ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue XII December 2024

Corporate Communication Strategy of Bank Mandiri (Persero) Tbk. Regarding the Implementation Process of Awareness Regulation in Cyber Resilience and Security

Wahyudi Maulana[1], Gloria Angelita[2]

Postgraduate, Sahid University[1]

Postdoctorate, Sahid University[2]

DOI: https://doi.org/10.51244/IJRSI.2024.11120054

Received: 22 December 2024; Accepted: 28 December 2024; Published: 17 January 2025

ABSTRACT

Corporate communication has an important role in distributing information from a program in the company to all its employees and customers, especially large corporations that have a very high risk of hacking because the increasing size of the corporation is not balanced with a cyber security and resilience system and all elements of the company, not aware of the importance of cyber data security will cause a lot of losses that must be faced even to the point of losing reputation or bankruptcy. Cyber resilience and security are not only the task of securing the IT system but also the task of anyone related to it, be it internal, external employees, or customers, each have their own role in awareness in maintaining cyber resilience and security. Effective communication provided in a structured IT security system will create structured and measurable security and make the IT security system relatively more secure from cyber attacks from parties who want to take advantage of unjustifiable.

Keywords:cyber security, hacking, corporate communications, reputation

INTRODUCTION

The industrial revolution 4.0 has brought rapid digital transformation in various sectors, including the business world. The increasing dependence on the use of information and communication technology that is very intensive in company operations has increased efficiency and productivity. However, on the other hand, this also opens up opportunities for cybercriminals to launch increasingly sophisticated and organized attacks.

One sector that has great potential for hacking is companies in financial services, especially banking, which in this case, apart from having data from human resources, also has sources of funds that make banking companies a very vulnerable sector.

The National Cyber and Crypto Agency (BSSN) stated that the financial sector is one of the industries most vulnerable to cybercrime threats. Director of Cyber Security and Crypto for Finance, Trade, and Tourism BSSN, Edit Prima, revealed that the trend of internet traffic anomalies in Indonesia showed extraordinary numbers, namely 1.6 billion incidents in 2021, 976.4 million incidents in 2022, and 151.4 million incidents in 2023.

Hacking of company data can cause huge losses, both financially and non-financially. (According to Dancor: 2023) there are at least six major impacts that will occur if a company experiences hacking, namely loss of revenue, damage to brand reputation, loss of intellectual property, hidden costs, experiencing online vandalism, difficulty in getting new employees.

In line with the direction of the Financial Services Authority, digital transformation driven by rapid advances in Information Technology has fundamentally changed the landscape of the financial services industry, especially the banking sector. Banking institutions can now take advantage of various technological

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue XII December 2024

innovations, such as artificial intelligence, big data analytics, and cloud computing, to optimize all aspects of operations, from opening accounts to managing investment portfolios.

The application of information technology provides a number of significant benefits. Business processes that previously took a long time and involved a lot of manualization can now be done automatically and in real time, thereby drastically increasing efficiency and productivity. In addition, the integration of information systems allows banks to collaborate more closely with various parties, including fintech, technology companies, and payment service providers, to provide more comprehensive financial solutions.

However, behind all the convenience and benefits offered, increasing reliance on technology also brings a number of new risks. Cyber threats such as ransomware attacks, data theft, and system disruptions can disrupt bank operations, damage reputations, and cause significant financial losses. Therefore, it is important for the banking industry to continue to improve information system security and implement good technology governance.

One of the biggest challenges faced by the banking industry due to the rapid development of information technology is the increasing cyber risk. Cyber threats such as ransomware attacks, phishing, and theft of customer personal data can paralyze the bank's operational system, resulting in significant financial losses, and damaging the institution's reputation. Therefore, banks are not only required to build a strong cybersecurity system, but also must have the ability to respond quickly and effectively in detecting, responding to, and recovering systems affected by cyber incidents.

