IJSSR
International Journal of Social Service and Research

Vol. 03, No. 11, November 2023
e - ISSN : 2807-8691 | p- ISSN : 2807-839X

Cooperation Between The Cimahi Police Criminal Investigation Unit and the Banking Sector in Disclosing Social Engineering Cases

Tono Listianto[1*], Chairul Muriman Setyabudi[2], Sutrisno[3]
Police Science Studies, School of Strategic and Global Studies, Universitas Indonesia, Indonesia [1,2,3]
Email: tonolistian@gmail.com[1], cak_iir1966@yahoo.com[2], sutrisnosuki18@gamail.com[3]

Keywords

Cooperation, Criminal Investigation Unit, Information Technology, Banking Sector, Social Engineering.

ABSTRACT

Information technology is increasingly advanced, coupled with the existence of the internet, which is now a global communication system that 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, both 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. There are many people who use social networks to commit crimes, such as cyber-crime in the form of social engineering. Social engineering allows malicious hackers to gain unauthorized access to an organization's networks, user accounts and emails, databases, smart devices, and electronics, such as laptops, personal webcams, and sensors, including network connectivity that allows all of these objects to exchange data. These hackers use a variety of methods to carry out social engineering attacks. The technical complexity of the information systems used in locating, examining, and analyzing relevant transaction data requires sufficient time and technical expertise to gather 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 many transactions need to be traced and analyzed.

INTRODUCTION

The development of IT information technology science is proliferating, and along with these advancements, the paradigm of Indonesian society development is very difficult to avoid its development. IT comprises any technology humans want to create, change, store, communicate, and disseminate information. IT capabilities combine high-speed computing and data, voice, and video communications (Kikerpill, 2023). IT consists of personal computers (laptops), telephones, televisions, electronic household appliances, and modern handheld devices such as mobile phones (Moses & Knutsen, 2019). Therefore, current IT advances are significant in supporting business activities and connecting every business to information technology (IT) systems (Mosin, et al., 2010).

IT security threats can be observed in one form, such as social engineering, which is increasingly rampant. From the document study data on research conducted by David, et al. (2018), it was found that several countries have the highest percentage of cyber attacks in the form of social engineering (Khan et al., 2018), which can be observed in the following figure :

https://doi.org/10.46799/ijssr.v3i11.611

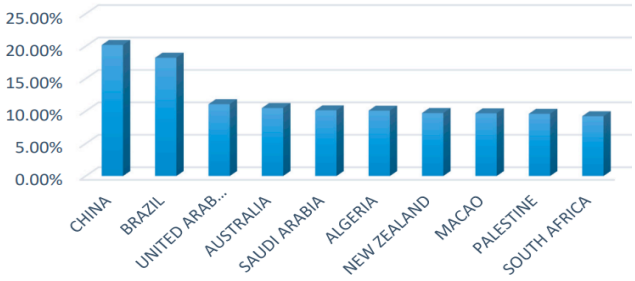

Figure 1. Countries with the Highest Percentage of Cyber Attack Victims
Source: (David et al., 2022)

The basis of this study is specifically to analyze the problems that exist in the Cimahi Police Station with many 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, obstacles or obstacles faced by the National Police and the banking sector in building cooperation to increase disclosure of social engineering cases in the jurisdiction of the Cimahi Police Station and strategies that can be implemented by the National Police and the banking sector to increase the synergy and effectiveness of cooperation in disclosing social engineering cases in the jurisdiction of the Cimahi Police Station, which can be explained in the following:

Johan and Helen (2021) explain synergy as a concept introduced in the 1960s in 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 was one of the building blocks in corporate strategy 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 a company's financial development perspective, such as share price, revenue, investment, or sources of value creation as evaluated by performance measurements (Bartolozzi et al., 2022; Pavlidis, 2023). Synergy is conceptualized around return on investment using four main categories of synergies: sales, operations, investment, and management (Al-fajri et al., 2020). Synergy encompasses a wide range of perspectives including creating value, the power of increasing profitability, sharing competencies and capabilities, managing purchasing synergies, the power 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 (Dessein et al., 2010).

