Social Engineering SWOT Analysis in Government-Owned Commercial Banks and National Private Commercial Banks

Nadillah Syafitri[1*] and Grisvia Agustin[2]

[1,2] Department of Development Economics, Faculty of Economics and Business, Universitas Negeri Malang

nadillahsyafitri@gmail.com

Abstract

This research examines the phenomenon of social engineering at government-owned commercial banks and national private commercial banks. The research method used is descriptive qualitative with a literature study. The research results show the bank's strengths, weaknesses, opportunities, and threats. In addition, several strategies are recommended for banks to prevent social engineering attacks, namely building information technology in banking according to the standards and regulations of the Financial Service Authority (Otoritas Jasa Keuangan), utilizing social media as an educational tool, training employees, monitoring and optimizing data security and banking information technology networks, suppressing the circulation of social issues on behalf of banks that can trigger social engineering, increasing financial literacy and awareness of data security personal customers and employees. To prevent social engineering attacks, banks can implement strategies that are considered adequate.

Keywords: social engineering, cybercrime, banking

JEL : G21; G28; K24

DOI : 10.24002/kinerja.v27i2.6685

Received : 12/16/2022 Reviewed: 06/08/2023 Final Version: 09/22/2023

1. INTRODUCTION

According to data from the Operations Center Security National Cyber Indonesia, in 2021, as many as 1.6 billion cyber-attacks in Indonesia experienced enhancement compared to 2020, which is 496 million cyber-attacks. One sector the most frequently caught problem cyber is sector banking with economic motives. Issues frequent cyber happening in the industry banking, among others, social engineering, OTP Fraud, weaknesses in the system banking, phishing, and SIM swaps. Social engineering is an art that influences people to obtain information secrets, such as passwords, addresses, and others obtained with methods that utilize human vulnerability, like feelings, beliefs, and habits (Chetioui et al., 2021). Frequent

social engineering modes are happening in the banking sector: internet banking fraud and online transactions, bank contact centers, and SMS fraud (Ratulangi et al., 2021). The destination of social engineering is to get illegal access to the system information banking to do fraud, infiltration the network, activity spy, tamper with the system or steal identity (Junaedi, 2017). In their research, Airehrour et al. (2018) mention that all risk from cyberspace influences banking and the country's economy, which will influence the reputation and infrastructure of finance banking and can cause damage to trusted customers. Banking is crucial to the country's economy, and all process performance companies always relate to society because the trusted public in banking is the foundation prominent in system banking (Bidari et al., 2020). Suppose this social engineering problem continues to occur and causes damage to the reputation of banks, causing banks to experience a decline in public trust and financial losses. In that case, other economic problems may arise (Indonesian Bankers Association, 2015). As mentioned in research conducted by Salahdine and Kaabouch (2019), social engineering that occurs in banking impacts significant loss, which needs detection early to social engineering attack. According to report data Implementation of Prevention Fraud Strategy Period Semester I 2020 – Semester I 2021, there were 7,087 fraud events committed in cyber mode. In fraud cyber mode, 76% happened in commercial banks owned by the government, 28% in private banks, and 0.3% in foreign banks (Otoritas Jasa Keuangan, 2019).

So, this study aims to examine the social engineering phenomenon for government-owned and national private commercial banks using SWOT analysis (Strengths, Weaknesses, Opportunities, Threats). In this study, SWOT analysis aims to evaluate social engineering in banking, primarily government-owned and national private commercial banks, which is expected to reduce weaknesses in the banking sector and push impact threats arising from social engineering.

2. LITERATURE REVIEW

Commercial banks are the executing bank activity effort from service in activities payments made good in a manner conventional nor with sharia principles. Services provided by commercial banks, that is, whole service banking and operating areas, could be carried out throughout the region. Commercial banks owned by the government are registered commercial bank establishment capital owned by the government so that the government will own the whole bank's profits. A commercial bank's private national is the entire bank or part magnitude privately owned, deed establishment founded by the private sector, and the bank's profits will be owned privately (Kasmir, 2019).

Definition of social engineering According to Wang et al. (2020), in the context of security cyber, social engineering is one type of cyber attack where attackers utilize vulnerable people through social interaction to get access to security cyber. People cover psychology, cognition, consciousness, thinking, behavior, and others in this vulnerability. Then, for safety cyber in question is the problem equipment safety electromagnetic system communication information, operating data, and applications system in cyberspace. According to Alzahrani (2020), there are four categories of behavior of people whom social engineering attackers can exploit for attacks, including carelessness, comfort, helpfulness, and fear.

Social engineering attacks can be classified into two main categories: attack direct and indirect social engineering. Social engineering attacks are directly conducted to contact in a manner direct among both perpetrator and victim from contact physical, contact eyes, and interaction sound. Meanwhile, social engineering attacks are not directly conducted with the help of technology, and there is no need for contact between perpetrator and victim. Social engineering attacks that are not direct could be conducted through email or SMS (Salahdine and Kaabouch, 2019). In his research, Grimes (2020) states that, in general, there are several types of social engineering: physical, social, technical, and social-technical approaches. Airehrour et al. (2018), in their research on social engineering attacks in Banking Zealand New, mention that social engineering is a growing threat that needs attention. Junaedi (2017), in his research, mentions that social engineering harms banking and, to reduce risk, recommend that banking should do staff training and education related to threat safety and method to recognize social engineering attack.

