

Rebuilding customer trust after cyberattacks: Examining the role of trust recovery in Indonesian Islamic digital banking

Dinda Dwi Nurritziana¹, Afifudin², Harun Alrasyid^{1*}

¹ Department of Islamic Banking, Faculty of Economics and Business, Universitas Islam Malang, Malang, Indonesia

² Department of Accounting, Faculty of Economics and Business, Universitas Islam Malang, Malang, Indonesia

*Corresponding Author(s) Email: harunalrasyid@unisma.ac.id

ABSTRACT

The increasing reliance on digital platforms in Islamic banking has heightened customers' vulnerability to cyberattacks, making post-crisis trust management a strategic priority. However, limited research has examined how trust can be effectively restored after such incidents. This study investigates the direct and indirect effects of system security, communication, and reputation on customer trust, with trust recovery as a mediating variable. A quantitative explanatory design was employed using Partial Least Squares Structural Equation Modeling (PLS-SEM) to analyze data from 252 users of an Islamic digital banking institution in Indonesia affected by a major cyberattack in 2023. The results reveal that system security, communication, and reputation do not directly influence customer trust but become significant when mediated by trust recovery. These findings indicate that customers place greater value on tangible recovery efforts than on pre-crisis institutional claims. This suggests that trust is not restored through declarative assurances alone but rather through demonstrable recovery actions that signal institutional competence and commitment. By integrating Islamic based ethical principles such as *amanah* (responsibility), *itqan* (professionalism), and transparency into recovery strategies, this study extends trust recovery theory in the context of Islamic digital services.

Keywords: Trust Recovery; Communication; Customer Trust; System Security; Cyberattack; Reputation; Islamic Banking

JEL Code:

G21, G41, M15, O33

DOI:

10.31106/jema.v22i1.24389

Article History:

Received 2025-02-14

Reviewed 2025-03-03

Revised 2025-04-21

Accepted 2025-04-30

Licensed:

CC-BY

How to Cite:

Nurritziana, D. D., Afifudin, A., & Alrasyid, H. (2025).

Rebuilding customer trust after cyberattacks: Examining the role of trust recovery in Indonesian Islamic digital banking. *JEMA: Jurnal Ilmiah Bidang Akuntansi dan Manajemen*, 22(1), 128-149. doi: 10.31106/jema.v21i2.24389

Introduction

Digital transformation has brought significant changes to the global banking sector, including Islamic banking, through the shift from conventional operational models toward technology-based services considered more efficient, faster, more accessible, and with broader reach (Khan & Khattak, 2024). Digitalization enables improved service quality, expands financial inclusion, and facilitates the integration of cross-platform services that align with the needs of modern customers (Hamadou et al., 2024). However, behind these advantages, reliance on digital infrastructure creates new vulnerabilities to increasingly complex cybersecurity threats. Such risks, as highlighted by Ahuchogu et al. (2024), not only have the potential to disrupt service continuity but may also erode public trust, which serves as the foundation for maintaining long-term relationships between banks and their customers.

The World Economic Forum (WEF, 2024) identifies cyberattacks as one of the top five systemic risks, with the potential to disrupt both economic stability and the integrity of global financial systems. In practice, several incidents illustrate the seriousness of these threats. For example, in 2018, a breach in Pakistan compromised nearly 20,000 debit card accounts, forcing banks to halt international transactions (Bajwa et al., 2023). In the United States, the 2019 Capital One incident data from more than 100 million customers, including highly sensitive details such as Social Security numbers (Neto et al., 2021). Going further back, the 2016 Central Bank of Bangladesh heist involved an attempted theft of USD 1 billion through the SWIFT network, ultimately resulting in losses of USD 81 million (Balu, 2022). Taken together, these cases highlight the particular vulnerability of the banking sector, which, as emphasized by Hasan et al. (2025), stems from the combination of high-value transactions, the vast amount of sensitive data it holds, and the potential for wide-ranging systemic repercussions.

Indonesia, as the largest digital financial services market in Southeast Asia, is not immune to similar risks (World Bank Group, 2024). The National Cyber and Encryption Agency (BSSN, 2024) reported over 330 million anomalous traffic events in 2023, ranking Indonesia among the countries with the highest levels of cyber threats worldwide. In May 2023, Bank Syariah Indonesia (BSI) was targeted by a ransomware attack launched by the LockBit group, marking one of the most severe incidents in the domestic banking industry (Sudana & Marlina, 2024). As the largest Islamic bank resulting from the merger of three state-owned banks, BSI experienced digital service paralysis for nearly a week. Although the investigation indicated that no data breach occurred, Amer and Al-Omar (2023) note that the

cyber disruption caused significant concern and damage to customers' long-term perceptions of the security and reliability of these digital service systems across the board.

Beyond the operational losses, this cyber crisis underscores that attacks of this nature can also disrupt psychological relationships between banks and their customers (Shehab et al., 2024). Digital service access is not only obstructed by technical issues, but it also undermines the confidence and certainty customers feel when making transactions. Some customers are so insecure that they cannot afford alternative, more trustworthy financial institutions (Nagamani et al. 2024). Trust in Islamic banking is a two-fold trait; it involves not only trust for its security and reliability, but also its ethical responsibility to uphold the principles of Shariah (Suhendar et al., 2023). As a result, the decline of trust in this industry has consequences that go beyond practicality, including the spiritual dimension where institutional credibility is indistinguishable from the Islamic values it represents.

Earlier studies indicate that customer trust in digital banking services is determined by three key factors: system security, effective communication, and institutional reputation. System security, as defined, refers to the ability to secure data by providing adaptive protection against cyber threats (Jafri et al., 2024). Beyond technical considerations, such as multi-factor authentication and encryption, the perception of security also encompasses a sense that customers can trust the bank's long-term commitment and system stability (Choudhuri et al., 2024).

