CUSTOMER DATA LEAKS AND CYBER ATTACKS IN BANKING INDUSTRY: A PHENOMENOLOGICAL RESEARCH

Mercurius Broto Legowo*
Perbanas Institute
*Corresponding Author: mercurius@perbanas.id

Deden Prayitno
Perbanas Institute
deden@perbanas.id

Budi Indiarto
Perbanas Institute
budi.indiarto@perbanas.id

Abstract *- There was a phenomenon of customer data leaks and cyberattacks on the banking sector in Indonesia some time ago. These phenomenon able to be concern for academics and practitioners in the banking industry to study. Appropriate Enterprise Risk Management in Banking in this study is a way of investigating these two phenomena. The main objective of this study is to examine the role of Enterprise Risk Management in the phenomenon of customer data leakage and cyber attacks in the banking industry using a phenomenological research approach. The phenomenological research method is a method in research to study how individuals subjectively experience and make sense of a phenomenon. The stages in identifying and analyzing the phenomenon of customer data leakage and cyber attacks in the banking industry had carried out at the beginning of the study. Then, giving meaning through the Enterprise Risk Management (ERM) framework analysis method. Finally the two risks of this phenomenon were described. The results of this study describe the risk phenomena that occur in banking related to customer data leaks and cyber-attacks through the Enterprise Risk Management framework approach. Proper Enterprise Risk Management will minimize the risk of customer data leaks and cyberattacks. This study is expected to contribute to making brief policy recommendations on risk management related to customer data leaks and cyber attacks for the Financial Services Authority in Indonesia, as the financial and banking regulator.*

Keywords: *cyber-attack risk, customer data leakage, ERM-framework, phenomenological research*

I. INTRODUCTION

In the past, there has been a phenomenon of customer data leakage and cyber attacks on the banking industry in Indonesia. There is a phenomenon where 15 million customer data for one of the biggest sharia banks in Indonesia experienced errors and data leaks in May this year. The total data leaked and stolen reached 1.5 Terabytes, including 15 million user data and passwords for internal access and services, as well as customer personal data and loan information(CNN Indonesia, 2023). In addition, the disruption to sharia banking services, which is strongly suspected of being the result of a ransomware-type cyber attack, should serve as a lesson for others banks in Indonesia. In another phenomenon, an insurance company owned by the National Bank in Indonesia also experienced a data leak incident in July 2021. Data on two million insurance customers owned by this national bank were leaked and sold online. Information on the customer data leak of BRI Life customer data had uploaded to a Twitter account on Tuesday, 27 July 2021. Hackers allegedly stole 250 gigabytes of the insurance company's customer data and sold it for US$ 7,000 or Rp. 101.5 million (Rosana, 2017).

According to the Ministry of Communication and Informatics, which had reinforced by data from the Coordinating Ministry for Political, Legal and Security Affairs, there is a phenomenon that Indonesia receives 1.225 billion cyber attacks every day(Yuliani, 2017). These phenomenon able to be concern for academics and practitioners in the banking industry to study.

Banking is an industry that must be responsive to various fundamental risks that can affect its performance(Kurniawan, Rahayu, & Wibowo, 2021). According to Vaidyula & Kavala(2018) Risk management in the banking industry is in the spotlight, especially after the recent turbulence, which had a very-bad impact on the existence of the banking sector as a viable industry. Not only banks but even various government agencies have recognized the result/impact of not managing risk effectively in the bank, and therefore several regulations have been enacted to control the risks that arise in the business of the banking industry.

These phenomenon able to be concern for academics and practitioners in the banking industry to study. Leakage of customer data is a phenomenon when sensitive data, such as customer personal data, is exposed on the internet. The risk of data leakage can occur from financial service actors selling consumer data, providing data to third parties and the possibility of data application systems that are easily accessed and hacked by hackers(Soemitra & Adlina, 2022).

