International Journal of Research and Review
Volume 11; Issue: 6; June 2024
Website: www.ijrrjournal.com
Review Paper *E-ISSN: 2349-9788; P-ISSN: 2454-2237*

Cybercrime Risk Management Efforts to Overcome Digital Fraud

Muh. Ardilla Amry

Indonesian National Police, Sespim Lemdiklat Polri

DOI: https://doi.org/10.52403/ijrr.20240660

ABSTRACT

This study aims to investigate the risk management efforts used to address smartphone fraud. This research identifies and analyzes various techniques and strategies used by organizations and individuals to manage fraud-related risks involving the use of smartphones. The research method used involved a literature study and documentation analysis of smartphone fraud cases that have occurred. The findings of this study reveal that effective risk management in addressing smartphone fraud involves a holistic and sustainable approach. Factors such as user awareness, technology security, transaction monitoring, and cooperation between the parties involved are important elements in a successful risk management strategy. In addition, this study also highlights the importance of education and training for smartphone users to improve their understanding of fraud threats and preventive measures.

Keywords: Fraud, Risk Management, Digital Fraud

INTRODUCTION

The development of Science and Technology has undergone many changes, especially in the field of telecommunications. This rapid development has made human life easier and unlimited, especially in communication. In Indonesia, the law that regulates telecommunication is contained in Law Number 36 Year 1999 on Telecommunication. Article 1 number (1) defines telecommunication, namely: "Telecommunication is any transmitting, sending and/or receiving of any information in the form of signs, signals, writings, pictures, sounds, and noises through wire, optical, radio or other electromagnetic systems." If associated with the above definition, then smartphones are included in telecommunications equipment. Smartphones or smartphones have become a mandatory requirement for the community due to the fast and easy access to information.

In line with the development of technology that brings good impacts, bad impacts can also arise from the use of these smartphones. Modes of crime have now developed, one of which is fraud through smartphones. Fraud through smartphones no longer uses threatening tones or horrendous things like other fraud cases, but a new mode that targets victims by pretending to be relatives or closest relatives to easily get into the flow of the fraud or commonly referred to as Social Engineering. Social Engineering is a technique or way to obtain personal data information and desired access by psychologically manipulating or subtly tricking the victim so that they do not realize that they have been cheated.

There are many crimes that use Social Engineering techniques, one of which is Pretexting. Pretexting is a technique carried out by the perpetrator by talking like or pretending to be an expert / close relative, for example a bank employee to provide

personal information such as telephone numbers, dates of birth, addresses and even pins or security codes. The rise of technology abuse that has a negative impact, it is important to carry out cyber risk management in order to manage the risks that can arise with the stages of risk management, namely risk identification, risk analysis, risk management, risk implementation and monitoring. The relationship of cyber risk management in the case discussed is from how the application of risk management to avoid the risk of crime that comes so that it can be prevented through a theoretical approach.

MATERIALS & METHODS

The method used in this research is descriptive qualitative using literature study. According to Purwono (2008), literature studies are characterized by several features which include the following steps:

1. Identification of sources: The process begins with the identification of sources that are relevant to the topic of the research being conducted. These sources include various types of literature such as books, scholarly journals, articles, papers, and so on.
2. Analysis and Evaluation: Once the sources have been identified, the next step is to analyze and evaluate the content of the materials. This involves an in-depth understanding of the content, ideas, findings, and arguments presented in the materials studied.
3. Information Gathering: Information deemed relevant from various sources was collected and organized in a structured manner. This process allowed the researcher to develop a comprehensive understanding of the conceptual framework and theoretical underpinnings related to the research topic.
4. Critical analysis and synthesis: The information collected was critically analyzed. The researcher evaluates the strengths and weaknesses of each source and attempts to synthesize the information into a coherent conclusion.
5. Presentation of Findings: The results of the literature review are presented in the form of a structured and systematic report or scientific paper. Researchers are expected to communicate their understanding of the topic under study and present relevant and valid information to the reader.

Therefore, the initial stages of desk research play an important role in the research process, potentially providing a deeper understanding of the material under study and contributing to further methodological development and discoveries in the field of scientific research.

RESULT

Cyber Risk Management

Risk management is a process of identifying, measuring risks and forming strategies to manage them through available resources. Cyber risk is a risk caused by a threat in cyberspace. This cyberspace is a set of computers connected in one network including services, computer systems, controllers, embedded processors, and information stored or transmitted through it. Cyber risk management is a process to form strategies to manage problems that will occur in cyberspace (Briliyant & Ashari, 2018). Because it needs to be underlined that reducing and preventing cyber attacks is not an easy task.

