Building Trust Through Effective Communication During a Cybersecurity Data Breach

Uduak Ekott[1]; Toyosi Kuteyi[2]; Onyinyechi Enwereazu[3]

Publication Date: 2026/01/22

Abstract: Organizations are constantly at risk from cybersecurity data breaches, which present serious communication challenges and technical threats. In addition to the operational and financial consequences, stakeholder trust, reputation, and resilience are all greatly influenced by organizational communication after a breach. Using Horsager's pillars of trust and communication framework of the National Institute of Standards and Technology's (NIST) Incident Response Recommendations, the paper discusses the crucial role that trust plays in cybersecurity communication. Using the Uber case study, it concludes that proactive and strategic communication can help reduce harm. According to the report, effective strategies for a successful response include employee training, preplanned communication protocols, and real-time monitoring. Finally, according to the study, companies can use data breaches as an opportunity to show more accountability and build trust, thereby protecting their reputation and stakeholder relationships in the process.

Keywords: *Cybersecurity Communication, Data Breaches, Crisis Communication, Organisational Trust, Stakeholder Trust, Transparency, Crisis Management, Trust-Building Strategies, Corporate Reputation.*

How to Cite: Uduak Ekott; Toyosi Kuteyi; Onyinyechi Enwereazu (2025) Building Trust Through Effective Communication During a Cybersecurity Data Breach. *International Journal of Innovative Science and Research Technology*, 10(9), 3182-3189. https://doi.org/10.38124/ijisrt/25sep1507

I. INTRODUCTION

Trust in an organization accelerates positive workplace interactions and improves employee collaboration, which is critical for achieving organizational goals (Guatam, 2024, p.560). According to Oldfield & Kushniryk (2025, p. 768) there is lack of trust around the world and looking at the public trust in the four main institutions (government, business, media, and non-governmental organizations), it can be said that it has drastically decreased. Furthermore, because trust is essential to organizational success, it can be difficult to establish and maintain in a multi-organizational setting (Oldfield & Kushniryk, 2025, p.768).

However, some of the causes of mistrust in modern society are corporate greed, fierce global competition, non-caring governments, downsizing and outplacement, mergers and acquisitions, and workforce diversity (Vokic et al., 2020, p. 70). As a result, communication is crucial for establishing and preserving trust in both personal and professional contexts (Appiah et al., 2020).

A data breach is any instance in which private, protected, or sensitive data is accessed without authorization and compromises the confidentiality, integrity, or availability of the impacted information asset. (Muzatko & Bansal, 2023, p.1629). Following a cybersecurity data breach, organizations with poor communication typically experience greater public backlash and a decline in stakeholder trust (Knight and Nurse, 2020, p.1). Therefore, transparency and prompt communication are vital components that contribute to reducing the negative consequences of data breaches. Organizations that openly address breaches, promptly share critical information, and provide sufficient support or redress are more trusted by stakeholders (Codex, 2023).

This article focuses on how important it is to communicate in a clear, timely, and transparent manner in order to build and maintain trust during cybersecurity data breaches. It examines how companies can use efficient communication techniques to lessen harm to their reputation, reassure stakeholders, and show accountability. The research emphasizes how organizations that are transparent about data breaches promptly provide accurate information, and offer assistance or support to stakeholders maintain and also enhance trust.

II. METHODOLOGY

This study integrates a systematic literature review with case study analysis using a qualitative research design. The objective is to investigate how stakeholder trust is impacted by organizational communication strategies in the event of data breaches.

To explore communication practices and trust-building mechanisms in greater detail, a qualitative approach was adopted. Qualitative methods are particularly helpful for exposing underlying meanings, relationships, and processes in social and organizational contexts (Creswell & Creswell, 2018, p.220).

➤ *Two Complementary Data Sources are Used in the Study:*

- *Literature Review:*
  Using databases like Sciencedirect, Emerald Insight, and Google Scholar, peer-reviewed books, journal articles, and industry reports were examined.

- *Case Study:*
  Uber (2016), a well-known corporate data breach, was chosen for examination. The case was selected because of its scale, the accessibility of trustworthy secondary data, and the communication difficulties the case highlights.