SWOT analysis compares external and internal factors: strengths and weaknesses, opportunities and threats (Rangkuti, 2016). SWOT analysis is a framework planning strategy used to evaluate the organization, plans, and business activities (Gürel, 2017). With knowing strengths, the company could develop strengths so that the performance company could be better in the future. So, if the weakness company is known, the company could do repairs if the opportunity company is known so that the company could utilize the opportunity as well as possible for the progress company. Meanwhile, the threat will be found, so the company must develop a strategy (Tamara, 2016).

Kapoor and Kaur (2017) use SWOT analysis to research the implementation of Basel III in India with results study that advises banks in India to accept Basel III so it will achieve harmonization with standard international. Alalie et al. (2019) study the SWOT analysis of superior competitive, sustainable sector banking in Iraq, showing research results where a SWOT analysis helps sector banking in Iraq identify positive and negative factors and develop a strategy for superior competitive sustainability. Jahan et al. (2022) use perspective SWOT analysis, investment, and determinants to adopt the practice of agroforestry as a mitigation change climate in Bangladesh shows results that although some prominent farmers already used to practice agroforestry, only a few are experienced. In their research, Citta et al. (2019) use SWOT analysis to analyze the influence of financial technology in the banking industry in South Sulawesi. The results show that financial technology application delivers strengths, weaknesses, threats, and opportunities to the banking industry, so banking must increase infrastructure technology information to collaborate with financial technology. Baidowi (2018), in his research, uses SWOT analysis to know the challenges and opportunities of using financial technology in Islamic banking. Research results show that using appropriate financial technology with the regulation will create a good opportunity for increased quality service in Islamic banking. However, it also can become a challenge for banking, where financial technology can swipe institution banking. Ririh et al. (2020) also use SWOT analysis in their research to implement artificial intelligence (AI) in Indonesia on business government and BUMN, with results showing high level AI implementation affected by improvements in effectiveness and efficiency company.

3. METHODOLOGY

The method research used in this study is descriptive qualitative. The research only deciphers responses about situations or events without explaining connection causality, nor does a hypothesis test (Wulannata, 2017). This study describes social engineering with SWOT analysis using knowing strengths, weaknesses, opportunities, and threats owned by government-owned and national private commercial banks with studies cases at Bank Rakyat Indonesia (BRI Bank) and Bank Central Asia (BCA Bank). Bank Rakyat Indonesia (BRI Bank) is a sample of commercial banks owned by the government, and Bank Central Asia (BCA Bank) is a sample of commercial banks private national. BRI Bank and BCA Bank were selected because both belong to Indonesia's Core Capital Bank Group IV category, namely banks with a capital of over Rp 70 trillion. BRI Bank has a core capital value of IDR 256.5 trillion, the largest of other government-owned commercial banks. BCA Bank has a core capital value of IDR 195.1 trillion, the only national private commercial bank in the Core Capital Bank Group IV group (Pahlevi, 2022). The data used in this study are secondary data obtained from studies literature, from annual banking reports 2021 on BRI Bank and BCA Bank websites, books, journal articles, and news. The data collection is done by collecting, reading, and studying various relevant sources to answer research problems.

4. RESULT AND DISCUSSION

Stages in to do SWOT analysis begins with step data collection. These activities are carried out at this stage: collecting data, classifying, and pre-analysis. Data is classed as internal data and external data. Internal data can be obtained from the report finance company, report human resources, report operational activity, and others. Meanwhile, external data could be obtained from market analysis, analysis of competitors, analysis of community, analysis of government, and others. Internal data analysis can be conducted with matrix Internal Factor Analysis Summary (IFAS). Moreover, external data could be analyzed using the matrix External Factor Analysis Summary (EFAS) (Rangkuti, 2016). Based on the results of a literature review from banking annual reports, journal articles, news, and books, it is known that internal and external factors are analyzed with EFAS, IFAS, and SWOT Matrix.

4.1. External Factor Analysis Summary (EFAS) and Internal Factor Analysis Summary (IFAS)

Giving weight to each factor is the maximum total weight is 1 (one). Giving a rating value for a positive factor (strength and opportunity) if the factor is the greatest strength, then it must be given the most significant positive rating, and vice versa. Meanwhile, giving a rating value to a negative factor (weaknesses and threats), if the weakness is the greatest, it must be given the most negative rating, and vice versa (Wardoyo, 2011).

Table 1. EFAS Matrix

Factors strategic external (Opportunity)	Weight	Ratings	Value (Weight x Rating)	Comment
Use of social media	0.40	4	1.60	Social media's utilization helps banks easily educate the public about social engineering.
Support from the government in preventing cyber crime banking	0.60	4	2.40	There are Financial Services Authority (OJK) regulations and governing laws about cyber crime banking
Total	**1**		**4.00**	
Factors strategic external (Threats)				
The low-level literacy of finance and awareness will personal data security in Indonesian society	0.30	-1	-0.30	Protection-related personal data security has become necessary in the digital age.
High-level cybercrime in Indonesia	0.40	-1	-0.40	The high level of cybercrime in Indonesia is an indication of the possibility of more development of social engineering crimes in Indonesia
Conditions and situations social	0.10	-2	-0.20	Attackers cyber capitalize on the momentum of the situation condition social happenings to attack
High-level Internet usage and activities operational banking conducted in a digital way	0.10	-1	-0.10	Ascension digital transactions can trigger more cybercrime
Total	**1**		**-1,00**	
Total EFAS			**3.00**	

Source: Processed data (2022).