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 and 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 integration issues may affect the potential to create synergies. Planned initiatives, 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 a thorough analysis of models to measure synergy potential effectively are not sufficiently developed (Holtström & Anderson, 2021).

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 The National Institute of Standards and Technology (NIST), social engineering attempts to trick someone into revealing information (such as passwords) to attack a system or network (Hadnagy, 2010; Zambrano et al., 2023). 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 (Raditya, 2023). 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)

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 (Greve & 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, 2011).

The theory used to analyze the problem of 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 is the theory of organizational synergy and the theory of inter organization . In contrast, the obstacles or obstacles faced by the National Police and the banking sector in building cooperation to increase the disclosure of social engineering cases in the jurisdiction of the Cimahi Police Station are analyzed with theory Organizational communication and organizational behavior theory. The formulation of strategies that can be implemented by the National Police and the banking sector to increase the synergy and effectiveness of cooperation in disclosing social engineering cases in the jurisdiction of the Cimahi Police Station are analyzed with strategic management theory and technology innovation theory. These problems are then examined through a qualitative approach carried out through field research methods with exploratory research types.

METHODS

This method uses field research because it allows researchers to obtain data and information directly from relevant and specific research locations. In addition, the selection of this field research method is also based on several reasons, such as: making it easier for researchers to access directly to information and participants involved in the synergy between the National Police and the banking sector in the jurisdiction of the Cimahi Police Station, so that researchers are easier to interact directly with related parties, such as police officers, bank representatives, or other related parties, to gain deeper insights and obtain accurate data.

Field research enables researchers to understand the local context directly. In the context of the synergy of the National Police and the banking sector, field research can uncover specific factors that affect cooperation in the jurisdiction of the Cimahi Police Station, such as local policies, social

characteristics, culture, or relevant security issues. Through field research, researchers can collect holistic data by involving various data collection methods such as direct interviews, observations, or document analysis. Thus, this research can produce rich and comprehensive data on the synergy of the National Police and the banking sector in disclosing social engineering cases. In addition, the selection of field research methods is also based on the ease of verifying and validating the data collected so that researchers can observe the situation, obtain diverse points of view, and ensure the validity of the data collected through direct confirmation with participants or other sources of information. In addition, social engineering and cooperation between the National Police and the banking sector is dynamic. By conducting field research, researchers can observe changes, trends, and recent developments that can affect the synergy. This allows researchers to gain a more complete and up-to-date understanding of the situation. By using field research methods, this research can produce deep insights, accurate data, and a holistic understanding of the synergy of the National Police and the banking sector in disclosing social engineering cases in the jurisdiction of the Cimahi Police Station.

RESULTS

When looking at the problems found in the field related to various actions taken by the Cimahi Police in making these efforts did not get 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 sent 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 the name of Andre and account number 707228232200 in the name of Nurbahagia SE, which gave the refusal due to the reason that the data is included in the Bank's confidentiality, on the other hand, based on data collected from the Cimahi Police Tipidter Unit, based on the Police report number: Lp.B/896/VII/2022/JBR/RES CMI, dated July 7, 2022. Whistleblower Drs. Darmawan and data request letter number: B/1530/VII/2022/Reskrim data related to the identity and flow of funds suspected to be a crime proceeds shelter account can be obtained by Cimahi Police investigators for reasons of closeness to the Bank providing the data in question but not under the hand through an official letter (Besong et al., 2022).

This fact shows the complexity of revealing social engineering cases carried out 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 letter 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 many transactions need to be traced and analyzed (Mbaidin et al., 2023; Patel et al., 2022).

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 (Hess et al., 2016). 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 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 benefit the community by increasing public awareness about social engineering risks 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 also exchange intelligence information about social engineering attacks that occur. 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 capacity of the banking sector in dealing with such attacks.

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 (Moore, 2014). Cooperation with the banking sector allows the National Police 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 (Johnson, 2023; Wang, 2023). This can help prevent financial crime before it happens. Some organized crime, such as money laundering by international criminal syndicates, often involves using the banking system to hide illegal assets (Thommandru & Chakka, 2023). Cooperation with the banking sector allows the National Police to follow financial trails and identify suspicious transactions that can assist in organized crime investigations (Broache et al., 2023; Ryan, 2022).

