The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

SYNERGY OF THE NATIONAL POLICE IN BUILDING COOPERATION WITH THE BANKING SECTOR TO INCREASE DISCLOSURE OF SOCIAL ENGINEERING CASES IN THE JURISDICTION OF THE CIMAHI POLICE STATION

TONO LISTIANTO [1]* and CHAIRUL MURIMAN SETYABUDI [2]

[1, 2] Police Science Studies, School of Strategic and Global Studies, Universitas Indonesia, Indonesia.
Email: [1] tonolistian@gmail.com (Corressponding Author) , [2] cak_iir1966@yahoo.com

Abstract

Information technology is developing rapidly along with the progress of community development, so it is difficult to avoid it. IT is any technology that allows humans to create, transform, store, communicate, and disseminate information. Unfortunately, not everyone uses the internet for a good cause. Many people use social networks to commit crimes, such as cybercrime in the form of social engineering or other forms of crime, especially in the jurisdiction of Cimahi Police Station. Therefore, synergy of the National Police is needed in building cooperation with the banking sector to increase the disclosure of social engineering cases in the jurisdiction of the Cimahi Police Station. The theories used include Organizational Synergy Theory, Interorganization Theory, Organization Communication Theory, Organization Behavior Theory, and Strategic Management Theory. This research method is carried out through a skin approach, with data collection techniques through interviews, observation, and data documentation. The results showed that cooperation between the National Police and the banking sector in combating social engineering cases is very important because this crime involves social manipulation to steal sensitive information. The National Police must actively communicate, provide resources, and share information with the banking sector. Public education and strong law enforcement are also important to raise awareness about social engineering risks. This cooperation faces obstacles such as data security issues, privacy regulations, differences in priorities, and costs. To overcome this, a commitment to data security, compliance with privacy regulations, education, and training is required. Transparency, strategic partnerships, maintaining confidentiality, understanding mutual benefits, leadership support, periodic evaluations, and cooperation with third parties where needed are steps that can help overcome these obstacles. Implementation strategies that can enhance the synergy and effectiveness of cooperation include the formation of special teams, regular information exchanges, joint training, efficient reporting systems, joint protocol development, and provision of additional resources, public education campaigns, and use of security technology, cooperation with relevant security agencies, and periodic evaluation and monitoring.

Keywords: Social Engineering, Banking Sector, Synergy.

INTRODUCTION

Information technology (IT) is developing rapidly along with the progress of community development, so it is difficult to avoid its development. IT is any technology that allows humans to create, transform, store, communicate and disseminate information. IT capabilities combine high-speed computing and data, voice, and video communications. IT consists of personal computers (laptops), telephones, televisions, electronic household appliances, and modern handheld devices such as mobile phones (Moses, 2019). Therefore, current IT advances are significant in supporting business activities and connecting every business to information

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

technology (IT) systems (Mosin, et al., 2010).

One of the advancements of IT systems is the existence of the internet, which is now a global communication system, which allows everyone around the world to meet and talk about almost anything. The internet has become a medium of communication, which is done through various media available on it. The internet provides various social media platforms for positive and negative reasons and has become the order of the day because nowadays, the world is so tied to the internet. Unfortunately, not everyone uses the internet for a good cause. Many people use social networks to commit crimes, such as cybercrime, in the form of social engineering (social engineering) or other forms of crime. Thus, all internet site users must be vigilant to protect themselves (Rusnaeni, Kaouthar, et al., 2021).

IT security threats can be observed in one form such as social engineering which is increasingly rampant. According to Wenni, et al., (2022), social engineering attacks manipulate victims by attacking the weakest link. Social engineering requires that the victim stand in an asymmetric knowledge relationship with the attacker, who uses this asymmetry to establish technocratic control over the victim. Social engineering is one of the few types of attacks that can be classified as non-technical attacks in general, but at the same time can be combined with technical types of attacks such as spyware and Trojans more effectively. Humans can be easily manipulated to provide information or other details that may be useful to the attacker (Islam, 2018).

Lindiwe T. Hove (2020), also explains that social engineering allows malicious hackers to gain unauthorized access to an organization's network; user accounts and emails; databases; smart devices; and electronics, such as laptops, personal webcams, and sensors, including network connectivity that allows all these objects to exchange data. These hackers use various methods to attack social engineering (Comia, 2017).

According to The National Institute of Standards and Technology (NIST), social engineering is an attempt to trick someone into revealing information (such as passwords) to attack a system or network. Successful social engineering attacks rely on targets being manipulated or tricked into revealing personal information. Social engineering attacks have evolved into phone calls, emails, and face-to-face interactions. Social engineering attack methods include impersonation, social engineering attacks on online communities or social media, automated social engineering, and semantic attacks. Various types of social engineering develop along with the spread of information technology (Wenni, et al., 2022).

These types of social engineering attacks can be classified into two categories according to which entity is involved: human or software. They can also be classified into three categories according to how the attack is carried out: social, technical, and physical-based attacks. Analyzing various classifications of existing social engineering attacks can also be classified into two categories, namely direct and indirect main attacks (Fatima and Naima, 2019).

Attacks classified in the first category use direct contact between the attacker and the victim to carry out the attack. They refer to attacks carried out through physical contact or eye contact or voice interaction. They may also require the presence of attackers in the victim's work area

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

to carry out attacks. These attacks include physical access, shoulder crawling, trash can diving, phone social engineering, pretexts, impersonation on help desk calls, and theft of important documents. Attacks classified in the indirect category do not require an attacker's presence to launch an attack. The attack can be launched remotely via malware software carried by e-mail attachments or SMS messages. These attacks include phishing, fake software, Pop-Up windows, ransomware, SMSishing, online social engineering, and social reverse engineering (Fatima and Naima, 2019).

Similar actions in finding ways to reduce social engineering threats are currently also being carried out by the Cimahi Regional Police. Cimahi Police has the authority to carry out these actions based on Law Number 2 of 2002 concerning the National Police of the Republic of Indonesia, Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (PP PSTE), Decree of the Minister of Communication and Information Technology Number 5 of 2020 concerning Guidelines for Handling Negative Content, and Telegram-2055 Letter concerning Notification of Disclosure of Bank Secrets and Assets.

