OPEN ACCESS
Jurnal Ilmiah Ilmu Terapan Universitas Jambi
Vol. 10 No. 2. April 2026, pp. 915-928 DOI. 10.22437/jiituj.v10i2.53556
Research Article

FEAR-DRIVEN DECISION-MAKING IN CYBER RISK MANAGEMENT AND DIGITAL TRANSFORMATION OF BANKING: A SYSTEMATIC LITERATURE REVIEW

M. Dedy Ompu Mataram[1], Rita Mulyanti[1], and Achmadi[1]
[1]Department of Management, Faculty of Economics and Business, Universitas Teknologi Muhammadiyah Jakarta, Jakarta, Indonesia
Corresponding author email: saya.dedy1@gmail.com

Article Info
Recieved: Jan 11, 2026
Revised: Feb 25, 2026
Accepted: Mar 27, 2026
OnlineVersion: Apr 29, 2026

Abstract
This study employs a Systematic Literature Review (SLR) approach to examine fear-driven decision-making in cyber risk management and digital transformation within the banking sector. The review follows the PRISMA framework and analyzes 25 peer-reviewed journal articles selected from Scopus and Web of Science databases published between 2020 and 2025. The findings reveal that fear operates as a latent psychological mechanism influencing strategic decision-making, particularly through risk amplification, regulatory pressure, and trust concerns. Fear-driven responses often lead to conservative strategies, delayed innovation, and excessive risk aversion, which may affect organizational resilience and governance effectiveness. This study contributes to the literature by explicitly conceptualizing fear as a central construct in cyber risk management and digital transformation, providing both theoretical insights and practical implications for banking institutions.

Keywords: Banking, Cyber Risk, Decision-Making, Digital Transformation, Organizational Behavior, Risk Governance

INTRODUCTION

Digital transformation has become a key strategic agenda in the global banking industry. The digitization of services, adoption of digital-only banking, and integration of financial technology improve operational efficiency but simultaneously increase exposure to cyber risks, operational disruptions, and reputational threats. Decision-making in this environment involves uncertainty, risk, and long-term consequences. In practice, decision-making is not always rational but is often influenced by emotional and psychological factors, particularly fear.

Fear is a fundamental human emotion that functions as a self-protection mechanism against perceived threats. However, in modern decision-making contexts, fear not only acts as an adaptive warning system but can also distort risk perception and create judgment bias. Fear can alter how individuals assess risks by exaggerating the probability of negative outcomes and encouraging risk-avoidance behavior (Ahmed, 2024). In organizational settings, such distortions may influence strategic decisions, particularly in industries characterized by high uncertainty such as banking and financial services.

Empirical studies indicate that increased cyber risk directly affects bank profitability, stability, and operational resilience, especially in developing economies (Opoko Apendi et al., 2025). Traditional banking risk management literature assumes that cybersecurity decisions are made rationally through probabilistic risk assessment and cost–benefit analysis (Percia David et al., 2020). However, this assumption has been increasingly questioned as banks demonstrate tendencies toward overinvestment in security and highly conservative strategies even when actual risk exposure is relatively controlled.

The relevance of fear-driven decision-making has increased in the digital era, where organizations and individuals are continuously exposed to information pressure, technological change, and competitive uncertainty. Fear manifests not only in the form of physical threats but also psychological concerns such as fear of failure, fear of irrelevance, fear of losing competitiveness, and fear of missing out. These emotional drivers may influence organizational responses to cyber threats, digital transformation, and innovation adoption.

Previous research shows that organizational responses to cyber threats are frequently driven by concerns about losing customer trust and institutional reputation rather than purely financial losses (Aisyah et al., 2025). In organizational behavior literature, this phenomenon reflects fear-driven decision-making, a condition in which strategic decisions are influenced by perceived threats, uncertainty, and institutional anxiety. Although fear has been widely discussed in psychology and behavioral sciences, banking literature tends to capture it indirectly through constructs such as perceived risk, job insecurity, regulatory pressure, and trust erosion (Purnamasari et al., 2025).

The concept of fear-driven decision-making explains how exaggerated perceptions of risk and uncertainty lead individuals and organizations to prioritize short-term emotional security over long-term strategic benefits. Fear can cause cognitive distortions that focus attention on worst-case scenarios, encourage avoidance-oriented behavior, and reduce openness to innovation (Ahmed, 2024). In organizational contexts, such dynamics may result in conservative decision-making, reactive strategies, and limited experimentation.

The literature on digital banking also highlights the limitations of rational decision models. Banks often face difficulties in accurately measuring cyber threat probabilities and impacts, leading to defensive strategies oriented toward extreme prevention rather than risk optimization (Gatzert & Schubert, 2022). Similarly, cyber threat intelligence is not always effectively integrated into strategic decision-making, causing organizations to rely on worst-case assumptions that reflect the dominance of fear over analytical evaluation (Ainslie et al., 2023). Competitive pressures further reinforce this behavior, as banks tend to imitate competitors' security practices to avoid reputational risks (Sulong et al., 2025) .

Fear also functions as an internal organizational mechanism. Studies indicate that digital transformation may create anxiety among employees regarding job security, reducing innovativeness and productivity and influencing managerial decisions about the pace of digital adoption (Ghosh and Golder, 2025). At the customer level, fear triggered by cyber incidents significantly affects trust and risk perception, often persisting even after technical recovery (Aisyah et al., 2025). Customers may adopt risk-averse behaviors, such as limiting digital service usage or switching providers perceived as more secure (McGregor et al., 2025).