III. THE ROLE OF TRUST IN CYBERSECURITY COMMUNICATION

Trust represents an individual's readiness to accept vulnerability in relation to another's actions, grounded in the expectation that the trusted party will ultimately fulfil its commitments (Chen et al., 2025). It is understood as confidence that a service provider will uphold its promises while safeguarding users from potential risks (Gupta et al. 2025). Within digital financial services, customer trust is shaped by several factors, including perceptions of reliability, privacy, competence, and security. Horsager (2019) asserts that trust is a set of behaviors and qualities that can be seen, developed, and quantified rather than a generalized ideal. According to his framework, trust is supported by eight "pillars," each of which makes a distinct contribution.

Table 1 The Role of Trust in Cybersecurity Communication

Pillars	Definition
Clarity	Being clear; having well-defined missions, purpose, expectations, and messages. People trust what is clear and mistrust ambiguity (Horsager, 2019).
Compassion	Demonstrating care beyond self-interest; showing that the organisation cares about stakeholders' welfare (Horsager, 2019).
Character	People notice those who do what is right ahead of what is easy. Acting with integrity and ethical behaviour; doing what's right rather than what's easy (Horsager, 2019).
Competency	A humble and teachable person keeps learning new ways of doing things and stays current on ideas and trends (Horsager, 2019).
Commitment	People believe in those who stand through adversity (Horsager, 2019).
Connection	Trust is building genuine relationships; being willing to engage, connect, and relate with gratitude (Horsager, 2019).
Contribution	Be a contributor who delivers real results (Horsager, 2019).
Consistency	It's the little things that are done consistently that makes the biggest difference (Horsager, 2019).

Trust is at risk during cybersecurity incidents because there is a greater chance of anxiety, and fear when private or sensitive data is revealed during a security breach. This can have serious consequences for both consumers and organizations (Ou et al., 2022, p.1). Both tangible and intangible assets may be subject to significant financial losses as a result of inadequate security protocols and poor business operations (Perera et al., 2022, p.1). The financial risks and privacy threats are the two main factors that affect consumers' willingness to do business with a company again after a security breach (Ou et al., 2022, p.2).

Delays in data breach disclosure by organizations can lead to harsher customer assessments and increased conjecture regarding the extent of the breach (Muzatko & Bansal, 2023, p.1633). As a result, organizations usually take a variety of actions to limit the harm and attempt to recover (Ou et al, 2022, p.1). On the other hand, prompt disclosure is essential for determining customer satisfaction, influencing their willingness to make another purchase, and lowering feelings of uncertainty (Muzatko & Bansal, 2023, p.1632).

IV. CHALLENGES OF COMMUNICATION DURING A DATA BREACH

Communication is the use of various platforms to convey messages through verbal and nonverbal cues. In order to have an impact, communication must be effective, as successful business operations in multicultural organizations depend on effective communication (Hendrith, 2018, p.5).

➤ *Some of the Challenges of Communication During a Data Breach Include:*

- *Ambiguity:*
  When a breach is discovered, organizations often do not have all the information they need. This implies that early claims could be vague, resulting in unclear messaging. On October 23, 2015, the CEO of TalkTalk, a well-known UK telecom provider, spoke about a data breach on BBC Radio Four's *Today Program* (BBC, 2015). The CEO's admission during the interview was unclear if the compromised data had been encrypted, which drew criticism on social media and traditional media (Knight & Nurse, 2020, p.1). The Information Commissioner's Office (ICO) fined the company £400,000 after the UK House of Commons opened an investigation into the incident a few days later (Knight & Nurse, 2020, pp.1-2).

By making messages clear, reducing ambiguity, reaffirming organizational values, and maintaining consistency in communication, organizations build trust (Gautam, 2024, p.562). Because no system is completely secure, breaches can still happen, so organizations must react appropriately. Businesses' reputation and share value can be greatly impacted by how they respond to customers and external stakeholders following such incidents, which frequently elevate breaches to the level of cyber crises (Knight & Nurse, 2020, p.2).

- *Delayed Information/Slow Disclosure:*

Studies on data breach detection reveal that many breaches go undetected for months, and in some cases, more than a year (Ibrahim et al., 2020, p.2). Nevertheless, because state-specific legal deadlines for breach notifications differ, some may allow delayed responses, which may give organizations time to conduct internal investigations and fulfil their legal and regulatory obligations (Nikkhah & Grover, 2024, p.1051).