Literature Review

The initial indicator of trust for new users is security, as per Musyaffi et al. (2024). This is reinforced by Wang et al. (2024), who emphasize that the perception of control over data protection can strengthen customer trust in a bank's digital services. Conversely, security failures can immediately reduce trust—particularly in the era of digital disruption, which is highly vulnerable to cyberattacks (Razikin & Soewito, 2022). Winata et al. (2024) further found that negative experiences resulting from security breaches nullify any previously established positive influence. This positions security as a strategic issue requiring serious attention and appropriate handling. Such conditions have prompted many banks to make substantial investments in protection systems, given their significant influence on customer trust levels (Asmar & Tuqan, 2024).

H₁: System security is positively associated with customer trust.

H₂: System security is positively associated with trust recovery.

Communication is not merely an information channel but also a relational mechanism that shapes customers' positive perceptions of an institution's credibility and commitment (Whyte, 2025). According to Sofiani et al. (2024), transparent and solution-driven communication is essential for sustaining trust during crises. In line with this, Cartwright et al. (2023) show that post-cyberattack recovery efforts benefit from proactive practices, including early alerts, continuous updates, and admitting mistakes, which collectively strengthen customer trust. Conversely, closed communication reinforces perceptions of institutional incapacity, fuels negative sentiment, and diminishes customer trust (Sudana & Marlina, 2024).

In Islamic banking, communication carries additional complexity as it must reflect the values of shiddiq (integrity) and tabligh (transparency) (Yusuf et al., 2023). Consistent, integrity-driven communication, accompanied by measurable corrective actions, can potentially restore trust that has been disrupted (Hammadi et al., 2024). Conversely, Alfarizi (2023) asserts that conveying narratives focused solely on public reassurance, without tackling the underlying causes, is often perceived as a defensive strategy to safeguard the institution's image, ultimately impeding the long-term restoration of customer trust. Thus, literature consistently affirms that communication has a significant impact on trust.

H₃: Communication is positively associated with customer trust.

H₄: Communication is positively associated with trust recovery.

Reputation is the collective public perception of an institution's integrity, competence, and consistency in ethical behavior (Arsalan et al., 2023). In the digital era, Mala et al. (2023) note that reputation is shaped not only by financial performance or brand image but also by the institution's consistency in operational conduct and customer protection. Responsiveness in maintaining system reliability and providing protection strengthens reputational perceptions both rationally and emotionally (Hasan et al., 2023), ultimately serving as symbolic capital to sustain trust during disruptions. Reputation also serves as a social guarantee of public expectations toward institutional responsibility (Todua & Gogitidze, 2024).

Studies by Al et al. (2024) demonstrate that a reputation founded on a track record of integrity positively influences trust and fosters loyalty through repeated positive interactions. Gli et al. (2024) confirm that institutions with positive reputations tend to be more trusted and enjoy higher loyalty. A reputation grounded in Shariah values holds greater symbolic strength, as it represents justice, sustainability, and dedication to the public interest (Wati et

al., 2024). This finding is consistent with Hubik (2024), who found that Islamic financial institutions receive a positive reception, even in non-Muslim majority countries, due to their perceived high moral values. These conditions warrant testing whether reputation remains a strategic factor after cyber incidents.

H₅: Reputation is positively associated with customer trust.

H₆: Reputation is positively associated with trust recovery.

While system security, communication, and reputation have been extensively studied, most research focuses on conventional banks or Islamic banking under normal conditions. Studies specifically addressing these three factors in Islamic banking during the post-cyberattack period remain scarce. Similarly, research on post-crisis recovery strategies in this sector remains limited, despite the fact that such measures are crucial for maintaining or restoring customer trust in digital services (Hoang & Le, 2024). Addressing this research gap is crucial due to the distinctive nature of Islamic banking, which combines economic mechanisms with Shariah-based ethical values, thereby necessitating recovery strategies consistent with these principles (Harsono & Atina, 2023).

According to Munawar and Hadiano (2024), recovery is both a strategic and psychological process aimed at repairing the relationship between banks and customers after a service failure. In the context of digital services prone to disruption, its urgency increases due to the lack of direct interaction (Bajwa et al., 2023). Customer evaluation is not solely based on technical success but also on the bank's responsiveness and moral integrity. Zulganef et al. (2023) demonstrate that sincere apologies, empathetic communication, and fair compensation can help restore trust, whereas closed responses can exacerbate crises. Beyond mere restoration, swift, fair, transparent, and empathetic handling can even enhance loyalty beyond that of uninterrupted service—a phenomenon known as the service recovery paradox (Lim et al., 2025). However, its success depends on fulfilling both emotional and functional expectations.

In Islamic banking, the success of recovery is highly dependent on the consistency of ethical principles that define the institution's identity. Chapra (2008) emphasizes that institutional failures addressed through Shariah-based solutions tend to be more sustainable than purely materialistic approaches. This level of consistency facilitates recovery to occur on both rational and spiritual levels (Suhendar et al., 2023), thereby reinforcing customer trust and commitment. Therefore, this study positions trust recovery as a mediating variable linking system security, communication, and reputation to customer trust after cyberattacks,

through an approach that integrates procedural and interactional justice, emotional sensitivity, and the moral-spiritual values of Islam (Haryanto et al., 2024).

H₇: Trust recovery is positively associated with customer trust.

H₈: Trust recovery is hypothesized to mediate the relationship between system security and customer trust.

H₉: Trust recovery is hypothesized to mediate the relationship between communication and customer trust.

H₁₀: Trust recovery is hypothesized to mediate the relationship between reputation and customer trust.

Methods

This study adopted a quantitative approach with an explanatory research design to examine the causal relationships among latent constructs influencing customer trust in Bank Syariah Indonesia's (BSI) digital services following a cyberattack. The mention of Bank Syariah Indonesia (BSI) in this study is for academic and research purposes only. The research does not intend to evaluate or criticize the institution's performance but to analyze customer perceptions in a post-cyberattack context. Following the guidelines of Hair et al. (2019), this design was appropriate for testing theoretically grounded hypotheses and identifying both direct and indirect effects between variables. Specifically, the research investigated how system security, communication, and reputation affect customer trust, either directly or through the mediating role of trust recovery. The quantitative method was chosen for its capacity to provide objective measurement using standardized instruments and its suitability for applying advanced statistical analyses to uncover complex inter-variable relationships.