Meanwhile, the risk of cyberattacks becoming a threat to stability in Indonesia financial institutions, particularly in the banking industry. Cyberattacks are one of the most threatening risks national security(Vimy et al., 2022). Cyber attack risk is the risk of harm from attacks through cyberspace by companies that disrupt, destroy, or maliciously control computing environments/infrastructures, destroy data integrity, or steal data and information(Luthfah,2021).Appropriate ERM (Enterprise Risk Management) in Banking in this study is a way of investigating these two phenomena.

In November of 2022, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) released a new and more detailed and complex ERM framework titled "Compliance Risk Management: Applying COSO-ERM Framework. The Coso ERM Framework"(COSO,2020) is an internal control framework consisting of five interrelated components and twenty ERM principles to assist company executives in understanding and managing risk to improve company performance, as shown in Figure 1.

Figure 1 ERM Framework with Five Components And The Principle(COSO, 2020)

Good ERM helps businesses maintain access to finance and enables them to implement their goals with value added investments. (Kumar, 2022).

Several academics previously conducted studies on consumer data leakage, cyberattacks in banking, and the ERM framework. This study from Haliwela(2023) aims to examine regulations related to the protection of customer personal data and to examine them supervision and law enforcement on the protection of banking customers' personal data of cases of data leakage that may occur. Tariq's study (2018) aims to explore the impact of cyberattacks at financial institutions. This study concludes that banking as a financial institution has a higher content cyber risks compared to other institutions(Tariq, 2018). Candy's study discusses Enterprise Risk Management Best Practices and their impact on the Performance of Rural Banks in Indonesia(Candy, 2021). This study is not related to the problem of data leakage and cyberattacks in the banking sector. According

to Oyewo's study (Oyewo, 2022), ERM improves long-term performance and effective risk management to competitive strategy to survey risk turbulence that usually occurs in the banking sector. Another study using phenomenological research by Bakioğlu et al,(2022) revealed that their qualitative study had been designed by the phenomenological design to explore the role of emotional orientations in academics' professional life. However, this research is not related at all to data leaks and cyberattacks in the banking industry.

Based on the risk phenomena that have been mentioned, it is necessary to have an appropriate analytical study using a phenomenological research approach. The phenomenological approach aims to explain specific things and identify phenomena through how individuals subjectively experience and give meaning to them(Larsen & Adu, 2021). In research, phenomenological design, a qualitative research method, was used (Greening, 2019),(Balikci, 2019).

This research aims to analyze the risk phenomenon of customer data leaks and cyberattacks in the banking industry through the Enterprise Risk Management Framework approach, particularly in Indonesia banking.

The following are the specific goals of this phenomenological study:

1) Bracketing to identify the process for a previous opinion or statement related to the risk phenomenon of customer data leaks and cyberattacks in the banking industry .
2) Intuition the views of experienced interviewees to generate a general understanding of the risk phenomenon of customer data leaks and cyberattacks in the banking industry.
3) To analyze and understand the risk phenomenon of customer data leaks and cyberattacks in the banking industry using the ERM Framework.
4) Describing the risk phenomenon of customer data leaks and cyberattacks in the banking industry through the ERM Framework analysis approach. research is not related at all to fintech and banking.

This study analyzes the risk phenomenon of customer data leaks and cyberattacks in the banking industry through an enterprise risk management framework, and a phenomenological research approach is a novelty produced in this research.

The results of this study contribute to making brief policy recommendations on customer data leaks and cyberattacks risk management for Indonesian banking regulators in the future.

II. METHODS

This phenomenological research on the risk management of customer data leaks and cyberattacks uses a qualitative approach. According to Alhazmi and Kaufmann(Alhazmi & Kaufmann, 2022), through phenomenology, a qualitative research technique, the researcher aims to understand how one or more participants perceive a phenomenon (event, situation, concept, etc.). There are several stages to conducting research using a phenomenological approach, including bracketing, intuition, analysis, and description(Greening, 2019; Larsen & Adu, 2021)