The function of risk management considers that risks can be reduced but still recommends in the approach to cloud computing and to maximize its success factors. Although it is very difficult to overcome risks in cyberspace, it does not mean that the impact that will occur cannot be minimized (Herdiana et al., 2021). The strategy used in minimizing cybercrime starts with ourselves who must always keep an eye on the security system of the devices we have. Storing important data such as personal, financial and other information not on devices that are easily accessible to

others as an initial form of preventing data leaks that one has in cyberspace.

Steps in Risk Management

1. Risk Identification

This process involves identifying risks that may occur in an activity. Identifying risks accurately and completely is vital in risk management, one of the important aspects is to list as many possible risks as possible. Typical techniques that can be used in risk identification include: brainstorming, surveys, interviews, historical information, working groups, and others.

2. Risk Analysis

After identifying the risk, the next step is to measure the risk by looking at the potential severity of damage and the probability of risk occurrence. Determining the probability of something happening is very subjective and based on reason or experience. Some risks are easy to measure but it is very difficult to ascertain the probability of a very rare event. It is important to determine the best guess in order to properly prioritize the implementation of risk management planning.

3. Risk Management

In managing the risks that arise, the company identifies them by creating a master list of related risks and developing a risk reduction plan. Based on the identification, the company will calculate the risk value, both the default risk value (before mitigation) and the residual risk value (after reduction). Risks can be managed in various ways, such as avoidance, retention, diversification, or transfer to other parties. Some types of ways to manage risk:

a. Risk avoidance, deciding not to carry out activities that contain risk at all. In deciding to do so, it must consider the potential gains and potential losses generated by an activity.
b. Risk reduction, a method that reduces the likelihood of a risk occurring or reduces the damage caused by a risk.
c. Risk transfer, transferring risk to another party, generally through an insurance contract, security services, or the authorities.
d. Risk deferral, the impact of a risk is not always constant. Risk deferral involves delaying aspects of a project until a time when the probability of the risk occurring is low.
e. Risk retention, although certain risks can be eliminated by reducing or transferring them, some risks must still be accepted as an important part of the activity.
f. Risk mitigation, in risk management, refers to the steps taken to reduce or control risks associated with information security or organizational security systems. The main objective of risk mitigation is to reduce the likelihood of security threats and the impact they can have.

4. Risk Management Implementation

Risk management enables companies to identify and identify risks before losses occur. Therefore, companies must implement an effective risk strategy to optimize risk response and improve decision-making in every element of its business.

Cyber Risk Management as an Effort in Addressing the Risk of Fraud via Smartphone

For individuals, the risk of crime can result from various aspects such as financial, business, technical, political, legal, cultural and various other sectors. According to Darmawi (2006) in Agustina (2010) defines risk management as an effort to find out, analyze and control risks in every activity with the aim of obtaining higher effectiveness and efficiency. Theoretically, there are several important points about how social engineering affects human weaknesses, namely through fear, trust, and a sense of wanting to help (Indrajit 2013). So that in preventing the risk of social engineering crime, the stages of risk management are carried out:

a. Risk Identification

This process includes identifying risks that will likely occur in an activity. researchers use discussion media, the experience of fraud victims, and several trusted sources to identify the risks that will arise when dealing with online fraudsters. ie:

1. the victim loses property
2. victims are threatened with important personal data
3. being a victim of smartphone fraud but feeling unscathed
4. victims are exposed to continuous terror via smartphones such as whatsapp, SMS, or telephone.

b. Risk Analysis

After identifying the risks, the researcher carries out the next stage, namely risk measurement by looking at the potential for how much damage severity and probability of risk occurrence.

c. Risk Management

After identifying and analyzing risks, researchers enter the risk management stage, as for some risks that can be managed from the results of the previous risk analysis, namely:

- Risk transfer, transferring risk to other parties, generally through an insurance contract, security services, or authorities.
- Risk avoidance, deciding not to carry out activities that contain risk at all. In the case of fraud committed with telecommunications media, there are times when you should not be too rash in taking actions that trigger fraud factors such as carelessness, negligence, and carelessness in order to avoid the risk of fraud.
- Risk reduction, a method that reduces the likelihood of a risk occurring or reduces the impact of damage generated by a risk. in the case of fraud via smartphones that is rampant, it is possible that the risk of being exposed is very frequent, so a way is needed to reduce the impact and probability of fraud so that it is close to the smallest loss.
- Risk mitigation, in risk management, refers to the steps taken to reduce or control risks associated with information security or organizational security systems. The main goal of risk mitigation is to prevent the possibility of security threats and the impact they can have, so fraud via smartphones can be prevented by reducing or eliminating the factors that cause fraud.

