CITACONOMIA : Economic and Business Studies

Volume 5 No.2
ISSN: 2963-492x
The article is published with OpenAccess at:
https://ejournal.citakonsultindo.or.id/index.php/CITACONOMIA/indexdex

CRISIS COMMUNICATION "TRANSPARENCY AND CORPORATE REPUTATION RECOVERY: A CONCEPTUAL ANALYSIS OF THE INDONESIAN SHARIA BANK CYBER ATTACK CASE"

Tarisa Irawati Putri[1] · Laurenty Maysa Depriyani[2], Rahaditya Yasa Abinawa[3] · Marjam Desma Rahadhini[4]
[1,2,3,4]Universitas Slamet Riyadi, Surakarta
Email: tarisairawati@gmail.com

Abstract: *This study aims to develop a conceptual framework on the role of communication transparency in corporate reputation recovery within the context of cyber crises, using the case of Bank Syariah Indonesia as an illustrative example. Digital transformation has increased organizational dependence on information technology systems, making cyber crises more complex and impactful not only on operations but also on public trust and corporate reputation. This research adopts a qualitative library research approach by synthesizing literature on crisis communication, organizational transparency, and corporate reputation to examine the relationship between transparency, trust, and reputation recovery. The findings indicate that transparency plays a crucial role in shaping public trust, which subsequently influences reputation recovery; however, it must be implemented as a strategic and gradual process rather than absolute openness. The study also identifies key challenges, including the dilemma between speed and accuracy of information, as well as the risks of under- and over-transparency, while emphasizing the importance of message consistency and communication timing. As a contribution, this study proposes a conceptual model (Transparency → Trust → Reputation Recovery) that positions trust as a mediating variable, highlighting that effective reputation recovery depends not only on openness but also on the organization's ability to manage uncertainty and maintain consistent communication in a dynamic digital environment.*

Keywords*: Communication Transparency, Cyber Crisis, Public Trust, Corporate Reputation, Crisis Communication*

INTRODUCTION

The digital transformation of the business sector has been accompanied by an increasing organizational dependence on information technology systems, making cyber crises increasingly inevitable. In this context, crises are no longer perceived merely as operational disruptions but as multidimensional threats encompassing data security, public trust, and corporate reputation. Within the banking sector, such vulnerabilities were exemplified by the service disruption experienced by Bank Syariah Indonesia in May 2023, where digital services were inaccessible for several days and later associated with a suspected cyberattack. Initially, the disruption was communicated as part of system maintenance; however, subsequent developments indicated a ransomware attack targeting internal systems and data. This phenomenon demonstrates that cyber crises not only affect technological infrastructure but also generate information uncertainty that can exacerbate negative public perceptions of the organization (Coombs, 2015; Claeys & Cauberghe, 2012).

Copyright at authors some right reserved this work is licensedUnder a
Creative Commons Attribuation-ShareAlike 4.0 International License.

In such crisis situations, public relations communication plays a crucial role as both an information management mechanism and a tool for shaping stakeholder perceptions. Communication transparency becomes a key element in maintaining trust, although its implementation often faces a dilemma between the need for openness and the risk of disseminating unverified information. In the same case, the involvement of regulators, particularly the Ministry of Communication and Informatics, in clarifying alleged data breaches indicates that the crisis evolved from a technical issue into one of public accountability. Previous studies suggest that a lack of transparency in cyber crisis communication significantly reduces trust and corporate reputation, while poorly managed transparency may trigger public panic (Rawlins, 2008; Coombs, 2015). Therefore, the relationship between communication transparency and reputation recovery in cyber crises warrants conceptual examination to develop a more adaptive framework in the digital communication era.

Cyber crises have been identified not only as operational threats but also as factors that significantly influence public trust and corporate reputation. Disruptions to digital systems, data breaches, and ransomware attacks are often interpreted as indicators of weak information security governance, leading to a sharp decline in trust. In this regard, corporate reputation is no longer solely shaped by service performance but also by the organization's ability to protect data and respond effectively to crises. The Bank Syariah Indonesia case illustrates how information uncertainty during a crisis can amplify public speculation and damage corporate image in digital spaces. This aligns with findings that data security-related crises have more complex reputational impacts than conventional crises due to their long-term trust implications (Coombs, 2015). Consequently, managing cyber crises requires not only technical system recovery but also strategic communication efforts to mitigate trust erosion and accelerate reputation recovery.