Table 4. IFAS Matrix

Factors strategic internal (Strength)	Weight	Ratings	Score (Weight x Rating)	Comment
Build digital transformation has other digital innovations and Implement high-availability banking services by building data centers and cloud technology.	0.20	4	0.80	Government-owned commercial banks and national private commercial banks have built a digital transformation system that works, looking from mobile banking and internet banking as well service other digital innovations at government-owned, commercial banks and national private commercial banks have adopted cloud technology as well as building data centers to give high availability banking services to customers
Have a policy for the security of customer data privacy	0.20	4	0.80	Government-owned commercial banks and national private commercial banks have policy-related

				efforts security and protection of customer data privacy
Have a security program to prevent cybercrime act	0.40	4	1.60	Government owned commercial banks and national private commercial banks have a security program to prevent cybercrime act
Give education to customers related to social engineering and personal data security	0.20	3	0.60	Government-owned commercial banks, and national private commercial banks provide education to customers related to cybercrime, especially social engineering, and also educate customers on related importance of guarding personal data security through various media as well in a manner direct to customer
Total	**1**		**3.80**	
Factors strategic internal (Weakness)				
A large number of customers and employees	0.90	-1	-0.90	Many employees and customers can become threats to social engineering if the knowledge of technology information, especially social engineering and personal data security, still needs improvement.
Total			**-0.90**	
Total IFAS			**2.90**	

Source: Processed data (2022).

From calculations of the EFAS matrix and IFAS matrix, it is known that the score of the IFAS matrix is 2.90; meanwhile, the score of the EFAS matrix is 3.00, which is known as point coordinates. The X axis describes IFAS factors, and the Y axis describes EFAS factors. For the SWOT diagram, the point coordinate is (3.00; 2.90). Thus, it is known that government-owned and national private commercial banks are in quadrant I, which means the company has the opportunities and strengths to utilize them. A strategy must be set to support an aggressive strategy policy (Rangkuti, 2016).

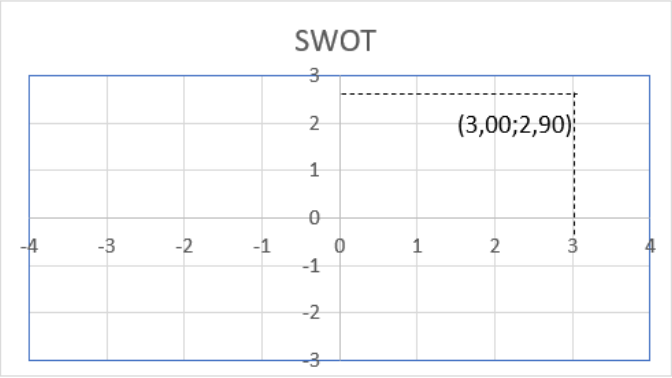

Figure 1. SWOT Diagram

4.2. SWOT Matrix

Diagram 1. SWOT Matrix

IFAS	STRENGTHS (S)	WEAKNESSES (W)
EFAS	1. Build digital transformation with internet banking, mobile banking, and service other digital innovations and implement high availability banking services by building a data center and cloud technology. 2. Have a policy for security and customer data privacy. 3. Have a security program to prevent to follow cybercrime. 4. Give education to customers related to social engineering and personal data security.	1. A larger number of employees and customers.
OPPORTUNITIES (O) 1. Use of social media 2. Support from the government in preventing cyber crime banking	**S-O STRATEGY** 1. Build technology information on banking by established standards and rules determined by the Financial Services Authority. 2. Active use of social media as a means to give education to customers.	**W-O STRATEGY** 1. Active training to employees related to system technology information and cybercrime. 2. Utilize and apply reasonable existing regulations and rules set by the government utilization of technology information.
TREATHS (T) 1. The low finance literacy and awareness level will affect personal data security in Indonesian society. 2. High cyber crime in Indonesia. 3. Conditions and situations social 4. High level Internet usage and activities operational banking digitally	**STRATEGY S-T** 1. Active monitor and optimize data and network security technology banking information 2. Suppressing the circulation of social issues on behalf of banks that can trigger social engineering	**W-T STRATEGY** 1. Add expertise and knowledge about related technology information and risks for employees. 2. Increase literacy finance and awareness of personal data security customers and employees.

Source: Processed data (2022).

Strength:

Build digital transformation and other digital innovation services and implement high-availability banking services by building data centers and cloud technology.

Based on the 2021 annual report issued by government-owned and national private commercial banks, the two banks developed a digital transformation of the business system. Government-owned commercial banks build a capability-driven digital strategy framework to develop grouped digital products by digitizing core, digital ecosystem, and new digital prepositions. Innovations made by government-owned commercial banks in their business processes are seen in the presence of several digital products. Besides, government-owned commercial banks' digital products strive to develop and strengthen system technology information with 3 (three) data center (DC) facilities that have reached tier 3, supporting active DC continuity business when disaster occurs to support the high availability of banking services. Government-owned commercial banks also started utilizing cloud technology to increase capability infrastructure to support the business's growth and give the best service to customers (Bank Rakyat Indonesia, 2021).