Data Collection

This study's data collecting method is related a phenomenon of customer data leakage and cyber attacks on the banking industry in Indonesia. First, data collection from literature study(Creswell & Creswell, 2023) used in the bracketing stage of this phenomenological research. Second, conduct interviews(Creswell & Creswell, 2023) with informants from praktisi perbankan representatives who understand the customer data leaks and cyberattacks in their business, as well as representatives akademisi who have knowledge competence about customer data leaks and cyberattacks. Data from the interview results as data input for the second stage of this study. Third, document study data from the COSO of the Treadway Commission's Enterprise Risk Management Framework(COSO, 2020) for input to the analyzing stage of this study. Finally, field

observations(Creswell & Creswell, 2023) to complement the data collection had also carried out at several banks that have managed customer data leaks and cyberattacks in business. Triangulation of this research will ensure the credibility of the study results.

Data Analysis

There are four risk phenomena of customer data leaks and cyberattacks (F-1 and F-2) as initial data to be analyzed.

In phenomenological research, data analysis had carried out through four research stages. In the first stage of Phenomenological Research (FR-1), namely bracketing by identifying four risk phenomena (F-1 and F-2) by referring to related references. Next, the second stage (FR-2) is intuition by interpreting the results of stage 1 according to experience derived from interviews with two informants representing banking and fintech. In the Analysis Phase (FR-3), the results of the second stage are then analyzed by aligning the ERM framework concept, namely through the five related ERM components. Describing is the final stage of phenomenological research (FR-4), where all the results in the previous one, the risk phenomena of customer data leaks and cyberattacks, are explained more accurately in line with the ERM Framework. Analysis of these four stages is something in phenomenological research

III. RESULTS AND DISCUSSION

The results and discussion of this study are based on the results of the four stages of phenomenological research. Furthermore, the findings of each research stage and the implications of the research are contained in the discussion section.

Results

Results in phenomenological research, according to the State of the Art in this study. The stages of the results are as follows:

1) Bracketing Stage

Bracketing is the identifying process for a previous opinion or statement related to the risk phenomenon of bank and fintech collaboration. The risk identification of customer data leaks and cyberattacks consists of two risk phenomena. Each of these risks is identified by referring to previous studies. Table 1 displays the outcomes of the risk identification of bank and fintech collaboration.

Table 1 Risk Phenomenon Identification

Risk phenomenon	Identification
Risk of leakage of customer data	The risk of customer data leakage is the risk resulting from excessive uploading of sensitive personal data to the internet. The risk of data leakage can occur from financial service actors selling consumer data, providing data to third parties and the possibility of data application systems that are easily accessed and hacked by hackers(Soemitra & Adlina, 2022).
Risk of Cyber Attacks	Cyberattacks are one of the most threatening risks national security(Vimy et al.,2022). Cyber attack risk is the risk of harm from attacks through cyberspace by companies that disrupt, destroy, or maliciously control computing environments/infrastructures, destroy data integrity, or steal information(Luthfah, 2021).

2) Intuiting Stage

Intuiting, which is the process that occurs when the researcher is open to the meaning associated with the phenomenon based on the views of participants who experience it, results in a general understanding of the risk phenomenon in this study. In this stage, the opinion of a representative from banking praktisi (BP=Bank Practioner Representative) and Representatives of academics who are also bank customers who understand IT and banking are considered competent to contribute to research had selected for research subjects or participants who understand the

risk of customer data leakage and the risk of cyber attacks. Summary of interview results and opinions of participants, in Table 2.

Table 2 Summary of Interview Results and Opinions of Paticipants

Risk phenomenon of Leakage of Customer Data and Cyber Attacks	Summary of Interview Results and Opinions of Participants
Risk of leakage of customer data	Banking Practitioner Representative: Banks are required to maintain the trust of their customers by preventing data leakage. Many things lead to the risk of leakage of bank customer data, one of which is the intentional element of selling customer data. Academic Representative: Data leakage in current banking services is inseparable from two factors: The first is the consumer factor due to consumer behavior in online banking transactions and providing personal data. Second, the data leaks from financial service actors by selling consumer data and providing data to third parties, and data banking system applications to be easily hacked by hackers.
Risk of Cyber Attacks	Banking Practitioner Representative: Banking realizes that the more use of the internet and digital technology a bank makes, the higher the risk of cyberattacks it faces. The banking industry is aware of all threats from internal and external cyberattacks. Academic Representative:: Overcoming the risk of cyber attacks in banking can be done through proactive actions, strengthening regulations, and establishing a reliable framework or procedure for cyber security governance.