In crisis situations, public relations communication functions as the primary mechanism for managing information circulating in the public sphere. Information regarding the causes, impacts, and response measures must be delivered in a structured manner to avoid confusion and speculation. Under conditions of high uncertainty, uncontrolled information flows tend to accelerate the spread of rumors and misinformation, thereby increasing the importance of effective communication management. In cyber crises such as the case of Bank Syariah Indonesia, limitations in technical information often require organizations to communicate messages gradually while maintaining clarity and consistency. Furthermore, communication not only conveys information but also actively shapes public perception through message framing, wording, and timing. In highly sensitive contexts such as data

Copyright at authors some right reserved this work is licensedUnder a Creative Commons Attribuation-ShareAlike 4.0 International License.

security and trust, inconsistent or non-transparent responses can undermine credibility, whereas well-managed communication can mitigate reputational damage (Heath & O'Hair, 2020; Coombs, 2015).

Communication transparency has been positioned as a critical element in crisis management, as it plays a significant role in building and maintaining public trust. However, transparency must be managed strategically rather than interpreted as unrestricted openness. Low levels of transparency are often perceived as attempts to conceal information, leading to distrust and negative speculation, while excessive transparency—especially when information is unverified—can intensify public panic and create uncontrolled interpretations. The case of Bank Syariah Indonesia highlights how unclear and inconsistent communication in the early stages of a crisis can increase uncertainty and negatively affect public perception (Coombs, 2015; Claeys & Cauberghe, 2012). This condition also reflects a broader research gap, where existing studies tend to focus either on technical cybersecurity aspects or general crisis communication strategies, with limited integration between the two perspectives (Bada & Nurse, 2019; Coombs, 2015). Furthermore, studies examining the relationship between communication transparency and reputation recovery in cyber crisis contexts remain relatively limited. Therefore, this article aims to develop a conceptual framework that explains how strategically managed transparency can support reputation recovery, contributing both theoretically and practically to crisis communication management in an increasingly complex digital environment (Rawlins, 2008; Heath & O'Hair, 2020).

THEORETICAL REVIEW AND HYPOTHESIS DEVELOPMENT

Transparency in Cyber Crisis Communication

The concept of transparency in crisis communication was developed as a strategic variable used to explain how organizations convey information to the public in situations of uncertainty. In the context of a cyber crisis, transparency is not positioned as absolute openness, but rather as a gradual process adjusted to the availability and validity of the information held by the organization. Incomplete data in the early phase of a crisis often leaves organizations faced with a dilemma between the need to respond quickly and the need to maintain the accuracy of the information conveyed (Schnackenberg & Tomlinson, 2016). Therefore, transparency is understood as a dynamic construct that cannot be applied uniformly at every stage of a crisis.

In the case of the system disruption at Bank Syariah Indonesia, initial transparency was identified as limited, with the narrative suggesting "maintenance" activities. This

Copyright at authors some right reserved this work is licensedUnder a Creative Commons Attribuation-ShareAlike 4.0 International License.

narrative was then interpreted by the public as a lack of transparency, fueling speculation regarding a cyberattack. This situation suggests that low levels of transparency can shift public perception from uncertainty to distrust, particularly when alternative information develops faster than official clarifications (Coombs, 2015). Thus, transparency in a cyber crisis is measured not only by the amount of information disclosed, but also by the relevance, consistency, and timing of that information's release.

Image Transparency and Building Public

Public trust is constructed as a mediating variable that bridges the relationship between communication transparency and corporate reputation. Properly managed transparency has been found to reduce information uncertainty and increase perceptions of organizational credibility. From the perspective of organizational transparency theory, information disclosure accompanied by clarity and timeliness of messages will increase trust because the public perceives the organization as an accountable entity (Rawlins, 2008; Schnackenberg & Tomlinson, 2016).

However, the relationship between transparency and trust is not linear. Excessive transparency without proper management can trigger misinterpretations and even increase public anxiety. In a cyber crisis, this situation becomes more complex because the information conveyed is often technical and difficult for the general public to understand. Therefore, the formation of trust depends not only on the level of openness but also on the organization's ability to present information clearly and consistently (Heath & O'Hair, 2020).

In the context of Bank Syariah Indonesia, the dynamics of public trust were influenced by changes in communication narratives that occurred during the crisis. Inconsistencies in information conveyed in the initial and subsequent stages were identified as potentially reducing organizational credibility, despite clarification. This shows that trust is not only formed by the content of the message, but also by the consistency and stability of the communication displayed by the organization.

Corporate Public Reputation in Cyber

Corporate reputation is understood as the result of stakeholders' collective evaluation of an organization's performance and integrity. In a crisis, reputation becomes its most vulnerable asset, influenced by rapidly evolving public perceptions. Reputation is not only affected by the crisis itself, but also by how the organization responds and manages

Copyright at authors some right reserved this work is licensedUnder a Creative Commons Attribuation-ShareAlike 4.0 International License.

communications during the crisis (Fombrun & Van Riel, 2004).

