International Journal of Multicultural and Multireligious Understanding

http://ijmmu.com
editor@ijmmu.com
ISSN 2364-5369
Volume 12, Issue 3
March, 2025
Pages: 416-423

Indodax Reputation Restoration After Cyber Attack on Social Media

Putu Puteri Surinegara

Master of Communication Science, Faculty of Philosophy & Civilization, Paramadina University, Jakarta, Indonesia

http://dx.doi.org/10.18415/ijmmu.v12i3.6695

Abstract

This study aims to analyze the crisis communication strategy carried out by Indodax, the largest crypto asset exchange platform in Indonesia, after experiencing a cyber attack that occurred on September 11, 2024. This research is a quantitative research with a constructivist paradigm. The content analysis method is used to evaluate the content of messages posted by Indodax on its official social media platforms. In addition, public reactions to crisis messages are analyzed to understand the effectiveness of such communication in managing perceptions. From this research, it is known that Indodax has implemented various crisis communication strategies that are in accordance with the Situational Crisis Communication Theory (SCCT) framework in responding to the cyberattack that occurred. The rebuild strategy implemented by Indodax has proven effective in dealing with the crisis and restoring the company's reputation after the cyberattack. This effectiveness is reflected in the high level of public engagement generated from social media uploads.

Keywords: *Cyberattack; Crisis Response Strategies; Content Analysis; Social Media*

Introduction

Crypto investment has become a global phenomenon in recent years, attracting the attention of individuals and institutions from various backgrounds. These blockchain-based digital assets have not only revolutionized the way people invest, but have also opened up new opportunities in the financial world. Nakamoto (2008), the creator of Bitcoin, said that cryptocurrencies were created to offer a decentralized and transparent financial system, unlike traditional systems that are often controlled by banks or governments. Advantages such as anonymity, transaction speed, and the potential for high returns make crypto attractive to many investors, especially the younger generation who are tech-savvy. With the increasing popularity of digital currencies such as Bitcoin, Ethereum, and thousands of other coins, crypto investment provides a great opportunity to gain profits, but also carries quite high risks. Crypto, with all its opportunities and risks, requires a careful approach and in-depth knowledge.

Founded in 2014, Indodax is a technology-based company in the blockchain field and the largest crypto asset in Indonesia. Indodax trades Bitcoin, Ethereum, Ripple, and more than 160 other crypto assets from around the world with 24-hour market activity. Currently, Indodax has been registered with the Commodity Futures Trading Regulatory Agency (BAPPEBTI) and has 3 international

certificates, namely ISO 9001: 2015, ISO 27001: 2013 and ISO 27017: 2015. This national and international recognition makes Indodax a trusted crypto asset investment platform provider in Indonesia.

In this connected digital era, the threat of cyber attacks is a significant challenge for companies in various sectors. On September 11, 2024, Indodax experienced a cyber attack that resulted in hundreds of billions of rupiah in losses to its users' funds. This hack was successfully carried out in a relatively short time, namely in just about 2 hours. The hack began when one of Indodax's employees received a freelance job offer with a very tempting salary. The employee did the job using Indodax's office laptop, which turned out to be a trap designed by hackers. In the process, the hacker sent a file that had been infiltrated by malware. Although the employee only had access to a regular server, the malware managed to spread to the company's main server. After an investigation, it was discovered that the hacker was connected to the Lazarus hacker group from North Korea. Indodax immediately took mitigation steps by temporarily stopping all trading activities and conducting an internal investigation and tightening its operational procedures. Indodax is also working with the authorities to investigate this case.

These attacks not only giving a financial and operational losses, but also damaging the company's reputation in the eyes of the public. A company's reputation is a very valuable intangible asset for a company and plays a key role in the long-term survival and success of an organization, especially in industries that depend on customer trust, such as crypto asset trading platforms. Barnett, Jermier, and Lafferty (2006) also stated that reputation is not only influenced by the products and services provided by a company, but also by the ethical behavior and social responsibility shown to stakeholders. They put forward that companies with a good reputation tend to have stronger relationships with stakeholders, which allows the company to survive even in times of crisis.