3) Analyzing Stage

Analyzing is a process that involves another research process, namely the ERM Framework analysis approach to reveal the meaning of the risk phenomenon of leakage of customer data leaks and cyberattacks.

The results of the interviews were analyzed by considering the risk phenomenon of customer data leaks and cyberattacks and related ERM framework components shown in Table 3.

Table 3 Analysing Based on the Risk Phenomenon of Leakage of Customer Data and Cyber Attacks

ERM Framework Components	Analysing Based on the Risk Phenomenon of Leakage of Customer Data and Cyber Attacks
Governance and Culture	Reliable governance will help determine preventive and corrective action steps for risks of customer data leakage and cyberattacks in the future by reinforcing the importance of sustainable banking activities.
Strategy and Objective-setting	Methods for formulating planning strategies in mitigating risks include risk management strategies, and a collection of objects. Planning Strategies considers all the risks of customer data leakage and possible cyberattacks. Implementing this strategy according to these two types of risks that may occur forms the basis for identifying, assessing, and responding to that risks that arise in the future.
Performance	The risks of customer data leaks and cyber attacks certainly have the potential and impact on banking performance problems. Then strategy implementation is reviewed and assessed to minimize that risks that occur. Organizations must be able to identify the level of risk and develop alternative strategies based on priorities that lead to opportunities for corporate development by implementing risk management strategies to improve the quality of banking performance.
Review and Revision	Banking must be able to review and revise all activities that had carried out as a consideration to estimate the various factors for the occurrence of these two risks so that they can be prevented and avoided in the future by developing new planning strategies following the ongoing results of banking risk management, to ensure that everything goes according with relevant risk control level procedures.
	Banking that has implemented risk

ERM Framework Components	Analysing Based on the Risk Phenomenon of Leakage of Customer Data and Cyber Attacks
Information, Communication and Reporting	management needs to make a report that describes all information related to ongoing processes starting from identification to resolution of risks as an action to carry out risk management of customer data leakage problems and cyber attacks on a regular and continuous basis, where the results of these reports will be communicated to all stakeholders so that the results of the information obtained can be the basis for decision making.

4) Describing Stage

Describing is the stage in which researchers describe the risk phenomenon of customer data leakage and cyber attacks through the ERM Framework analysis approach; the results are in Table 4.

Table 4 Summary of Interview Results and Opinions of Paticipants

Risk phenomenon of Leakage of Customer Data and Cyber Attacks	Describing Risk phenomenon of Leakage of Customer Data and Cyber Attacks through the ERM Framework Analysis
Risk of leakage of customer data	Laws and regulations from the government, as well as banking risk management strategies through the ERM framework, must protect public data from cases of leakage of bank customer data that are currently common.
Risk of Cyber Attacks	Cyberattacks pose significant banking management risks. Following the ERM framework, banking performance requires governance and culture readiness measures in cyberattack risk identification, control of implementing personnel, multiple authentication, periodic audits, protection of critical data, and risk testing.

Discussion

This study emphasizes the analysis of the risk phenomenon of customer data leakage and cyber attacks through the Enterprise Risk Management framework in phenomenological research.The use of phenomenological research on the grounds that this research is to study how individuals (practitioners and banking customers) subjectively experience and give meaning to this phenomenon. The phenomenological research methodology is often associated with the four necessary stages: Bracketing, Intuiting, Analyzing, and Explain(Greening, 2019).