For instance, Florida mandates that organizations notify stakeholders within 30 days, whereas Ohio and Alabama allow up to 45 days (Nikkhah & Grover, 2024, p.1051). For stakeholders, a breach disclosed by a third party often has negative implications, as it suggests that expectations of prompt detection and security were not met which can indicate that the company either deliberately concealed the incident or was unaware of it due to weak security systems (Nikkhah & Grover, 2024, p.1051). One prominent example is Uber, which paid $100,000 to silence the hackers in order to hide its November 2016 breach that compromised the personal information of 57 million people (BBC, 2015). When outside parties eventually discover and make the breach public, such cover-ups put the company at risk of exposure.

Consequently, competition in global businesses increasingly requires the ability to develop trustworthy relationships with partners (Vokic et al., 2020, p.70) as people trust those who care beyond themselves (Horsager, 2022).

- *Lack of Transparency:*

Firms can lessen consumers’ feelings of vulnerability by promoting transparency and allowing them some control over their personal data (Ho et al., 2023, p.4). Similarly, employees who receive accurate and timely updates on important decisions, strategies, and objectives are better able to understand and support organizational transparency. There is less trust when there is insufficient disclosure or dishonest communication. Having access to such relevant information reduces uncertainty and increases staff trust (Gautam, 2024, p.562).

Mistrust among key stakeholders is greatly increased by delayed disclosure, a lack of transparency, and unclear communication during data breaches. Because stakeholders usually react negatively to such incidents, data breaches can cause significant losses for affected organizations in terms of both revenue and reputation (Nikkah & Grover, 2024, p.1043). Data breaches also have the potential to significantly erode consumer trust, which harms an organization's reputation and therefore influences consumers' protective behaviors (Ho et al., 2023, p.3).

Delays and ambiguous statements give consumers the sense that businesses are hiding information, which heightens negative perceptions and makes them feel more vulnerable (Muzatko & Bansal, 2023). According to studies, customers' trust is damaged when businesses don't provide timely and transparent updates, which lowers customer satisfaction and repurchase intentions (Muzatko & Bansal, 2023).

Employees are also impacted because ambiguous or inconsistent messaging lowers morale and undermines internal trust by leaving staff members unsure of their own role in remediation as well as organizational responsibilities (Gautam, 2024, p.562). According to Vokic et al. (2020, p. 70). Employees' trust in their organizations not only comes before their job performance, commitment, and satisfaction, but it also fosters organizational innovation and learning, performance outcomes, and effective crisis management.

Regulators worry about accountability and adherence to legal reporting obligations when there is ambiguity and delayed notification. According to research, these kinds of failures often have legal repercussions and can damage an organization's reputation (Nikkhah & Grover, 2024). Collectively, these communication challenges exacerbate reputational damage and increase mistrust among all parties involved.

V. EFFECTIVE COMMUNICATION STRATEGIES TO BUILD TRUST DURING A BREACH

➢ *Clarity:*

It is important to clearly state the breach and the next steps (Horsager, 2019). By lowering uncertainty, giving stakeholders clear information during a crisis helps to reduce their anxiety (Coombs, 2015, p.142). It is important for organizations to state what is known and what is unknown, avoid technical jargon, and provide stakeholders with specific next steps because initial communications that are clear, cut down misunderstanding (Harvard Business Review, 2016).

➢ *Compassion:*

This emphasizes that organizations should be considerate of stakeholders and affected users (Horsager, 2019). Open with sincere concern and acknowledgement of harm (not boilerplate). In addition to lowering stakeholder anxiety, empathetic communications demonstrate that the company prioritizes its reputation (ProAssurance, 2024).

➢ *Character:*

Maintain integrity and openness despite adverse effects (Horsager, 2019).

When a data controller informs individuals about a breach, the communication should be transparent, timely, and effective (European Data Protection Board (EDPB), 2023, p. 27). Transparent communication includes direct channels such as email, SMS, or direct messages, as well as high-visibility notifications like website banners, postal letters, or printed media advertisements. In contrast, limiting disclosure to a press release or a corporate blog is considered insufficient for reaching affected individuals. The EDPB advises controllers to select communication methods that maximize the likelihood of successfully informing all impacted persons (EDPB),2023, p. 21).

Organisations gain an advantage by being the first to release information about a crisis, as reputational harm worsens when external parties break the news instead (Coombs, 2015, p.144).