When a crisis occurs, the key to mitigating negative impacts and restoring public trust is the ability of the organization to respond quickly, transparently, and effectively. According to Coombs (2007), a crisis is an unexpected event that can cause serious threats to an organization's reputation. This study focuses on the analysis of crisis communication content conducted by Indodax on social media after a cyber attack. Social media has become a dominant communication channel in the digital era, influencing the way companies and organizations interact with their publics. In the context of crisis communication, social media has a very important role in building and maintaining public trust. As a platform that allows direct interaction between companies and audiences, social media provides an opportunity for organizations to communicate their responses in real time, which is essential to reducing uncertainty and maintaining a positive image.

Based on the press release of the Indonesian Internet Service Providers Association (APJII), internet users in Indonesia in 2024 will increase to 221 million users. The biggest reason for internet users in Indonesia is to use the internet to access social media such as Facebook, Twitter, Instagram, Whatsapp, Youtube and so on (www.apjii.or.id). Social media, according to Brown (2012) is a digital application that allows users to create and exchange information and sources, where this is the result of social interaction via the internet. This indicates that internet media content is no longer monopolized by interested parties, but can be uploaded by all internet users and encourages the development of citizen journalism practices through social media.

Kim and Rhee (2011) also revealed that audiences tend to trust information delivered directly by companies through social media, compared to information from other sources. This shows that companies that actively communicate through social media have a greater chance of building trust and maintaining good relationships with their audiences, even in the midst of uncertain situations. These data are relevant to what Indodax does, which is utilizing its social media platform as the main of communication channel carried out in order to provide security guarantees to its users. Indodax proactively provides information regarding the situation that occurred, the steps taken to secure the system, and guidance to customers to keep their accounts safe. Through this transparent approach, Indodax seeks to ease public concerns and maintain customer loyalty.

From the background mentioned above, this study aims to analyze the crisis communication strategy carried out by Indodax on social media after the cyber attack, and evaluate its effectiveness in restoring the company's reputation. It is very interesting to understand how the use of narratives, messages, and the selection of approaches taken by Indodax in order to restore its reputation after the incident, considering that cyber attacks are one of the biggest threats in the digital era, especially for companies engaged in technology and finance such as Indodax.

Literature Review

A. Cyber Attack

Based on the Regulation of the Minister of Defense No. 82 of 2014 concerning Cyber Defense, a *cyberattack* is any form of action, word, thought, whether intentionally or unintentionally carried out by any party, with any motive and purpose, carried out in any location, targeted at electronic systems or their contents (information) or equipment that is highly dependent on technology and networks on any scale, against vital or non-vital objects in the military and non-military spheres, which threaten state sovereignty, territorial integrity and national safety. This action is usually carried out by individuals, groups, or organizations. Cyberattacks can be categorized as a significant threat in the digital era because of their ability to damage globally interconnected systems. The main characteristics of cyberattacks include the speed of the attack, the anonymity of the perpetrator, and the potential for extensive damage, including financial, reputational, and national security impacts.

Cybercrime itself has evolved and is diverse in number, cybercrime is divided into several, including: *hacking, cyber sabotage, cyber espionage, garding, cyber attack, vandalism, spyware,* and power grid attacks (Subagyo, 2015: 98-99). The difference in each of these cybercrimes lies in the type of technology used, the type of crime or loss committed and the purpose of the cyber crime. Of the many types of cybercrime that can occur, *hacking* is one of the most dangerous.

B. Situational Crisis Communication Theory (SCCT)

Situational Crisis Communication Theory (SCCT) developed by W. Timothy Coombs is one of the theories that focuses on crisis communication. This theory provides a framework for understanding and managing crisis communication based on the situation faced by the organization. According to SCCT in order to overcome the crisis, the company must respond according to the severity of the crisis experienced, for that SCCT classifies crises into three crisis clusters, namely (1) *Victim Cluster* , which is a crisis that occurs without the organization's fault, such as natural disasters or cyber attacks by external parties, (2) *Accidental Cluster* , where the crisis occurs due to unintentional actions from the organization, and the last (3) *Preventable Cluster* , which is a crisis caused by negligence or intentional actions from the organization.