The population comprised users of BSI's digital services, particularly those who actively utilized mobile banking features. A purposive sampling technique was employed to ensure the inclusion of respondents who had experienced the 2023 cyberattack, thereby aligning the sample with the study's objectives (Etikan, 2016). In accordance with the sample size recommendation by Hair et al. (2019), which suggests a minimum of ten respondents per indicator for the construct with the highest number of measurement items, this study required at least 220 participants, as it involved 22 observed indicators.

Data were collected through an online survey distributed via Google Forms between December 2024 and January 2025, reaching respondents across multiple Indonesian provinces. The use of an online platform was justified by its cost-efficiency, accessibility, and

Table 1. Measurement of Constructs

Constructs	Sources
System Security (SYS)	
Customers' perceptions of the security and effectiveness of the bank's cybersecurity systems.	(Amer & Al-Omar, 2023; Hammadi et al., 2024; Saif et al., 2022)
Communication (COM)	
The bank's ability to communicate effectively during times of crisis is reflected in the clarity and accuracy of the information provided to customers.	(Choudhuri et al., 2024; Gli et al., 2024; Sudana & Marlina, 2024)
Reputation (REP)	
Customers' perception of the institution's public image and overall credibility.	(Hubik, 2024; Rumanto, 2024; Yudiana, 2021)
Trust Recovery (YRC)	
Customers' belief that the bank took sufficient ethical and corrective steps to rebuild trust after crisis.	(Bajwa et al., 2023; Razikin & Soewito, 2022; Sivasubramanian & Rekhapriyadharshini, 2022)
Customer Trust (CST)	
The degree of customer confidence in the bank's capability and integrity	(Lim et al., 2025; Munawar & Hadiano, 2024; Winata et al., 2024)

-ability to generate timely responses (Razikin & Soewito, 2022). The questionnaire was structured around five key constructs derived from established studies. Each construct was measured using validated items on a five-point Likert scale, ranging from strongly disagree (1) to strongly agree (5). Table 1 presents the operationalization of variables.

Data analysis was conducted using Partial Least Squares Structural Equation Modeling (PLS-SEM) with SmartPLS version 4.0, following the two-step procedure recommended by Hair et al. (2019). The first stage involved evaluating the measurement model to establish the validity and reliability of the indicators, while the second stage examined the structural model to test the hypothesized relationships among latent variables.

Convergent validity was assessed through indicator loadings and the Average Variance Extracted (AVE). All outer loadings exceeded the minimum recommended value of 0.70, and all AVE values were above 0.50 (Hair et al., 2019), with loadings ranging from 0.724 to 0.882 and AVE values between 0.679 and 0.735 (Table 2 and 3). These results confirmed that the measurement items adequately represented their corresponding constructs. Reliability was further established using Cronbach's Alpha (CA) and Composite Reliability (CR), both of

which surpassed the 0.70 threshold (Hair et al., 2019). The CA values ranged from 0.841 to 0.910, while CR values ranged between 0.894 and 0.933 (Table 2 and 3), indicating strong internal consistency across all constructs.

Table 2. Convergent Validity and Reliability of Reputation, Trust Recovery, and Customer Trust

Constructs	Code	Corresponding Items	LF	CA	CR	AVE
Reputation (REP)	REP1	I perceive BSI as consistently applying Sharia principles in its digital services.	0.832	0.864	0.907	0.710
	REP2	BSI's reputation as a Sharia bank gives me confidence in using its services.	0.816			
	REP3	BSI's positive reputation during service disruptions reassures me.	0.881			
	REP4	I evaluate BSI's digital services based on media coverage and public perception.	0.841			
Trust Recovery (TRC)	TRC1	I feel that BSI's digital services have been properly restored and improved after the incident.	0.836	0.868	0.910	0.717
	TRC2	BSI takes corrective steps to strengthen its systems as a form of accountability.	0.850			
	TRC3	BSI apologized and offered fair solutions to affected customers, showing genuine empathy.	0.824			
	TRC4	I believe BSI communicates openly and responds sincerely to customer complaints.	0.877			
Customer Trust (CST)	CST1	I intend to continue using BSI's digital services despite the cyber incident.	0.872	0.841	0.894	0.679
	CST2	I trust BSI with my personal data, believing in its responsibility and accountability.	0.834			
	CST3	I am confident that BSI acts with integrity and genuinely cares for its customers.	0.857			
	CST4	I would recommend BSI's digital services to my family and friends.	0.724			

Table 3. Convergent Reliability and Validity of System Security, Communication

Constructs	Code	Corresponding Items	LF	CA	CR	AVE
System Security (SYS)	SYS1	BSI protects customer data from unauthorized access.	0.837	0.886	0.916	0.687
	SYS2	I believe BSI uses advanced security technology against cyber threats.	0.837			
	SYS3	I am confident that BSI implements multi-layered verification for transaction security.	0.874			
	SYS4	BSI has an automated monitoring system for suspicious activities.	0.777			
	SYS5	I believe BSI's security system complies with cybersecurity standards.	0.817			
Communication (COM)	COM1	I receive official information promptly during digital service disruptions.	0.829	0.910	0.933	0.735
	COM2	BSI educates customers about digital security.	0.882			
	COM3	BSI explains service disruption causes transparently.	0.858			
	COM4	I am confident that the complaint channels provided are accessible and responsive.	0.849			
	COM5	I receive regular updates on the progress of service recovery.	0.868			

Table 4. Discriminant Validity of Constructs (Fornell-Lacker Criterion)

	COM	CST	REP	SYS	TRC
Communication	0.858				
Customer Trust	0.612	0.824			
Reputation	0.658	0.700	0.843		
System Security	0.667	0.690	0.775	0.829	
Trust Recovery	0.648	0.768	0.735	0.726	0.847

The assessment of the constructs' discriminant validity included the Fornell–Larcker criterion (Fornell & Larcker, 1981). For each construct, the square root of its AVE exceeded its correlations with other constructs, confirming satisfactory discriminant validity. As shown in

Table 5, the square roots of AVE (represented on the diagonal) were higher than the inter-construct correlations, thereby confirming the distinctiveness of each latent variable. For instance, the Communication construct reported a square root of AVE value of 0.858, which exceeded its correlations with all other constructs (ranging from 0.612 to 0.667). Customer Trust construct also showed a higher value of 0.824 than the correlations with other latent variables (0.612–0.768). These results indicate that each construct shares more variance with its own indicators than with those of other constructs, demonstrating conceptual distinctiveness among constructs (Sarstedt et al., 2017).