This study has objective differences from previous studies on phenomenological research, customer data leakage, cyber attacks, and ERM Framework research. Phenomenological study from Bakioğlu et al.(2022) explore the role of emotional orientation in the professional life of academics. However, this research is unrelated to data leaks and cyberattacks in the banking industry. Haliwela's (2023) study on the protection of banking customer personal data or another study from Tariq (2018) on the impact of cyberattacks on financial institutions, without using the ERM framework application and not phenomenological research. Other studies related to the application of ERM in banking can support this study, but are not similar and related to customer data leakage and cyber attacks(Candy, 2021; (Oyewo, 2022).

The first risk phenomenon related to Risk of leakage of customer data.It identified that The risk of customer data leakage can occur from financial service actors selling consumer data, providing data to third parties and the possibility of data application systems that are easily accessed and hacked by hackers(Soemitra & Adlina, 2022). This risk phenomenon is in line with the results of interviews with Banking Practitioner Representative, who revealed that *banks must maintain the trust of their customers by preventing data leakage*. Furthermore, Academic Representative: stated that *the leakage factor from the perpetrators of financial services by selling consumer data, providing data to third parties, and data application systems easily hacked by hackers*. So according to the ERM Framework, this phenomenon is most important from a governance and cultural perspective as part of a collaborative planning strategy. In describing

the stage, this risk phenomenon has an impact on performance. Laws and regulations from the government, as well as banking risk management strategies through the ERM framework, must protect public data from cases of leakage of bank customer data that are currently common. So it requires regular and clear reviews and revisions of all information, communication, and reporting.

The second risk phenomenon related to Risk of Cyber Attacks. In the Bracketing Stage, the study from Luthfah in 2021 identified that cyber attack risk is the risk of harm from attacks through cyberspace by companies that disrupt, destroy, or maliciously control computing environments / infrastructures, destroy data integrity, or steal information.(Luthfah, 2021).

Bank Representatives (BR) stated that *the financial and banking sector be aware of the threat of cyber attacks from internal sources and external cyber-attacks*, and supported by statements a person from Fintech Representatives(FR) that *cyber attacks or cybercrime in Fintech through proactive actions, strengthening regulations, and establishing a reliable cyber security framework or procedure.* Referring to the ERM Framework, the risk of a cyber attack necessitates internal or external security governance and prevention culture, regular and clear review and revision, periodic information, communication, and reporting. The results at describing stage conclude that government laws or strategies to prevent possible cyberattacks within the risk management framework must have the best possible plan to protect public data from cases of data leaks that currently occur frequently, which are also caused by cyberattacks.\

This research has theoretical and practical implications for government efforts to develop concise risk management laws and regulations for the banking ecosystem, as well as the role of the ERM Framework in preventing future customer data leaks and cyberattacks on the banking industry.

This study has limitations in discussing only the risk of customer data leakage and the risk of cyberattacks in the context of the banking industry in Indonesia. The other risk phenomena tin the banking industry related to the ERM Framework not discussed in this study.

IV. CONCLUSION

This study emphasizes analyzing the Risk phenomenon of Leakage of Customer Data and Cyber Attacks through the Enterprise Risk Management framework in phenomenological research.

This phenomenological research generally concludes that: (1) the stages of identifying customer data leaks and cyber attacks are the initial stages of research that carried out; (2At the intuition stage, the views of participants, including representatives of banking practitioners and academics who understand and experience this in a clear understanding of the phenomenon of risk of customer data leakage and cyber attacks; (3) In the analysis stage, the risks of customer data leakage and cyber attacks are analyzed through the ERM Framework approach for strategies to minimize those risks in the short and long term; (4) The description stage describes the importance of the ERM framework analysis approach in bank risk management related to the risk of customer data leakage and cyber attacks.

For further research, it is necessary to study the development of IT risk management through the use of Artificial Intelligence in banking, which has attracted the attention of many researchers.

ACKNOWLEDGMENT

The authors would like to express their appreciation to the Directorate of Higher Education of the Ministry of Education, Culture, Research, and Technology in the Republic of Indonesia for its assistance in providing research grants with the third-year Fundamental Basic Research Scheme in 2023

(contract number:1174/LL3/AL.04/2023, dated May 10, 2023).