Regulatory pressure represents another major source of institutional fear in digital banking. Increasing cybersecurity and data protection regulations encourage compliance-oriented governance, where decisions are driven by fear of sanctions rather than strategic resilience (Hidayat et al., 2025a). Within the ESG framework, cybersecurity policies are often strengthened to maintain institutional legitimacy, although such measures may not always improve operational effectiveness (Bruno et al., 2025). Consequently, governance becomes more symbolic than adaptive, limiting organizational flexibility in responding to evolving cyber threats.

Digital transformation and innovation introduce additional psychological challenges. The adoption of fintech and digital banking technologies creates strategic dilemmas between competitiveness and operational risk. Fear of system failure, technological disruption, and service instability often encourages incremental rather than radical innovation (Percia David et al., 2020). Although this approach reduces short-term uncertainty, it may limit long-term digital capability development.

Organizational governance mechanisms, particularly ambidextrous IT governance, play an important role in managing this tension. By balancing exploration and exploitation activities, such governance structures enable banks to maintain stability while adapting to technological change (Mulyana

et al., 2024), Although fear is not always explicitly addressed, governance systems function as institutional responses to organizational anxiety related to technological uncertainty and risk exposure.

Overall, existing literature demonstrates that fear consistently appears as an implicit factor influencing strategic decisions in banking, particularly in relation to cyber risk, regulatory pressure, trust, and digital transformation. However, fear is rarely conceptualized as a central construct. Instead, it is embedded within derivative concepts such as perceived risk, trust erosion, job insecurity, and compliance pressure. This condition limits a comprehensive understanding of the behavioral mechanisms underlying banking decisions.

Despite extensive research on cyber risk and digital transformation in banking, existing studies tend to focus primarily on rational and technical perspectives, often overlooking the role of psychological factors such as fear. Fear is typically embedded within constructs such as perceived risk, trust, and regulatory pressure, rather than being explicitly conceptualized as a central mechanism influencing decision-making. This gap limits a comprehensive understanding of how banking organizations respond to uncertainty and risk in the digital era.

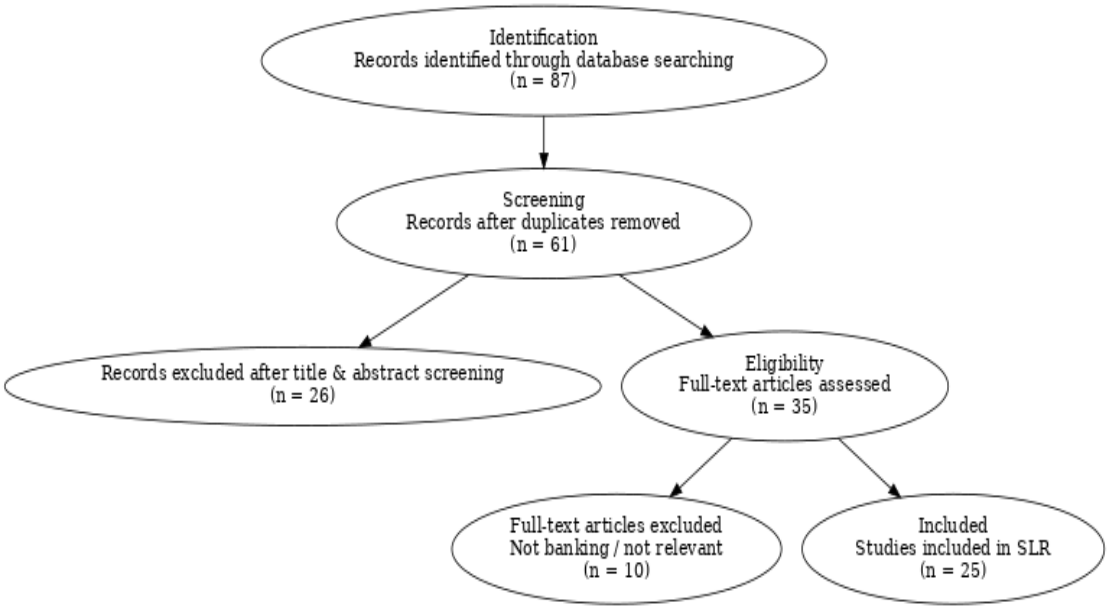
Therefore, this study aims to synthesize existing literature to position fear as a latent psychological mechanism that mediates the relationship between cyber risk exposure, institutional pressures, and strategic decision-making in banking organizations. By explicitly conceptualizing fear, this research contributes to extending rational models of risk management and digital transformation toward a more comprehensive behavioral perspective in understanding organizational responses to uncertainty.

RESEARCH METHOD

This study employed a Systematic Literature Review (SLR) approach to examine fear-driven decision-making in cyber risk management and digital transformation within the banking sector. This study does not involve primary data collection such as surveys or interviews. Instead, it relies exclusively on secondary data derived from published journal articles, consistent with the Systematic Literature Review (SLR) approach. The SLR method was chosen to enable a structured, transparent, and replicable synthesis of relevant scholarly literature. The review process followed the principles of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework to ensure methodological rigor in identifying, screening, and selecting relevant articles.