To manage cyber risk comprehensively, banks need to implement good information technology governance, including conducting regular risk assessments, developing clear security policies, and integrating cybersecurity into all business processes. In addition, banks must also proactively carry out prevention, detection, and response efforts to cyber threats, such as using intrusion detection systems, conducting security training for employees, and collaborating with cybersecurity experts.

In order to support banking efforts in maintaining cybersecurity, the Financial Services Authority (OJK) has issued Regulation Number 11/POJK.03/2022 concerning the Implementation of Information Technology by Commercial Banks (POJK PTI). POJK PTI regulates in detail the cybersecurity requirements that must be met by banks, ranging from customer data protection, cyber risk management, to handling security incidents. Furthermore, OJK also issued a circular to provide more specific technical and implementation guidance for banks in complying with the provisions of POJK PTI.

Corporate communication is the way a company interacts with various groups of people. These groups include internal publics, such as employees, as well as external publics, such as competitors, suppliers, customers, and others (Argenti, 2009).

Cyber resilience is a capability that enables a banking institution to maintain its business continuity in the face of increasingly complex and dynamic cyber threats. This includes the ability to anticipate, detect, respond to, and recover from cybersecurity incidents. Meanwhile, cybersecurity itself refers to a series of actions and mechanisms aimed at protecting the confidentiality, integrity, and availability of information assets. The concept of cybersecurity has evolved beyond these traditional aspects, now also encompassing broader information security principles such as authentication, non-repudiation, and reliability. In other words, cybersecurity is a strong foundation for cyber resilience, enabling banks to operate safely and efficiently in a digital environment full of risks.

Effectiveness of communication in organizations, especially in the banking sector, is a crucial factor in achieving business goals. The linear communication model proposed by Shannon and Weaver (1949) provides a basic framework for understanding the communication process. This model describes communication as a one-way process involving a sender, the message itself, a communication channel, a receiver, and potential noise. However, in the context of modern organizations, communication is often two-way and involves complex interactions between various parties. Noise in organizational communication is not limited to semantic or technical issues, but can also be influenced by cultural, structural, and psychological factors.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue XII December 2024

Cornelissen (2008) emphasizes the importance of considering the social and cultural context in understanding \the dynamics of organizational communication.

The Financial Services Authority (OJK) has issued a regulation requiring banks to implement strict cybersecurity standards. This regulation aims to protect customers from various cyber threats, such as data theft, malware, and phishing attacks.

As of June 2022, Bank Mandiri has formed an EDA (Enterprise Data Analytics) Division consisting of more than 140 data scientists and data analysis professionals. In addition, the bank operates a CISO Division, consisting of 87 employees dedicated to managing cybersecurity threats. To ensure compliance with international standards and best practices, Bank Mandiri has also implemented and obtained certifications in various fields:

1. ISO 27001 for Security Operations Centers that manage cyber security threats in banking systems and cyber operations.
2. ISO 9005 for Contact Centers, Data Center Operations, Disaster Recovery Centers and IT Infrastructure.
3. ISO 20000 for IT Application Support.
4. ISO 37001:2021 for Anti-Bribery Management Support.
5. ISO 17025:2017 for Digital Forensic Laboratories.
6. ISO 90001 for Contact Centers, Data Centers, Disaster Recovery Centers and IT Infrastructure.
7. Bank Mandiri has a CSIRT (Computer Security Incident Response Team) that is able to detect and respond well to cyber security incidents that are registered with the National Cyber and Crypto Agency (BSSN).

Bank Mandiri maintains a CSIRT that has the expertise to detect and respond to cybersecurity incidents effectively. As a commitment to strengthen cybersecurity defense and actively contribute to national cybersecurity efforts, Bank Mandiri's CSIRT is registered with the National Cyber and Crypto Agency (BSSN).

The scope of the personal data protection strengthening program is not only for customer personal data, but also for the processing of employee personal data and personal data of third parties who collaborate with Bank Mandiri.

According to (Fornia Kempilasari: 2024) Cybersecurity has become a top priority in various industrial sectors around the world. Companies not only need to protect their data, but also ensure that every employee understands the importance of their role in maintaining that security. Employee education in cybersecurity is one of the most important investments a company can make to protect its digital assets.