In order to respond to the crisis, SCCT emphasized the importance of choosing appropriate communication strategies to minimize reputational damage. These strategies include:

Table 1. SCCT Crisis Response Strategy

SCCT Response Strategy
response strategy: denial 1) *Attack the accuser:* attack and accuse the group that says there is a problem; 2) *Denial:* the organization emphasizes that no crisis has occurred; 3) *Scapegoat:* blaming other people and groups outside the organization for the crisis.
Crisis response strategy *diminish*

4) *Excuse:* trying to reduce the burden on the organization by proving that the organization has not done anything negative; 5) *Justification:* taking responsibility and minimizing the damage that occurs due to the crisis.
Crisis response strategy *rebuild* 6) *Compensation:* providing compensation to victims of the crisis; 7) *Apology:* an apology by the organization for the crisis that occurred.
Supportive crisis response strategy (*bolstering*) 8) *Reminder:* the organization reminds the public about good work/things; 9) *Ingratiation*: winning the public's heart with the good things the organization has done; 10) *Victimimage*: stating to stakeholders that the organization is also a victim of the crisis.

Source: (Coombs, 2007)

C. Previous Research

There are no journals that discuss Post-Cyber Attack Reputation Recovery on Indodax, but there are several previous studies that are relevant to this research, and are used as references in compiling this journal, namely as follows:

Title	Objective	Theory	Method	Research result
Analysis of Banyumas Regent's Instagram content regarding handling of the Covid-19 hoax crisis	Knowing the efforts to manage the Covid-19 hoax crisis communication in Banyumas	SCCT	Qualitative content analysis	The implementation of the three crisis response strategies by Achmad Husein succeeded in providing comparative and holistic information for the Banyumas community. Furthermore, through this strategy, Achmad Husein also succeeded in turning the information crisis due to Covid-19 hoaxes into a strategic opportunity in building his positive reputation.
PT. BSI Tbk Crisis Management After Customer Data Hacking	Knowing how BSI public relations carried out crisis management in the case of customer data hacking.	SCCT	Descriptive qualitative	BSI responded to the crisis transparently through a press release that included an apology, responsibility, and recovery efforts, in accordance with the principles of (SCCT).
Analysis of Indonesian Sharia Bank's Image Recovery Strategy After Alleged Cyber Attack	The strategy that BSI uses it as an image recovery tool after a cyber attack.	SCCT and Image Restoration Theory	Descriptive qualitative	BSI demonstrates its commitment to improving its image and rebuilding customer trust through good communication strategies.

Methodology

This is a quantitative research with a constructivist approach, which combines quantitative elements with constructivist theory that views social meaning as a result of interaction in communication. This approach emphasizes that data collected from social media is a construction of meaning that can be analyzed quantitatively to understand how crisis communication strategies are formed and received by the public.

Using a content analysis method, according to Eriyanto (2011), content analysis is defined as a scientific assessment technique that is shown to determine the description of the characteristics of the content and draw inferences from the content, and is intended to systematically identify the content of the communication that appears. Researchers will analyze social media content issued by Indodax during the crisis period to identify and calculate the frequency of the categories of crisis communication strategies used.

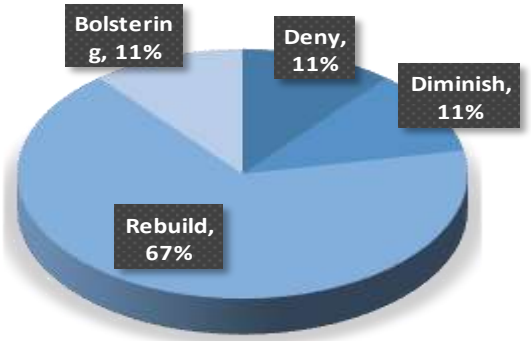
According to Sugiyono (2019), data collection techniques refer to the steps taken to obtain the information needed in the study. In this study, the data used is documentation of social media content, where all posts and interactions related to the crisis will be collected for further analysis. The data in question are all posts published by Indodax on Indodax's official social media platforms, namely Twitter, Instagram, and Youtube, during the crisis period due to cyber attacks, namely September 11-14, 2024. These posts were selected by considering the relevance to the crisis that occurred, namely those containing information or clarification from Indodax regarding the incident. These data allow researchers to analyze various types of messages conveyed by the company, as well as the crisis communication strategies used to restore the company's reputation on social media.