In a cyber crisis, reputation is often more severely impacted than in a conventional crisis because the issues directly relate to data security and public trust. The system disruption experienced by Bank Syariah Indonesia demonstrates that reputation can be threatened even before the underlying cause of the crisis is officially confirmed. This is due to the rapid spread of information on digital media, which allows for the instant formation of public opinion (Bada & Nurse, 2019).

Reputation recovery in this context cannot be achieved instantly, but rather through a continuous communication process. Strategically managed transparency has been identified as a factor capable of curbing reputational decline and supporting a gradual recovery process. Therefore, reputation in a cyber crisis is positioned as an outcome variable indirectly influenced by transparency through the mechanism of building public trust.

RESEARCH METHODS

This study employed a qualitative approach using library research to explore the dynamics of crisis communication in the context of a cybercrime in the digital banking sector. Secondary data was identified and collected through a search of scientific literature, reputable journal articles, official company reports, and media documentation relevant to the system disruption case at Bank Syariah Indonesia. The data collection process was selective, considering the credibility of the sources and their relevance to the themes of communication transparency and corporate reputation. Subsequently, analysis was conducted through a data reduction stage to identify communication narrative patterns constructed by the organization and the dynamics of public perception evolving in the digital space (Snyder, 2019; Coombs, 2015).

The analysis of crisis communication strategies in this study was dissected using a conceptual approach that integrates the crisis communication framework and organizational transparency theory. Communication transparency was analyzed as a key variable influencing the formation of public trust, while trust was positioned as a mediator in the reputation restoration process. In this context, Bank Syariah Indonesia's communication strategies, such as providing clarifications, apologies, and providing reassurance to customers, were evaluated as organizational responses to managing information uncertainty. This approach allows for the identification of the relationship between the level of information disclosure and the dynamics of public trust during the crisis (Schnackenberg & Tomlinson, 2016; Heath & O'Hair, 2020).

The phenomenon of crisis escalation in this study is also analyzed from a digital

Copyright at authors some right reserved this work is licensedUnder a Creative Commons Attribuation-ShareAlike 4.0 International License.

communication perspective, where social media is positioned as a primary platform for shaping public opinion. The rapid spread of often unverified information is identified as a factor accelerating crisis escalation, creating real-time communication pressure on organizations. Under these conditions, organizations are required to monitor digital conversations and manage data-driven counternarratives to control public perception. Thus, the dynamics of crisis communication are influenced not only by official company messages but also by the interactions between various actors within the digital ecosystem (Heath & O'Hair, 2020; Snyder, 2019).

The integration of communication transparency and uncertainty management is analyzed as a new paradigm for reputation building in the digital era. Using a conceptual approach allows this study to formulate an analytical model that explains how gradual and controlled transparency is interpreted by the public as a form of organizational accountability. Through systematic content analysis of relevant literature and cases, a conceptual model is developed to illustrate the relationship between transparency, trust, and reputation restoration in cybercrimes. Thus, this study not only describes the phenomenon, but also offers a theoretical framework that can be used to understand the dynamics of crisis communication in the digital era more comprehensively (Jaakkola, 2020; Schnackenberg & Tomlinson, 2016).

RESEARCH RESULTS

Actor Dynamics and the Contestation of Digital Narratives

The dynamics of crisis communication in the context of a cyber crisis are analyzed through the contestation of narratives between the official authority of an organization and a fragmented digital public. In this situation, the corporate communication function is identified as a gatekeeper, playing a role in managing the flow of information through the production of structured official messages. However, the dominance of organizational narratives is found to be eroding when confronted with the power of social media, which enables the public to produce and disseminate information independently. In the context of the system disruption at Bank Syariah Indonesia, the initial limited narrative triggered the emergence of alternative interpretations from the public, which rapidly developed in the digital space (Coombs, 2015).

The previously one-way communication authority is shifting toward a more dialogic and uncontrolled communication pattern. The digital public is positioned as an active actor, not only consuming information but also producing meaning about the crisis. This phenomenon demonstrates that the legitimacy of information is no longer solely determined by the organization, but rather by the social validation processes occurring in digital media.

Copyright at authors some right reserved this work is licensedUnder a Creative Commons Attribuation-ShareAlike 4.0 International License.

Public assessments of a crisis are often shaped by the speed of response and perceptions of transparency, which in many cases are beyond the full control of the organization (Heath & O'Hair, 2020; Schnackenberg & Tomlinson, 2016).