➢ *Competency:*

Demonstrate technical and crisis management expertise (Horsager, 2019). According to NIST (2012, p. 30), incident response teams rely on the expertise, judgment, and assistance of a number of other departments, including management, information assurance, IT support, legal services, public relations, and facilities management.

➢ *Commitment:*

Share information about continuous attempts to fix the security flaw and safeguard interested parties. To guarantee that media communications stay accurate and consistent, maintain a current record of the incident's status (NIST, 2012, p.11).

➢ *Connection:*

Involve stakeholders by providing frequent updates and providing open avenues for input (Horsager, 2019). Make use of a variety of channels, including social media, email, website updates, and customer service lines, and give a clear way to contact someone with questions. According to the Harvard School Review (2016), two-way communication (Q&A, help lines) restores relationship trust and guards against false information.

➢ *Contribution:*

Connect actions to observable outcomes and safeguards (Horsager, 2019). While expressing sympathy can lessen feelings of rage, outlining corrective measures reassures stakeholders that steps are being taken to prevent recurrence (Coombs, 2015, p.142). Following established protocols and keeping thorough records of all actions taken, the incident response team must quickly evaluate and validate each incident (NIST, 2025, p. 29).

➢ *Consistency:*

Throughout the crisis, keep your messaging consistent. Organizations must avoid making contradicting statements and interact with external stakeholders, such as other response teams, law enforcement, the media, vendors, and impacted organizations, while handling incidents (NIST, 2012, p.2).

VI. CASE STUDY OF UBER

Uber acknowledged that it had a significant hack in October 2016 that exposed the personal information of 57 million drivers and passengers globally, but at the time, it did not notify the affected parties or authorities (The Guardian, 2017). Uber acknowledged its lack of transparency by disclosing the breach in November 2017 (BBC, 2018). The business also revealed that it had paid the hackers $100,000 to remove the stolen data and keep quiet about the event (The Guardian, 2017). Although Uber insisted that more sensitive information like location, payment, banking, and social security details remained unaffected, the hack only revealed the names, email addresses, phone numbers, and driver's license information of about 600,000 drivers in the United States (The Guardian, 2017). Later, Uber consented to a settlement with the U.S. government and 50 states over its failure to promptly report the incident (BBC, 2018). Uber's response to the 2016 data breach reveals a breakdown in a number of Horsager's communication framework because the company intentionally kept the incident a secret from drivers, customers, and regulators; thus, it lacked clarity and transparency. Additionally, because its actions went against its declared values of safety and trust, this omission compromised consistency. Uber jeopardized competence and character by paying hackers to keep quiet. Pittsburgh Uber driver Robert Judge expressed disapproval of the company's response to the hack, claiming that the hack and subsequent cover-up were motivated by Uber's own interests and not considering the drivers and customers. He went on to say that he had heard about the incident from media reports rather than directly from the company (The Guardian, 2017).

VII. RECOMMENDATIONS

➢ *Develop a Pre-Planned Communication Protocol for Breach Incidents.*

According to Coombs (2015, p.141), companies that have a crisis communication strategy do better when it comes to reputation preservation. Crisis communication must be strategic, with actions intended to support stakeholders and protect the organization during a crisis.

One of the most widely used incident response frameworks is the NIST guidelines. These guidelines advise taking the following actions:

- Govern (GV): Where policies and strategies for risk management are established and tracked
- Identify (ID): Recognizing present dangers
- Protect (PR): Putting precautions in place to control risks
- Detect (DE): Identifying and evaluating possible assaults
- Respond (RS): Addressing incidents that have been identified
- Recover (RC): Restoring operations and assets that have been impacted (NIST, 2025, p.5).

Rather than being specific components of incident response, Govern, Identify, and Protect are part of larger cybersecurity risk management procedures.

The top-level definition of the incident response cycle is Detect, Respond, and Recover.

At the middle level, the Improvement Category (ID.IM) within the Identify Function places a strong emphasis on continuous improvement, where lessons learned from all functions are assessed, given priority, and used to improve subsequent efforts (NIST, 2025, p.5).