With the advancement of technology and the rise of cyber threats, the need for comprehensive cybersecurity training for employees is becoming increasingly urgent. Cyberattacks can happen at any time, and employees are often the starting point of attacks through phishing, malware, or other social engineering techniques. Therefore, a basic understanding of cybersecurity practices needs to be instilled in every individual in the organization.

Formulation of the Problem

Looking at the description of the background, the main problem is how to implement corporate communication strategies in adapting customer service in implementing regulations on cyber resilience and security at Bank Mandiri in the Gambir area?

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue XII December 2024

The sub-problems are:

1. How is the implementation of corporate communication strategies within Bank Mandiri employees?
2. How do customers respond to the implementation of Bank Mandiri's Awareness program?
3. What are the inhibiting factors in corporate communication strategies within Bank Mandiri Gambir Branch employees?

Scope of Problem

From the background and identification of the problem above, the problem limitations in this study are as follows:

1. The object to be studied is the strategy of Bank Mandiri (Persero) Tbk in the IT Security Awareness division.
2. This research's corporate communication strategy is interpreted as a form or model of strategy for implementing the IT Security Awareness program.
3. Samples were taken from employees, especially in the Service Division at Bank Mandiri Gambir Branch.

Research Purposes

The purpose of this study is to collect relevant data to solve the problems that have been formulated in the problem formulation. The specific objectives of this study include:

a. Identifying the role of Bank Mandiri's corporate communication strategy in implementing Security Awareness to all employees.

b. Analyze and identify supporting elements in the implementation of cyber security and resilience programs.

LITERATURE REVIEW

Definitions and Basic Concepts

Corporate communication is the integration of various organizational communication functions, marketing, and management to create a unified organizational message. This definition refers to the view of Van Riel (1995), who identified corporate communication as a framework that aligns various communication specializations to form a consistent organizational identity and image, which aims to improve organizational performance.

Paul A. Argenti (2009) expanded on this concept, stating that corporate communications is a strategic function on par with finance, marketing, and human resources. Its primary focus is on managing the organization's reputation through consistent communication to both internal and external constituents. In the digital age (Argenti, 2023), communication integration is crucial to maintaining message continuity across channels, supporting a positive image, and addressing the challenges of a dynamic business environment.

Corporate communications encompasses more than just public relations; it involves internal, investor, and media communications, as well as strategic messaging that supports the company’s vision and mission. Strong relationships with internal constituents increase employee engagement, while external communications help maintain relationships with customers and regulators, supporting corporate sustainability.

Communication Strategy Components

According to Argenti (2023), the core elements of corporate communication include identity, image, and

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue XII December 2024

reputation. Identity represents how the company wants to be known; image is the public's perception of the company; while reputation is the result of evaluating both aspects. Consistency between identity and image ensures a strong reputation, which is a strategic tool for building trust.

Strategic communication is a planned process to convey messages to audiences with the aim of supporting organizational strategies. Hardjana (2008) highlights the importance of thorough strategic planning, including the preparation of contingency plans to deal with crisis situations.

Strategy to Increase Regulation Awareness

In the face of regulatory changes, companies are required to be proactive in managing public perception through strategic communication. Hardjana (2008) emphasized the importance of a strong corporate reputation as a foundation for sustainability. In the digital era, cybersecurity regulations are a major concern, with strategic communication playing a role in building organizational trust and resilience (Argenti, 2023).

The use of internal media, such as intranets and applications, accelerates the dissemination of information to employees. In external communications, social media and digital education campaigns help raise customer awareness of regulations and cybersecurity.

Strategic Planning and Implementation

Dowling (1986) highlighted that strong internal communication supports organizational culture, which contributes to external image. In the context of cyber threats, Bank Mandiri can use public campaigns and training to increase public awareness.

The combination of direct and digital communication allows companies to reach a wider audience. Argenti (2023) underlines that message consistency across channels is critical to reputation management.