Following the confirmation of measurement model adequacy, the structural model was analyzed to test the causal hypotheses. Multicollinearity was examined through the Variance Inflation Factor (VIF), and all values, ranging from 1.979 to 3.089 (Table 5), were well below the conservative upper limit of 5, indicating the absence of multicollinearity concerns (Hair et al., 2019). Collectively, these results confirm that the model meets the required validity and reliability criteria, providing a solid foundation for hypothesis testing in subsequent analysis.

Result and Discussion

The demographic profile of the 252 respondents presented in Table 5 provides a comprehensive overview of Bank Syariah Indonesia's (BSI) digital service users. The data reveal that a majority of users are female (61.1%), suggesting strong participation of women in digital banking activities. Most respondents fall within the 21–30 years age group (77.4%), indicating that BSI's digital services are primarily adopted by younger, tech-oriented customers. In terms of education, more than half hold a Bachelor's degree (56.7%), reflecting a well-educated user base capable of adapting to technological innovations in financial services. The income distribution shows that nearly half of respondents earn less than IDR 2 million per month (49.5%), suggesting that BSI's digital platform effectively reaches lower-to middle-income customers, consistent with its inclusive banking mission. Furthermore, a significant proportion of respondents have been active users for two to three years (67.1%), while 32.9% have used the service for over three years, indicating sustained customer engagement. In terms of usage frequency, more than half access digital services one to two times per week (51.3%), and about one-third use them three to four times weekly (32.5%), reflecting consistent reliance on BSI's digital platform for routine financial transactions.

The structural model was assessed using a bootstrapping procedure with 5,000 resamples to evaluate the statistical significance of the hypothesized relationships. Path coefficients, t-statistics, and p-values were analyzed to determine the strength and direction of the

relationships among the latent constructs. Consistent with the criteria recommended by Hair et al. (2019), a path is considered statistically significant when the t-value exceeds 1.96 and the corresponding p-value is below 0.05. As shown in Table 6, the direct path analysis revealed that system security, communication, and reputation did not have a significant direct effect on customer trust, leading to the rejection of H₁, H₃, and H₅. This finding underscores the sensitivity of trust dynamics in digital banking following crisis events. In the aftermath of the 2023 cyberattack on Bank Syariah Indonesia (BSI), a nearly week-long service disruption appeared to diminish prior perceptions of reliability, overshadowing the positive influence of security features, reputation, and communication efforts. These results are consistent with Bajwa et al. (2023), who noted that digital trust is particularly fragile in banking contexts, where technological failures are perceived not merely as operational shortcomings but also as

Table 5. Demographic Profile

Profiles		Frequency	Percentage (%)
Gender	Male	98	38.9
	Female	154	61.1
Age	< 20 years	5	2
	21-30 years	195	77.4
	31-40 years	19	7.5
	41-50 years	26	10.3
	> 50 years	7	2.8
Education background	High school or below	90	35.7
	Bachelor's	143	56.7
	Master's	15	6
	PhD	4	1.6
Monthly income	< 2 million	125	49.5
	2-3 million	45	17.9
	3-5 million	31	12.3
	5-7 million	24	9.5
	7-10 million	12	4.8
	>10 million	15	6
Active users since.	2-3 years	169	67.1
	> 3 years	83	32.9
Weekly usage	1-2 times a week	129	51.3
	3-4 times a week	82	32.5
	5-6 times a week	24	9.5
	Every day	17	6.9

Table 6. Hypothesis Testing

Hypothesis					Original Sample	Sample Mean	Std. Deviation	t-Value	p-Value	VIF	Decision
H ₁	SYS	->	CST		0.150	0.172	0.101	1.484	0.138	3.064	Rejected
H ₂	SYS	->	TRC		0.312	0.312	0.074	4.235	0.000	2.805	Accepted
H ₃	COM	->	CST		0.091	0.104	0.077	1.177	0.239	2.089	Rejected
H ₄	COM	->	TRC		0.203	0.205	0.069	2.947	0.003	1.979	Accepted
H ₅	REP	->	CST		0.180	0.202	0.117	1.535	0.125	3.089	Rejected
H ₆	REP	->	TRC		0.359	0.361	0.084	4.276	0.000	2.747	Accepted
H ₇	TRC	->	CST		0.468	0.420	0.168	2.794	0.005	2.648	Accepted
H ₈	SYS	->	TRC	-> CST	0.146	0.127	0.053	2.755	0.006	3.064	Accepted
H ₉	COM	->	TRC	-> CST	0.095	0.085	0.046	2.091	0.037	2.805	Accepted
H ₁₀	REP	->	TRC	-> CST	0.168	0.146	0.060	2.807	0.005	2.089	Accepted

violations of *amanah* (trustworthiness) and *itqan* (professional diligence). Such perceptions amplify user disappointment and intensify the erosion of confidence among customers who expect both ethical integrity and technological reliability from Islamic financial institutions.

Unlike the present findings, Musyaffi et al. (2024) identified security as the main factor shaping customers' initial trust in using a bank's digital platforms. However, during a service crisis, customers tend to shift their focus from declarative confidence to tangible operational evidence. The current results further reveal that post-attack communication was not sufficiently effective in rebuilding trust. Even minor errors can have a considerable impact once a cyberattack has heightened public anxiety. In such situations, honesty, transparency, and prompt action are essential (Whyte, 2025).