However, the problems found in the field related to various actions taken by the Cimahi Police in making these efforts did not receive a good response by the banks, which so far can be seen in the example of rejection cases as can be observed in the letter from the CIMB bank with Number 008/SKR/BCD/III/2003 which is a reply to the letter filed by the Cimahi Police at letter number No. R/704/11/2023/Sat Reskrim dated March 16, 2023 regarding Request for Mobile Number, data related to withdrawals or transactions and referring to Letter No. 8/720/11/2023/Sat Reskrim dated March 16, 2023 regarding Request for transaction data related to account number 707224064500 in Andre's name and account number 707228232200 in the name of Nurbahagia SE, which gave the refusal due to the reason that the data was included in the Bank's confidentiality.

This fact shows the complexity of revealing social engineering cases by the Cimahi Regional Police. This is due to factors such as strict legal requirements to be used to disclose bank transaction data, which must involve submitting an official application to the bank customer and a license from the Financial Services Authority (OJK) which further has an impact on slow data access and protection of privacy and confidentiality of bank customer data; The technical complexity of the information systems used in locating, examining, and analyzing relevant transaction data requires sufficient time and technical expertise in gathering robust evidence to support the case for social engineering, which involves in-depth analysis of bank transaction data related to the attack. This process can be time-consuming, especially if there are many transactions that need to be traced and analyzed.

To overcome this obstacle, the Cimahi Regional Police as law enforcement must establish close cooperation with the Banking to support each other in investigating social engineering cases. Therefore, synergy is needed between the National Police and the Banking sector in building cooperation to improve the disclosure of social engineering cases in the jurisdiction of the

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

Cimahi Police Station so that Cimahi Police Investigators can access the data needed from the banking sector quickly and precisely to uncover social engineering cases. With good cooperation, the banking sector can help provide access and facilitate the process of collecting the necessary data, thus speeding up the investigation and investigation of the case. Through this synergy, Cimahi Police can also obtain information about the modus operandi of social engineering and Cimahi Police investigators can also interact directly with customers. This synergy can also provide benefits to the community so that together they can increase public awareness about the risks of social engineering and how to protect themselves from the threat of social engineering crimes. In addition, through good cooperation, Cimahi Regional Police and the banking sector can exchange intelligence information about social engineering attacks. This information can help Cimahi police analyze attack patterns, identify perpetrators, and take more effective preventive measures. In addition, this exchange of information can also strengthen the banking sector's capacity to deal with such attacks.

THEORETICAL FOUNDATION

1. Organizational Synergy Theory

Johan and Helen (2021) explain synergy as a concept introduced in the 1960s in the field of strategic management. Johan and Helen (2021) describe synergy as the superior use of resources to better adapt to a changing environment with increased competitive pressure. A common illustration of synergy is two integrated units wanting to achieve more than separate units can. Synergy is one of the building blocks in corporate strategy and during the 1960s and early 1970s, and synergy is the motive of a company's strategic development through diversification.

Most mergers and acquisitions (M&A) models evaluate synergies in acquisitions from the perspective of a company's financial development such as share price, revenue, investment or sources of value creation as evaluated by performance measurements. Synergy is conceptualized around return on investment using four main categories of synergies: sales, operations, investment, and management. Synergy encompasses a wide range of perspectives including creating value, increasing power of profitability, sharing competencies and capabilities, managing purchasing synergies, strength of market-related performance over cost savings, acquisition results measured through different types of performance or effects on other stakeholders, integration processes related to long-term company performance, potential synergies as an effect of the duration of the integration period, degree of autonomy of goals and potential synergies, and the effect of managers on acquisition performance (Wouter, Luis and Robert, 2008).

Management implemented by the organization can identify potential synergies early in the acquisition process through integrated critical activities early on to realize synergies. These activities may include sharing technology, production resources or coordinating marketing and distribution. There are several potential difficulties in realizing the synergies referred to in the post-acquisition phase, namely the acquisition motive may change the expected results and there may be integration issues that affect the potential to create synergies. Planned initiatives,

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

pre-acquisitions, may not arise while other effects or initiatives may appear, post-acquisition. The reason for this has been identified by organizations and assumed that efficiency is achieved by streamlining overestimated benefits and overestimated costs. The identified potential may not be realized after thorough analysis or models to measure synergy potential effectively are not sufficiently developed (Johan and Helen, 2021).

Organizational synergy theory is a powerful concept but is not always easy to achieve. For synergy to occur, both organizations must work together effectively. They must also be willing to share resources and information. There are a number of benefits of organizational synergy. When two organizations merge, they can often increase their profits. This is because they can achieve economies of scale, or because they can expand their market reach. Synergy can also increase efficiency. This is because both organizations can often eliminate dual functionality or negotiate better deals with suppliers. Synergy can also increase innovation. This is because both organizations can share ideas and resources and create a more dynamic and creative environment (Gaisina et al., 2017).

Based on this explanation, this organizational synergy theory describes how two or more organizations work together to achieve a common goal more effectively than if they worked separately. In this case, the National Police and the banking sector are trying to build cooperation to increase the disclosure of social engineering cases. Organizational synergy theory can be used to analyze how partnerships between the National Police and the banking sector can combine their resources, competencies, and knowledge to achieve better results in countering social engineering.

2. Interorganization Theory

According to Agnieszka Rzepka (2017), interorganization theory is a theory that examines how organizations interact with each other. This theory focuses on relationships between organizations, and how these relationships affect the behavior of each organization. Interorganization theory is a valuable tool for understanding how organizations interact with each other. This theory can be used to identify the factors that influence these interactions, and to predict how these interactions will affect the behavior of individual organizations.

According to Zawawi (2018), interorganization theory includes a process in which companies value interdependence and pool resources to obtain net benefits that cannot be obtained by each partner independently. Net benefits, including mutual benefit, risk reduction, organizational learning, knowledge sharing and social integration. This cooperation arrangement can be categorized as formal or informal. Formal cooperation arrangements are characterized by formal contractual obligations, for example, equity joint ventures, whereas greater flexibility and norms of behavior characterize informal cooperation arrangements, for example, the exchange of information through trade associations. The choice of form of cooperation follows the assessment of two or more companies, about the perceived benefits associated with cooperation.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

Interorganization theory has been used to study a wide range of phenomena including strategic alliances, which are formal agreements between two or more organizations to work together on a particular project or activity. Outsourcing: The practice of hiring another organization to perform previously performed in-house functions. A joint venture is a partnership between two or more organizations to create a new organization. Collaboration is the process of working with other organizations to achieve common goals (Zawawi, 2018).