Temporarily, national private commercial banks also consistently invest in system technology information, system security, and innovation to provide solution banking for customer needs. Digital innovation carried out by national private commercial banks in their business processes is seen from the availability of digital products. National private commercial banks also support the presence of bank digital products, implement a high availability system strategy by adopting cloud technology, building a new data center, and modernizing infrastructure and security technology information well as forming team special that stand by 24/7 for guard availability systems and services in serve transaction big customers, national private commercial banks ensures IT systems always active with no downtime (Bank Central Asia, 2021). Research conducted by Owusu-tucker (2019), Yenew (2019), and Cheng et al. (2022) in their research for evaluating the role of cloud technology in reaching convenience sector strategy banking shows that cloud utilization makes more infrastructure flexible and fast time provision, saving time and money, and risk operational. Banking that adopts cloud technology has more profit with more low costs. However, it increases the risk of operational banking.

Have a policy for the security of customer data privacy.

Government-owned commercial banks and national private commercial banks have their own and apply policies for the security and protection of customer data privacy, as loaded in the report annual 2021. National private commercial banks to protect customer data, implement solution internal data security policies, prevent data loss, procedures, and technology for data leaks, and disguise sensitive data to prevent data leaks. National private commercial banks also use machine learning and artificial intelligence (AI) to detect anomalies in data access (Bank Central Asia, 2021). Government-owned commercial banks also have set policies and guidelines that safeguard customer data throughout operational work units listed in various internal regulations, e.g., external regulation compliance, data secrecy policy, IT security policy, etc.

Besides that, government-owned commercial banks also have applied a policy for asking permission from customers to perform the opening process account related to agreement from candidate customers for the use of candidate data customers necessity offer bank products and services. Government-owned commercial banks have instructed the implementation of bank secrets, delayed transactions, and reporting to the third (Bank Rakyat Indonesia, 2021). Rinaldi and Krisnadi (2019) stated that open information demands industry players to protect company and personal data. Abubakar and Handayani (2022) state that reinforcement and implementation regulation are crucial for preventing the potency of the risks involved in technology information and data protection. In their research, Palinggi and AlloLinggi (2020) state that the constitution on personal data protection could solve ITE issues and minimize the potency of internal data leaks in the Fintech business in Indonesia.

Have a security program to prevent cybercrime.

Government-owned and national private commercial banks have a security program to prevent cybercrime, as loaded in the 2021 annual report. Government-owned commercial banks have policy-regulated cyber security related where bank information whose cybersecurity policies are arranged based on standard ISO27001:2013, PCI DSS, and POJK regulatory policy No. 38/POJK.03/2016 concerning Application Management Risk in the use of technology information by Commercial Banks and government-owned commercial banks has part particular about Security Operation Center (SOC), which monitors cyber threats continuously for 24 hours, every week, 365 days. The bank has a procedure for handling incident security information and team responsive incident corresponding cyber (CSIRT). Bank cooperation with experienced international security experts in facing cyber-attacks. Bank also confirmed that all the talent in the security field is already standardized, certified, and has the appropriate skills standard international. For facility technology, government-owned commercial banks' information and products during 2019-2021 have succeeded in getting International Standards Certification such as ISO and PCI. And have successful digital apps that obtain ISO 20000-1:2018 recommendations. Government-owned commercial banks also have a brand protection program on duty to monitor Brand abuse on social media. The bank also cooperates with third parties to identify bank system vulnerabilities and review bank information security periodically independently through vulnerability assessments, penetration tests, and simulations of cyberattacks (Bank Rakyat Indonesia, 2021).

National private commercial banks also try to prevent the potency threat cyber, where the bank is committed to increasing the protection of infrastructure, network, application, and data, reinforcing security monitoring centers and management risk security cyber with keep going strengthen where data security system management security bank information is successful get ISO 27001:2013 certification. Besides that, national private commercial banks also get PCI DSS 3.2.1 certification for data centers (global data security), ISO 20000-1:2018 for management IT services, ISO 90001:2015 for network data centers, assurance IT quality & contact centers, ISO 20000-1:2011 for network data center & management incident. To ensure the protection of transactions, national private commercial bank customers take advantage of the latest technology to protect internet banking transactions, including the ability to detect transactions intercepted by "parties third." Besides that, the bank also makes use of its Security Orchestration and Automation Response (SOAR)

arranges response in a manner automatic for all detected anomalies. Bank has started using Security Information and Event Management (SIEM) to find patterns or connections from a few incidents for the next possible suspicious activity to anticipate and deal with related transaction banking fraud. Bank periodically operates simulations or practices incident security to ensure deep bank readiness to face cyber-attacks and increase cyber resilience. The bank also improves governance security cyber through application policies, standards, procedures, and practices throughout the organization (Bank Central Asia, 2021).

In their research, Masyrifah et al. (2020) mention that the application ISO standard 2700:2013 has influenced positive and significant personal data security user technology financial. Meanwhile, the International Standard, The Payment Card Industry Data Security Standard (PCI DSS), or the mandatory PCI security standard implemented by each stakeholder interest, where are requirements technical and operational stipulated by the Standards Board Security Industry Card Payment for protect holder data card (Rofi, 2022). Research conducted by Syafie (2022) shows that in operational banking that requires banks to interact with society, in the era of the current industrial revolution, this protects systems and networks could be implemented cyber security harder or strengthening security network and system.

Give education to customers related to social engineering and personal data security.