CONCLUSION

In Indonesia, the law governing telecommunications is contained in Law No. 36/1999 on Telecommunications. In the context of cybercrime, especially in cases of fraud, crimes are increasingly evolving with the help of increasingly sophisticated technology. The current shift in crime patterns can be understood through a common routine approach, involving potential targets, lack of security awareness on social media, and offender motivation. Cyber risk management is important in identifying, measuring and managing risks associated with information security systems. While reducing cyber risks is not easy, steps such as keeping devices secure, not sharing sensitive information carelessly, and adopting risk mitigation strategies can help protect against cybercrime. Stages in risk management include risk identification, risk analysis, risk management, and risk strategy implementation. Implementing effective risk management can optimize responses to risks and increase success in dealing with security threats.

Declaration by Authors

Acknowledgement: None
Source of Funding: None
Conflict of Interest: The authors declare no conflict of interest.

REFERENCES

1. Briliyant, C. O., & Ashari, A. R. (2018). Rencana Penerapan Cyber-Risk Management Menggunakan NIST CSF dan COBIT 5. *Jurnal Sistem Informasi*, *14*(2).
2. Criminologyweb.com. *Routine Activities Theory: Definition Of The Routine Activity*

Approach To Crime. Accessed 4 May 2023. https://criminologyweb.com/routine-activities-theory-definition-of-the-routine-activity-approach-to-crime/

3. Darmaningrat, E. W. T., Ali, A. H. N., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi. *Sewagati*, *6*(2), 159-168.
4. Eristya Maya Safitri, Z. A. (2020). Analisis Teknik Social Engineering Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur. JIFTI - Jurnal Ilmiah Teknologi Informasi dan Robotika, 2(2).
5. Federal Trade Commission (2021). Pretexting: Don't Let Them Trick You. Diakses pada 8 Maret 2024. https://www.consumer.ftc.gov/articles/pretexting-dont-let-them-trick-you
6. Felson, M., & Cohen, L. E. (1980). Human ecology and crime: A routine activity approach. Human Ecology, 8(4), 389-406. doi:10.1007/BF01561008
7. Herdiana, Y., Munawar, Z., Putri, N. I., & Kunci, K. (2021). Mitigasi Ancaman Risiko Keamanan Siber Di Masa Pandemi Covid-19. *Jurnal ICT : Information Communication & Technology*, *21*(1), 42–52.
8. Kamran, M. & Maskun. (2021). *Penipuan Dalam Jual Beli Online: Perspektif Hukum Telematika*. 1(1), 40-45.
9. Mahardika, D. M. (2020). Kejahatan Siber Hoax di Ruang Digital Masyarakat Indonesia melalui Teori Aktivitas Rutin. *Jurnal Kriminologi Indonesia*, *16*(2).
10. Nurhadiyanto, L. (2020). Analisis Cyber Bullying Dalam Perspektif Teori Aktivitas Rutin Pada Pelajar Sma Di Wilayah Jakarta Selatan. *Jurnal IKRA-ITH Humaniora*, *4*(2).
11. Purwono. (2008). *Studi Kepustakaan.* Yogyakarta: Pustakawan Utama UGM.
12. Rafizan, O. (2013). Analisis Penyerangan Social Engineering. *Masyarakat Telematika dan Informasi*, *2*(2), 115-126.
13. Rizki, F. M., & Zaky, M. (2019). Analisis Kriminologis Korban Cyber Fraud Pada Transaksi Game Online Melalui Steam. *Anomie*, *1*(1). www.valvesoftware.com
14. Siti Hadijah. (2021). *Serem! Begini 5 Teknik Penipuan Social Engineering yang Bisa Bikin Melarat.* Diakses pada 4 Mei 2023. https://www.cermati.com/artikel/serem-begini-5-teknik-penipuan-social-engineering-yang-bisa-bikin-melarat
15. Zahrulswendar, I. dkk. (2021). *Penegakan Hukum Tindak Pidana Penipuan Melalui Sarana Panggilan Suara dari Telepon Seluler.* Vol 2, No. 3. (147-149).

How to cite this article: Muh. Ardilla Amry. Cybercrime risk management efforts to overcome digital fraud. *International Journal of Research and Review*. 2024; 11(6): 546-550. DOI: *https://doi.org/10.52403/ijrr.20240660*

******