According to David C. Ellis (without years) an organization is a system of more than one person engaged in cooperative action and is a system of structured social interaction. Therefore, every organization must understand the behaviors, attitudes, and performance of the people who contribute to its success. An organization's progress directly depends on the effective use of human resources based on applied behavioral science. The atmosphere that facilitates the achievement of the general goals of the organization and certain tasks by its employees is of great importance because human behavior translates into the effectiveness of the organization or, conversely, its ineffectiveness. An organization's luck depends on how people are organized and how they relate to each other, clients and customers, and other related people.

Nortey (2018) explains, the behavior of people in an organization contributes to the ability of that organization to achieve its goals and success management often begins with successful management of organizational behavior. In the perspective of inter-organizational relations, increasing the competitiveness of an organization is carried out by cooperation. As a result, a competitive advantage is gained against the rest of the non-cooperating entities. This cooperation, or creating and practicing solutions based on various forms of cooperation, becomes the basic value of networks between organizations. Corporate cooperation is an alternative to compete. The essence of this relationship boils down to the voluntary relationship of the company in the common interest.

This interorganization theory focuses on the relationships between different organizations and how those relationships can create added value through the exchange of resources and knowledge. In the synergy between the National Police and the banking sector, interorganizational theory can be used to analyze how the National Police and the banking sector can share information, experiences, and best practices in an effort to improve the disclosure of social engineering cases. This theory can help understand the factors that influence the success of cooperation between the National Police and the banking sector and how the exchange of resources and knowledge can create added value in the fight against social engineering.

3. Organizational Communication Theory

Muhammad, Harrison and Yang (without years) explained that organizational communication theory is a field of study that examines communication processes within organizations. This theory focuses on the role of communication in shaping organizational culture, structure, and performance. Organizational communication theory has been used to study a wide variety of phenomena including the role of communication in decision making, the impact of communication on organizational culture, the relationship between communication and

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

performance, and communication challenges in virtual teams. Communication involves aspects of interpersonal, intergroup and interorganizational interactions, emphasizing the transmission of messages of experience, behavior, way of life, daily practices and viewpoints

Andi Schimdt (2012) explained that communication has taken an important role in the management process in the context of organizations. Communication in organizations must be treated integrally, permeating all organizational actions, making their cultural and identity constructs permanent and marking their unique style and way of protecting themselves outward leads to the construction of their image. In this sense, the organization is seen as a unit of collective action formed to achieve certain objectives and directed by a force that forms a form of authority that determines the status and role of its members. Information in the process of communication from now on is considered an intermediate variable between communication and organization. The way in which information is perceived and interpreted by the receiver determines the concretization of communication.

Within the sphere of the organization, communication took a new direction, fragmented, limited at the tactical level, and began to take a very strategic role, integrating itself into decision-making processes in all sectors and departments of the organization. Communication began to consider a systemic dimension that made it possible to unify the concept of organization, accumulate common interests, and avoid fragmentation. For communication to be successful it is necessary to establish a corporate dialogue with its internal and external publics, must meet the specific characteristics of each public segment, create channels and vehicles directed to their needs, aspirations and expectations. Through its scope, communication can be established through the company's dialogue with its internal and external public through interaction between several publishers and recipients at once. In this sense, communication is a transport system of an idea, concept, philosophical body and action carried out by an organization (Andi Schimdt, 2012).

This organizational communication theory focuses on the communication processes that occur within organizations and how factors such as perceptions, communication channels, and communication barriers affect the effectiveness of cooperation. In this synergy between the National Police and the banking sector, organizational communication theory can be used to analyze communication constraints between the National Police and the banking sector in building cooperation. This can include misunderstandings, differences in perception, or communication barriers that hinder the effective exchange of information between the two parties.

4. Organizational Behavior Theory

Organizational behavior deals with people's thoughts, feelings, emotions, and actions in the work environment. Understanding individual behavior is itself a challenge, but understanding group behavior in an organizational environment is a monumental managerial task. Organizational behavior is explained as the study of human behavior in organizational settings, the interface between human behavior and the organizational context, and the organization itself. This definition has three facets: individual behavior, organization and the interface

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

between the two (AR. Saravanakumar, 2019). Each individual brings to the organization a unique set of beliefs, values, attitudes, and other personal characteristics and characteristics all these individuals must interact with each other to create an organizational setting. Organizational behavior is specifically concerned with work-related behavior that occurs within the organization. Organizational behavior theory is a major part of organizational study, as behavioral reasoning is found in various theoretical approaches (Henrich and Linda, 2015).

Organizational behavior offers three main ways to understand the context of the basic elements of each member's work; Man as an organization, man as a resource, and man as a human being. Most importantly, organizations are people; And without people there would be no organization. So, if managers want to understand the organization they work for, they must first understand the people who make up that organization (Julian Barling and Cary L. Cooper, 2008).

As a resource, people are one of an organization's most valuable assets. People create organizations, guide and direct their paths, and revive and revive them. People make their decisions, solve their problems, and answer their questions. As managers increasingly realize the value of potential contributions by their employees, it will become increasingly important for managers and employees to understand the complexities of organizational behavior (Henrich R. and Linda Argote, 2015).

Organizational behavior deals with the characteristics and behavior of employees in isolation; characteristics and processes that are part of the organization itself; and characteristics and behaviors generated directly from people with their individual needs and motivations working within organizational structures. One cannot fully understand an individual's behavior without learning something about that individual's organization. Similarly, he cannot understand how an organization operates without studying the people who compose it. Thus, organizations influence and are influenced by individuals (Fred Luthans, 2011).

Organizational behavior theory studies the behavior of individuals and groups in an organizational context. In this context, organizational behavior theory can be helpful in analyzing psychological, social, and cultural factors that influence the efforts of the National Police and the banking sector in building cooperation. Constraints such as differences in interests, lack of motivation, or resistance to change can be analyzed using organizational behavior theory. Theories of organizational behavior can answer questions about why humans behave the way they do in the work environment, and how to create effective and efficient organizations.