The literature search was conducted using two internationally recognized academic databases, namely Scopus and Web of Science, which provide comprehensive coverage of peer-reviewed journals in management, finance, organizational studies, and information systems. The search focused on journal articles published between 2020 and 2025 and written in English to capture recent developments in digital banking and cybersecurity. The search strategy applied predefined keywords combined with Boolean operators. The search string used was: (“fear” OR “organizational anxiety” OR “risk perception”) AND (“decision making” OR “strategic decision”) AND (“cyber risk” OR “cybersecurity” OR “information security”) AND (“digital transformation” OR “fintech” OR “digital banking”) AND (“bank” OR “banking” OR “financial institution”).

Figure 1. PRISMA flow diagram of article selection process



The initial database search identified 87 records. After removing duplicate articles across databases, 61 unique records remained for further screening. The screening process was conducted in stages in accordance with the PRISMA procedure. First, title and abstract screening were performed to eliminate studies that were not related to banking, cyber risk, digital transformation, or decision-making. At this stage, 26 records were excluded due to lack of relevance, leaving 35 articles for full-text assessment. Subsequently, full-text screening was conducted to evaluate conceptual relevance and methodological clarity. Articles were excluded if they did not focus on the banking sector, lacked discussion on decision-making processes, or did not relate substantively to cyber risk and digital transformation. During this stage, 10 articles were excluded. As a result, a final sample of 25 peer-reviewed articles was included in the systematic review. The complete selection process is illustrated in the PRISMA flow diagram presented in Figure 1.

The selected articles were analyzed using a qualitative thematic coding approach. The analysis began with systematic data extraction, documenting research objectives, theoretical perspectives, methodological approaches, and key findings from each article. This was followed by open coding to identify recurring concepts related to fear, risk perception, regulatory pressure, trust erosion, innovation resistance, compliance behavior, and technological uncertainty. The identified concepts were then organized through axial coding into broader thematic categories, including cyber risk perception, regulatory and governance pressures, trust dynamics, digital transformation dilemmas, and organizational control mechanisms. Finally, selective coding was conducted to integrate these themes and construct a conceptual explanation of fear as a latent psychological and organizational mechanism influencing strategic decision-making in digital banking.

Thematic synthesis was applied to identify consistent patterns across the reviewed studies. Rather than treating fear as an explicitly measured variable, this study conceptualized fear as a latent construct inferred from observable behavioral patterns such as excessive risk aversion, conservative strategic orientation, compliance-driven governance, defensive innovation strategies, and symbolic reinforcement of cybersecurity policies. Cross-study comparison was conducted to ensure conceptual consistency across different geographical contexts and methodological approaches. By applying explicit inclusion criteria, structured screening stages, and systematic coding procedures, this study ensured analytical transparency, reliability, and conceptual robustness.

RESULTS AND DISCUSSION

Based on a literature selection process using the PRISMA approach, this study identified and analyzed 25 scientific articles relevant to the topics of cyber risk, digital transformation, governance, and decision-making in the banking sector. These articles were published between 2020 and 2025 and originated from reputable journals, most of which are indexed.

Methodologically, the studies reviewed included quantitative approaches (e.g., panel regression, SEM), qualitative approaches (case studies), and systematic literature reviews. In terms of context, the majority of studies focused on the conventional and digital banking sectors, with geographical variations covering developed and developing countries. This diversity of approaches and contexts provides a strong basis for conducting a thematic synthesis across studies.

Explaining Fear-Driven Decision-making Defining Perspectives

A review of the literature shows that fear-driven decision-making is a consistent pattern of decision-making, even though most studies do not explicitly discuss fear. Fear in this context can be understood as a psychological mechanism shaped by various environmental inputs, particularly cyber risks, regulatory pressures, and the complexity of digital transformation.

The literature on decision psychology shows that fear influences risk assessment by increasing the perception of threat and decreasing tolerance for uncertainty, thereby encouraging defensive and risk-averse decisions(Ahmed, 2024). In the banking context, exposure to cyber risk serves as a major input that triggers organizational fear, because such risks not only have technical implications but also threaten the reputation and trust of stakeholders. (Al-Sartawi et al., 2025).

In addition, regulatory pressure reinforces institutional fear by encouraging organizations to prioritize compliance in order to avoid sanctions, even though this approach does not always improve long-term cyber resilience. (Bruno et al., 2025; Hidayat et al., 2025a) The combination of cyber risks and regulatory pressure creates conditions that reinforce fear before strategic decisions are made.

Thus, fear-driven decision-making can be positioned as the result of an environmental input perspective that reinforces the organization's response to uncertainty. Fear serves as a reinforcing mechanism that bridges inputs in the form of risk and pressure with strategic decisions that tend to be conservative in digital banking.

Table 1. Eligibility and Elimination Criteria.