Cyber Resilience and Security

In the digital era, cyber threats pose a major challenge to a company's reputation. An integrated corporate communications strategy, including an emergency response plan, is needed to effectively manage this risk (Argenti, 2023).

Regular training and threat simulations help companies build a security-aware culture, which supports risk mitigation efforts.

Crisis Communication and Reputation Management

Contingency planning is key in dealing with a crisis. Lerbinger (1997) asserts that transparency in communication helps manage public perception, which is critical to preventing crisis escalation.

A strong reputation is built through consistency in communication, products, and services. Hardjana (2008) notes that strategic communication plays a vital role in maintaining relationships with stakeholders and supporting long-term profits.

METHOD

This study uses a qualitative descriptive method with the aim of describing the corporate communication strategy implemented by Bank Mandiri Area Gambir in conveying messages about cyber resilience and security. The qualitative descriptive method aims to gain an in-depth understanding of the phenomenon being studied through words, images, and observations, not numbers. This approach is used because it focuses more on ideas, perceptions, and opinions that cannot be measured quantitatively. This study also uses a constructive interpretive approach, where researchers describe and analyze events that occur at Bank Mandiri Area Gambir through interviews, field notes, and documentation.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue XII December 2024

The paradigm used in this study is postpositivism, which recognizes that knowledge cannot be achieved absolutely through observation alone. This approach considers various influencing factors as well as in-depth analysis of existing data. This study focuses on the institutional conditions of Bank Mandiri Area Gambir before and after the implementation of the cybersecurity system.

The subjects of the study were people who were considered relevant in Bank Mandiri Gambir Area, especially those who had knowledge about the communication strategies implemented. This study used purposive sampling techniques to select informants who met certain criteria that were in accordance with the objectives of the study. The object of the study was the corporate communication strategy implemented by Bank Mandiri in building brand reputation, which includes internal and external communication.

The data used in this study were obtained from several sources directly related to the research topic. The main sources came from the Service section at Bank Mandiri Gambir Branch, with additional data from the IT Security Support Department, internal employees of Bank Mandiri Gambir Branch, and Bank Mandiri customers.

Some data collection techniques used in this study include:

1. Observation: Researchers make direct observations of the situation in the field to get a realistic picture.

2. In-depth Interviews: Used to dig up more detailed information about the thoughts and behavior of the source regarding the communication strategy implemented.

3. Documentation: Collecting data from various written sources to support interview and observation results.

After the data was collected, analysis was carried out using a qualitative descriptive approach, which involved organizing, identifying themes and patterns, and drawing conclusions based on the existing data.

To check the validity of the data, this study uses three main techniques:

1. Data Triangulation: Verifying the accuracy of data by collecting information from various sources and at different times.

2. Audit Trail: Recording research steps in detail to ensure transparency and clarity in the research process.

3. Thick Description: Provides an in-depth description of the context, individuals, and processes involved in the research, so that readers can understand the situation more clearly.

With this approach, researchers can ensure the validity and reliability of the data obtained, so that the research results can be trusted and provide a better understanding of the implementation of corporate communication strategies at Bank Mandiri Gambir Area.

RESULTS AND DISCUSSION

Key findings from interviews on the implementation of the cybersecurity program at Bank Mandiri indicate a combination of successes and challenges. The cybersecurity awareness program has succeeded in increasing employee understanding of the importance of protecting company data. However, there are still gaps in internal communication, especially in effectively communicating complex security policies to all levels of employees. In addition, balancing data security with customer convenience in transactions is a challenge. Nevertheless, customers generally have high trust in Bank Mandiri's cybersecurity. The use of technology such as e-learning platforms and phishing simulations has contributed positively to this program. However, to continue to improve the effectiveness of the program, ongoing evaluation and closer collaboration between various departments at Bank Mandiri are needed.