5. Strategic Management Theory

Omalaja and Eruola (2011) explain that strategic management theory is a theory that examines how organizations develop and implement strategies to achieve their goals. This theory focuses on the processes involved in strategic planning, decision-making, and implementation. Strategic management theory is used to study various phenomena, including the development of corporate strategy, formulation of business unit strategy, implementation of strategic initiatives, and evaluation of strategic performance. This theory can identify factors that

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

influence strategic decision making and predict how those factors will affect organizational outcomes.

Jofre (2011) explains strategic management is the process and approach to determine organizational goals, develop policies, programs, paradigms, and plans to achieve those goals, and allocate resources to implement policies, programs, paradigms, and plans. In other words, strategic management can be seen as the combined management of components of the three stages of the strategy process: strategy development, strategy implementation, and strategy evaluation. Strategic management involves understanding the strategic position of the organization, strategic choices for the future and managing strategy in action.

Richard (2015) explains strategic management involves exploring and managing an organization's corporate strategy. It also involves modeling and analyzing the system's overall corporate strategy to include the organization's strategic position, strategic choices by the organization, and strategy in actions in and around the organization. Strategic positioning deals with the strategic impact of the external environment, the organization's strategic capabilities (resources and competencies), the expectations and influence of stakeholders, and cultural and historical influences such as the organization's historical, sectoral and national parameters.

Strategic choice in this theory involves understanding the underlying basis for future strategy at the business unit, corporate and international levels and the option to develop strategy in terms of both direction and method of development. Strategy in action is concerned with ensuring that the developed strategy works in practice, usually includes thorough consideration of the process of strategy development in the organization, structuring and restructuring (reengineering) the organization to support effective and efficient performance (optimal productivity) in terms of organizational structure, processes and relationships, also includes resource strategy, strategic change and strategy practices (Jofre, 2011).

Effendi et al, (2020) explained that innovation diffusion provides a 5-stage framework which includes the knowledge, persuasion, decision, implementation, and confirmation stages. In the knowledge stage, innovators gain an understanding of the innovation experience. The understanding gained by innovators in the knowledge stage can motivate innovators to acquire further knowledge to formulate their innovative ideas. At the knowledge stage, organizations can use technology with a customer-focused approach to improve their understanding of consumer preferences and the rapidly changing business environment. At the persuasion stage, the organization builds a like or dislike attitude towards the innovative ideas generated at the knowledge stage. At the decision stage, the organization participates in activities to encourage or discourage innovation ideas and puts innovations to use in the implementation phase. Finally, the decision maker can reverse an innovation if the results of the implementation stage do not meet management's expectations or the decision maker has found alternatives in the implementation phase.

The theory of strategic management theory deals with the process of strategic decision making in organizations. Strategic management theory can be used to analyze strategies adopted by the National Police and the banking sector to increase synergy and effectiveness of cooperation.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

This includes setting common goals, identifying tactical measures, allocating appropriate resources, and monitoring outcomes to achieve success in uncovering social engineering cases.

RESULT AND DISCUSSION

Analysis of Efforts Made by the National Police in Building Cooperation with the Banking Sector to Improve Disclosure of Social Engineering Cases in the Jurisdiction of Cimahi Police Station

Social engineering crimes involve social manipulation of individuals or organizations to obtain confidential information, access to computer systems or networks, or obtain financial gain. Social engineering criminals don't rely on computer hacking techniques or malicious software but try to exploit human vulnerabilities. Social engineering crimes are often highly secretive and difficult to detect because they rely on social engineering. Therefore, education and awareness about these potential threats is essential so that individuals and organizations can be more vigilant against these kinds of manipulation attempts.

The banking sector is one of the main targets of social engineering criminals as they seek access to bank accounts and financial information. Banks have valuable data on financial activity and often spearhead the detection and tracking of these crimes. With close cooperation, the National Police can gain faster access to relevant information from the banking sector, such as suspicious transactions or fraudulent IP addresses. This will enable faster investigation and more effective disclosure of social engineering cases.

Criminals try to obtain confidential information such as passwords or credit card numbers by posing as a trusted entity through fake emails or fake websites. This tactic involves fake phone calls from parties claiming to be financial institutions, governments, or trusted organizations to steal sensitive information from victims. Criminals create false stories or pretexts to request victims' personal or confidential information. They often pretend to be people or entities with authority. Criminals provide "decoys" in the form of interesting-looking files or devices, which, if downloaded or used, can infect victims' computers with malware or steal important information.

In tailgating tactics, criminals try to enter a building or secure location by following someone legitimate, such as an employee, without permission. This often happens in buildings with limited access. Criminals offer victims something (for example, technical assistance or free service) in exchange for personal information or passwords. Criminals redirect internet traffic from legitimate websites to fake websites they control, with the aim of stealing login information or other sensitive data. Criminals impersonate legitimate individuals or entities, such as co-workers, friends, or family members, to solicit information or transactions. Social engineering crimes are often highly secretive and difficult to detect because they rely on social engineering.

Cooperation between the National Police and the banking sector has an important role in increasing the disclosure of social engineering cases in the jurisdiction of the Cimahi Police Station and throughout Indonesia. Social engineering is a social engineering technique used by

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

criminals to manipulate individuals into revealing confidential information or committing certain harmful acts, such as financial fraud. This cooperation is not only about disclosure, but also about prevention. By sharing information and experience, the National Police and the banking sector can work together to identify potential threats early, develop better prevention strategies, and raise public awareness of social engineering risks.

Social engineering crimes can harm individuals and organizations by losing money, stolen personal information, or other financial losses. The cooperation aims to protect communities and organizations from such losses, thus creating a safer environment. The banking sector often has greater resources to develop and implement advanced security technologies. National Police can leverage this knowledge and resources to develop their technological capabilities in detecting and tracking social engineering criminals.