Social engineering and personal data security of government-owned commercial banks and national private commercial banks actively educate customers and workers to prevent this from happening. Government-owned commercial banks routinely conduct a care program data and information security through posters and internal publications, e-learning and webinars, and phishing campaign emails to all bank employees. Temporarily, to educate customers, government-owned commercial banks use the advantages of social media via YouTube, Twitter, Instagram, and print media and give education directly to customers when they visit the bank (Khoirunnisaa, 2022). National private commercial banks consistently prevent social engineering crimes and personal data security by increasing customer awareness through webinars, social media, and company website activities and implementing e-learning, phishing, and smishing simulations for all employees (Bank Central Asia, 2021). Junaedi (2017) educates customers and workers rated capable of preventing follow crime through social engineering. Aldawood and Skinner (2019) state the importance of giving training and education to employees related to social engineering to prevent the following of crime in social engineering.

Weaknesses:

Amount large employees and customers.

Junaedi (2017) also mentions that four groups of individuals in companies are often the target of crime social engineering, i.e., receptionist or help desk, supporter technical from the technology division information, system administrators and computer users, partners work or company vendors, and new employees. Sometimes, the perpetrator of social engineering could pretend to become a bank employee to commit a social engineering crime against the customer. Airehrour et al. (2018) state that social engineering attacks only depend on factor humans. Attackers

could use behavior man to attack the system information by manipulating targets. Chetioui et al. (2021) also mention that social engineering attacks the vulnerability of people with a focus on how people think, behave, and react. That could conclude that large employees and customers can be one bank's weakness face action social engineering if no accompanied knowledge will follow crime social engineering and its importance guard data security. It supported research conducted by Aldawood and Skinner (2019), which states that employees have an important role in protecting interest organizations from social engineering attacks.

Opportunity:

Use of social media

Social media users in Indonesia are very high, according to a Hootsuite survey (We are Social) (Indonesia Digital Report, 2019). It is known that 150 million Indonesians use social media (Anggraeni and Djuwita, 2019). In his research, Setyadi (2020) states that social media means communication between the company and the consumer. His research shows four classifications of relative content dominant in interaction companies with consumers on Twitter, including questions, complaints, education, and collaboration. Nur (2021), in his research, states that social media is a means for giving information to the public both online or manually during the COVID-19 pandemic. Using social media to give information and education, government-owned commercial banks and national private commercial banks can prevent crime through social engineering because there are more social media users than expected. More customers and the public who understand and know related social engineering could be spared from social engineering attacks. This is in line with the results of research conducted by Fitriani (2021), which states that using social media as a suggestion of content digital education helps its users add knowledge and outlook and helps the user understand the theory education provided.

Support from the government in preventing cyber crime banking.

According to Constitution Number 19 of 2016, which is a change from Constitution Number 11 of 2008 concerning Information and Transactions Electronic state in Indonesia, cybercrime is crimes with illegal activity, act-related penalties with interference, act criminal facilitates prohibited acts. It acts as criminal forgery of information or document electronics. Cybercrime in service finance and banking is social engineering and skimming (Ratulangi et al., 2021). Supported by Management Consultative Paper Risk Security Commercial Bank Cyber issued by the Financial Services Authority in 2021, which contains direction settings management risk security cyber for Commercial Banks (Otoritas Jasa Keuangan, 2021). Besides, the Financial Services Authority also issued Regulation Financial Services Authority Republic of Indonesia Number 11/POJK.03/2022 Concerning Administration Technology Information by Commercial Banks expected to increase resilience and readiness of commercial bank operations in maintenance technology information. Regulations could become a reference at a time of support for banking to keep doing security and protection in maintenance technology information on banking to avoid and detect cyber crime attack (Maizal Walfajri, 2022).

Threats:

The low-level finance literacy and awareness will personal data security in Indonesian society.

In 2019, according to Financial Services Authority data, the finance literacy index among Indonesian people increased by 38.03%. It experiences an increase if compared to years before. However, it still belongs low. Financial literacy is understanding features, benefits, risks, rights, and obligations related to product and service finance (Kusnandar, 2022). A survey conducted by Saptoyo and Galih (2022) shows that from 1,014 respondents in 34 provinces in Indonesia, as many as 46.5% of respondents do not know and realize online activity is an important data source. From the data above, it could be concluded that Indonesian people's literacy and awareness of personal data security is still low. It naturally could become a cybercrime threat, as disclosed by the Ministry of Communication and Informatics (Pratiwi, 2021). This is also supported by research conducted by Wicaksana et al. (2020), which mentions robust protection systems and technologies for data security. However, the human factor becomes vital security information.

High cybercrime in Indonesia.

Data from the Operations Center Security National Cyber revealed that in 2021, as many as 1.6 billion cyber-attacks occurred in Indonesia. One of the most frequent sectors caught problems is sector banking, with social engineering as a motive for cybercrime. Junaedi (2017) states that high cybercrime could threaten banking, where banking is one sector of potential cyber-attack.

Conditions and situations are social.

Perpetrator social engineering often utilizes situations and conditions middle social in society to attack, as mentioned by Hanafi (2021) in his research that amidst the COVID-19 pandemic, anxiety and worry about related health and economic triggers make highly public use of system electronics and transactions electronics in the end exploited by the perpetrator's cyber crime for to do cyber crime like design attack with use COVID-19 theme for trap society and then To do data theft. Alzahrani (2020) also states that during the COVID-19 pandemic, cybercrime exploitation worries people for stealing confidential information and data to do social engineering. Herdiana et al. (2021) mention that during the COVID-19 pandemic, three types of cyber threats are fraud and phishing, malware, and denial service distributed (DDoS). Hijji and Alam (2021) also mention that during the Covid- 19 pandemic, several types of social engineering attacks, i.e., phishing, scamming, spamming, smishing, and vishing, combined with the most frequently used socio-technical methods: fake emails, websites, and mobile applications.