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, some several obstacles or obstacles 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 investigation process. Regarding customers' personal 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 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 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 own investigations. Sometimes, 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 (Ogbeide et al., 2023).

To overcome obstacles or obstacles in building cooperation between the National Police and the banking sector in an effort to increase the 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 the 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 provide training to bank staff on how to work with authorities in the investigation of 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.
5. Strategic Partnership
   Building a strong partnership between the National Police and the banking sector can address concerns about reputation and differing agendas. By focusing on the common goal of protecting the public from social engineering cases, such partnerships can become a top priority.
6. Confidentiality Maintained
   The National Police and banks can sign confidentiality agreements setting out the limits and permissible actions 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 improving their ability to detect and stop fraud and protecting their customers.
8. Supportive Leadership
   Leadership on both sides must 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 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 essential information in investigating these cases. Social engineering crimes, such as 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 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 can be implemented:

1. Formation of Special Teams
   The National Police and banking sector representatives can form a special team that handles 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 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 on 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, such as 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

The researchers conducted a comprehensive analysis of findings related to the collaboration between the National Police and the banking sector in addressing social engineering cases within the jurisdiction of the Cimahi Police Station. This collaboration is deemed crucial due to the nature of social engineering crimes targeting sensitive information in the banking sector. The study identified obstacles, including data security issues, privacy regulations, and cost concerns, emphasizing the need for commitment to security measures, compliance with regulations, education, transparency, and strategic partnerships. Despite these challenges, the researchers propose implementation strategies to enhance the synergy and effectiveness of cooperation, such as forming special teams, facilitating regular information exchanges, conducting joint training, developing efficient reporting systems and protocols, allocating additional resources, launching public education campaigns, utilizing security technology, and collaborating with relevant security agencies. These measures aim to fortify the collaboration between the National Police and the banking sector, ensuring a more robust response to social engineering threats and safeguarding the public and their financial data in the Cimahi Police Station area.

REFERENCES

Al-fajri, B. H., Fauzi, R., & Mulyana, R. (2020). Perancangan Manajemen Risiko Operasional Spbe/e-gov Pada Kategori Risiko Infrastruktur, Aplikasi, Layanan, Data Dan Informasi Berdasarkan Permen Panrb Nomor 5 Tahun 2020 (studi Kasus: Pemerintah Kota Bandung). *EProceedings of Engineering*, *7*(2).

Bartolozzi, D., Gara, M., Marchetti, D. J., & Masciandaro, D. (2022). Designing the anti-money laundering supervisor: The governance of the financial intelligence units. *International Review of Economics and Finance*, *80*, 1093–1109. https://doi.org/10.1016/J.IREF.2022.03.009

Besong, S. E., Okanda, T. L., & Ndip, S. A. (2022). An empirical analysis of the impact of banking regulations on sustainable financial inclusion in the CEMAC region. *Economic Systems*, *46*(1). https://doi.org/10.1016/J.ECOSYS.2021.100935

Broache, M. P., Cronin-Furman, K., Mendeloff, D., & McAllister, J. R. (2023). The International Criminal Court at 25. *Journal of Human Rights*, *22*(1), 1–3. https://doi.org/10.1080/14754835.2022.2150518

David, D., Robet, R., & Raymond, R. (2022). Aplikasi Pengenalan Ikan Berformalin Melalui Deteksi Mata Menggunakan Metode Template Matching Dan Metode Klasifikasi KNN. *Jurnal Ilmiah Core IT: Community Research Information Technology*, *10*(4).

Dessein, W., Garicano, L., & Gertner, R. (2010). Organizing for synergies. *American Economic Journal: Microeconomics*, *2*(4), 77–114.

Fred, L. (2011). *Organizational Behavior An Evidence-Based Approach Twelfth Edition*. mc ggaw hill.