Efforts made by the National Police in building cooperation with the banking sector to improve the disclosure of social engineering cases in the jurisdiction of the Cimahi Police Station can involve several important strategies and steps. Some of the efforts that can be done by the National Police, including:

1. Active Cooperation

The National Police must be active in establishing partnerships with banking institutions. This can include regular meetings, discussion forums, or joint working groups to discuss security issues, fraud trends, and disclosure strategies.

2. Resource Provisioning

The National Police needs to provide sufficient resources to support efforts to disclose social engineering cases. This includes special training for police members in charge of handling the case, as well as the necessary technology and equipment.

3. Information Sharing

The National Police and the banking sector must develop mechanisms to share information quickly. This could be reports of suspicious cases, data on emerging fraud patterns, or relevant security intelligence.

4. Use of Technology

Technology can be a very important tool in detecting and preventing fraud. The National Police and the banking sector can cooperate in developing or using sophisticated security systems, such as cyber threat detection and data analysis.

5. Joint Investigation

The National Police can collaborate with banks in investigating social engineering cases. This can involve sharing clues, access to footage-surveillance, or even assignments with a team of investigators.

6. Strict Law Enforcement

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

The National Police must show commitment to take firm action against perpetrators of social engineering cases. This can give the message that such actions will not be tolerated, which can be a deterrent factor for criminals.

7. Public Education

In addition, the National Police can work with the banking sector to raise public awareness about social engineering risks and how to protect themselves from fraud. This can be done through counseling and education campaigns.

8. Coordination with Related Agencies

The National Police also need to coordinate with other government agencies, such as the Corruption Eradication Commission (KPK) or the State Intelligence Agency (BIN), if needed, to address more complex threats.

The importance of cooperation between the National Police and the banking sector in dealing with social engineering cases has an impact on the disclosure of these cases and on better prevention and protection for the public and financial institutions. In order to achieve this goal, cooperation between the National Police and the banking sector must be based on trust, confidentiality, and a commitment to fighting social engineering crimes. By collaborating effectively, they can provide better protection to communities and reduce the impact of these kinds of crimes.

Analysis of Obstacles or Obstacles Faced by the National Police and the Banking Sector to Build Cooperation in an Effort to Improve Disclosure of Social Engineering Cases in the Jurisdiction of Cimahi Police Station

The banking sector is one of the sectors most vulnerable to various types of financial crimes such as fraud, money laundering, and other illegal acts. The National Police has an important role to play in preventing and investigating these kinds of crimes. Cooperation with the banking sector allows the National Police to have better access to the financial information needed to uncover these crimes. Cooperation between the National Police and the banking sector also aims to protect customers. The National Police can help monitor illegal banking practices or abuse that can harm customers.

The National Police and the banking sector are working together to improve preventive measures, such as training banking staff on signs of fraud or money laundering. This can help prevent financial crimes before they happen. Some organized crime, such as money laundering by international criminal syndicates, often involves using the banking system to hide illegal assets. Cooperation with the banking sector allows the National Police to follow financial trails and identify suspicious transactions that can help in organized crime investigations.

In building cooperation between the National Police and the banking sector to improve the disclosure of social engineering cases in the jurisdiction of the Cimahi Police Station, there are several obstacles or obstacles that may be faced. Banks have very sensitive data about their customers. Sharing this data with authorities such as the National Police can be a security and privacy issue. Banks need to ensure that customer data remains secure and is not misused in

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

the investigation process. When it comes to customers' data, there are many privacy regulations to follow. Banks must ensure that they comply with all these regulations, such as the Personal Data Protection Regulation (UU PDP) or similar regulations in Indonesia.

Social engineering investigations often involve technical aspects, such as malware analysis or tracking down the source of an attack. Cooperating with the National Police in this regard may require special technical knowledge that not all members of the banking sector possess. Banks have a reputation that must be maintained. They may worry that being involved in social engineering cases could create a bad image of their security or could affect customer trust. This can make banks less willing to collaborate openly with the National Police. The National Police and the banking sector may have different priorities and agendas. National police may want to pursue enforcement and disclosure, while banks may focus more on customer protection and risk mitigation. This can create tension in joint decision-making.

Political constraints or vested interests within the organization can be obstacles. Individuals within the organization may have different views on the importance of this cooperation. Banks may be concerned about the confidentiality of their investigations. In some cases, they may not want to disclose internal information about their security methods or vulnerabilities. Increasing this cooperation can also require investment in resources, such as training, technology, or additional personnel. This can be an obstacle especially if the bank feels financial stress.

To overcome obstacles or obstacles in building cooperation between the National Police and the banking sector in an effort to increase disclosure of social engineering cases in the jurisdiction of the Cimahi Police Station, several steps can be taken, including:

1. Commitment to Data Security

Banks and National Police need to work together to develop strong protocols to keep customer data safe, including encrypting shared data, regulating strict access, and only allowing access to authorized parties.

2. Privacy Regulation Compliance

Banks must ensure that they comply with all applicable privacy regulations when sharing data with the National Police. This can include obtaining consent from customers or ensuring that personal data is hidden or anonymous when shared.

3. Education and Training

The National Police can train bank staff on how to work with authorities to investigate social engineering cases. This can help overcome technical understanding deficiencies and priority differences.

4. Transparency

National police and banks need to communicate openly about the objectives, methods, and policies involved in cooperation, which help address uncertainty and concerns.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

5. Strategic Partnership

Building a strong partnership between the National Police and the banking sector can address concerns about reputation and differing agendas. Such partnerships can become a top priority by focusing on the common goal of protecting the public from social engineering cases.

6. Confidentiality Maintained

The National Police and banks can sign confidentiality agreements setting out the limits and actions allowed in joint investigations. This will help maintain the necessary confidentiality in the investigation.

7. Understanding the Benefits of Mutual

National police and banks need to understand the benefits they can reap through this partnership, such as increased ability to detect and stop fraud, and protect their customers.

8. Supportive Leadership

Leadership on both sides needs to support these cooperative efforts and ensure that their staff have sufficient support to collaborate effectively.

9. Periodic Evaluation

During cooperation, it is important to conduct periodic evaluations to assess joint efforts' effectiveness and identify improvement areas. Overcoming these obstacles to cooperation will require strong commitment, cooperation, and communication between the National Police and the banking sector. Along with changes in banking regulations and financial law, cooperation with the National Police helps the banking sector to comply with applicable legal provisions. The National Police can provide guidance and assistance in terms of compliance with these regulations. These measures can build effective cooperation in countering social engineering cases and protecting the public and sensitive data.