The involvement of vendors and partners in the digital ecosystem of a company as large as Bank Mandiri is a crucial factor in maintaining cybersecurity. Further analysis can explore how Bank Mandiri ensures that its

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue XII December 2024

vendors and partners also implement high security standards. This includes a strict vendor selection process, service level agreements (SLAs) that cover security aspects, and mechanisms for monitoring vendor activities on a regular basis. In addition, it is important to understand how Bank Mandiri manages the risks arising from dependence on third parties, especially in terms of data transfer and access to internal systems.

To measure the effectiveness of its cybersecurity program, Bank Mandiri needs to develop comprehensive and relevant metrics. In addition to traditional metrics such as the number of security incidents, incident response time, and customer satisfaction levels, more sophisticated metrics such as Return on Security Investment (ROSI) can be used to measure the financial impact of cybersecurity investments. In addition, it is important to compare internal metrics with industry benchmarks to understand Bank Mandiri's competitive position.

Cyber threats continue to evolve rapidly, so Bank Mandiri needs to be proactive in anticipating new threats. Further analysis can focus on how Bank Mandiri conducts research and development to address threats such as more sophisticated ransomware attacks, AI-based attacks, and threats emerging from new technologies such as blockchain. In addition, it is important to understand how Bank Mandiri collaborates with the cybersecurity community to share information on the latest threats and develop joint solutions.

Close collaboration with regulators such as OJK is essential to ensure that Bank Mandiri always meets applicable regulatory requirements. Further analysis can examine how Bank Mandiri participates in industry forums that discuss cybersecurity issues, as well as how Bank Mandiri provides input to regulators regarding the development of relevant regulations.

An in-depth analysis of Bank Mandiri’s cybersecurity implementation shows that the company has made significant efforts to protect its digital assets. However, there is still room for improvement, especially in terms of collaboration with vendors, measuring program effectiveness, and preparing for future threats. By continuing to evaluate and adapt, Bank Mandiri can maintain its position as a leader in cybersecurity in the banking industry.

Based on the analysis that has been conducted, there are several recommendations to improve the cybersecurity program at Bank Mandiri. First, more intensive efforts need to be made to personalize security messages, so that the information delivered is more relevant and effective for each individual. Second, there needs to be an increase in two-way communication channels between the cybersecurity team and employees, so that employees feel more involved and can provide valuable input. Third, simplifying technical language in security communications is very important so that messages can be understood by all levels of employees. In addition, the implementation of gamification can increase employee involvement in the cybersecurity program. Fourth, there needs to be closer collaboration with customers, for example through interactive education programs, to increase their awareness of the importance of cybersecurity. Fifth, evaluations of security policies need to be carried out periodically to ensure that they remain relevant and effective. Finally, clear metrics need to be set to measure the success of the cybersecurity program, so that continuous improvements can be made.

Based on the analysis that has been conducted on the implementation of the cybersecurity program at Bank Mandiri, it can be concluded that Bank Mandiri has made significant efforts in building a strong security system. An intensive cybersecurity awareness program has succeeded in increasing employee understanding of the importance of protecting company data. However, there is still room for improvement, such as improving internal communication, involving customers more actively in efforts to maintain security, and strengthening collaboration with external parties. Overall, Bank Mandiri has demonstrated a strong commitment to cybersecurity, but needs to continue to adapt to the evolving threat landscape. By implementing the recommendations that have been proposed, Bank Mandiri can further strengthen its position as a leader in cybersecurity in the banking industry.

Based on the analysis that has been done, there are several interesting areas that can be further studied from a communication science perspective related to the implementation of cybersecurity programs at Bank Mandiri. One area that stands out is the effectiveness of internal communication in cybersecurity programs. Research can dig deeper into the most effective communication channels to reach various levels of employees, the easiest language to understand, and how to measure the level of employee understanding of cybersecurity messages. In

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue XII December 2024

addition, research can also explore how to build a strong and interesting narrative around cybersecurity so that employees feel more motivated to participate in maintaining the security of company data.

