American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Digital Trust Recovery Following Organizational Data Breaches

Dr. Daniel A. Williams

Associate Professor, University of Bristol, United Kingdom

Abstract

Organizational data breaches create more than technical and regulatory problems. They can undermine the digital trust through which customers, employees, partners, investors, and other stakeholders accept organizational claims regarding privacy, cybersecurity, accountability, and responsible data stewardship. Trust recovery therefore requires more than repairing the technical vulnerability that enabled an incident. Empirical research has shown that delayed breach announcements can produce larger reductions in consumer trust than prompt announcements and can constrain subsequent trust-repair efforts, even when organizations later provide protective services such as identity-theft monitoring. Contemporary incident-response guidance similarly emphasizes forensic investigation, vulnerability remediation, documentation, coordinated communication, and notification of affected parties as integrated elements of breach management.

This study develops a multidimensional Digital Trust Recovery Framework for organizations responding to material data breaches. The conceptual-methodological design integrates breach-response guidance, stakeholder theory, crisis communication, privacy accountability, service-recovery research, and information-security governance. Six recovery mechanisms are examined: rapid transparent disclosure, technical remediation, stakeholder assistance, meaningful accountability, independent assurance, and sustained governance improvement. A simulation-based trust-recovery model demonstrates how an illustrative pre-breach trust index of 88 may decline to 54 after a breach and subsequently recover to 86 through a cumulative sequence of transparent notification, technical remediation, victim support, independent assurance, and sustained governance.

These values are explicitly synthetic and do not represent observations from an actual organization. The study argues that trust restoration is neither automatic nor equivalent to reputation management. Trust can be rebuilt only when organizational communication is supported by verifiable corrective action, stakeholder protection, demonstrable learning, and continued evidence that security and privacy governance have materially improved.

Keywords: digital trust, data breach, trust recovery, cybersecurity incident response, crisis communication, privacy governance, stakeholder trust, organizational accountability, breach notification, cyber resilience

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

1. Introduction

Digital trust has become an important organizational asset because customers, employees, partners, and other stakeholders routinely provide personal information and rely on digital services without having direct visibility into the technical controls that protect their information. This relationship is partly dependent on an assumption that the organization will collect and use data responsibly, apply adequate safeguards, communicate honestly when problems occur, and provide meaningful remedies when those safeguards fail. A data breach can therefore create a dual failure. The immediate failure concerns unauthorized access, disclosure, loss, alteration, or destruction of information, while the secondary failure concerns stakeholder confidence in the organization's competence, integrity, and willingness to act responsibly after the incident. The Information Commissioner's Office defines a personal data breach broadly enough to include accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access, emphasizing that breach management must consider more than simple data theft.

The organizational consequences of a breach are shaped partly by how the organization communicates after discovering it. Muzatko and Bansal experimentally examined the timing of breach announcements and found that delayed disclosure produced a greater reduction in consumer trust than immediate disclosure. Their study further showed that later provision of identity-theft protection and credit monitoring could improve trust, but organizations that delayed the original announcement remained at a lower repaired-trust level. These findings are significant because they indicate that communication timing is not merely a public-relations choice. Delay can become evidence through which stakeholders infer organizational honesty, competence, and respect for their interests.

Technical recovery is equally important. NIST revised its principal incident-response guidance in April 2025 through SP 800-61 Revision 3, integrating incident response more directly with Cybersecurity Framework 2.0 risk-management activities. The guidance emphasizes preparation, detection, response, recovery, and the use of lessons learned and root-cause analysis to improve wider cybersecurity risk management. The Federal Trade Commission's business guidance similarly recommends preserving forensic evidence, identifying the data and people affected, addressing compromised access, correcting vulnerabilities, reviewing service-provider involvement, and creating a coordinated communications plan for affected stakeholders. Trust repair that consists only of an apology without verifiable operational improvement can therefore remain fragile because stakeholders may interpret communication as symbolic rather than substantive.