Furthermore, reputation also failed to sustain customer trust—contrary to Hasan et al. (2023), who view reputation as symbolic capital in times of crisis. In a post-cyberattack context, reputation must therefore be reaffirmed through consistent institutional conduct. To address this, banks should strengthen their operational readiness to respond quickly to cyber incidents, ensuring that security systems are routinely audited and updated. Additionally, providing alternative communication channels during service disruptions can help minimize customer uncertainty and maintain two-way interaction between the bank and digital service users (Wijanarko et al., 2024).

Subsequent analysis shows that system security, communication, and reputation significantly contribute to trust recovery, thereby supporting H₂, H₄, and H₅. For customers, visible technical improvements, such as strengthening firewalls, closing security vulnerabilities, and conducting comprehensive audits, serve as signals that the bank has

learned from the crisis and is committed to preventing future incidents (Ridwan et al., 2025). Meanwhile, communication efforts have become more structured compared to the initial response phase. Providing timely service updates and alternative transaction options has helped foster more positive customer perceptions.

From an Islamic perspective, these actions go beyond technical measures; they embody the principles of *amanah* (responsibility) and *mas'uliyah* (accountability), which reinforce the bank's moral relationship with its customers (Harsono & Atina, 2023). As a result, the damaged reputation has begun to recover as the public perceives alignment between the bank's declared values and its actual practices. To sustain this renewed trust, banks should continue providing digital security education to customers, thereby strengthening confidence and reducing user-related risks.

These findings are consistent with Wang et al. (2024), who emphasize that post-crisis enhancements to security systems are more effective than pre-crisis assurances of safety or technological advancement. Institutions that respond swiftly to a crisis with a proactive communication strategy can restore trust more effectively than those adopting a passive or defensive approach (Wijanarko et al., 2024). From a Sharia perspective, such practices reflect *shiddiq* (integrity) and *tabligh* (transparency), which, when consistently upheld, accelerate trust recovery. Therefore, successful post-crisis recovery requires an integrated approach that combines technical remediation, ethical communication, and reputational reconstruction (Alwabel, 2024). This study thus urges banks to adopt strategic crisis protocols that unite technical solutions, proactive communication, and regulatory coordination, ensuring that recovery efforts proceed swiftly, purposefully, and in full compliance with applicable standards.

The findings demonstrate that trust recovery exerts a significant influence on customer trust, thereby confirming H₇. In the aftermath of a cyberattack, trust is no longer shaped by the symbolic representation of values or historical reputation, but rather by tangible, transparent, and fair recovery experiences. For customers, the success of recovery that they directly experience becomes the primary benchmark for reassessing the bank's credibility. This process demonstrates that operational proof carries greater weight than inherited image during a service crisis (Sudana & Marlina, 2024). Moreover, within the framework of Islamic banking, recovery processes are not merely technical but are imbued with spiritual values, reflecting the principles of *itqan* (professionalism) and *ihsan* (excellence) embedded in every recovery step, serving as tangible validation of the institution's commitment to upholding these ethical values. Theoretically, these findings align with the Service Recovery Theory

proposed by Tax et al. (1998), which emphasizes that fair, transparent, and effective recovery, encompassing both technical and relational aspects, is essential to rebuilding trust after service failures. As further highlighted by Munawar & Hadiano (2024), recovery effectiveness depends on a combination of technical improvements, sincere communication, acknowledgment of mistakes, and a firm commitment to preventing recurrence.

In contrast to the direct paths, the analysis of indirect effects reveals that system security, communication, and reputation have a significant influence on customer trust when mediated by trust recovery, thereby supporting H₈, H₉, and H₁₀. This finding diverges from the previous literature, which has positioned institutional attributes such as system security, communication, and reputation as the primary determinants of trust (Choudhuri et al., 2024). Positive perceptions of these attributes only transform into trust when they are materialized in tangible and directly experienced recovery efforts. This condition marks a shift in customer focus from declarative claims to operational proof.

Theoretically, these findings refine the Commitment-Trust Theory (Morgan & Hunt, 1994) by emphasizing that trust is essential for sustaining customer commitment to digital banking services, even in the midst of a cyber crisis. In this context, institutional attributes thus attain their highest strategic value when converted through effective recovery. In other words, strengthening system security, structuring communication, and aligning reputation within recovery actions are the mechanisms that restore customer trust and reinforce institutional legitimacy. From a Sharia perspective, this process reflects the continuous application of Sharia-based ethical values, wherein every claim of integrity and security must be substantiated by concrete actions as the primary mechanism for maintaining credibility (Afrida & Lubis, 2021). Banks that consistently validate their claims through concrete operational practices, supported by regular emergency response drills and continuous employee training, will be better prepared to withstand cyber threats. In this way, customer trust and commitment to digital services can be preserved in an era of escalating digital risks.

Conclusion and Suggestion

This study demonstrates that in the context of a cyber crisis, customer trust in Islamic banks is influenced less by institutional attributes such as security, communication, or reputation, and more by customers' perceived experiences of recovery. While these factors do not directly enhance trust, they become significant through the mediating role of trust recovery, which transforms institutional claims into tangible actions that restore confidence. This finding challenges the conventional assumption that institutional attributes are the

principal determinants of trust, suggesting instead that their impact is conditional upon the bank's ability to translate perceptions into credible recovery measures.

The findings extend the understanding of trust recovery by emphasizing the role of Islamic ethical values, *amanah* (responsibility), *itqan* (professionalism), and transparency, as the foundation of customer trust. In Islamic banking, trust is both a moral and operational commitment; therefore, recovery efforts that reflect these values are crucial for maintaining legitimacy and customer confidence. Practically, Islamic banks should develop crisis management protocols that combine adaptive security systems, transparent communication, and close coordination with regulators. Regular employee training, recovery simulations, and alternative communication channels are essential to ensure continuity and minimize reputational damage during service disruptions.