Analysis of Strategies that Can Be Implemented by the National Police and the Banking Sector to Increase Synergy and Effectiveness of Cooperation in Disclosing Social Engineering Cases in the Jurisdiction of Cimahi Police Station

Social engineering cases can cause significant financial losses for bank customers. Close cooperation between the National Police and the banking sector ensures better protection of customers and recovery of lost funds. Social engineering often involves moving money or assets through bank accounts. As a result, the banking sector has access to information that is essential in investigating these cases. Social engineering crimes like phone, electronic messaging, or offline fraud are increasingly sophisticated and detrimental. This increasing threat requires a collaborative effort between the National Police and the banking sector to deal with it.

Cooperation can help create a shared understanding of the social engineering tactics used and the best methods to identify and counter them. It also helps in raising awareness among bank staff and police officers. The National Police and the banking sector can utilize their resources

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

more efficiently and effectively through collaboration. This includes police investigative expertise and financial transaction data held by banks. By sharing information and experience, the National Police and the banking sector can identify and address potential social engineering threats before they become bigger problems. In the digital age, economic stability depends heavily on the security of the financial system. Good cooperation between the National Police and the banking sector helps maintain order and economic stability in the jurisdiction of the Cimahi Regional Police. Strong collaboration allows the National Police and the banking sector to continuously learn from each case and improve their strategies in the face of evolving tactics from social engineering actors. In order to face the growing threat of social engineering, synergy and effective cooperation between the National Police and the banking sector is key to protecting the public, reducing financial losses, and maintaining economic stability. Social engineering cases are increasingly complex, requiring cooperation allowing faster and more precise access to information required by police investigations. Many regulations require financial institutions to report financial crimes. Good cooperation ensures that banks comply with these obligations, which in turn can reduce legal risks. To increase the synergy and effectiveness of cooperation between the National Police (Polri RI) and the banking sector in disclosing social engineering cases in the jurisdiction of the Cimahi Police Station, several strategies that can be implemented are:

1. Formation of Special Teams

National Police and banking sector representatives can form a special team that focuses on handling social engineering cases. This team should consist of members trained in identifying these cases and have a strong understanding of the social engineering methods used.

2. Regular Information Exchange

Establish a schedule of meetings or regular coordination sessions between the police and banks. The latest information on social engineering trends and safety tips can be shared during these meetings. This helps in increasing the shared understanding of the existing threats.

3. Joint Training

The National Police and the banking sector must cooperate in organizing joint training. The National Police can provide training on investigative techniques, while the banking sector can provide insight into social engineering tactics that fraudsters may use.

4. Efficient Reporting System

Build an efficient and centralized incident reporting system. Banks can report social engineering incidents directly to the Cimahi police station, so that investigative steps can be taken quickly.

5. Joint Protocol Development

The National Police and the banking sector should develop a joint protocol to handle social engineering cases. This should include procedures for securing electronic evidence, cooperation in tracking offenders, and coordination with other agencies such as the State

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

Intelligence Agency (BIN) if needed.

6. Provision of Additional Resources

Together, the National Police and the banking sector could consider allocating additional resources, such as cybersecurity experts or more sophisticated technological equipment to track and analyze fraudsters' online activities.

7. Public Education Campaign

The National Police and the banking sector can work together in public education campaigns to raise public awareness about the threat of social engineering. This can be seminars, workshops, or online educational materials.

8. Use of Security Technology

Encourage the banking sector to adopt high-security technologies like two-factor authentication, real-time transaction monitoring, and advanced cybersecurity tools.

9. Cooperation with Related Security Agencies

The National Police and the banking sector must cooperate with relevant security institutions such as Kominfo (Ministry of Communication and Information) and CERT (Computer Emergency Response Team) to strengthen defenses against social engineering attacks.

10. Periodic Evaluation and Monitoring

Conduct periodic evaluations of this cooperation to assess its effectiveness. If there are problems or improvements needed, act quickly to improve cooperation.

By implementing these strategies, the National Police and the banking sector can increase the synergy and effectiveness of their cooperation in dealing with social engineering cases in the jurisdiction of the Cimahi Regional Police. This will help protect society and reduce the harm inflicted by such crimes.

CONCLUSION

Based on the explanation above, conclusions can be drawn:

1. Cooperation between the National Police and the banking sector in combating social engineering cases is very important. Social engineering is a crime that involves social engineering to steal sensitive information or harm individuals and organizations. The banking sector has valuable data that is often targeted, so this cooperation allows for more effective case disclosure. The National Police needs to actively communicate, provide resources, and share information with the banking sector. In addition, public education and strict law enforcement are also important. This collaboration will protect the public and raise awareness about social engineering risks.
2. Social engineering is a crime that involves social engineering to steal sensitive information. While important, this cooperation faces several obstacles, such as data security issues,

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

privacy regulations, priorities, and costs. To address this, it requires commitment to data security, compliance with privacy regulations, education and training, transparency, strategic partnerships, maintaining confidentiality, understanding mutual benefits, leadership support, periodic evaluations, and cooperation with third parties where necessary. With these measures, the National Police and the banking sector can build effective cooperation in countering social engineering and protecting the public and their sensitive data.

3. Cooperation between the National Police and the banking sector to uncover social engineering cases in the Cimahi Police Station area has great importance in protecting customers and economic stability. Implementation strategies that can increase the synergy and effectiveness of this cooperation involve the formation of special teams, regular information exchanges, joint training, efficient reporting systems, joint protocol development, provision of additional resources, public education campaigns, use of security technology, cooperation with relevant security agencies, and periodic evaluation and monitoring. With these measures, the National Police and the banking sector can work more effectively in confronting social engineering threats and protecting the public and their financial data.

SUGGESTION

Based on the explanation above, suggestions to be able to increase the synergy of the National Police in building cooperation with the banking sector to increase the disclosure of social engineering cases in the jurisdiction of the Cimahi Police Station, namely:

1. High Commitment from Leaders

The leadership of the National Police and the highest level representatives in the banking sector need to openly and actively support this cooperation. With high support from above, motivating personnel on both sides to collaborate well is convenient.