Legal and regulatory obligations also influence trust recovery, although requirements vary by jurisdiction and sector. Under current UK guidance, organizations subject to the UK GDPR must notify the ICO of notifiable personal data breaches without undue delay and, where feasible, within 72 hours of becoming aware of them. Where a breach is likely to create a high risk to individuals' rights and freedoms, affected individuals must also be informed without undue delay. Organizations are expected to maintain breach records and document facts, effects, and remedial actions. These obligations illustrate an important governance principle: responsible post-breach behavior requires both external communication and an internal evidentiary record capable of demonstrating accountability.

The present study develops a Digital Trust Recovery Framework that integrates these technical, communicative, ethical, and stakeholder dimensions. The paper does not claim that trust can always be restored completely or that identical recovery strategies will work across all breach types. Breach

severity, organizational responsibility, sensitivity of the compromised information, prior trust, stakeholder vulnerability, regulatory context, and previous incidents can all affect recovery. Instead, the study asks which institutional mechanisms are most important for creating a credible pathway from breach recognition to sustained trust restoration and how organizations can distinguish short-term reputation management from long-term digital trust recovery.

2. Objectives of the Study

2.1 To Identify the Core Determinants of Post-Breach Digital Trust Recovery

The first objective is to identify the principal organizational actions through which trust may be damaged or restored following a data breach. The study considers disclosure timing, accuracy of communication, admission of responsibility where appropriate, technical remediation, stakeholder assistance, compensation or protective support, independent verification, leadership accountability, and evidence of long-term governance improvement.

The framework treats trust recovery as cumulative. A strong communication response cannot compensate indefinitely for weak remediation, while a technically effective recovery may still fail to rebuild confidence if stakeholders believe that the organization concealed material information or minimized the consequences of the incident.

2.2 To Distinguish Immediate Incident Recovery from Long-Term Trust Reconstruction

The second objective is to distinguish the restoration of systems from the restoration of stakeholder confidence. Incident containment may occur within hours or days, whereas trust reconstruction can continue for months or years.

Technical recovery focuses on stopping unauthorized access, preserving evidence, removing attacker persistence, restoring services, changing credentials, repairing vulnerabilities, and validating affected systems. Trust reconstruction additionally requires repeated evidence that the organization has learned from the event and altered practices in ways that make recurrence less likely.

2.3 To Develop an Operational Digital Trust Recovery Framework

The third objective is to translate trust-repair principles into a structured governance model that organizations can apply following material data breaches.

The proposed framework evaluates six domains: transparent disclosure, technical remediation, affected-person support, accountability, independent assurance, and sustained privacy and security governance.

3. Review of Literature

3.1 Trust Violation, Disclosure Timing, and Crisis Communication

Trust can be understood as a willingness to remain vulnerable to another actor based partly on expectations regarding that actor's competence, integrity, and intentions. Data breaches can damage all three dimensions simultaneously. Stakeholders may question whether the organization was technically competent enough to protect the data, sufficiently honest in communicating what happened, and adequately concerned about the consequences experienced by affected individuals.

Bansal and Zahedi examined trust violation and repair from an information-privacy perspective and showed that the nature of a privacy breach and the organization's response strategy influence trust-repair outcomes. Their work is important because it demonstrates that recovery does not depend only on the existence of an apology. Stakeholders interpret the response in relation to what they believe caused the violation and whether the response appears appropriate to that cause.

Muzatko and Bansal provide especially direct evidence concerning disclosure timing. Their survey experiment compared immediate breach announcement with a two-month delay and found that delayed disclosure generated a larger decline in consumer trust. Identity-theft protection and credit monitoring improved trust after the incident, but delayed-disclosure organizations remained disadvantaged during the recovery stage. Timeliness therefore has both an immediate and residual effect. Ruohonen, Hjerppe, and Kortesuo's qualitative research on data-breach crisis communication similarly emphasizes early communication, organizational responsibility, apology, and notification of authorities within successful response patterns, while less successful responses exhibited blame shifting, excessive victim framing, or failure to notify appropriately. This finding supports a broader crisis-management principle: stakeholders evaluate not only the incident but the organization's behavior while the incident is unfolding.