REFERENCES

Alhazmi, A. A., & Kaufmann, A. (2022). Phenomenological Qualitative Methods Applied to the Analysis of Cross-Cultural Experience in Novel Educational Social Contexts. *Frontiers in Psychology*, *13*(April), 1–12.

Bakioğlu, A., Keser, S., Korumaz, M., & Ala, Ş. D. (2022). A phenomenological research on the role of emotional orientation in academics' professional lives. *Journal of Pedagogical Research*, *6*(1), 196–213.

Balikci, A. (2019). A Phenomenological Research on the Evaluation of Teacher Candidates from the Perspective of School Administrators. *International Journal of Contemporary Educational Research*, *6*(2), 468–482.

Candy. (2021). Best Practice of Enterprise Risk Management : the Impact on Rurals ' Bank Performance. *International Journal of Economics, Business and Accounting Research (IJEBAR)*, *2021*(2), 231–237.

CNN Indonesia. (2023). Kominfo Clarifies the Alleged BSI Data Leakage Circulating. In *CNN News*. Retrieved from https://www.cnnindonesia.com/teknologi/20230522122857-192-952382/kominfo-klarifikasi-soal-dugaan-bocoran-data-bsi-yang-beredar

COSO. (2020). *Compliance Risk Management: Applying The COSO ERM Framework*. *COSO*. Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Creswell, J. W., & Creswell, J. D. (2023). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. *SAGE Publications, Inc* (Sixth Edit). SAGE Publications Asia-Pacific Pte. Ltd.

Greening, N. (2019). Phenomenological Research Methodology. *Scientific Research Journal*, *VII*(V).

Haliwela, N. S. (2023). The Essence of Legal Protection of Personal Data of Customers In Banking Transactions. *Sasi*, *29*(3), 548.

Kumar, S. (2022). Risk Management Framework. *SSRN Electronic Journal*, (January), 3–24.

Kurniawan, A., Rahayu, A., & Wibowo, L. A. (2021). The Effect of Digital Transformation on the Performance of Regional Development Banks in Indonesia. *Jurnal Ilmu Keuangan Dan Perbankan (JIKA)*, *10*(2), 158–181.

Larsen, H. G., & Adu, P. (2021). *The Theoretical Framework in Phenomenological Research*. *The Theoretical Framework in Phenomenological Research*. Routledge.

Luthfah, D. (2021). Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law. *Jurnal Hukum Humaniter Dan HAM*, *3*(1), 11–22.

Oyewo, B. (2022). Enterprise risk management and sustainability of banks performance. *Journal of Accounting in Emerging Economies*, *12*(2), 318–344.

Rosana, F. C. (2017). BRI Life Customer Data Leaks Evidence of Weak Protection and Regulation. In *Tempo.co.id*. Retrieved from https://fokus.tempo.co/read/1488710/kebocoran-data-nasabah-bri-life-bukti-lemahnya-proteksi-dan-regulasi

Soemitra, A., & Adlina. (2022). Consumer Protection Against Data Leakage in Financial Services in Indonesia. *Jurnal Insitusi Politeknik Ganesha Medan Juripol*, *5*, 288–303.

Tariq, N. (2018). Impact of Cyberattacks on Financial Institutions. *Journal of Internet Banking and Commerce*, *23*(2), 5391–5423.

Vaidyula, S. R., & Kavala, J. (2018).

Enterprise Risk Management for Banks.

Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & ... (2022). The Threat of Cyber Attacks on Indonesia's National Security. *Jurnal Kewarganegaraan*, *6*(1), 2319–2327.

Yuliani, A. (2017). Indonesia Attacked by Hackers Billion Times Every Day. In *KOMINFO.go.id*. Retrieved from https://www.kominfo.go.id/content/detail/11956/indonesia-diserang-hacker-miliaran-kali-tiap-hari/0/sorotan_media