2. Regular Forum

Establish a forum for regular meetings between the National Police and banking sector representatives. This meeting can be a forum for sharing information, updating crime trends, and evaluating existing cooperation.

3. Special Representative

Select or appoint members from both parties who are specifically responsible for managing and monitoring this cooperation. They can act as intermediaries and coordinators in the implementation of cooperative tasks.

4. Joint Education Approach

In addition to cooperation in law enforcement, take a joint educational approach. The National Police can provide training on social engineering tactics, while the banking sector can share knowledge on transaction security and best practices in protecting customers.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

5. Transparency and Openness

Build a culture of transparency and openness. This includes openly sharing information about the progress of case investigations and prevention efforts. The more parties know, the better the cooperation.

6. Information Sharing

Establish a mechanism that facilitates and ensures the rapid and secure exchange of information between the National Police and the banking sector. This involves reporting suspicious cases, data on fraud patterns, and relevant security intelligence.

7. Joint Protocol Development

Jointly develop a clear and detailed joint protocol for handling social engineering cases. This includes how evidence will be secured, how the investigation will be conducted, and the role of each party.

8. Cooperation with Related Security Agencies

In addition to the banking sector, consider cooperation with relevant security agencies such as Kominfo or CERT to strengthen defenses against increasingly sophisticated social engineering attacks.

9. Periodic Evaluation

Conduct periodic evaluations of this cooperation to assess its effectiveness. Identify repairs that may be needed and follow up with appropriate corrective steps.

References

Books

1) AR Saravanakumar. 2019. *Unit 1 Organisational Behaviour*. Alagappa university SIM Mode Book.
2) Fabozzi, F. J., Modigliani, F., & Jones, F. J. 2020. *Foundations of Financial Markets and Institutions (4th ed.).* Pearson Prentice Hall.
3) Fred Luthans. 2011. *Organizational Behavior: An Evidence-Based Approach, 12th Edition.* McGraw-Hill.
4) Goldstein, J. 2018. *Clearing the Way for Justice: Evidence Disclosure in Criminal Cases.* Prentice Hall.
5) Griffin, R. W., & Moorhead, G. 2018. *Organizational Behavior: Managing People and Organizations (12th ed.).* Cengage Learning.
6) Hadnagy, C. 2018. *Social Engineering: The Science of Human Hacking (2nd ed.).* Wiley.
7) Hargie, O., & Tourish, D. 2019. *Auditing Organizational Communication: A Handbook of Research, Theory and Practice.* Routledge.
8) Henrich R. Greve dan Linda Argote. 2015. *Behavioral Theories of Organization*. McGraw-Hill.
9) Julian Barling dan Cary L. Cooper. 2008. *The SAGE Handbook of Organizational Behavior Vol. 1 Micro Approaches*. SAGE Publications.
10) Mishkin, F. S., Eakins, S. G., & Nelson, D. B. 2018. *Financial Markets and Institutions (8th ed.).* Pearson Education Limited.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

11) Mohamad Irhas Effendi, Dyah Sugandini, Yuni Istanto dan Rahajeng Arundat. 2020. *Inovasi Teknologi Informasi dan Kinerja Bisnis UKM*. Zahir Publishing.

12) Moore, T. 2019. *Cybercrime: Investigating High-Technology Computer Crime (2nd ed.).* Routledge.

13) Nunn, S., & Nelson, C. 2016. *Criminal Investigation: The Art and the Science (8th ed.).* Pearson Education Limited.

14) Robbins, S. P., Coulter, M., & DeCenzo, D. A. 2019. *Fundamental of Management*. Pearson Education Limited.

15) Rusnaeni, N., Gursida, H., Sasongko, H., & Hakim, D. R. (2023). Financial performance, capital structure, and firm's value: The moderating role of dividend policy. Journal of Business, Social and Technology (Bustechno), 4(1), 1-15.

16) Saunders, A., & Cornett, M. M. 2019. *Financial Institutions Management: A Risk Management Approach (9th ed.).* McGraw-Hill Education.

17) Sugiyono. 2016. *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Bandung: PT Alfabeta.

18) _____. 2012. *Memahami Penelitian Kualitatif.* Bandung: PT Alfabeta.

19) _____. 2010. *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Bandung: PT Alfabeta.

20) Todaro, M. P., & Smith, S. C. 2015. *Economic Development (12th ed.).* Pearson Education Limited.

21) West, M. A. 2019. *Effective Teamwork: Practical Lessons from Organizational Research (3rd ed.).* Wiley-Blackwell.

22) World Bank. 2016. *World Development Report 2016: Digital Dividends*. World Bank.

Scientific Journals

1) Agnieszka Rzepka. 2017. Inter-organizational relations as a source of competitive advantage for contemporary enterprises in the era of globalization. *Procedia Engineering 174 (2017) 161 – 170.*

2) Andi Schimdt. 2012. *Modern Theories of Organizational Communication chapter 4.* An Introduction to Organizational Communication.

3) Anna Visvizi, Miltiadis D. Lytras, dan Linda Daniela. 2019. The Future of Innovation and Technology in Education: Policies and Practices for Teaching and Learning Excellence. *Article*. Emerald Publishing Limited.

4) Asma A. Alsufyani, dkk., 2020. Social engineering, New Era of Stealth and Fraud Common Attack Techniques and How to Prevent Against. *International Journal of Scientific & Technology Research Volume 9, Issue 10.*

5) Bandar S. Almutairi dan Abdurahman Alghamdi. 2022. The Role of Social engineering in Cybersecurity and Its Impact. *Journal of Information Security, 2022, 13, 363-379.*

6) Chandra Sekhar Bhusal. 2021. Systematic Review on Social engineering: Hacking by Manipulating Humans. *Journal of Information Security, 2021, 12, 104-114.*

7) Dalal Alharthi dan Amelia Regan. 2021. A Literature Survey and Analysis on Social engineering Defense Mechanisms and Infosec Policies. *International Journal of Network Security & Its Applications (IJNSA) Vol.13, No.2, March 2021.*

8) David Airehrour, Nisha Vasudevan Nair, dan Samaneh Madanian. 2018. Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model. *Article*. Information 2018, 9, 110.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

9) David C. Ellis. Tanpa Tahun. Theorizing International Organizations: The Organizational Turn in International Organization Theory. *Article*. U.S. Department of Defense.