The FTC's breach-response guidance reflects the same practical concern by recommending a comprehensive communications plan, plain-language answers, information for all affected audiences, and avoidance of misleading statements or withholding details that people need to protect themselves. Effective communication is therefore both informational and protective.

3.2 Apology, Compensation, and Stakeholder Recovery

Post-breach recovery research has increasingly examined actions that go beyond notification. Goode, Hoehle, Venkatesh, and Brown's study of user compensation following the Sony PlayStation Network breach investigated compensation as an organizational data-breach recovery mechanism and demonstrated the importance of recovery justice and user responses to organizational remedial action. The study helped establish that post-breach recovery can involve substantive stakeholder support rather than communication alone.

Masuch, Greve, and Trang later examined apology and compensation strategies in the context of health-service providers. Their experimental investigation found substantial support for the proposition that recovery actions such as apology and compensation can improve satisfaction with organizational recovery efforts, although effective recovery depends on alignment with stakeholder expectations. These findings suggest that there is no universal recovery package applicable to every breach. A person exposed to payment-card fraud, for example, may require different support from someone whose email address was exposed or whose medical information was disclosed.

Mohammed's conceptual study broadens the recovery problem beyond customers alone. Using stakeholder theory and illustrative analysis of Anthem, Equifax, and Citrix, the study identifies customer, employee, process, and regulatory recovery as distinct but interacting areas requiring organizational attention. This perspective is particularly valuable because breach response often concentrates on public customer communication while employees, business partners, investors, regulators, and service providers may also experience consequences.

Stakeholder recovery should therefore be based on actual harm pathways. Appropriate measures may involve account protection, credential reset, credit monitoring, fraud support, identity-theft assistance, dedicated help channels, compensation where justified, or additional support for employees whose personal information was exposed. ICO guidance similarly recommends giving individuals clear advice about how to protect themselves and identifies actions such as forced password resets, use of strong unique passwords, and heightened attention to phishing or fraudulent activity where relevant.

3.3 Technical Remediation, Accountability, and Long-Term Assurance

Trust recovery can fail when an organization communicates effectively but does not demonstrate that the underlying security weaknesses have been corrected. NIST SP 800-61 Revision 3 emphasizes that incident-response lessons and root-cause analysis should feed back into cybersecurity risk management so that incidents become sources of institutional learning rather than isolated operational events. The FTC likewise advises organizations to work with forensic experts, restrict unnecessary access, examine network segmentation, verify the data affected, evaluate service-provider access, and implement recommended remedial measures promptly.

Accountability adds another dimension. Current ICO guidance requires organizations to keep records of personal data breaches and document relevant facts, effects, and remedial actions, even where not every breach requires external notification. The accountability principle more broadly requires organizations to take responsibility for how personal data are processed and to maintain measures and evidence capable of demonstrating compliance. Documentation therefore has trust significance as well as regulatory significance: it makes later claims of remediation auditable.

Independent assurance can strengthen this evidence. External forensic review, penetration testing, security assessments, audit, certification, regulatory monitoring, or publication of meaningful corrective-action progress can reduce the information asymmetry between organizations and stakeholders. Affected individuals usually cannot inspect security architecture directly, so they rely partly on credible third parties to evaluate whether remediation claims are justified.

Long-term trust recovery consequently depends upon a transition from incident communication to governance evidence. Organizations must show not only that they contained the immediate event but that leadership, investment, accountability, privacy controls, third-party oversight, detection, incident preparation, and organizational culture have changed sufficiently to reduce the likelihood and impact of recurrence.