High Internet usage and activities operational banking conducted digitally.

Parulian et al. (2021), in their research, mention that existing online technology requires the public to be more careful because of the higher risk they will face, which is cyber-attacks. Machine learning and artificial intelligence cause social engineering attacks to be increasingly efficient and aggressive (Wang et al., 2021). Progress technology caused banking to adopt artificial intelligence, delivering a positive impact that could give convenience and efficiency to customers and systems banking. However, behind the positive impact, it turns out there is also a negative

impact where utilization of technology information on where the perpetrators are cybercrime potentially steal customer data or company (Nathanael and Puspita, 2021). Research conducted by Arofah and Priatnasari (2020) shows that Internet banking positively and significantly affects cybercrime banking in Tegal City.

Based on the analysis of the results with the use of a SWOT matrix of several internal factors, in the form of strengths and weaknesses, as well as factor external form opportunities and threats, the strategy can carry out by government-owned commercial banks and national private commercial banks companies are building technology information on banking in accordance established standards and rules determined by the Financial Services Authority, active use social media as means give education to the customer, active doing training to employees related system technology information and cyber crime, utilize and apply with reasonable existing regulations and rules set by the government related banks utilization technology information, active monitor and optimize data and network security technology banking information. Suppressing the circulation of social issues on behalf of banks that can trigger social engineering, add expertise and knowledge of related technology information and risks to employees, and increase literacy finance and awareness of personal data security customers and employees.

5. CONCLUSION

The banking sector is potentially a target for cyberattacks with an economic motive. A social engineering attack is one type of cyberattack in the banking sector. Social engineering research with SWOT analysis on government-owned and national private commercial banks shows the strengths, weaknesses, opportunities, and threats that must prevent social engineering from occurring. The study results also recommend several strategies considered effective in overcoming social engineering attacks for banks. Researchers realize that many things still need to be improved in studying this. However, the expected study could contribute to and benefit readers and researchers on studies related to social engineering attacks in banking. Moreover, for stakeholders' policy from neither company banking nor government, this study could become a consideration in preventing crime through social engineering in banking.

REFERENCES

Abubakar, L. and Handayani, T., 2022. Penguatan regulasi: Upaya percepatan transformasi digital perbankan di era ekonomi digital. *Masalah-Masalah Hukum,* 51(3), pp. 259–270. doi: 10.14710/mmh.51.3.2022.259-270.

Airehrour, D., Nair, N. V. and Madanian, S., 2018. Social engineering attacks and countermeasures in the New Zealand Banking System: Advancing a user-reflective mitigation model. *Information (Switzerland),* 9(5). doi: 10.3390/info9050110.

Alalie, H. M., Harada, Y. and Noor, I. M., 2019. Impact of strength, weakness, opportunities, threats (SWOT) analysis on realizing sustainable competitive advantage in banking industry sector in Iraq*. International Journal of Scientific*

and Research Publications (IJSRP), 9(3), p. p8708. doi: 10.29322/ijsrp.9.03.2019.p8708.

Aldawood, H. and Skinner, G., 2019. Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. *Future Internet,* 11(3). doi: 10.3390/fi11030073.

Alzahrani, A., 2020. Coronavirus social engineering attacks: Issues and recommendations. *International Journal of Advanced Computer Science and Applications,* 11(5), pp. 154–161. doi: 10.14569/IJACSA.2020.0110523.

Anggraeni, R. and Djuwita, D, 2019. Analisis pemanfaatan social media marketing terhadap customer loyalty yang menggunakan brand trust sebagai variabel mediasi. *Jurnal Riset Manajemen dan Bisnis (JRMB) Fakultas Ekonomi UNIAT,* 4(3), pp. 445–455. Available at: http://jrmb.ejournal-feuniat.net/index.php/JRMB/article/view/304.

Arofah, N. R. and Priatnasari, Y., 2020. Internet banking and cyber crime: A case study in national banking. *Jurnal Pendidikan Akuntansi Indonesia,* 18(1), pp. 107–119.

Baidhowi, B., 2018. Sharia banking opportunities and challenges in the digital era. *Proceedings of the 1st International Conference on Indonesian Legal Studies (ICILS 2018)*. doi:10.2991/icils-18.2018.30.

Bank Central Asia, 2021. *Annual Report 2021 - Innovation and Collaboration for a Better Tomorrow.* Available at: https://www.bca.co.id/-/media/Feature/Report/File/S8/Laporan-Tahunan/2022/20220217-buku-ar-bca-2021-EN.pdf.

Bank Rakyat Indonesia, 2021. Digitalisasi: Go Smaller, Go Shorter, Go Faster. Available at: https://www.ir-bri.com/newsroom/a970f6d946_3a26c95533.pdf

Bidari, A. S., Simangunsong, F. and Siska, K., 2020. Sektor perbankan di COVID-19', *Jurnal Pro Hukum : Jurnal Penelitian Bidang Hukum Universitas Gresik,* 9(1), pp. 1–9. doi: 10.55129/jph.v9i1.1129.