Criterion	Eligibility	Elimination
Type of articles	"Research articles published in peer-reviewed journals indexed "	"Books, book chapters, conference proceedings, editorials, and non-research articles"
Selection of articles	"Articles focusing on fear, risk perception, decision-making, cybersecurity, digital transformation, and organizational behavior in the banking and financial services sector"	"Articles not related to decision-making, fear, cybersecurity, or not focused on banking and financial services"
Database source	"Studies retrieved exclusively from Scopus and Web of Science electronic databases using predefined search strings"	"Peer-reviewed articles published outside Scopus and Web of Science databases"
Language of the articles	"English-language articles"	"Non-English articles"
Subject area of the articles	"Business, Management, Finance, Information Systems, Social Sciences, and related interdisciplinary fields"	"Articles from unrelated subject areas (e.g., pure technical engineering without organizational or managerial context)"
Timeline coverage	"Publications from 2020 to 2025"	"Publications published before 2007"

Table 2. Conceptual Framework: Understanding fear-driven decision-making from literature

Theme	Code	Definition
Fear Definition	Fear-Driven Decision-making	*Fear-driven decision-making* refers to a psychological and organizational condition in which strategic decisions are predominantly shaped by perceived threats, uncertainty, and anticipated losses rather than purely rational cost–benefit evaluations. In the context of digital banking, fear arises from cyber risks, regulatory pressures, and reputational threats, shifting decision-making toward defensive and risk-averse strategies.
	Perceived Cyber Threat	The extent to which organizations perceive cybersecurity threats as severe and potentially disruptive to data integrity, operational continuity, and service reliability. Heightened perceptions of cyber threats tend to amplify fear and encourage conservative decision-making.
	Risk Amplification	A cognitive process through which perceived risks are exaggerated beyond their objective likelihood or impact due to fear, leading organizations to prioritize maximum protection over efficiency or innovation.
Fear Sources	Fear of Cyber Disruption	Organizational fear associated with the possibility of large-scale operational disruptions resulting from cyberattacks, system failures, or technological dependencies. This fear often constrains experimentation and limits transformative innovation.
	Fear of Regulatory Sanctions	Fear arising from potential legal consequences, financial penalties, or operational restrictions due to non-compliance with cybersecurity and data protection regulations. This fear strongly influences governance and compliance-oriented decisions.
	Fear of Trust Erosion	Fear related to the potential loss of customer and stakeholder trust following cybersecurity incidents or failures in risk management, which can undermine organizational legitimacy and long-term performance.
Strain Facets	Compliance Pressure Stress	Psychological and organizational strain generated by complex and evolving regulatory requirements, which increases anxiety in strategic decision-making and reinforces compliance-focused behavior.
	Technological Complexity Stress	Stress resulting from the growing complexity of digital technologies and financial systems, which heightens organizational uncertainty and fear in managing digital transformation.
	Decision-making Anxiety	A collective state of anxiety that affects strategic decision processes, causing organizations to delay decisions or avoid options associated with higher uncertainty.
Behavioral Responses	Defensive Strategy Orientation	A strategic posture emphasizing stability, risk control, and loss prevention, often at the expense of flexibility, experimentation, and long-term innovation.
	Compliance-Driven Governance	A governance approach primarily focused on meeting regulatory and procedural requirements as a means of reducing institutional fear and external scrutiny.
	Preference for Incremental Innovation	The tendency to favor gradual, incremental innovations over radical transformation as a response to fear of disruption and technological uncertainty.
Coping Mechanisms	Ambidextrous IT Governance	An IT governance mechanism that balances exploration (innovation and flexibility) and exploitation (control and stability) to manage organizational fear while enabling digital transformation.

Theme	Code	Definition
	Risk Formalization	Organizational efforts to reduce fear through the formalization of policies, procedures, audits, and risk management frameworks, providing a sense of control and predictability.
Outcomes	Organizational Resilience	The organization's ability to withstand, adapt to, and recover from cyber risks and environmental pressures while maintaining operational continuity and stakeholder confidence.
	Legitimacy Preservation	The strategic outcome of sustaining institutional legitimacy by signaling security, compliance, and reliability to regulators, customers, and other stakeholders.

Table 3. Understanding Fear-Driven Decision-making: research papers, codes, and findings

No	Research Paper Title and Year, Author	Codes	Explanation / Key Findings
1	*Cyber Risk Management and Bank Competition* (2025)	Cyber Risk; Competitive Pressure; Risk Aversion; Defensive Strategy	The study shows that cyber risk increases competitive anxiety among banks, leading to conservative and defensive strategic decisions aimed at avoiding reputational and market share losses rather than maximizing innovation outcomes.
2	*Cyber Risk Management in US Banking* (2025)	Cyber Risk; Regulatory Fear; Risk-Averse Decision-making	Findings indicate that heightened cyber risk exposure leads banks to adopt risk-averse strategies driven by fear of financial loss and regulatory penalties, negatively affecting profitability.
3	*Cybersecurity and Banks' Performance: Evidence from GCC* (2024)	Cybersecurity Investment; Trust Preservation; Fear of Reputation Loss	The research reveals that cybersecurity investments are primarily motivated by the need to preserve stakeholder trust and institutional legitimacy rather than direct efficiency gains.
4	*Assessment of Cybersecurity Risks and Threats on Banking and Financial Services* (2023)	Cyber Threats; Operational Fear; Systemic Risk	This study identifies malware and phishing as dominant threats, highlighting systemic fear of service disruption and large-scale operational failure.
5	*Customers' Trust in Islamic Banking Post-Cyberattack* (2025)	Fear; Trust Erosion; Behavioral Intention	Findings show that fear mediates the relationship between cyberattacks and reduced customer trust and service usage, even after technical recovery.
6	*Big Data Security and Psychological Resilience* (2023)	Psychological Fear; Stress; Digital Risk	The study demonstrates that fear and stress persist despite increased cybersecurity knowledge, emphasizing the emotional dimension of risk perception.
7	*Whaling-Style Cyber Attacks in Banking* (2022)	Executive Fear; Targeted Phishing; Defensive Controls	Results show that fear of executive compromise leads to excessive security controls and highly conservative decision-making.
8	*Effect of Financial Innovation and Stakeholder Satisfaction on Investment Decisions* (2023)	Fear Reduction; Symbolic Security; Stakeholder Assurance	Cybersecurity is shown to function as reassurance for stakeholders, reducing anxiety rather than directly enhancing financial returns.