Another interesting area of research is the influence of external communication on customer perceptions of cybersecurity. Research can analyze how Bank Mandiri's external communication, whether through social media, websites, or direct interactions with customers, affects the level of customer trust in the security of their data. In addition, research can also identify the types of messages and communication channels that are most effective in increasing customer awareness of the importance of cybersecurity and encouraging them to take preventive measures article.

Existing Condition of Bank Mandiri Cyber Security

People:

Bank Mandiri implements a security awareness program that must be followed by all employees. This training is designed to improve understanding of information security and integrate security culture throughout the organization. In its implementation, employees are required to complete annual information security certification. This initiative aims to form the foundation of a consistent information security culture.

Process:

Bank Mandiri's information security framework adopts international standards, including ISO 27001 and the NIST Cybersecurity Framework. The risk management process includes threat identification, risk evaluation, and implementation of mitigation measures. The Bank has also implemented internal policies that regulate comprehensive cyber risk management.

Effectiveness of Corporate Communication Strategy in Increasing Cyber Awareness

Internal Communication:

Systematic training programs have helped create a better understanding of cybersecurity among employees. Structured communication through digital channels such as intranets and internal applications hastens the delivery of security policies.

Employee involvement in training shows the success of the communication strategy. However, resistance to change is one of the challenges that needs to be overcome with more persuasive communication and involving a value-based approach.

External Communication:

Bank Mandiri uses social media and websites to educate customers about cyber threats, such as phishing and malware. The digital campaign includes practical guides to protecting personal data, increasing customer trust in the bank.

Visual approaches such as infographics and short videos have proven effective in reaching a wider audience. This strategy is in line with the principles of visual communication stated by Argenti (2023), which emphasizes the importance of visual appeal in increasing audience engagement.

Risk Management in Cyber Security

Reputational Risk:

Bank Mandiri has demonstrated its commitment through transparency in handling cyber incidents. For example, emergency response protocols help mitigate the impact of security incidents on public perception.

Collaboration with external institutions, such as OJK and cybersecurity solution providers, strengthens the company's image as an organization that is proactive in maintaining security.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue XII December 2024

Legal Risks:

Compliance with the Indonesian PDP Law and OJK regulations is a key focus in the cybersecurity strategy. Bank Mandiri has ensured that all its operational steps comply with applicable regulations, including the protection of customers' personal data.

Communication Strategy Performance

The level of employee engagement in security awareness programs has increased, as demonstrated by participation in training and campaigns.

Customer response to cybersecurity campaigns on social media has been positive, with increased interactions and sharing of educational content.

The use of key performance indicators (KPIs) such as employee and customer security incident reports helps evaluate the effectiveness of the communication strategy.

Based on interviews with three competent sources at Bank Mandiri, namely Tahta Darmawan (Lead IT Security Awareness), Indhah (Branch Operation Manager Bank Mandiri KC Gambir), and Bahtiar (Bank Mandiri Customer), as well as the data analysis matrix collected, it can be concluded that Bank Mandiri has made significant efforts in implementing the IT Security Awareness program to improve cyber resilience and security among employees and customers. This program involves various communication channels, both one-way and two-way, to ensure effective message delivery to all parties involved.

Bank Mandiri implements two main approaches in its IT Security Awareness communication strategy, namely one-way and two-way approaches. The one-way approach includes the use of media such as monthly newsletters, physical and digital posters, which are sent routinely to employees. The two-way approach is more interactive and involves more direct communication, such as quarterly podcasts, sharing sessions, mandatory e-learning, and the "IT Goes to Branch" program aimed at branches with the lowest e-learning scores.

To ensure the effectiveness of the strategy, Bank Mandiri conducted various trials and campaigns, such as phishing grill (simulated phishing attacks), SEOJK campaigns, and social engineering exercises. In addition, Bank Mandiri also measured the level of participation in the e-learning program and conducted measurements through other indicators to assess the success of the program. Based on the interview results, this program is very important considering the threat of financial sanctions from violations of personal data protection laws, as well as to avoid negative impacts on the bank's reputation that can arise from hacking.