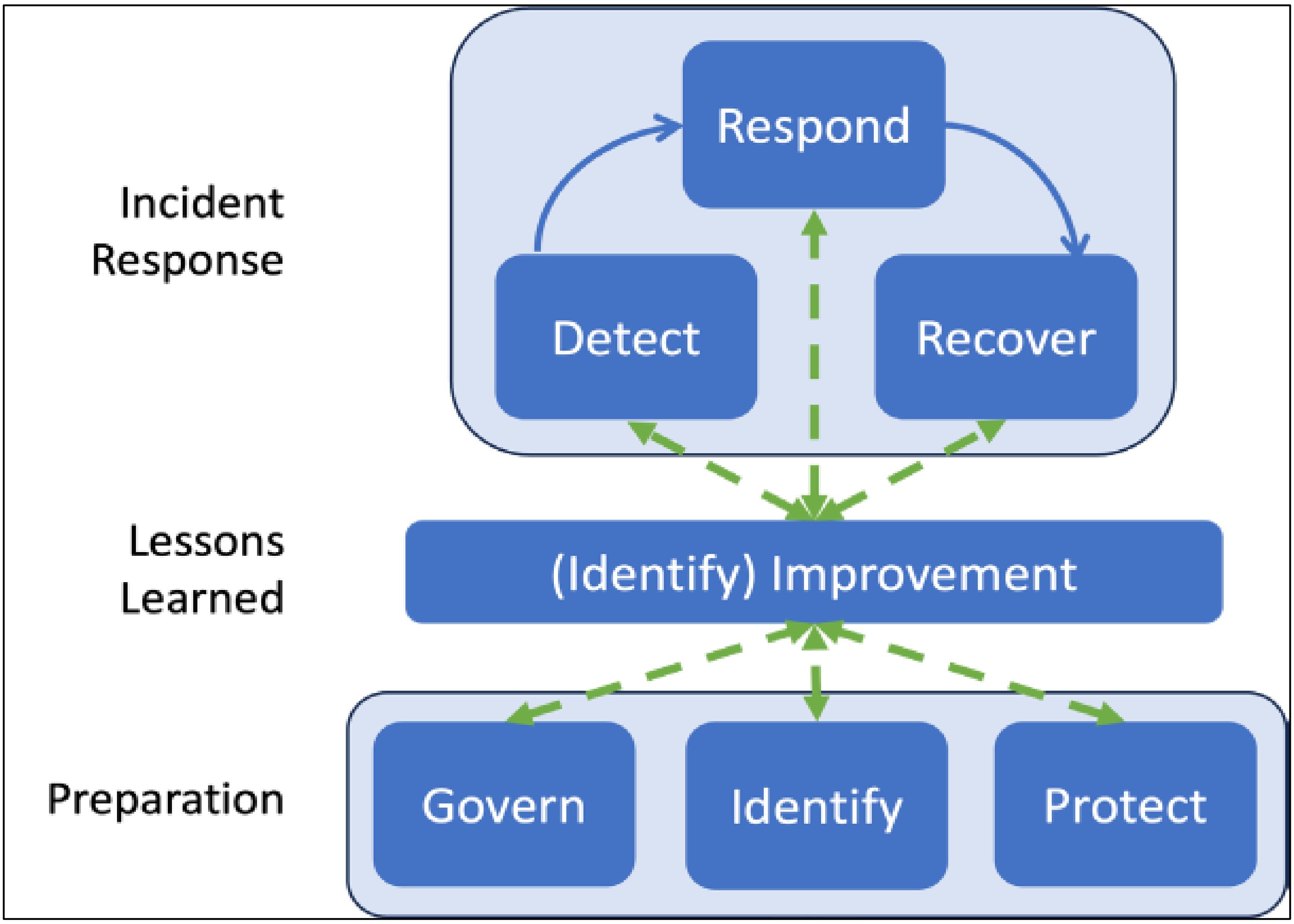


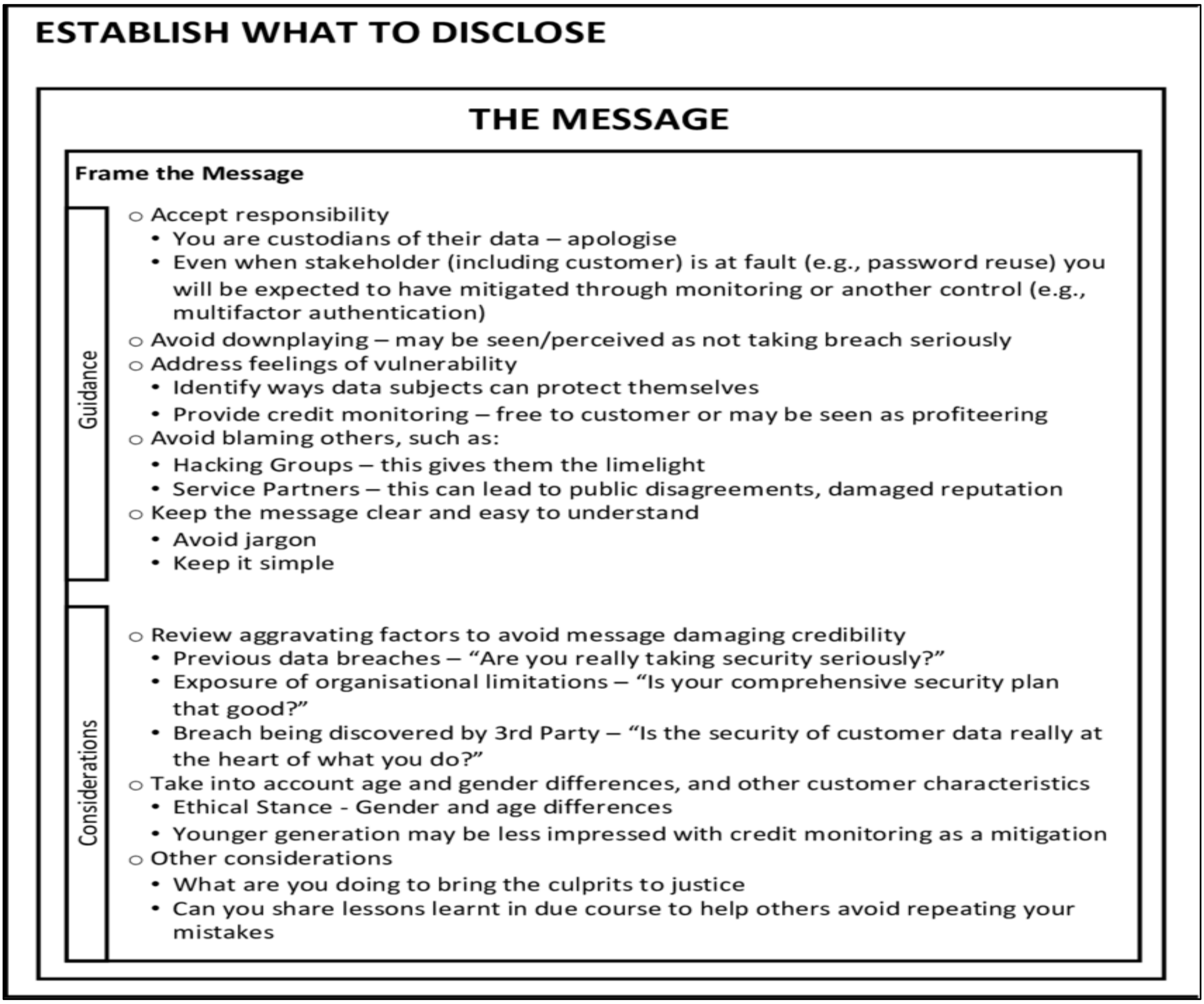
Fig 1 Incident Response Life Cycle Model Based on CSF 2.0 Functions (NIST, 2025, p.5)

➢ *Train Communication Teams on Trust-Building Principles During Cybersecurity Events*

Employees should receive training on how to use trust-building techniques in crisis communications, such as consistency, clarity, transparency, and empathy (Horsager, 2012). Because stakeholders frequently feel that organizations could have prevented or detected attacks by implementing stronger access controls, improved employee training, or more stringent monitoring systems (NIST, 2025, p.21), employees should receive cybersecurity awareness and training to ensure they can carry out tasks related to cybersecurity (Nikkhah & Grover, 2024, p.1047).

Furthermore, as companies become more team-oriented and less hierarchical, the effectiveness of managers is hinged on their capacity to win over their subordinates and employees (Poloski et al., 2020, p. 70).