Nevertheless, this study is limited by its focus on a single institution, its cross-sectional design, and the absence of measurable constructs representing Sharia-based values. Future research should expand the sampling frame to include multiple Islamic financial institutions, employ longitudinal or mixed-method approaches, and develop validated measurement instruments that explicitly capture Sharia principles within the trust recovery framework. Such an approach would not only improve external validity but also enhance the theoretical robustness of digital trust models in Islamic banking.

Disclosure the Use of AI Technologies

During the preparation of this work, the author(s) used Grammarly-AI and WriteHuman-AI to translate, paraphrase, and correct the grammar. After using these tools/services, the author(s) reviewed and edited the content as needed and take full responsibility for the final content of the publication.

References

- Afrida, Y., & Lubis, M. Z. M. (2021). Islamic bank brand reputation in Indonesia. *Maqdis: Jurnal Kajian Ekonomi Islam*, 6(1), 110–123. <https://doi.org/10.15548/maqdis.v6i1.527>.
- Ahuchogu, M. C., Sanyaolu, T. O., & Adeleke, A. G. (2024). Balancing innovation with risk management in digital banking transformation for enhanced customer satisfaction and security. *International Journal of Management & Entrepreneurship Research*, 6(9), 3022–3049. <https://doi.org/10.51594/ijmer.v6i9.1566>

- Al, S. M., Senior, I., Corresponding, B., & Al Imran, S. M. (2024). Customer expectations in Islamic banking: A Bangladesh perspective. *Research Journal in Business and Economics*, 2(1), 12-24. <https://doi.org/10.61424/rjbe.v2i1.159>
- Alfarizi, M. (2023). Assessing the relationship between customer satisfaction and digital service retention: Evidence from Indonesian Islamic banking. *International Journal of Islamic Economics and Finance*, 6(1), 151–180. <https://doi.org/https://doi.org/10.18196/ijief.v6i1.16824>
- Alwabel, R. A. (2024). The role of cyber security in customer trust: Data science perspectives. *World Journal of Advanced Research and Reviews*. Retrieved from <https://www.researchgate.net/publication/384188419>
- Amer, T. B., & Al-Omar, M. I. A. (2023). The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector. *International Journal of Advanced Computer Science and Applications*, 14(8), 371–380. <https://doi.org/10.14569/IJACSA.2023.0140841>
- Arsalan, M., Ali, U. A., Hussain, S., Quratul-ain-Kazmi, S., & Mubashir, A. (2023). Exploring customer experience in bancassurance: The role of awareness, trust with bank reputation as a moderator in Pakistan's banking industry. *Research Journal for Societal Issues*, 5, 258–273. <https://doi.org/10.56976/rjsi.v5i3.14>
- Asmar, M., & Tuqan, A. (2024). Integrating machine learning for sustaining cybersecurity in digital banks. *Heliyon*, 10(17), e37571–e37571. <https://doi.org/10.1016/j.heliyon.2024.e37571>
- Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: An empirical evidence from the Pakistani banking sector. *Information and Computer Security*, 31(5), 635–654. <https://doi.org/10.1108/ICS-11-2022-0179>
- Balu, R. (2022). *Bangladesh bank cyber heist: Incident analysis*. Retrieved from <https://repository.gatech.edu/server/api/core/bitstreams/df3d1c19-47be-4738-a855-9c049b709d52/content>
- BSSN. (2024). Lanskap Keamanan Siber Indonesia 2024. In Badan Siber dan Sandi Negara. <https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf>

- Cartwright, A., Cartwright, E., & Edun, E. S. (2023). Cascading information on best practice: cyber security risk management in UK micro and small businesses and the role of IT companies. *Computers and Security*, 131. <https://doi.org/10.1016/j.cose.2023.103288>
- Chapra, M. U. (2008). Ethics and economics: An Islamic perspective. *Islamic Economic Studies*, 16(2), 1-24. Retrieved from <https://ideas.repec.org/a/ris/isect/0047.html>
- Choudhuri, S., Rastogi, E., Singh, A., Ravi, R., H N, B. M., & Professor, A. (2024). An analysis of factors influencing consumer trust in online banking security measures. *Educational Administration: Theory and Practice*, 30(2), 660–666. <https://doi.org/10.53555/kuey.v30i2.1742>
- Etikan, I. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1-4. <https://doi.org/10.11648/j.ajtas.20160501.11>
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50. <https://doi.org/https://doi.org/10.2307/3151312>
- Gli, D. D., Tweneboah-Koduah, E. Y., Odoom, R., & Kodua, P. (2024). The effect of corporate reputation on customer loyalty in the Ghanaian banking industry: The role of country-of-origin. *African Journal of Economic and Management Studies*, 15(1), 73–87. <https://doi.org/10.1108/AJEMS-12-2022-0492>
- Hair, J. F., Ringle, C. M., Gudergan, S. P., Fischer, A., Nitzl, C., & Menictas, C. (2019). Partial least squares structural equation modeling-based discrete choice modeling: An illustration in modeling retailer choice. *Business Research*, 12(1), 115–142. <https://doi.org/10.1007/s40685-018-0072-4>
- Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, 31(1), 2–24. <https://doi.org/10.1108/EBR-11-2018-0203>
- Hamadou, I., Yumna, A., Hamadou, H., & Jallow, M. S. (2024). Unleashing the power of artificial intelligence in Islamic banking: A case study of Bank Syariah Indonesia (BSI). *Modern Finance*, 2(1), 131–144. <https://doi.org/10.61351/mf.v2i1.116>
- Hammadi, M. Al, Río, J. A. J.-D., Ochoa-Rico, M. S., Montero, O. A., & Vergara-Romero, A. (2024). Risk management in Islamic banking: The impact of financial technologies