Regarding the impact of the hacking case, although Bank Mandiri has experienced a data leak incident that was traded on the dark web, the data is no longer valid. However, the case has an impact on the bank's reputation and is one of the main reasons to accelerate the implementation of this cybersecurity program. Bank Mandiri wants to maintain its reputation better and avoid similar incidents in the future.

The IT Security Awareness program at Bank Mandiri also involves various parties in its formulation. In this case, SEOJK regulations, input from the board of directors, the internal IT Security team, and consultation with independent parties and IT consultants also play an important role. This collaboration shows Bank Mandiri's efforts to build a comprehensive security system by paying attention to applicable rules and regulations.

Although the program has been well implemented, there are several challenges that need to be considered. One of them is the lack of early socialization about the policy changes that were implemented, which caused discomfort among employees and customers. Employees found it difficult to adapt to the sudden restrictions, especially regarding their interactions with customers. In this case, employees suggested the need for more direct communication with end-users, because electronic media alone was considered less effective in conveying messages comprehensively.

From the customer side, although most understand and appreciate the efforts made by Bank Mandiri to protect

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue XII December 2024

their data, some customers feel burdened by the more complicated security process, such as difficulties in sending data. Therefore, they proposed a clearer warning feature in the bank's application to increase their awareness of potential cyber threats.

Some customers also appreciate the education provided by Bank Mandiri via SMS containing information about threats such as dangerous links and the importance of maintaining the confidentiality of personal data such as PINs and OTPs. Some customers have also taken independent steps to protect their data, such as changing passwords regularly.

Suggestions for Program Success

To increase the effectiveness of this program, several suggestions emerged, including:

1. **Closer collaboration between IT Security and customer service** to provide more direct education to customers and employees.

2. **Use of more interesting and effective communication media**, such as utilizing the lock screen on the desktop for security-related posters.

3. **More massive socialization** and campaign optimization through various channels to ensure that all parties, both employees and customers, understand the importance of cybersecurity awareness.

The results of the analysis of the data collected in the coding matrix provide a clearer picture of the strategy and effectiveness of this program. The following table presents the results of the analysis related to the strategy, messages, and constituents involved:

Table 1: Corporate Analysis and Coding Matrix

No	Category	Question	Answer	Coding
1	What do you want to achieve?	What is the IT Security strategy for delivering awareness programs?	There are two approaches: one-way (newsletter, poster) and two-way (podcast, sharing session, e-learning)	IT Security awareness strategy
2	What resources are available?	What is the IT Security strategy for delivering awareness programs?	Newsletter, posters, e-learning, podcasts, collaboration with IT Infra and IT consultants	Communication media
3	How is the company's reputation?	Have there been any cases of hacking from Bank Mandiri before?	There have been cases of data leaks, affecting reputation, even though the data was outdated and invalid.	Impact of hacking on reputation

Table 2: Message Analysis and Coding Matrix

No	Category	Question	Answer	Coding
1	Best communication channels	What is the IT Security strategy for delivering awareness programs?	1-way: Newsletter, poster; 2-way: Podcast, sharing session, e-learning, IT Goes to Branch	Communication strategy, awareness
2	How corporations craft messages	How to ensure the strategy works well?	SEOJK campaign, phishing grill, appreciation for those who report, publication of names of those who are aware	Strategy evaluation, testing
3	Suggestions for program success	Suggestions for program success	Need direct communication with end-users, not only through digital media	Optimizing communication

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue XII December 2024

CLOSING

Conclusion

Based on the results of interviews regarding the implementation of cybersecurity programs at Bank Mandiri, it can be concluded that the bank has made significant efforts to increase cybersecurity awareness among employees and customers through various programs such as newsletters, posters, podcasts, e-learning, and phishing simulations. These programs have succeeded in increasing employee understanding of the importance of protecting company data. However, there are challenges related to the lack of initial socialization which causes discomfort to employees and customers, as well as the need for improvements in internal communication so that the policies implemented can be clearly understood. Despite concerns regarding customer comfort, their level of trust in Bank Mandiri's cybersecurity efforts remains high. To improve the effectiveness of the program, continuous evaluation and closer collaboration between departments are needed. Overall, despite significant efforts, there is still room for improvement, especially in terms of internal communication, customer engagement, and evaluation of security policies to ensure more sustainable program success.