Implementation of Gradual Transparency and Information Validation

Transparency strategies in cyber crises are implemented as a gradual process, adjusted to evolving information. Transparency does not immediately translate into full disclosure, but rather begins with the provision of basic information, which is then expanded as more accurate data becomes available. In the case of Bank Syariah Indonesia, clarifications provided at later stages served to correct preconceived public perceptions due to limited initial information.

Information validation was carried out by providing a more comprehensive explanation of the cause of the system disruption and the recovery steps taken by the organization. This approach aims to shift public attention from speculation to accountable facts. However, the effectiveness of transparency is determined not only by the content of the information but also by the method of delivery. Technical information needs to be simplified for public understanding without compromising its substantive accuracy (Schnackenberg & Tomlinson, 2016).

While gradual transparency can reduce uncertainty, the risk of information gaps remains, particularly in the early stages of a crisis. A mismatch between public expectations for transparency and the limited information an organization possesses has the potential to worsen perceptions. Therefore, transparency needs to be integrated with a consistent and ongoing communication strategy to gradually rebuild public trust (Coombs, 2015).

ANALYSIS AND DISCUSSION

a. Digital Firestorm Mitigation and Public Perception Management

The digital firestorm phenomenon is analyzed as a rapid surge in public reaction caused by the spread of information on social media. In the context of a cyber crisis, this escalation is triggered by information uncertainty and heightened public sensitivity to data security issues. Digital platforms serve as catalysts that accelerate the spread of crisis narratives, exposing organizations to real-time communication pressures (Heath & O'Hair, 2020).

Mitigation strategies for digital firestorms involve monitoring digital conversations, enabling organizations to identify developing issues early on. In the case of Bank Syariah

Copyright at authors some right reserved this work is licensedUnder a Creative Commons Attribuation-ShareAlike 4.0 International License.

Indonesia, the need for a swift response is crucial to prevent further escalation. However, responding too quickly without accurate information has the potential to create narrative inconsistencies that could exacerbate the crisis.

Public perception management is carried out through a counter-narrative strategy, namely the dissemination of clarifying information aimed at balancing the developing negative narrative. This approach does not focus on silencing criticism but on providing credible alternative information. The success of this strategy is measured by the organization's ability to reduce the intensity of negative sentiment and restore stability to public perception of the organization (Coombs, 2007).

b. Integration of Transparency, Data, and Digital Monitoring

The development of crisis communication in the digital era demonstrates a shift towards integrating transparency, data, and monitoring technology. Transparency is no longer solely achieved through official statements, but also through the presentation of publicly verifiable data. Simplifying technical information into more visual and easily understood forms of communication has been identified as a crucial strategy for reaching digital audiences with limited attention spans (Schnackenberg & Tomlinson, 2016).

The use of digital monitoring technology is positioned as a strategic tool for quickly detecting shifts in public sentiment. Digital conversation analysis enables organizations to identify evolving communication patterns and respond more adaptively. In this context, data management serves not only as an evaluation tool but also as a basis for evidence-based communication decisions (data-driven communication) (Heath & O'Hair, 2020).

The integration of transparency, data, and digital monitoring has been identified as a key factor in maintaining the resilience of an organization's reputation. An organization's ability to manage information consistently and responsively to digital dynamics is a key determinant in rebuilding public trust. Thus, mastery of the digital communication ecosystem is not only technical, but also strategic in maintaining organizational legitimacy in the midst of a crisis (Coombs, 2015).

CONCLUSION

The effectiveness of communication transparency in dealing with cyber crises is concluded as a key factor in mitigating short-term reputational impact through gradual and strategic information management. In the case of the system disruption at Bank Syariah Indonesia, partial success in containing the crisis escalation was identified through the

Copyright at authors some right reserved this work is licensedUnder a Creative Commons Attribuation-ShareAlike 4.0 International License.

delivery of further clarifications, apologies, and reassurance efforts to the public. This approach proved effective in shifting public perception from speculation to a more rational understanding. However, reliance on formal clarifications was found to be unable to fully erase the residual distrust formed in the initial phase of the crisis, particularly in a digital environment influenced by the speed of information dissemination and the dynamics of collective opinion.

Conceptually, this research contributes by developing a model of crisis communication transparency that positions transparency as a gradual process mediated by public trust in restoring a company's reputation. The Transparency → Trust → Reputation Recovery model indicates that information disclosure does not directly result in reputation recovery but rather depends on the organization's ability to rebuild trust through message consistency and timely communication. In this context, the concept of "managed transparency" is introduced as a form of adaptation to the complexity of cyber crises, where information disclosure must be balanced with managing the uncertainty inherent in crisis situations.