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25sep1507



ESTABLISH WHAT TO DISCLOSE

THE MESSAGE

Frame the Message

Guidance

- ○ Accept responsibility
  - You are custodians of their data – apologise
  - Even when stakeholder (including customer) is at fault (e.g., password reuse) you will be expected to have mitigated through monitoring or another control (e.g., multifactor authentication)
- ○ Avoid downplaying – may be seen/perceived as not taking breach seriously
- ○ Address feelings of vulnerability
  - Identify ways data subjects can protect themselves
  - Provide credit monitoring – free to customer or may be seen as profiteering
- ○ Avoid blaming others, such as:
  - Hacking Groups – this gives them the limelight
  - Service Partners – this can lead to public disagreements, damaged reputation
- ○ Keep the message clear and easy to understand
  - Avoid jargon
  - Keep it simple

Considerations

- ○ Review aggravating factors to avoid message damaging credibility
  - Previous data breaches – “Are you really taking security seriously?”
  - Exposure of organisational limitations – “Is your comprehensive security plan that good?”
  - Breach being discovered by 3rd Party – “Is the security of customer data really at the heart of what you do?”
- ○ Take into account age and gender differences, and other customer characteristics
  - Ethical Stance - Gender and age differences
  - Younger generation may be less impressed with credit monitoring as a mitigation
- ○ Other considerations
  - What are you doing to bring the culprits to justice
  - Can you share lessons learnt in due course to help others avoid repeating your mistakes

Fig 2 What to Disclose (Knight & Nurse, 2020, p.12).

➢ *Implement Real-Time Monitoring and Feedback Loops to Adapt Messages as the Situation Evolves.*

The ability of a system to respond instantly, nearly at the same time as the event, is commonly referred to as real-time. Because it allows for quick responses to transient events, real-time data analysis is crucial in a variety of fields (Kebande et al., 2020, p.4). Real-Time Monitoring (RTM) lowers the risk of downtime in networks by enabling administrators and engineers to identify and resolve problems like faults, failures, performance issues, system health, and usage delays as they arise (Kebande et al., 2020, p.4).

VIII. CONCLUSION

Cybersecurity data breaches are communication crises that test an organization's resilience and integrity, more than technical malfunctions, and trust is the most important factor in determining how stakeholders view and respond to such crises. Experience and evidence have demonstrated that withholding, divergent, or indifferent communication exacerbates reputational loss and undermines trust, as evidenced by incidents such as Uber. Conversely, open, consistent, and compassionate communication can lessen harm.

It is clear from frameworks like Horsager's pillars of trust and NIST's incident response recommendations that crisis communication needs to be responsible, timely, and strategic. For corrective actions and stakeholder involvement to establish credibility, organizations can respond swiftly and consistently through pre-planned communication protocols, staff training, real-time observation, and feedback mechanisms.

Effective cybersecurity communication is not only about managing immediate fallout but also about safeguarding long-term relationships. Organizations can use crises as opportunities to build trust, safeguard their brand, and show that they genuinely care about the welfare of stakeholders by putting an emphasis on transparency, clarity, and empathy.

REFERENCES

[1]. Appiah, B., & Maharjan, R. (2020). Developing and Maintaining Trust Within Organizations: Tech One Global in Nepal. *Master's thesis, University of Gavle.* https://www.diva-portal.org/smash/get/diva2:1441710/FULLTEXT01.pdf

[2]. BBC. (2015, October 23). *TalkTalk cyber-attack: website hit by 'significant' breach* https://www.bbc.co.uk/news/uk-34611857

[3]. BBC. (2018, September 27). *Uber pays $148m over data breach cover-up.* https://www.bbc.com/news/technology-45666280?utm

[4]. Chen, SY., Ahlstrom, D., & Uen, JF. (2025). Organizational trust and employee work outcomes: A moderated mediation model. Curr Psychol 44, 6565–6578 (2025). https://doi.org/10.1007/s12144-025-07626-0

[5]. Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). Sage.

[6]. Codex Y. (2023). Understanding the impact of data breaches on consumer perception and reputation management: a review of effective communication and trust building strategies. *Yubetsu codex computer science,* 1(4). https://codex.yubetsu.com/article/eb84a2d618cd40cf9d2e14f1e0689dfd

[7]. Coombs, W.T. (2015). The value of communication during a crisis: Insights from strategic communication research, *Business Horizons,* 58 (2), 142. https://www.sciencedirect.com/science/article/pii/S0007681314001505

[8]. European Data Protection Board (EDPB). (2023). *Guidelines on personal data breach notification under GDPR Version 2.0.* https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf?utm

[9]. The Guardian (2017, November 22). *Uber concealed massive hack that exposed data of 57m users and drivers.* https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack?utm

