highest average value was the confidentiality of customer personal data with a value of 4.75. Respondents indicated that maintaining customer personal data and being responsible for the confidentiality of customer data is the responsibility of all respondents as a form of loyalty of every banking employee. This principle is contained in Law No. 32 of 2009 concerning Environmental Protection and Management,.

The indicator with the lowest average value, namely developing a cyber security strategy, obtained a value of 3.85. This shows that even with the lowest average value, it has a fairly high value which causes respondents to be able to develop an understanding of cyber security strategies and make cyber security a top priority for every organization, including in protecting their valuable assets, namely data and information. Employees as users of company devices and systems are at the forefront of cyber defense..

Therefore, developing a cyber security strategy for employees is an important investment to minimize the risk of cyber attacks and maintain the security of organizational data. By developing an effective and sustainable cyber security strategy, organizations can increase employee awareness and knowledge of cyber security, reduce the risk of data breaches, protect the organization's reputation, increase productivity, and comply with applicable regulations and standards. Investing in cyber security for employees is key to protecting an organization's valuable assets and ensuring its success in the digital age.

The results of this study are in line with the theory put forward by Malthis (2021) which explains that motivation is a desire within a person that causes the person to act unusually, people act for a reason to achieve goals. Understanding motivation is very important because performance, reactions to compensation and other human resource issues are influenced and affect motivation. Thus, the results of this study show that cybersecurity and technical skills are one way to increase employee work motivation. When cybersecurity is implemented and understood properly, it can increase employee work motivation in various work contexts, help protect customer personal data, influence customer privacy policies, and improve security. Likewise with technical skills, when employees have technical skills and have in-depth knowledge of cyber security, they will tend to have a higher level of motivation, because employees have good technical skills in an in-depth understanding of cyber security.

The results can be concluded that the variables of cybersecurity and technical skills can affect the work motivation of Indonesian Islamic bank employees. This is in line with research (Febriawan, 2023 and Rika Yuniati, 2021), which shows the results of the study that Cybersecurity and technical

skills have a simultaneous positive influence on the work motivation of Indonesian Islamic bank employees. This study explains that employees must be able to maintain cyber security, because cyber security is very important in implementing the work motivation of Indonesian Islamic Bank employees..

CONCLUSION

The results of this study indicate that in partial testing, the cybersecurity and technical skill variables have a positive and significant effect on employee work motivation with a large percentage of 17.05% and 11.17%, respectively. And the cybersecurity and technical skill variables simultaneously have a positive and significant effect on employee work motivation with an R Square value of 94.7%.

Suggestions that are used as input for BSI KCP Jatibarang Employees include Bank BSI KCP Jatibarang needs to hold cybersecurity training for all employees periodically. and provide opportunities for employees to develop their technical skills through training, workshops, or certification programs. The next input for further research is suggested to be able to expand the research variables by developing or adding other variables that influence employee work motivation and taking respondents from other banks with a variety of samples and populations.

BIBLIOGRAPHY

- Aji, M. P. (2022). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) *Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective* . *ekonomi politik Universitas Pembangunan Nasional "Veteran" Jakarta*, 14-15.
- Alexander anggono, T. M. (2021). *Cybercrime dan cybersecurity pada fintech sebuah tinjauan pistaka sistematis* . *Jurnal Manajemen dan Organisasi* , 241-243.
- Ardika, O. P., & Hariyanti, S. (2022). Review Artikel: Transformasi Digital Dalam Bisnis Dan Manajeme. *Proceedings of Islamic Economics, Business, and Phi*, 143-144.
- Arifin, z. (2022). *keamanan dan ancaman pada cyberspace*. jakarta: MSIM4404.
- Burhan, f. a. (2023, Mei Rabu). *Bisnis.com* . Retrieved Mei Rabu , 2023, from Nasabah Keluhkan BSI mobile eror tiga hari, Kena *Ransoware*: [http://www. Bisnis.com](http://www.Bisnis.com)
- Cheryta, R. &. (2022). Evaluasi kebijakan *cyber security* sektor perbankan bank BTN Cabang surabaya . *jurnal apresiasi Ekonomi vo*;. 10 No. 3, 321-322.
- Dijen, L. K. (2022). *Pengaruh Technickill skill dan Enterprenership skill terhadap prestasi kerja karyawan PT. ardeni jaya sentosa disurabaya. Jurnal Teds Vol 02 No 02*, 2-3.
- Edy soesanto, a. r. (2023). Analisis dan peningkatan keamanan *cyber* studi kasus dan solusi dalam lingkungan digital untuk mengamankan objek vital dan file. *SAMMAJIVA Jurnal penelitian bisnis dan manajemen* , 191-192.
- Fadlih, D. C. (2023). analisis evaluasi kebijakan pada *cyber security* perbankan . *jurnal Trends Vol 01 No. 01* , 20-21.
- Hasanatul M, Y. M. (2022). bank Digital Syariah.Banjarmasin: PT. Borneo *Develpoment Project. perbankan syariah* , 6-7.
- OJK. (2023, September Rabu). *sikapiuangmu*. Retrieved september Rabu, 2023, from ojk.go: <https://sikapiuangmu.ojk.go.id/FrontEnd/Article/40774>
- Rahmawati, C. (2020). Tantangan dan ancaman keamanan siber indonesia di era revolusi Industri 4.0. *Seminar nasional sains teknologi dan inovasi indonesia* , 300-301.
- Yaldi, E. P. (2022). jurnal ilmiah manajemen dan kewirausahaan . *penerapan uj multikolinieritas* , 95-101.