No	Research Paper Title and Year, Author	Codes	Explanation / Key Findings
9	*Cybersecurity Implementation Maturity in Indonesian Digital Banking* (2025)	Regulatory Pressure; Compliance Fear; Governance	The study finds high regulatory compliance but limited adaptive capability, indicating fear-driven compliance-oriented governance.
10	*Cybersecurity Policy, ESG, and Operational Risk* (2025)	ESG Pressure; Legitimacy Fear; Institutional Governance	Cybersecurity policies are used to mitigate fear of ESG failure and reputational damage rather than to improve operational efficiency.
11	*Cybersecurity Risk Analysis on Digital Banking Adoption* (2024)	Risk Perception; Adoption Anxiety; Fear Misalignment	Findings reveal a misalignment between actual cyber risk and perceived fear, influencing adoption decisions inconsistently.
12	*Cyber-Threat Intelligence for Security Decision-making* (2023)	Uncertainty Fear; Decision Anxiety; Reactive Strategy	The review highlights that insufficient threat intelligence integration leads to fear-driven, reactive security decisions.
13	*Financial Risk Management in Digital-only Banks* (2020)	System Failure Fear; Defensive Risk Management	Digital-only banks exhibit high defensiveness due to fear of large-scale system collapse in cashless environments.
14	*Impact of Cyber Risk on Egyptian Banks' Profitability* (2024)	Financial Loss Fear; Risk Aversion; Performance Impact	The study demonstrates that fear of cyber losses drives conservative financial strategies that reduce profitability.
15	*Impacts of Digitization on Operational Efficiency in Banking* (2023)	Digital Disruption Fear; Efficiency Trade-off	Digital transformation improves efficiency but simultaneously increases fear of operational disruption.
16	*E-Banking, Job Security, Innovativeness, and Productivity* (2023)	Job Insecurity Fear; Innovation Resistance	Fear of job loss negatively affects innovation and productivity, shaping managerial decisions on digital transformation.
17	*Knowledge Absorption for Cybersecurity* (2022)	Learning Fear; Vigilance; Behavioral Adaptation	Fear enhances vigilance and learning but leads to over-cautious behavior when unmanaged.
18	*Evaluation of Cybersecurity Protocols in the U.S. Financial Sector* (2025)	Compliance Fear; Overengineering	Excessive security controls are implemented due to fear of non-compliance rather than risk-based reasoning.
19	*FinTech Adoption and Traditional Banking: A Systematic Review* (2024)	Disruption Fear; Incremental Innovation	Banks prefer incremental innovation due to fear of technological disruption and uncertainty.
20	*Revealing the Realities of Cybercrime in SMEs* (2023)	Fear Taxonomy; Cognitive Fear; Decision Bias	The study categorizes fear types and shows how fear biases organizational decision-making under cyber threat.
21	*Cybersecurity Awareness and Mobile Banking* (2024)	User Fear; Protective Behavior	Increased awareness heightens fear, leading to cautious user behavior rather than increased adoption.
22	*Cybersecurity and Digital Transformation for Competitive Advantage* (2024)	Strategic Fear; Competitive Pressure	Fear motivates digital transformation as a survival strategy rather than opportunity-seeking behavior.

No	Research Paper Title and Year, Author	Codes	Explanation / Key Findings
23	*Ambidextrous IT Governance in Bank Rakyat Indonesia* (2024)	Fear Management; Governance Balance; Control vs Innovation	The study shows that ambidextrous IT governance mitigates organizational fear by balancing innovation and control mechanisms.
24	*Fear and Decision-making: How Fear Affects Risk Assessment and Behavioral Choices* (Ahmed, 2024)	Fear-Driven Decision-making; Risk Assessment Bias; Risk Aversion; Anxiety and Stress; Behavioral Avoidance	This study examines fear as a fundamental psychological mechanism influencing decision-making. The findings show that fear alters risk assessment by exaggerating perceived threats and potential negative outcomes, leading to conservative and risk-averse behavioral choices. Fear and anxiety reduce cognitive flexibility, amplify defensive decision-making, and encourage avoidance strategies, particularly under conditions of uncertainty and stress.
25	*Fenomena Fear of Missing Out (FOMO) terhadap Keputusan Pembelian Restoran Viral Karen's Diner Jakarta* (Wachyuni et al., 2024)	Fear of Missing Out (FOMO); Emotional Fear; Social Pressure; Behavioral Decision-making; Purchase Decision	This research demonstrates that FOMO—characterized by fear, anxiety, and worry about missing social experiences—has a significant positive effect on consumer decision-making. The study finds that emotional fear and social influence drive purchasing decisions more strongly than rational evaluation, indicating that fear-based mechanisms play a critical role in shaping behavioral choices in digital and social-media-driven environments.