[10]. Gautam, P. K. (2024). Crisis to resilience: cultivating effective internal communication for employee engagement and organizational trust. *Quest Journal of Management and Social Sciences,* 6(3), 560. https://doi.org/10.3126/qjmss.v6i3.72488

[11]. Gupta, R., Pandey, P., Singh, V.K. & Sinha, K. (2025). Effectiveness of Cybersecurity Measures in Building Customer Trust in Digital NBFC Services. International Journal of Latest Technology in Engineering Management & Applied Science, 14(6), 890-899. https://doi.org/10.51583/IJLTEMAS.2025.140600098

[12]. Harvard Business Review. (2016, Octobeer 7). *Your Company Needs a Communications Plan for Data Breaches.* https://hbr.org/2016/10/your-company-needs-a-communications-plan-for-data-breaches?utm

[13]. Hendrith, M. (2018). The effects culture and communication have on business. *Integrated Studies,* 120. https://core.ac.uk/download/pdf/158221587.pdf

[14]. Horsager, D. (2019). *Trust: The Leading Indicator (The 8 Pillars of Trust).* https://davidhorsager.com/category/8-pillars/?utm_source=chatgpt.com

[15]. Ibrahim, A., Thiruvady D., Schneider J.G, & Abdelrazek .M. (2020). The challenges of leveraging threat intelligence to stop data breaches. *Frontiers in Computer Science,* 2. https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2020.00036/full

[16]. Kebande, V.R., Karie, N.K., Ikuesan, R.A. (2020). Real-time monitoring as a supplementary security component of vigilantism in modern network environments. *International Journal of Information & Technology.* 4. https://arxiv.org/pdf/2012.03622

[17]. Knight R., & Nurse, J.R.C. (2020). A framework for effective corporate communication after cyber security incidents. *Computer and Security Journal*, 99. https://www.sciencedirect.com/science/article/pii/S0167404820303096

[18]. Muzatko, S. & Bansal, G. (2024); It pays to be forthcoming: timing of data breach announcement, trust violation, and trust restoration. *Internet Research*; 34 (5): 1629–1663. https://www.emerald.com/intr/article/34/5/1629/1224207/It-pays-to-be-forthcoming-timing-of-data-breach

[19]. National Institute for Standards and Technology (NIST). (2012). *Computer security incident handling guide. United States of America* https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf?utm

[20]. National Institute for Standards and Technology (NIST). (2024). *Data confidentiality: Detect, respond to, and recover from data breaches.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-29.pdf

[21]. National Institute for Standards and Technology (NIST). (2025*). Incident response recommendations and considerations for cybersecurity risk management. United States. of America.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

[22]. Nikkhah, H. R., & Grover, V. (2024). Strategizing Responses to data breaches: a multi-method study of organizational responsibility and effective communication with stakeholders. *Journal of Management Information Systems*, *41*(4), 1042–1077. https://doi.org/10.1080/07421222.2024.2415774

https://www.tandfonline.com/doi/epdf/10.1080/07421222.2024.2415774?needAccess=true

[23]. Oldfield, N.D. & Kushniryk, A. (2017). Building and protecting organizational trust with external publics: Canadian senior executives' perspectives. *Canadian Journal of Communication* 42 (5), 768. https://cjc.utppublishing.com/doi/pdf/10.22230/cjc.2017v42n5a3076

[24]. Ou, C.X., Zhang, X., Angelopoulos, S. Davison, R.M., Janse, N. (2022). Security breaches and organization response strategy: Exploring consumers' threat and coping appraisals. https://www.sciencedirect.com/science/article/pii/S0268401222000299?utm_source=chatgpt.com

[25]. Perera, S., Jin, X., Maurushat, A., & Opoku, G. J. (2022). Factors affecting reputational damage to organisations due to cyberattacks. *Informatics*, *9*(1), 28. https://doi.org/10.3390/informatics9010028

[26]. ProAssurance. (2024). *Crisis communication strategies after a healthcare data breach.* https://riskmanagement.proassurance.com/article-library/crisis-communication-strategies-after-a-data-breach?utm_source=chatgpt.com

[27]. Vokić, P., Bilušić, M.R., Najjar, D. (2020). Building organizational trust through internal communication. *Corporate Communications: An International Journal* 26 (1), 70. https://www.emerald.com/ccij/article-pdf/26/1/70/408900/ccij-01-2020-0023.pdf