Greve, H. R., & Argote, L. (2015). Behavioral theories of organization. *International Encyclopedia of the Social & Behavioral Sciences*, 481–486.

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons.

Hess, K. M., Orthmann, C. H., & Cho, H. L. (2016). *Criminal investigation*. Cengage learning.

Holtström, J., & Anderson, H. (2021). Exploring and extending the synergy concept–a study of three acquisitions. *Journal of Business & Industrial Marketing*, *36*(13), 28–41.

Johnson, D. (2023). Can competition law aid the United Kingdom in its fight against financial crime? *Journal of Economic Criminology*, *2*, 100025. https://doi.org/10.1016/J.JECONC.2023.100025

Khan, R., McLaughlin, K., Laverty, J. H. D., David, H., & Sezer, S. (2018). Demonstrating cyber-physical attacks and defense for synchrophasor technology in smart grid. *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, 1–10.

Kikerpill, K. (2023). The crime-as-communication approach: Challenging the idea of online routine activities by taking communication seriously. *Journal of Economic Criminology*, *2*, 100035. https://doi.org/10.1016/J.JECONC.2023.100035

Mbaidin, H. O., Alsmairat, M. A. K., & Al-Adaileh, R. (2023). Blockchain adoption for sustainable development in developing countries: Challenges and opportunities in the banking sector. *International Journal of Information Management Data Insights*, *3*(2). https://doi.org/10.1016/J.JJIMEI.2023.100199

Moore, R. (2014). *Cybercrime: Investigating high-technology computer crime*. Routledge.

Moses, J. W., & Knutsen, T. L. (2019). *Ways of knowing: Competing methodologies in social and political research*. Bloomsbury Publishing.

Ogbeide, H., Thomson, M. E., Gonul, M. S., Pollock, A. C., Bhowmick, S., & Bello, A. U. (2023). The anti-money laundering risk assessment: A probabilistic approach. *Journal of Business Research*, *162*. https://doi.org/10.1016/J.JBUSRES.2023.113820

Patel, R., Migliavacca, M., & Oriani, M. E. (2022). Blockchain in banking and finance: A bibliometric review. *Research in International Business and Finance*, *62*. https://doi.org/10.1016/J.RIBAF.2022.101718

Pavlidis, G. (2023). The dark side of anti-money laundering: Mitigating the unintended consequences of FATF standards. *Journal of Economic Criminology*, *2*, 100040. https://doi.org/10.1016/J.JECONC.2023.100040

Raditya, B. C. (2023). Juridical Review Regarding Transfer of The Right to Occupate Service House of Police. *Asian Journal of Engineering, Social and Health*, *2*(2), 91–106. https://doi.org/10.46799/ajesh.v2i2.38

Ryan, M. J. (2022). Criminal Justice Secrets. *Am. Crim. L. Rev.*, *59*, 1541.

Rzepka, A. (2017). Inter-organizational relations as a one of sources of competitive advantage of contemporary enterprises in the era of globalization. *Procedia Engineering*, *174*, 161–170. https://doi.org/10.1016/j.proeng.2017.01.195

Thommandru, A., & Chakka, D. B. (2023). Recalibrating the Banking Sector with Blockchain Technology for Effective Anti-Money Laundering Compliances by Banks. *Sustainable Futures*, *5*, 100107. https://doi.org/10.1016/J.SFTR.2023.100107

Wang, Z. (2023). Money laundering and the privacy design of central bank digital currency. *Review of Economic Dynamics*. https://doi.org/10.1016/J.RED.2023.06.004

Wenni, S., Lijun, H. O. U., Jiawei, T., Chunyuan, M. U., Haoyu, Z., & Tao, X. U. (2022). Experimental Investigation of Underwater Blast Injuries to Beagles. *Acta Armamentarii*, *43*(9), 2172.

Zambrano, P., Torres, J., Tello-Oquendo, L., Yánez, Á., & Velásquez, L. (2023). On the modeling of cyber-attacks associated with social engineering: A parental control prototype. *Journal of Information Security and Applications*, *75*. https://doi.org/10.1016/J.JISA.2023.103501