10) Fatima Salahdine dan Naima Kaabouch. 2019. Social Engineering Attacks: A Survey. *Future Internet* 2019, 11, 89.

11) Hazel Comia. 2017. Social engineering: Exploring Social Engineering Toolkits. *Article*. Asia Pacific Collage.

12) Hussain Aldawood dan Geoffrey Skinner. 2020. Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions. *Institute of Electrical and Electronics Engineers (IEEE) Volume 8, 2020.*

13) Ida Nurhayati dan Indianik Aminah. 2020. Credit Fraud as One of the Dimensions in the Banking Crime. *Advances in Social Science, Education and Humanities Research, Volume 544.*

14) Islam Abdalla Mohamed Abass. 2018. Social Engineering Threat and Defense: A Literature Survey. *Journal of Information Security*, 2018, 9, 257-264.

15) J. Wendorf Muhamad, T. R. Harrison, and F. Yang. Tanpa tahun. Organizational Communication Theory and Practice. *Article*.

16) Jofre, S. 2011. Strategic Management: The theory and practice of strategy in (business) organizations. *DTU Management 2011 No. 1.*

17) Johan Holstrom dan Helen Anderson. 2021. Exploring and extending the synergy concept – a study of three acquisitions. *Journal of Business & Industrial Marketing, April 2021*. Emerald Publishing Limited.

18) Kaouthar Chetioui, dkk. 2021. Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science* 198 (2022) 656–661.

19) Kwadwo Kyeremeh, dkk. 2019. A Study into the Social Engineering Risk and Its Effects in the Public Institutions in Ghana. *SSRN*. June 14, 2019.

20) Lindiwe T. Hove. 2020. Strategies Used to Mitigate Social Engineering Attacks. *Dissertations*. Walden Dissertations and Doctoral Studies Collection 2020.

21) Lyutsiya Mugtabarovna Gaisina, dkk. 2017. Principles and methods of synergy modeling management system at oil and gas enterprises. *Revista Espacios Vol. 38 No. 33 Hal. 5.*

22) Mercurius B.L., Step S., dan Fangky A.S. 2020. A Conceptual Framework of Technological Innovation for Indonesia's Financial and Banking Industry. *International Journal of Information, Bussiness and Management,* Vol. 12 No. 4 2020.

23) Mohammad Fadarisman dan Bambang Tri Bawono. 2021. Implementation of Disclosure of Bank Confidentiality in The Effort to Eradicate Money Laundering Crime. *Law Development Journal. Volume 3 Issue 2.*

24) Mohammad Hijji and Gulzar Alam. 2021. A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. *IEEE ACCESS*, Volume 9, 2021.

25) Montañez R, Golob E dan Xu S (2020) Human Cognition Through the Lens of Social engineering Cyberattacks. *Frontier Psychology 11:1755.*

26) Moses Isdory Mgunda. 2019. The Impacts Information Technology on Business. *JICP*. 02 September 2020.

27) Mosin Hasan, Nilesh Prajapati dan Safvan Vohara. 2010. Case Study on Social Engineering Techniques for Persuasion. *International journal on applications of graph theory in wireless ad hoc networks and sensor networks* (GRAPH-HOC) Vol.2, No.2, June 2010.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.8394160

28) Nur Haiza Muhammad Zawawi. 2018. Actor-Network Theory and Inter-Organizational Management Control. *International Journal of Business and Society, Vol. 19 S2, 2018, 219-234.*

29) Omalaja M.A. dan Eruola O.A. 2011. Strategic Management Theory: Concepts, Analysis, and Critiques in Relation to Corporate Competitive Advantage from the Resource-based Philosophy. *Economic Analysis 2011, Vol. 44, No. 1-2, 59-77.*

30) Richard Scroggins. 2015. Strategic Management Theories. *Global Journal of Computer Science and Technology: Information & Technology Volume 15 Issue 1 Version 1.0 Year 2015. Double Blind Peer Reviewed International Research Journal.* Global Journals Inc. (USA).

31) Samuel Carvalho De Benedicto, dkk. 2018. Organizational Communication: A Theoretical Discussion. *REUNA, Belo Horizonte - MG, Brasil, v.23, n.1, p.20-37, Jan. – Mar. 2018.*

32) Sowjanya Manyam. 2022. Artificial Intelligence's Impact on Social engineering Attacks. *Thesis*, Governors State University University Park.

33) Venkatesha Sushruth, K. Rahul Reddy, dan B. R. Chandavarkar. 2021. Social engineering Attacks During the COVID-19 Pandemic. *Springer Nature Journal, Computer Science 2:78.*

34) Vicentia Nortey. 2018. Inter-Organizational Collaboration Between University-Linked Innovation Organizations - A Case Study of Drivhuset and STORM. *Article*. Malmo University.

35) Walter Fuertes, dkk. 2022. Impact of Social Engineering Attacks: A Literature Review. *Smart Innovation, Systems and Technologies* 255.

36) Wenni Syafitri, dkk. 2022. Social Engineering Attacks Prevention: A Systematic Literature Review. *Digital Object Identifier*, Volume 10, 2022.

37) Wouter Dessein, Luis Garicano, dan Robert Gertner. 2008. Organizing for Synergies: A Theory of Hybrid Organizations. *Article*. Graduate School of Business. The University of Chicago.

Internet

1) Adi Ahdiat. 2023. Jumlah Serangan Phishing yang Dilaporkan ke APWG (Januari 2019-Desember 2022). Sumber: https://databoks.katadata.co.id/datapublish/2023/05/17/tren-serangan-phishing-terus-meningkat-capai-rekor-tertinggi-pada-2022. Diakses 13 Juli 2023, Pukul 07.38 WIB.

Legislation Report

2) Undang-Undang Nomor 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia.

3) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).

4) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

5) Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE).

6) Keputusan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Pedoman Penanganan Konten Negatif.

7) Surat Telegram-2055 tentang Pemberitahuan Pembukaan Rahasia Bank dan Harta Kekayaaan.