Cheng, M., Qu, Y., Jiang, C. and Zhao, C., 2022. Is cloud computing the digital solution to the future of banking? *Journal of Financial Stability,* 63, p. 101073. doi:10.1016/j.jfs.2022.101073.

Chetioui, K., Bah, B., Alami, A.O. and Bahnasse, A., 2022. Overview of social engineering attacks on social networks. *Procedia Computer Science,* 198, pp.656-661 doi: 10.1016/j.procs.2021.12.302.

Citta, A.B., Dekrita, Y.A., Yunus, R. and Ridha, A., 2019, August. SWOT analysis of financial technology in the banking industry of south sulawesi: Banking survey in South Sulawesi*. In 3rd International Conference on Accounting, Management and Economics 2018 (ICAME 2018)*, pp. 119-126. Atlantis Press. doi: 10.2991/icame-18.2019.13.

Fitriani, Y., 2021. Pemanfaatan media sosial sebagai media penyajian konten edukasi atau pembelajaran digital*. Journal of Information System, Applied, Management, Accounting and Research,* 5(4), pp. 1006–1013. doi: 10.52362/jisamar.v5i4.609.

Grimes, R. A., 2020. Social engineering attacks. *Hacking Multifactor Authentication,* 4(6), pp. 259–273. doi: 10.1002/9781119672357.ch12.

Gürel, E., 2017. SWOT analysis: A theoretical review. *Journal of International Social Research,* 10(51), pp. 994–1006. doi: 10.17719/jisr.2017.1832.

Hanafi, F., 2021. Serangan siber di masa pandemi: Banyak agresi minim proteksi. *Jurnal Almishbah: Jurnal Ilmu Dakwah dan Komunikasi*, 17(1), pp. 1–20.

Herdiana, Y., Munawar, Z. and Indah Putri, N., 2021. Mitigasi ancaman resiko keamanan siber di masa pandemi COVID-19. *Jurnal ICT: Information Communication & Technology,* 20(1), pp. 42–52. doi: 10.36054/jict-ikmi.v20i1.305.

Hijji, M. and Alam, G., 2021. A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions. *IEEE Access,* 9, pp. 7152–7169. doi: 10.1109/ACCESS.2020.3048839.

Indonesian Bankers Association, 2015. Risk Management (First Edition). PT Gramedia Pustaka Tama: Jakarta.

Jahan, H., Rahman, M.W., Islam, M.S., Rezwan-Al-Ramim, A., Tuhin, M.M.U.J. and Hossain, M.E., 2022. Adoption of agroforestry practices in Bangladesh as a climate change mitigation option: Investment, drivers, and SWOT analysis perspectives. *Environmental Challenges,* 7, p.100509. doi: 10.1016/j.envc.2022.100509.

Junaedi, D. I., 2017. Antisipasi dampak social engineering pada bisnis perbankan. *Infoman's,* 11(1), pp. 1–10. doi: 10.33481/infomans.v11i1.13.

Kapoor, S. and Kaur, M., 2017. Basel III norms: A SWOT and TOWS approach. *Vision,* 21(3), pp. 250–258. doi: 10.1177/0972262917716759.

Kasmir, 2019. *Bank dan Lembaga Keuangan Lainnya.* Revision Edition. PT Raja Grafindo Persada: Jakarta.

Khoirunnisaa, J., 2022. *Marak Penipuan & Kejahatan Siber, Ini Upaya BRI Lindungi Data Nasabah,* detikNews, 20 September. Available at: https://news.detik.com/berita/d-6302038/marak-penipuan--kejahatan-siber-ini-upaya-bri-lindungi-data-nasabah.

Kusnandar, V. B., 2022. *Tingkat Literasi Keuangan Masyarakat Indonesia Masih Rendah*, Katadata.co.id, p. 2021. Available at: https://databoks.katadata.co.id/datapublish/2022/09/26/tingkat-literasi-keuangan-masyarakat-indonesia-masih-rendah.

Masyrifah, I. and Oktaroza, M.L., 2022, January. Pengaruh Penerapan Standar ISO 27001: 2013 terhadap Keamanan Data Pribadi Pengguna Teknologi Finansial. *In Bandung Conference Series: Accountancy* (Vol. 2, No. 1, pp. 604-610).

Nathanael, J. J. and Puspita, N. Y., 2021. Perlindungan data nasabah terkait pemanfaatan artificial intelligence dalam aktifitas perbankan di Indonesia. *Jurnal Komunikasi Hukum,* 7, pp. 387–402.

Nur, E., 2021. Nur, E., 2021. Peran media massa dalam menghadapi serbuan media online. *Majalah Semi Ilmiah Populer Komunikasi Massa,* 2(1), 01 Juni, pp. 51–64. Available at: https://jurnal.kominfo.go.id/index.php/mkm/article/download/4198/1561.