- Rebuilding customer trust after cyberattacks: Examining the role of trust recovery in Indonesian Islamic digital banking by Dinda Dwi Nurriksiana, Afifudin, Harun Alrasyid through empirical insights from the UAE. *Risks*, 12(2), 1–15. <https://doi.org/10.3390/risks12020017>
- Harsono, M., & Atina, V. Z. (2023). Islamic banking literature review. Is Islamic banking in accordance with sharia principles? *Amwaluna: Jurnal Ekonomi dan Keuangan Syariah*, 7(1), 116–132. <https://doi.org/10.29313/amwaluna.v7i1.11023>
- Haryanto, S., Safriliana, R., Ridloah, S., Ariefudin, M. U., & Khotimah, L. K. (2024). Determinants of risk in Indonesian Islamic banking: An empirical investigation. *SHARE: Jurnal Ekonomi dan Keuangan Islam*, 13(1), 24–42. <https://doi.org/10.22373/share.v13i1.20758>
- Hasan, M. M., Jalal Siam, S. A., & Haque, A. (2023). The significance of customer service in establishing trust and enhancing the reputation of the banking industry in Bangladesh. *Business and Economics in Developing Countries*, 1(2), 71–75. <https://doi.org/10.26480/bedc.02.2023.71.75>
- Hasan, M., Naseem, M. R., Salman, S. M., Iqbal, A., & Aziz, A. (2025). Evaluating the impact of financial literacy and cyber security perceptions on customer satisfaction with online banking services in Pakistan. *Journal for Social Science Archives*, 3(1), 703–723. <https://doi.org/10.59075/jssa.v3i1.153>
- Hoang, T. K. L., & Le, V. (2024). Customer experience for digital banking service quality in Vietnam. *International Journal of Science and Research Archive*, 12(2), 1371–1381. <https://doi.org/10.30574/ijrsra.2024.12.2.1391>
- Hubik, V. (2024). Introducing Islamic banking in the Czech Republic: A customer perspective study. *Journal of Business Sectors*, 2(2), 73–81. <https://doi.org/10.62222/ALAK1693>
- Ivanova, A., & Yeon KIM, J. (2022). Acceptance and use of mobile banking in central Asia: Evidence from modified UTAUT model. *Journal of Asian Finance*, 9(2), 217–0227. <https://doi.org/10.13106/jafeb.2022.vol9.no2.0217>
- Jafri, J. A., Mohd Amin, S. I., Abdul Rahman, A., & Mohd Nor, S. (2024). A systematic literature review of the role of trust and security on fintech adoption in banking. *Heliyon*, 10(1), e22980–e22980. <https://doi.org/10.1016/j.heliyon.2023.e22980>
- Khan, N. A., & Ahmed Khattak, M. (2024). Digital transformation and the banking market: Friend or foe? A country-level study. *Journal of Central Banking Law and Institutions*, 3(1), 129–152. <https://doi.org/10.21098/jcli.v3i1.167>

- Lim, W. M., Saha, V., & Das, M. (2025). From service failure to brand loyalty: Evidence of service recovery paradox. *Journal of Brand Management*, 32, 257–281. <https://doi.org/10.1057/s41262-025-00380-5>
- Mala, C. M. F., Hosen, M. N., & Al Arif, M. N. R. (2023). An analysis of market power and efficiency of Islamic banking in Indonesia and Malaysia. *Jurnal Ekonomi & Keuangan Islam*, 9(1), 1–16. <https://doi.org/10.20885/jeki.vol9.iss1.art1>
- Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing*, 58(3), 20-38. <https://doi.org/10.2307/1252308>
- Munawar, M. M., & Hadianto, B. (2024). Banking service recovery and consumer loyalty: The mediating role of satisfaction. *International Journal of Applied Economics, Finance and Accounting*, 20(1), 35–45. <https://doi.org/10.33094/ijaefa.v20i1.1921>
- Musyaffi, A. M., Johari, R. J., Sobirov, B., Oli, M. C., Rahmi, & Afriadi, B. (2024). Examining initial trust in adoption of digital banking platform: A personal innovativeness and security perspective. *Journal of System and Management Sciences*, 14(1), 67–86. <https://doi.org/10.33168/JSMS.2024.0105>
- Nagamani, G., Mathur, B., Bala, R., Datere, G., & Kathuria, A. (2024). Impact of trust and service quality on retail banking customers' satisfaction and loyalty. *Journal of Informatics Education and Research*, 4(3), 2651-2656. <https://doi.org/10.52783/jier.v4i3.1623>
- Neto, N. N., Madnick, S., de Paula, A. M. G., & Borges, N. M. (2021). A case study of the capital one data breach: Why didn't compliance requirements help prevent it? *Journal of Information Systems Security*, 17(1), 49–78. <https://doi.org/10.2139/ssrn.3570138>
- Razikin, K., & Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal*, 23(3), 383–404. <https://doi.org/10.1016/j.eij.2022.03.001>
- Ridwan, M., Puspitasari, R., Winarsih, T., Wangsih, I. C., Sudarmanto, E., & Dahlan, A. (2025). The effect of digital banking adoption, trust in fintech, perceived security, and customer satisfaction on financial inclusion in Indonesian banking. *West Science Business and Management*, 3(1), 158–168. <https://doi.org/DOI:10.58812/wsbm.v3i01.1794>