Suggestion

Suggestions to improve the effectiveness of the IT Security Awareness program at Bank Mandiri include integrating a more interactive and personal communication approach. Although existing communication channels, such as newsletters, posters, and e-learning, are effective in conveying messages, the program still needs to be strengthened with a direct approach to employees and customers. Collaboration between the IT Security team and customer service can be an important step in delivering education in a more understandable way, especially considering that electronic media is often less effective in attracting attention. In addition, to overcome operational problems arising from sudden restrictions, more massive and structured initial socialization must be carried out so that employees can adapt better. The implementation of clearer warning features in the application, as proposed by customers, can also increase awareness and vigilance towards potential cyber threats. Finally, giving awards to individuals who demonstrate high awareness of cybersecurity, as well as the use of more attractive media such as posters on the lock screen, can strengthen employee commitment in carrying out this program. A more holistic and personal approach will help create a stronger and more effective cybersecurity culture.

BIBLIOGRAPHY

1. Agdelia Meiva Azarine. 2023. Bank BSI Pasca Serangan Siber: Mengungkap Potensi Kompensasi Bagi Nasabah.
2. Argenti, P. A. (2009). Corporate Communication. Jakarta: Salemba Humanika.
3. Argenti, P. A. (2023). Corporate Communication: Managing Reputation in the Digital Age. Boston: McGraw-Hill.
4. Ahmad Elki Prayogi, F. G., Herdi Syaputra, M. M., & Refauzan Adi Nursatyo, R. W. (2023). WASPADA TERHADAP APLIKASI ATAU WEBSITE BERBAHAYA YANG MENGATASNAMAKAN INSTANSI TERTENTU UNTUK MENGAMBIL DATA PRIBADI PENGGUNA.
5. Annual Report PT. Bank Mandiri (Persero) Tbk. 2023.
6. Argenti, Paul A. 2010. Komunikasi Korporat. Jakarta : Salemba Humanika.
7. Bahtar, Burhan. 2019. Metodologi penelitian Kuantitatif.
8. Bobbins, James G. dan James, Barbara S., 2006, Komunikasi yang efektif untuk pemimpin, Pejabat atau Usahawan, Cetakan ke 5, (Alih bahasa Drs. R. Turman Sirait) Jakarta: CV Pedoman Ilmu Jaya
9. Dancor. 2023. dampak besar kebocoran data terhadap reputasi perusahaan
10. Dowling, G. R. (1986). Managing Your Corporate Images. California Management Review, 28(3), 100-113.
11. Cornelissen, Joep. 2004. Corporate Communication Theory and Practice. London. SAGE
12. Cutlip, S. M., Center, A. H., dan Broom G. M. 2006. Effective Public Relations. Jakarta: Prenada Media Group.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue XII December 2024

13. H. Nugroho, M. N. Ihsan, A. Haryoko, F. Màarif, and F. Alifah, “Edukasi Keamanan Digital Untuk Meningkatkan Kewaspadaan Masyarakat Terhadap Link Phising,” J. Pengabdi. Masy. Multidisiplin, vol. 1, no. 2, pp. 28–40, 2023.
14. Hardjana, A. A. (2008). Komunikasi dalam Manajemen Reputasi Korporasi. Jurnal Ilmu Komunikasi.
15. Lerbinger, O. (1997). The Crisis Manager: Facing Risk and Responsibility. Mahwah: Lawrence Erlbaum Associates.
16. Surat Edaran OJK. No.29/SEOJK.03/2022. 2022. Kethanan dan keamanan siber bagi bank umum
17. UU PDP No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.
18. Van Riel, C. B. M. (1995). Principles of Corporate Communication. London: Routledge.
19. Van, Riel.2007. Essentials of Corporate Communication. London: Routledge