4. Research Methodology

4.1 Research Design and Evidence Base

The study adopts a conceptual-methodological design supported by simulation-based trust-recovery analysis. It does not use confidential breach records, affected-person survey data, customer databases, or observations of a real company.

The evidence base integrates peer-reviewed research on data-breach trust repair, crisis communication, compensation, stakeholder recovery, and privacy violations with authoritative incident-response and privacy-governance guidance. Current NIST guidance is used to structure the cybersecurity

recovery dimension, while FTC and ICO materials inform operational communication, remediation, breach documentation, and notification principles.

The framework is intentionally jurisdiction-neutral at the conceptual level. Where regulatory examples are discussed, they are identified as jurisdiction-specific rather than presented as universal legal requirements.

4.2 Digital Trust Recovery Dimensions

The proposed framework evaluates six dimensions that collectively contribute to recovery.

Table 1: Proposed Digital Trust Recovery Framework

Recovery Dimension	Core Question	Principal Organizational Actions	Trust Function
Transparent Disclosure	Did the organization communicate accurately and promptly enough for stakeholders to understand material risk?	Timely notification, plain-language explanation, uncertainty disclosure, regular updates	Supports perceived honesty and integrity
Technical Remediation	Has the organization actually corrected the weaknesses that enabled or worsened the breach?	Forensics, containment, patching, access review, segmentation, credential reset, root-cause analysis	Restores confidence in competence
Stakeholder Protection	Has the organization reduced the practical harm experienced by affected people?	Protective monitoring, support channels, fraud guidance, compensation where justified	Demonstrates concern and responsibility
Organizational Accountability	Is responsibility visible and are decisions documented?	Executive ownership, documented breach record, regulator cooperation, internal review	Reduces responsibility diffusion
Independent Assurance	Can stakeholders rely on credible evidence beyond organizational self-reporting?	Independent security review, audit, external testing, assurance reporting	Strengthens credibility of remediation claims
Sustained Governance	Are improvements continuing after media and regulatory attention declines?	Security investment, privacy governance, training, third-party oversight, monitoring, repeated testing	Supports long-term trust reconstruction

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Source: Author-developed framework informed by NIST incident-response guidance, FTC breach-response guidance, ICO accountability requirements, and trust-repair research.

4.3 Simulation Model and Trust-Recovery Logic

The model deliberately stops below the original trust level. The assumption is not that every organization permanently loses trust, but that a serious breach may create residual uncertainty even after strong recovery.

In some contexts, trust could eventually exceed pre-breach levels if stakeholders conclude that the organization has become substantially more transparent and secure; in other contexts, complete recovery may never occur.

5. Analysis

5.1 Simulated Sequence of Trust Loss and Recovery

Table 2: Simulated Digital Trust Recovery Following a Data Breach

Recovery Stage	Trust Change	Cumulative Trust Index	Principal Interpretation
Pre-Breach Trust	—	88	Stakeholders possess relatively strong confidence in organizational data stewardship
Breach Impact	-34	54	Security failure creates major competence, integrity, and privacy concerns
Rapid Disclosure	+8	62	Prompt communication reduces uncertainty and signals respect for affected stakeholders
Technical Remediation	+10	72	Verified corrective action provides evidence that underlying weaknesses are being addressed
Victim Support	+6	78	Practical assistance demonstrates responsibility for downstream harm
Independent Assurance	+5	83	External review increases credibility of organizational remediation claims
Sustained Governance	+3	86	Continued improvement shows that security reform extends beyond short-term crisis management

Note: All numerical values are simulated methodological examples. They do not represent measured trust levels from an actual company or breach.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

The largest single loss occurs at breach discovery because the incident directly challenges the organization's prior promise—explicit or implicit—that personal information will be handled responsibly.

The largest simulated recovery contribution comes from technical remediation. This reflects the assumption that communication alone cannot sustain trust unless stakeholders believe the organization has materially reduced the likelihood of recurrence.