- Rumanto, A. (2024). Islamic digital bank adoption in developing countries: A case study on millennials in Indonesia. *NISBAH: Jurnal Perbankan Syariah*, 10(1), 20-32. <https://doi.org/10.30997/jn.v10i1.13491>
- Saif, M. A. M., Hussin, N., Husin, M. M., Alwadain, A., & Chakraborty, A. (2022). Determinants of the intention to adopt digital-only banks in Malaysia: The extension of environmental concern. *Sustainability*, 14(17). <https://doi.org/10.3390/su141711043>
- Sarstedt, M., Ringle, C. M., & Hair, J. F. (2017). Partial least squares structural equation modeling. *Springer International Publishing*, 1-40. https://doi.org/10.1007/978-3-319-05542-8_15-1
- Shehab, R., s.alismail, A., Amin Almaiah, Dr. M., Alkhdour, Dr. T., AlWadi, Dr. B. M., & Alrawad, Dr. M. (2024). Assessment of cybersecurity risks and threats on banking and financial services. *Journal of Internet Services and Information Security*, 14(3), 167–190. <https://doi.org/10.58346/jisis.2024.i3.010>
- Sivasubramanian, G., & Rekhapriyadharshini. (2022). The mediating effect of customer satisfaction on the relationship between service quality and customer loyalty in digital banking. *Journal of Contemporary Issues in Business and Government*, 28(1), 20-31. <https://doi.org/10.47750/cibg.2022.28.01.003>
- Sofiani, M., Ramadhanty, D. P., & Jubaedah, S. (2024). Cyber risk management disclosure: The impact of firm size, profitability, and intangible asset. *IJEBD (International Journal of Entrepreneurship and Business Development)*, 7(5), 929–937. <https://doi.org/10.29138/ijebd.v7i5.2844>
- Sudana, S., & Marlina, L. (2024). Customer decision to save in sharia banks following a ransomware attack: An analysis of the role of word of mouth, trust, perception of cybersecurity, and perception of sharia label. *BISNIS & BIROKRASI: Jurnal Ilmu Administrasi dan Organisasi*, 31(1). <https://doi.org/10.20476/jbb.v31i1.1497>
- Suhendar, S., Muetia, M., Taqi, M., & Hanifah, I. (2023). Analysis of the impact of Islamic corporate governance and bank reputation on Islamic bank performance in Indonesia. *ICOSTELM 2022*, 2009. <https://doi.org/10.4108/eai.4-11-2022.2328784>
- Tax, S. S., Brown, S. W., & Chandrashekar, M. (1998). Customer evaluations of service complaint experiences: Implications for relationship marketing. *Journal of Marketing*, 62(2), 60–76. <https://doi.org/10.2307/1252161>

- Todua, N., & Gogitidze, N. (2024). Consumer attitude towards digital banking services (Case of Georgia). *International Journal of Professional Business Review*, 9(11), 1-23. <https://doi.org/10.26668/businessreview/2024.v9i11.5096>
- Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers and Security*, 147. <https://doi.org/10.1016/j.cose.2024.104051>
- Wati, A., Rahmawati, R., Malahayatie, M., Lestari, A. F., & Rehan, M. (2024). Financial options trends: Digging the reasons behind the growth of customer interest in sharia bank Indonesia. *FINANSIA : Jurnal Akuntansi Dan Perbankan Syariah*, 7(1), 87–102. <https://doi.org/10.32332/finansia.v7i1.8530>
- WEF. (2024). *The Global Risks Report 2024*. In World Economic Forum. www.weforum.org
- Whyte, H. (2025). Crisis communication strategies and organizational resilience: Lessons from Nigerian financial institutions. *International Journal of Research and Innovation in Social Science*, 9(4), 2357-2374. <https://doi.org/10.47772/IJRISS>
- Wijanarko, D., Rustono, B., & Nurjanah, F. (2024). Effectiveness of communication and cooperation in security section employees bank Indonesia. *European Journal of Psychological Research*, 11(2), 101-111. www.idpublications.org/ejpr-vol11-no-2-2024/
- Winata, H., Thoyib, A., Rohman, F., & Yuniarinto, A. (2024). From experience to loyalty: Understanding the dynamics of customer trust in Indonesia's mobile banking industry. *Journal of Lifestyle and SDG'S Review*, 5(2), 1-23. <https://doi.org/10.47172/2965-730X.SDGsReview.v5.n01.pe02597>
- World Bank Group. (2024). *Individuals using the Internet* (% of population). In World Bank Group Data. <https://data.worldbank.org/indicator/IT.NET.USER.ZS?view=map>
- Yudiana, F. E. (2021). Exploration of switching behavior of sharia banking customer in Indonesia with satisfaction as an intervening variable. *Annual International Conference on Islamic Economics and Business*, 2021, 227–238. <https://doi.org/10.18326/aicieb.v1i0.18>
- Yusuf, M., Komarudin, P., Rahmani Abduh, M., Farhanah, S. A., & Nafisah, H. (2023). The role of Islamic banks in Indonesia: A systematic literature review. *Al-Mashrafiyah: Jurnal Ekonomi, Keuangan, dan Perbankan Syariah*, 7(1), 16–35. <https://doi.org/10.24252/al-mashrafiyah.v7i1.36115>

Zulganef, Z., Pratminingsih, S. A., & Salsabil, I. (2023). Maintaining customer loyalty and satisfaction in service recovery through Javanese philosophy. *Asian Journal of Business Research*, 13(1), 19-40. <https://doi.org/10.14707/ajbr.230140>

About the Authors

Dinda Dwi Nurrikkiana, a bachelor's graduate from the Department of Islamic Banking, Faculty of Economics and Business, Universitas Islam Malang. She has a strong passion for banking and cybersecurity, with a particular interest in exploring the intersection between Islamic financial ethics and digital risk management. As the lead author of this study, she conceptualized the research ideas, formulated the objectives and hypotheses, and aligned them with the overarching research framework.

Afifudin, a distinguished figure in the field of Accounting, has made significant contributions to the paper through his expertise and research focus areas, including Islamic Accounting, General Accounting, Islamic Social Finance, and Taxation. Overall, Afifudin's contributions have enriched the analysis and discussion sections of the paper, providing comprehensive insights and addressing reviewer inquiries with depth and clarity.

Harun Alrasyid, a prominent figure in the field of Islamic Finance, earned a Doctorate in Islamic Banking from World Islamic Sciences and Education (WISE) University, Amman, Jordan. His recent research focuses on investigating Islamic fintech, Islamic social finance, shariah parameter in muamalah, maqashid syariah and digital economy. As the corresponding author of the study, he supervised the overall research design, refined the conceptual and analytical framework, ensured methodological rigor, and provided critical guidance throughout the manuscript's development and revision process.