Cyber Risk as a Trigger for Organizational Fear

Most studies show that increased exposure to cyber risk serves as a major trigger for organizational fear. Cyber risk is not only understood as a technical threat, but also as a threat to operational stability, reputation, and business continuity of banks. Findings across studies show that perceptions of cyber threats often exceed the objective risks measured, prompting organizations to adopt a highly cautious and risk-averse approach. (Gatzert and Schubert, 2022; Shehab et al., 2024)

In this context, fear influences how organizations assess risk through a process of risk amplification, which then shapes preferences for defensive strategies and avoidance of uncertainty. (Ahmed, 2024; Ainslie et al., 2023).

Fear, Trust, and Stakeholder Response

The review results show a strong relationship between fear and trust, both at the customer and organizational levels. Several studies have found that cyber incidents trigger fear that directly impacts a decline in trust, even after the system has been technically restored. The fear experienced by customers and stakeholders is persistent and affects their intention to use digital services and their perception of the bank's credibility. (Aisyah et al., 2025; McGregor et al., 2025).

At the organizational level, fear of erosion of trust drives banks to increase investment in cybersecurity as a signal of legitimacy to the public and regulators. In this context, cybersecurity serves not only as a risk mitigation tool, but also as a symbolic mechanism for maintaining stakeholder trust.(Al-Sartawi et al., 2025; Pea-Assounga et al., 2024).

Regulatory Pressure and Institutional Fear

The next prominent theme is the role of regulatory pressure as a source of institutional fear. Studies focusing on governance and cybersecurity maturity show that regulatory compliance is often a top priority in strategic banking decisions.(Hidayat et al., 2025b)

Fear of regulatory sanctions, fines, and legal consequences drives organizations to adopt compliance-driven governance. However, several studies also show that this compliance orientation is not always accompanied by an increase in adaptive capacity to dynamic cyber risks, creating a potential imbalance between formal compliance and long-term resilience.(Alam et al., 2025; Bruno et al., 2025).

Fear of Disruption and Innovation Patterns

The review results show that fear also plays an important role in shaping banking innovation patterns. In both traditional and digital banks, fear of large-scale operational disruption encourages organizations to choose incremental innovation over radical innovation (Ghosh and Golder, 2025).

Although this approach can reduce the risk of short-term failure, the literature shows that such strategies have the potential to limit long-term digital capability development and sustainable competitive advantage. Thus, fear functions as a mechanism that shapes the innovation boundary in banking digital transformation (Bueno et al., 2024; Metibemu, 2025).

Mechanism for Managing Fear through Governance

The final theme that emerged was the role of governance as a mechanism for managing fear. Several studies showed that IT governance structures, audit systems, and risk management frameworks serve as institutional tools for mitigating organizational anxiety about technological uncertainty and cyber risks. (Ainslie et al., 2023; Bruno et al., 2025).

Specifically, the ambidextrous IT governance approach has emerged as a mechanism that enables organizations to balance the needs for innovation and control. Ambidextrous governance helps organizations manage fear without completely hindering digital transformation and long-term adaptive capacity. (Mulyana et al., 2024).

Synthesis Pattern of Results

Overall, the review results show that fear operates as a latent mechanism that links cyber risk, regulatory pressure, stakeholder trust, and strategic banking decisions. Fear influences how organizations assess risk, determine strategic priorities, and respond to environmental uncertainty.

Although the reviewed literature rarely models fear explicitly, the consistency of reported behavioral patterns such as risk aversion, compliance orientation, and preference for incremental innovation indicates that fear is an important factor that has not been fully explored in digital banking studies.

This study aims to synthesize the literature on cyber risk, digital transformation, and strategic decision-making in the banking sector by placing fear-driven decision-making as the main analytical lens. The results of the systematic literature review show that although fear is rarely explicitly conceptualized in banking studies, it consistently operates as a latent psychological and organizational mechanism that influences banks' strategic responses to cyber risk and digital uncertainty.

These findings indicate that fear is not merely a transient emotional response but an institutionalized element shaping how banking organizations assess and manage risk, prioritize compliance, manage trust, and limit innovation. This section discusses these findings by linking them to previous literature and highlighting their theoretical and practical implications.

Fear as a Latent Mechanism in Cyber Risk Management

The results of the study show that fear influences the decision-making process by changing the way organizations assess risk. The decision psychology literature explains that fear increases the perception of threat and decreases tolerance for uncertainty, thereby encouraging risk-averse decision-making (Ahmed, 2024) These findings are consistent with studies on cyber risk management in the banking sectors of the United States and Egypt, which show that increased cyber risk encourages banks to adopt conservative strategies, including excessive security controls, despite their negative impact on financial performance (Bueno et al., 2024; Sulong et al., 2025).

In addition, the Assessment of Cybersecurity Risks and Threats on Banking and Financial Services study shows that cyber threats are often perceived as systemic risks that are difficult to predict, thereby reinforcing organizations' fears of potential large-scale operational disruptions. This condition causes risk amplification, where perceived risks exceed measurable objective risks(Hashem, 2025).

Fear, Trust, and Institutional Legitimacy

The relationship between fear and trust is an important finding in this study. The study Customers' Trust in Islamic Banking Post-Cyberattack shows that customer fear acts as a mediator between cyber incidents and a decline in trust and intention to use digital services, even after the system has been technically restored (Aisyah et al., 2025). This finding is reinforced by the Consumer Perceptions of Personal Cybersecurity study, which shows that fear of personal data misuse has a greater influence on customer behavior than objective assessments of system security levels. (Maréchal et al., 2025; McGregor et al., 2025)

At the organizational level, the study Cybersecurity and Banks' Performance: Evidence from GCC shows that cybersecurity investments are often made to maintain legitimacy and stakeholder trust, rather than solely to improve operational efficiency. (Al-Sartawi et al., 2025). In this context, fear of erosion of trust encourages banks to use cybersecurity as a signal of institutional credibility.