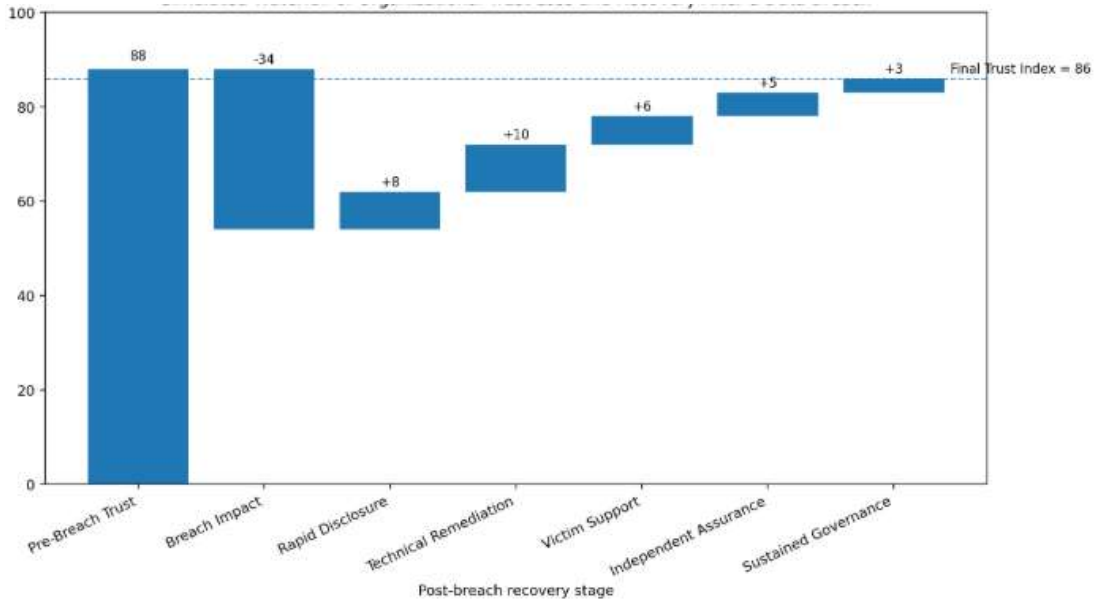
Rapid disclosure contributes eight simulated points. This assumption is supported conceptually by Muzatko and Bansal's experimental finding that immediate breach notification produced less trust damage than delayed announcement.

Victim support produces a further six-point recovery. This stage reflects the importance of recovery actions identified in work by Goode and colleagues and Masuch and colleagues, where compensation or other protective responses can influence stakeholder reactions after a breach.

Independent assurance and sustained governance provide smaller incremental improvements but perform a different function: they help convert short-term recovery claims into evidence of longer-term institutional change.

5.2 Waterfall Analysis of Digital Trust Recovery

Graph 1: Simulated Waterfall of Organizational Digital Trust Loss and Recovery Following a Data Breach



The waterfall chart illustrates trust recovery as an accumulated sequence rather than an immediate rebound. The breach reduces the illustrative index from 88 to 54, after which recovery mechanisms progressively rebuild confidence.

The chart is especially useful because it demonstrates that no single action restores the original trust position. Transparent disclosure helps, but the organization remains well below its pre-breach level.

Technical remediation produces the largest recovery movement because it addresses the organizational capability that stakeholders may now question most strongly. Stakeholder support, independent assurance, and sustained governance then progressively narrow the remaining trust deficit.

The final simulated index reaches 86 rather than returning mechanically to 88. This residual difference represents a continuing memory of the breach and the possibility that some stakeholders remain more cautious even after strong remediation.

5.3 Trust-Recovery Governance Sequence

The proposed recovery sequence begins with facts before image management. Organizations should establish an incident command structure, preserve forensic evidence, determine what is known and unknown, assess affected information, and avoid unsupported claims. NIST and FTC guidance both emphasize investigation, evidence preservation, and coordinated incident management.