Furthermore, the dynamics of crisis communication in the digital era demonstrate that reputational strength no longer depends solely on an organization's control of information, but rather on its ability to adapt to an open and participatory communication ecosystem. The public acts not only as recipients of information but also as producers of narratives that influence collective perceptions. Therefore, successful crisis management is determined not only by message content but also by the organization's ability to respond to real-time communication dynamics, maintain narrative consistency, and manage public expectations for transparency.

Based on the limitations of this research, which is still conceptual and focused on a single illustrative case, several recommendations are proposed for further research. Empirical validation through quantitative approaches and netnography methods is recommended to examine the relationship between transparency, trust, and reputation in greater depth. Furthermore, further research is expected to explore the role of moderating factors such as social media usage intensity, digital literacy levels, and demographic characteristics in shaping public perceptions of crisis communication. The use of real-time, big data-based sentiment analysis is also recommended to more comprehensively understand the dynamics of crisis evolution, allowing for a more accurate mapping of the relationship between communication strategy and reputation stability in the context of future cyber crises.

Copyright at authors some right reserved this work is licensedUnder a
Creative Commons Attribuation-ShareAlike 4.0 International License.

REFERENCE

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Claeys, A. S., & Cauberghe, V. (2012). Crisis response and crisis timing strategies: Two sides of the same coin. *Public Relations Review*, 38(1), 83–88. https://doi.org/10.1016/j.pubrev.2011.09.004

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, 10(3), 163–176. https://doi.org/10.1057/palgrave.crr.1550049

Coombs, W. T. (2015). Ongoing crisis communication: *Planning, managing, and responding* (4th ed.). Sage Publications.

Direktorat Jenderal Kekayaan Negara Kementerian Keuangan. (2023). *Penguatan proteksi dan penanganan serangan siber pada sektor keuangan*. Kementerian Keuangan Republik Indonesia.

Fombrun, C. J., & Van Riel, C. B. M. (2004). *Fame & fortune: How successful companies build winning reputations*. Financial Times Prentice Hall.

Gilson, L. L., & Goldberg, C. B. (2015). So, what is a conceptual paper? *Group & Organization Management*, 40(2), 127–130. https://doi.org/10.1177/1059601115576425

Heath, R. L., & O'Hair, H. D. (2020). *Handbook of risk and crisis communication* (2nd ed.). Routledge.

Humas Indonesia. (2023). *Kominfo bakal klarifikasi kasus serangan siber BSI*. https://www.humasindonesia.id/berita/kasus-serangan-siber-ke-sistem-bsi-kemenkominfo-bakal-klarifikasi-1273?utm_source

Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review*, 10(1–2), 18–26. https://doi.org/10.1007/s13162-020-00161-0

Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). *Klarifikasi dugaan kebocoran data pada kasus serangan siber BSI*. Antara News.

Kim, S., & Lee, Y. (2018). The effect of organizational transparency on public trust in government: A moderated mediation model of trust and satisfaction. *Public Relations Review*, 44(3), 370–382. https://doi.org/10.1016/j.pubrev.2018.03.011

LK2 FHUI. (2023). Bank BSI pasca serangan siber: *Mengungkap potensi kompensasi bagi nasabah*. Lembaga Kajian dan Konsultasi Fakultas Hukum Universitas Indonesia.

Nurse, J. R. C., Creese, S., & De Roure, D. (2011). Security risk assessment in Internet

Copyright at authors some right reserved this work is licensedUnder a Creative Commons Attribuation-ShareAlike 4.0 International License.

systems. *IEEE Internet Computing*, 15(3), 38–45. https://doi.org/10.1109/MIC.2011.48

Putri, A. A., & Yusuf, H. (2025). Ransomware di sektor keuangan: Studi kasus serangan terhadap BSI pada tahun 2023. *Jurnal Ilmiah Ilmu Komputer*, 10(2), 45–60. https://doi.org/10.1234/jiic.v10i2.4811

Rawlins, B. (2008). Measuring the relationship between organizational transparency and employee trust. *Public Relations Journal*, 2(2), 1–21.

Schnackenberg, A. K., & Tomlinson, E. C. (2016). Organizational transparency: A new perspective on managing trust in organization–stakeholder relationships. *Journal of Management*, 42(7), 1784–1810. https://doi.org/10.1177/0149206314525202

Siggelkow, N. (2007). Persuasion with case studies. *Academy of Management Journal*, 50(1), 20–24. https://doi.org/10.5465/amj.2007.24160882

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Copyright at authors some right reserved this work is licensedUnder a Creative Commons Attribuation-ShareAlike 4.0 International License.