After the data is collected, the data is analyzed using frequency analysis. Frequency analysis in this study is used to calculate how often each type of crisis communication strategy is applied by Indodax on social media during the crisis period. Each post that has been collected will be analyzed to identify the category of communication strategy used, such as apology, clarification of information, corrective steps, or strengthening reputation. The frequency of each category is then calculated to see the pattern of dominance of the strategy used by Indodax. The results of this frequency analysis provide an overview of the company's main focus in responding to the crisis, as well as how much the public is exposed to certain types of strategies through social media. Thus, this frequency analysis helps measure the implementation and consistency of the communication strategy used in restoring the company's reputation.

Result

Based on the data obtained, researchers conducted data analysis by categorizing the response strategies carried out by Indodax on its official social media on the Instagram, Twitter, and Youtube platforms based on the responses according to SCCT.

The results of the study show that the dominant pattern of Indodax's crisis communication strategy after the cyber attack was dominated by the *rebuild strategy* (67%), while the other 3 strategies, namely *deny*, *diminish*, and *bolstering*, had the same value (11%).



Gambar 1. Pola dominasi strategi
Sumber: Hasil olahan peneliti (2024)

Rebuild strategy is used intensively to restore public trust through corrective measures, such as transparency regarding the development of the system maintenance process carried out directly by the Indodax CEO to provide a sense of security for customers over their assets, then efforts to strengthen the security system, and an apology to customers. In addition, Indodax made several other efforts to convince its customers by showing *the Proof of Reserve* owned related to the balance of crypto assets managed to reassure customers that their funds are 100% safe, and data can be accessed by customers, then Indodax also held a giveaway for customers with a total of IDR 3 million for 3 people every hour during the maintenance process.

Diminish strategy was implemented to reduce the perception of damage by emphasizing that customer data remains secure and the attack did not significantly impact core services. In addition, the *bolstering strategy* was used to strengthen the company's positive image through messages of appreciation for customer support and emphasizing service success. On the other hand, the *denial strategy* , which stated that the cyberattack was an illegal act by a third party, was used at the end of the crisis, namely after the investigation results were completed, the CEO of Indodax provided information that the cyberattack experienced by Indodax was connected to the North Korean *hacker group* Lazarus. This pattern reflects Indodax's adaptive efforts in adjusting strategies based on the dynamics of the crisis and the need to maintain the company's reputation.

Table 1. Correlation between strategy and public *engagement*

Strategy	Comments per post
Deny	1,658
Diminish	5,500
Rebuild	35,500
Bolstering	100

Source: Author's processed results (2024)

The analysis results in Table 1 above show that there is a correlation between the crisis communication strategy used by Indodax and the level of public engagement on social media. The *rebuild strategy* was recorded as generating the highest engagement, with an average of 35,500 comments per upload. This shows that the public responded positively to Indodax's efforts to be transparent, make corrections, and take recovery steps after the cyberattack. The *diminish strategy*, which focuses on strengthening the company's positive image, also recorded quite high engagement, at 5,500 comments per upload. Meanwhile, the *denial strategy*, which aims to reduce the perception of damage caused by the crisis, generated an average of 1,658 comments, and the *bolstering strategy*, which provides information about the perpetrators of the cyberattack who are third parties, received the lowest *engagement*, at an average of 100 comments. These findings indicate that proactive and solution-oriented strategies, such as *rebuild*, are more effective in attracting attention and gaining public support. This pattern underscores the importance of a responsive and transparent approach in building trust during a crisis.

Due to the hacking incident that occurred, to provide a sense of security to its application users, Indodax has taken the right communication steps. According to Harold D. Lasswell (1948), communication is the process of conveying a message consisting of five main components: who said, what was said, through what channel, to whom, and with what impact. Generally, communication is carried out by the communicator, namely the message giver to the message giver or can also be called the communicant, orally or verbally that can be understood by both parties. DeVito (2013), also said that communication is the key to creating healthy and meaningful relationships. He stated that effective communication involves the ability to listen, understand, and respond appropriately.