The second stage is protective transparency. Communication should occur early enough to permit affected stakeholders to take protective action while avoiding speculation that may later require correction. Under UK GDPR requirements, where a breach creates high risk to individuals, affected people must be informed without undue delay and should receive advice regarding protective steps.

The third stage is credible remediation. Organizations should explain what categories of security improvements are being made without revealing operational details that could create new risks. Independent assessment becomes especially valuable at this stage.

The fourth stage is stakeholder-specific recovery. Employees, customers, regulators, partners, and investors may require different information and support. Mohammed's recovery model demonstrates the importance of identifying which stakeholder groups have been affected and aligning recovery actions with customer, employee, process, and regulatory recovery areas.

The final stage is governance persistence. Trust recovery should remain visible after the immediate crisis through board oversight, privacy governance, security investment, recurring testing, third-party risk management, staff training, and documented closure of corrective actions.

6. Discussion

6.1 Timely Transparency Reduces Uncertainty but Cannot Substitute for Competence

The analysis reinforces the importance of disclosure timing. When an organization delays communication after it has sufficiently established that a material breach occurred, stakeholders may interpret the delay as a second violation distinct from the original security failure. Muzatko and Bansal's study is particularly important because delayed announcement not only produced greater initial trust loss but also constrained later trust repair after the organization provided protective services. This suggests that communication behavior becomes part of the incident itself rather than merely a response to it.

Transparency should nevertheless not be confused with instantaneous publication of unverified claims. Early incident information is frequently incomplete. ICO guidance explicitly recognizes that an organization may not possess every required detail within the initial reporting period and permits information to be supplied in phases under relevant UK GDPR provisions, while still expecting urgent investigation and notification where required. A credible organization should therefore communicate the boundary between established facts and ongoing investigation. Statements such as what has been

confirmed, what remains under examination, what categories of people may be affected, and when the next update will occur can provide useful transparency without presenting speculation as certainty.

Trust is unlikely to recover through communication alone. A technically weak organization can issue a carefully written apology while remaining vulnerable to recurrence. Stakeholders will ultimately evaluate whether remedial claims are supported by observable changes. NIST's incident-response framework deliberately connects incident lessons with wider cybersecurity risk management, emphasizing the need to use root-cause evidence to improve organizational resilience. This provides a useful distinction between reputation recovery and trust recovery: reputation management concerns how the organization is perceived, while trust recovery requires changes that justify improved perception.

6.2 Stakeholder Protection Converts Organizational Regret into Observable Responsibility

Apology can communicate empathy and acceptance of responsibility, but stakeholders affected by a breach may incur costs that words alone cannot address. They may need to change credentials, monitor financial accounts, manage phishing attempts, correct identity misuse, communicate with banks or public agencies, or spend significant time understanding whether they remain at risk. Recovery actions therefore need to respond to the type of information compromised and the plausible harm associated with it.

Masuch, Greve, and Trang demonstrate that apology and compensation can influence customer reactions following data breaches, while Goode and colleagues establish compensation as a substantive post-breach recovery mechanism rather than merely a communication device. These findings support a proportionality principle. Compensation or monitoring should not be offered mechanically to create favorable publicity; support should correspond to expected stakeholder harm.

The same principle applies to employees. Mohammed's stakeholder-oriented recovery model identifies customer, employee, process, and regulatory recovery as separate areas requiring attention after breaches. Employee information can be highly sensitive and may expose workers to fraud, impersonation, harassment, or additional cyberattacks. If an organization protects customers publicly but provides weaker internal support for employees, the resulting inconsistency can undermine internal trust and organizational legitimacy.

Stakeholder protection also provides information about organizational values. A company that focuses exclusively on legal minimums may satisfy regulatory requirements yet fail to demonstrate broader stewardship. Conversely, excessive promises that cannot be delivered may create further disappointment. Effective recovery therefore requires an evidence-based understanding of the affected population, plausible harms, available protective measures, and realistic organizational capacity.