Otoritas Jasa Keuangan, 2019. *Cetak Biru Transformasi Digital Perbankan*, pp. 9–25. Available at: https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/Cetak-Biru-Transformasi-Digital-Perbankan.aspx

Otoritas Jasa Keuangan, 2021. *Consultative Paper 2021.* Available at: https://www.ojk.go.id/id/kanal/perbankan/implementasi-basel/Documents/Pages/Consultative-Papers/Consultative%20Paper%20Manajemen%20Risiko%20Keamanan%20Siber%20Bank%20Umum.pdf

Owusu-tucker, E., 2019. An exploratory study assessing the role cloud computing has in achieving strategic agility with the banking industry. Presented at the Hawaii International Conference on System Sciences (HICSS-51), Hawaii, 3rd-6th January 2018, pp. 0–10. Available at: https://hdl.handle.net/2134/26905

Pahlevi, R., 2022. *Ini 4 Bank Indonesia Terbesar Berdasarkan Nilai Modal Inti.* Available at: https://databoks.katadata.co.id/datapublish/2022/08/26/ini-4-bank-indonesia-terbesar-berdasarkan-nilai-modal-inti

Palinggi, S. and Allolinggi, L. R., 2020. Analisa deskriptif industri fintech di Indonesia: Regulasi dan keamanan jaringan dalam perspektif teknologi digital. *Ekonomi dan Bisnis,* 6(2), pp. 177–192. doi: 10.35590/jeb.v6i2.1327.

Parulian, S., Pratiwi, D. A. and Cahya Yustina, M., 2021. Ancaman dan solusi serangan siber di Indonesia. *Telnect,* 1(2), pp. 85–92. Available at: https://ejournal.upi.edu/index.php/TELNECT/article/view/40866.

Pratiwi, T. H., 2021. *Pentingnya Pelindungan Data Pribadi di Era Digital,* aptika.kominfo.go.id, 17 October. Available at: https://aptika.kominfo.go.id/2021/10/pentingnya-pelindungan-data-pribadi-di-era-digital/.

Rangkuti, F., 2016. *Analisis SWOT: Teknik Membedah Kasus Bisnis Cara Perhitungan Bobot, Rating, dan OCAI.* PT Gramedia Pustaka Utama: Jakarta.

Ratulangi, C., Wahongan, A. and Mewengkang, F., 2021. Tindak pidana cyber crime dalam kegiatan perbankan. *Lex Privatum,* IX(5), pp. 179–187.

Rinaldi, R. and Krisnadi, I., 2019. Analisis dampak revolusi industri 4.0 terhadap keamanan data digital. Universitas Mercubuana, Manjemen ICT, pp. 1–8.

Ririh, K.R., Laili, N., Wicaksono, A. and Tsurayya, S., 2020. Studi komparasi dan analisis SWOT pada implementasi kecerdasan buatan (artificial intelligence) di Indonesia. *Jurnal Teknik Industri,* 15(2), pp.122-133. Available at: https://ejournal.undip.ac.id/index.php/jgti/article/view/29183.

Rofi, N., 2022. Analisis manajemen resiko operasional pengguna aplikasi e-wallet "Dana" dengan implementasi PCI DSS. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial,* 9(5), pp.1786-1794.

Saptoyo, R. D. A. and Galih, B., 2022. *KABAR DATA: Kesadaran Keamanan Data Pribadi Masyarakat dalam Angka,* Kompas.com. Available at: https://www.kompas.com/cekfakta/read/2022/02/10/090900082/kabar-data-kesadaran-keamanan-data-pribadi-masyarakat-dalam-angka?page=all.

Salahdine, F. and Kaabouch, N., 2019. Social engineering attacks: A survey. *Future Internet,* 11(4). doi: 10.3390/FI11040089.

Setyadi, D.K., 2019. Peran Twitter dalam digital customer relation management di industri perbankan. *Journal Communication Spectrum: Capturing New Perspectives in Communication,* 9(2), pp.110-124.

Syafie, S., 2022. Kesiapan teknologi informasi perbankan hadapi revolusi industri era 4.0. *JATISI (Jurnal Teknik Informatika dan Sistem Informasi),* 9(1), pp. 533–546. doi: 10.35957/jatisi.v9i1.1540.

Tamara, A., 2016. Implementasi analisis SWOT dalam strategi pemasaran produk mandiri tabungan bisnis. *Jurnal Riset Bisnis dan Manajemen,* 4(3). 395–406.

Walfajri, M., 2022. *Perkuat Pengawasan IT Perbankan, OJK Rilis POJK 11 Tahun 2022*, Available at: https://keuangan.kontan.co.id/news/perkuat-pengawasan-it-perbankan-ojk-rilis-pojk-11-tahun-2022

Wang, Z., Sun, L. and Zhu, H., 2020. Defining social engineering in cybersecurity. *IEEE Access,* 8, pp. 85094–85115. doi: 10.1109/ACCESS.2020.2992807.

Wang, Z., Zhu, H. and Sun, L., 2021. Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access,* 9, pp. 11895–11910. doi: 10.1109/ACCESS.2021.3051633.

Wardoyo, P., 2011. *Alat Analisis Manajemen.* First Edition, Semarang University Press, ISBN 978.602.9019.26.1.

Wicaksana, R.H., Munandar, A.I. and Samputra, P.L., 2020. Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 (A Narrative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid-19 Pandemic). *JURNAL IPTEKKOM (Jurnal Ilmu Pengetahuan & Teknologi Informasi),* 22(2), pp.143-158. Available at: http://dx.doi.org/10.33164/iptekkom.22.2.2020.143-158.

Wulannata, A. I., 2017. Analisis SWOT implementasi teknologi finansial terhadap kualitas layanan perbankan di Indonesia. *Jurnal Ekonomi Dan Bisnis,* 20(1), pp. 133–144.

Yenew, M. (2019) 'Designing Cloud Computing Architecture for Bank Industry : The Case of Dashen Bank', Digitalcommons.Kennesaw.Edu, pp. 1–8.