Regulatory Pressure and Compliance-Based Governance

The findings of this study also highlight the role of regulatory pressure as a major source of institutional fear. The Cybersecurity Implementation Maturity in Indonesian Digital Banking study shows that banks in Indonesia have a high level of regulatory compliance, but their adaptive capacity to dynamic cyber risks is still limited. (Hidayat et al., 2025b) This indicates that cybersecurity decisions are driven more by fear of regulatory sanctions than by a focus on long-term resilience(Ghosh and Golder, 2025).

Similar findings are shown in the Cybersecurity Policy, ESG, and Operational Risk study, which explains that cybersecurity policies are increasingly positioned as part of ESG strategies and institutional legitimacy. Fear of failing to meet ESG standards and pressure from stakeholders are driving organizations to strengthen formal policies, even though their operational effectiveness does not always increase proportionally. (Bruno et al., 2025). This condition reinforces the compliance-driven governance pattern in digital banking.

Fear of Disruption and Restrictions on Innovation

This study also shows that fear plays a role in shaping banking innovation patterns. The study Exploring the Effects of FinTech Adoption on Traditional Banking shows that traditional banks face a dilemma between the need for innovation and fear of operational disruption, thus tending to choose incremental innovation over radical innovation. A similar pattern was found in the study Financial Risk Management in Digital-only Banks, which shows that although digital banks are more agile, fear of large-scale system failure encourages very cautious decision-making (Percia David et al., 2020).

Thus, fear of disruption serves as a mechanism that shapes the innovation boundary in banking digital transformation (Opoko Apendi et al., 2025). Although this strategy can increase short-term stability, the literature shows that excessive conservatism has the potential to hamper the development of long-term digital capabilities.

Governance as a Mechanism for Managing Fear.

The findings of this study also show that governance plays an important role in managing organizational fear. The study Key Ambidextrous IT Governance Mechanisms for Successful Digital Transformation: Bank Rakyat Indonesia shows that the implementation of ambidextrous IT governance enables organizations to balance the needs for innovation and control, thereby helping to reduce fear without completely hindering digital transformation (Mulyana et al., 2024).

In addition, literature on cyber-threat intelligence and risk management formalization shows that governance structures, audits, and decision support systems can reduce uncertainty and prevent fear from dominating strategic decision-making.

Theoretical and Practical Implications

Theoretically, the results of this discussion expand the literature on risk management and digital transformation by placing fear as a latent psychological mechanism that bridges cyber risk, regulatory pressure, trust, and strategic banking decisions. In practical terms, these findings highlight the importance for bank management and regulators to distinguish between objective risk-based decisions and fear-based decisions, in order to avoid excessive conservatism that can hinder innovation and long-term competitiveness.

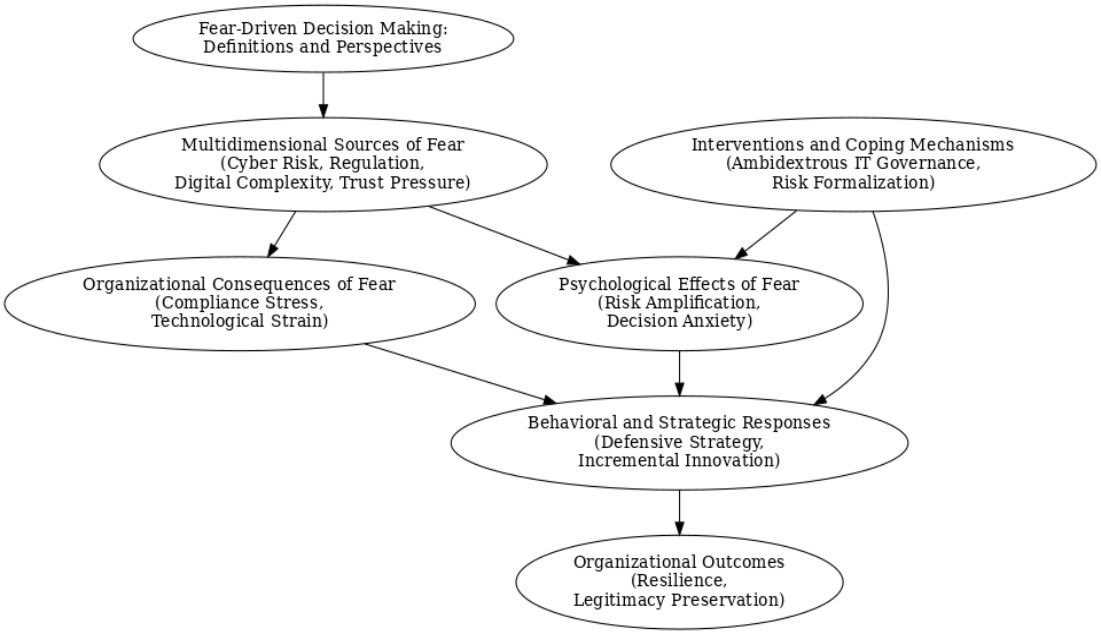


Figure 2. A conceptual framework of fear-driven decision-making in digital banking

Figure 2 illustrates a conceptual model of fear-driven decision-making that explains how fear acts as a psychological and organizational mechanism in strategic decision-making in digital banking. This model departs from the definition and perspective of fear as a response to perceived uncertainty and threats, which then develops into various multidimensional sources of fear. These sources include cyber risk, regulatory pressure, the complexity of digital transformation, and pressure on stakeholder trust.