6.3 Trust Recovery Becomes Sustainable Only When Governance Changes Remain Visible

The final implication concerns time. Most public and media attention is concentrated in the initial period after a breach, but the security weaknesses that contributed to the event may require months or years to correct fully. Sustainable trust recovery therefore depends on whether an organization continues investing after immediate reputational pressure declines.

Independent assurance can reduce this problem by creating external evidence that corrective commitments are being completed. Audits, targeted security testing, regulator-supervised improvements,

independent forensic review, and documented remediation milestones can provide more credible evidence than repeated statements that security is a priority. The FTC's breach-response guidance specifically recommends verifying that service providers have actually corrected identified vulnerabilities rather than relying solely on their assertions. The same verification principle should apply internally.

Governance changes should also address third parties. Many organizations rely on cloud services, outsourced customer support, payment processors, software vendors, and other processors that may possess access to sensitive information. Post-breach recovery should therefore evaluate whether third-party access remains necessary, whether contracts define breach-response responsibilities clearly, and whether monitoring adequately covers externally managed systems. ICO guidance requires relevant processor-controller breach-reporting responsibilities to be reflected in contractual relationships under applicable UK GDPR provisions.

Digital trust is therefore best interpreted as continuously earned rather than permanently restored. A breach can be contained, a regulatory investigation can close, and a compensation program can end, yet stakeholders may continue evaluating organizational behavior through later incidents, privacy changes, security practices, and transparency. The strongest recovery strategy institutionalizes the lessons of the breach so that future behavior provides continuing evidence of competence, honesty, and care.

7. Conclusion

Organizational data breaches create a distinctive form of trust violation because they expose a gap between the level of data stewardship stakeholders expected and the level the organization was able to provide. The consequences extend beyond the technical incident itself. Customers, employees, partners, and other affected parties evaluate whether the organization detected the breach responsibly, communicated honestly, reduced foreseeable harm, corrected underlying weaknesses, accepted appropriate responsibility, and demonstrated that the same institutional failures are less likely to recur. Digital trust recovery should therefore be approached as a multidimensional governance process rather than a short-term communication campaign.

The framework developed in this paper identifies transparent disclosure, technical remediation, stakeholder protection, organizational accountability, independent assurance, and sustained governance as mutually reinforcing components of recovery. The simulation illustrates the cumulative nature of these mechanisms. An illustrative trust index falls from 88 to 54 following the breach and then rises progressively through disclosure, remediation, support, assurance, and governance to a final value of 86. The figures are synthetic rather than empirical, but the pattern reflects an important theoretical principle: trust is unlikely to return because of one apology, one technical patch, or one compensation program. Recovery requires repeated evidence across several dimensions of organizational behavior.

The study also emphasizes that communication timing matters. Experimental evidence indicates that organizations delaying breach announcements may experience greater trust loss and weaker subsequent recovery than organizations communicating promptly. Yet transparency must remain accurate. Organizations should distinguish confirmed facts from unresolved questions and should continue updating stakeholders as investigations progress. Technical remediation should then provide

the competence evidence that communication alone cannot supply, while stakeholder support demonstrates that the organization recognizes responsibility for practical consequences experienced by affected individuals.

The broader conclusion is that digital trust after a data breach is recovered through verified organizational behavior rather than reassurance alone. Future empirical research should test the proposed Digital Trust Recovery Index using longitudinal stakeholder surveys, compare recovery across breach types and data sensitivities, examine differences between first-time and repeat breaches, and investigate the role of independent assurance in restoring confidence. Research should also explore whether organizations that adopt unusually transparent and accountable post-breach governance can eventually achieve trust levels above their pre-breach baseline. The long-term measure of successful recovery should not simply be whether public attention fades, but whether stakeholders have credible reasons to believe that the organization has become a more responsible steward of digital information.