Conclusion

From the results of the research that has been conducted, it can be concluded that Indodax has implemented various crisis communication strategies that are in accordance with the *Situational Crisis Communication Theory* (SCCT) framework in responding to cyber attacks that occur. The most widely used strategy is rebuild (67%), while 3 other strategies, namely *deny*, *diminish*, and *bolstering*, have the same value (11%).

rebuild strategy implemented by Indodax has proven effective in handling the crisis and restoring the company's reputation after the cyber attack. This effectiveness is reflected in the high level of public engagement generated from social media posts. The high level of *engagement* shows that the public is responding positively to the company's efforts to take responsibility, provide clear explanations, and commit to preventing similar incidents in the future.

Bibliography

Aditya, ARM, Putri, AWOK, Musthofa, DL, & Widodo, P. (2022). *Hacking tools attacks as cyber threats in the national defense system (Case study: Predator)*. *Journal of Cyber Defense*, *6(1)*, 35-46.

Aji, AR, & Purworini, D. (2024). Ministry of Finance's Crisis Communication Response Strategy in the Case of Tax Officials RAT (Analysis of CNN Indonesia and Kompas.com news).

Andhita, PR, Rasyid, MRA, & Hartanto, YT (2023). Analysis of the Banyumas Regent's Instagram content related to handling the Covid-19 hoax crisis. Journal of Communication Studies, 7, 335-354.

Barnett, M. L., Jermier, J. M., & Lafferty, B. A. (2006). *Corporate Social Responsibility and Reputation Risk Management*. Corporate Reputation Review.

Benoit, W. L. (2015). *Accounts, excuses, and apologies: Image repair theory and research* (2nd ed.). SUNY Press.

Coombs, WT (2007). *Ongoing Crisis Communication: Planning, Managing, and Responding.* Thousand Oaks, CA: Sage Publications.

DeVito, Joseph A. 2013. The Interpersonal Communication Book, ed. 13. United States: Pearson Education.

Diggs-Brown, B. (2012). Strategic Public Relations: An Audience-Focused Approach (International ed.). Wadsworth: Cengage Learning.

Eriyanto. (2011). *Content analysis: Introduction to theory and methods* (3rd ed.). Publishing Institute of the Faculty of Communication Sciences, University of Indonesia.

https://apjii.or.id/berita/d/apjii-nomor-user-internet-indonesia-tembus-221-juta-orang

https://blog.indodax.com/newsroom-about-us/

Kim, H. J., & Rhee, Y. (2011). *The Influence of Social Media on Crisis Communication: The Role of Transparency* . Public Relations Review

Kotler, P., & Keller, K. L. (2016). *Marketing Management* (15th ed.). Pearson.

Lasswell, Harold. 1960. The Structure and Function of Communication in Society, Urbana: University of Illinois Press.

Maulana, BR, & Nasrulloh, N. (2024). *Analysis of Bank Syariah Indonesia's image recovery strategy after an alleged cyber-attack*. *Eksisbank*, 7(1), 76-91.

Maulana, N., Laurens, T., Faiz, DHA, & Patrianti, T. (2024). Crisis Management of PT. BSI Tbk After Customer Data Hacking. INNOVATIVE: Journal Of Social Science Research, 4(1), 8244-8258

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from https://bitcoin.org/bitcoin.pdf.

Subagyo, A. 2018. "Synergy in Facing Cyber Warfare Threats." in Journal of Defense & National Defense Vol. 5 No. 1, pp 89-108. DOI: http://dx.doi.org/10.33172/jp bh.v5i1.350

Sugiyono. (2019). *Quantitative, qualitative, and R&D research methods* (12th ed.). Alfabeta.

Suharto, MA, & Apriyani, MN (2021). The Concept of Cyber Attack, Cyber Crime, and Cyber Warfare in the Aspect of International Law. Legal Treatise, 17(2), 98– 107.

Copyrights