References

1. Gillespie, N., & Dietz, G. (2009). Trust repair after an organization-level failure. *Academy of Management Review, 34*(1), 127–145. https://doi.org/10.5465/AMR.2009.35713319.
2. Gillespie, N., Dietz, G., & Lockey, S. (2014/2015). Organizational reintegration and trust repair after an integrity violation: A case study. *Business Ethics Quarterly, 24*(4), 1–35.
3. Dirks, K. T., Lewicki, R. J., & Zaheer, A. (2009). Repairing relationships within and between organizations: Building a conceptual foundation. *Academy of Management Review, 34*(1), 68–84.
4. Kim, P. H., Ferrin, D. L., Cooper, C. D., & Dirks, K. T. (2004). Removing the shadow of suspicion: The effects of apology versus denial for repairing competence- versus integrity-based trust violations. *Journal of Applied Psychology, 89*(1), 104–118.
5. Kim, P. H., Dirks, K. T., Cooper, C. D., & Ferrin, D. L. (2006). When more blame is better than less: The implications of internal versus external attributions for the repair of trust after a competence- versus integrity-based violation. *Organizational Behavior and Human Decision Processes, 99*(1), 49–65.
6. Ferrin, D. L., Kim, P. H., Cooper, C. D., & Dirks, K. T. (2007). Silence speaks volumes: The effectiveness of reticence in comparison to apology and denial for responding to integrity- and competence-based trust violations. *Journal of Applied Psychology, 92*(4), 893–908.
7. Gillespie, N., & Dietz, G. (2009). Trust repair after organization-level failure. *Academy of Management Review, 34*(1), 127–145.
8. Pfarrer, M. D., DeCelles, K. A., Smith, K. G., & Taylor, M. S. (2008). After the fall: Reintegrating the corrupt organization. *Academy of Management Review, 33*(2), 730–749.
9. Coombs, W. T., & Holladay, S. J. (2008). Comparing apology to equivalent crisis response strategies: Clarifying apology's role and value in crisis communication. *Public Relations Review, 34*(3), 252–257.
10. van Laer, T., & de Ruyter, K. (2010). In stories we trust: How narrative apologies provide cover for competitive vulnerability after integrity-violating blog posts. *International Journal of Research in Marketing, 27*(2), 164–174.

11. Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems, 71*, 62–73.
12. Choi, B. C. F., Kim, S. S., & Jiang, Z. (2016). Influence of firm's recovery endeavors upon privacy breach on online customer behavior. *Journal of Management Information Systems, 33*(3), 904–933. https://doi.org/10.1080/07421222.2015.1138375.
13. Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation Network breach. *MIS Quarterly, 41*(3), 703–727.
14. Fuoli, M., van de Weijer, J., & Paradis, C. (2017). Denial outperforms apology in repairing organizational trust despite strong evidence of guilt. *Public Relations Review, 43*(4), 645–660. https://doi.org/10.1016/j.pubrev.2017.07.007.
15. Lewicki, R. J., & Brinsfield, C. (2017). Trust repair. *Annual Review of Organizational Psychology and Organizational Behavior, 4*, 287–313. https://doi.org/10.1146/annurev-orgpsych-032516-113147.
16. Yuan, B., Dong, Y., & Li, W. (2017). The trust repair effect of apology: A systematic review and meta-analysis. *Advances in Psychological Science, 25*(7), 1103–1113.
17. Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation Network breach. *MIS Quarterly, 41*(3), 703–727.
18. Ponemon Institute. (2018). *2018 Cost of a Data Breach Study: Global Overview*. Ponemon Institute and IBM Security.
19. Kroll. (2018). *Data Breach Response: Seven Guidelines for Regaining Customer Trust After a Breach*. Kroll.
20. Rasoulian, S., et al. (2020). Trust recovery and organizational responses following service and privacy failures. *Service Industries Journal*.