In this model, the source of fear affects organizations through two main channels, namely psychological impact and organizational impact. The psychological impact of fear is reflected in the process of risk amplification and increased anxiety in decision-making (decision anxiety), which shifts rational evaluation towards risk avoidance orientation. Simultaneously, fear also produces organizational consequences in the form of compliance stress and technological strain, which reinforce the perception of organizational vulnerability.

These psychological and organizational impacts then shape the organization's behavioral and strategic responses. These responses are generally characterized by a defensive strategy orientation and a preference for incremental innovation over radical transformation. These decisions reflect the organization's efforts to reduce uncertainty and maintain stability in a high-risk environment.

This model also emphasizes the role of interventions and coping mechanisms, such as the implementation of ambidextrous IT governance and the formalization of risk management. These mechanisms serve as moderating factors that can mitigate the impact of fear, both at the psychological and organizational levels, thereby preventing excessive conservatism in decision-making.

Ultimately, the strategic response shaped by fear produces various organizational outcomes, particularly organizational resilience and legitimacy preservation. This model shows that although fear can promote short-term stability and protection, disproportionate management of fear has the potential to limit the adaptive and innovative capacity of banking organizations in the long term.

CONCLUSION

This study aims to examine and synthesize literature on cyber risk, digital transformation, and decision-making in banking organizations by placing fear-driven decision-making as the main analytical lens. Based on a systematic literature review of 25 reputable journal articles, this study finds that fear acts as a latent psychological mechanism that consistently influences how banking organizations assess risk and respond to uncertainty, even though most studies do not conceptualize it explicitly. The review results show that exposure to cyber risk, regulatory pressure, technological complexity, and threats to stakeholder trust serve as the main sources of organizational fear formation. Fear arising from these conditions reinforces threat perception (risk amplification), lowers tolerance for uncertainty, and encourages defensive, compliance-oriented decision-making that tends to avoid high-risk innovation. In this context, fear bridges the relationship between cyber risk and strategic banking decisions, including governance

choices and digital transformation strategies. This study also shows that fear has an ambivalent impact. On the one hand, fear can increase awareness and encourage the strengthening of risk control mechanisms. On the other hand, fear that is not managed proportionally has the potential to result in excessive conservatism, compliance-driven governance, and restrictions on innovation that can hinder long-term digital capability development. These findings emphasize the importance of governance mechanisms that can manage fear in a balanced manner, such as the implementation of ambidextrous IT governance and the formalization of risk management.

Theoretically, this study contributes by explicating the role of fear as a latent mechanism in the digital banking literature, complementing the rational approach that has dominated risk management and digital transformation studies. Practically, these findings imply that banking management and regulators need to distinguish between decisions based on objective risk and decisions driven by fear, in order to avoid overly defensive and non-adaptive strategic responses. Although this study provides a comprehensive conceptual synthesis, its main limitation lies in the literature-based nature of the study, which does not empirically test causal relationships. Therefore, further research is recommended to empirically test the role of fear as a mediating or moderating variable in the relationship between cyber risk, governance, and banking organizational performance, as well as to explore the dynamics of fear in different geographical and regulatory contexts.

AUTHOR CONTRIBUTIONS

Conceptualization, Author 1; Methodology, Author 1; Literature Review, Author 1; Writing – Original Draft Preparation, Author 1; Writing – Review and Editing, Author 2 and Author 3; Supervision, Author 2 and Author 3.

CONFLICTS OF INTEREST

The author(s) declare no conflict of interest.

REFERENCES

Ahmed, S. (2024). *Journal of Traumatic Stress Disorders and Treatment Fear and Decision Making : How Fear Affects Risk Assessment and Behavioral Choices*. https://doi.org/10.4172/2324-8947.100415

Ainslie, S., Thompson, D., Maynard, S., and Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers and Security*, *132*, 103352. https://doi.org/10.1016/j.cose.2023.103352

Aisyah, M., Sesunan, Y. S., and Wicaksono, A. T. S. (2025). Customers' trust in Islamic banking post-cyberattack leads to digital service breakdowns in Indonesia. *Sustainable Futures*, *10*(November 2025). https://doi.org/10.1016/j.sftr.2025.101530

Al-Sartawi, A. M. A. M., Sanad, Z., Shehadeh, M., and Binsaddig, R. (2025). Cybersecurity and Banks Performance: Evidence from Gulf Cooperation Council. *International Journal of Cyber Criminology*, *19*(1), 54–71. https://doi.org/10.5281/zenodo.47661903

Alam, M. A., Sarna, S. A., Rakibuzzaman, M., and Reza, J. (2025). Strengthening Cybersecurity Protocols to Safeguard U.S. Financial Infrastructure Against Emerging Threats. *Advances in Economics and Financial Studies*, *3*(2), 71–82. https://doi.org/10.60079/aefs.v3i2.506

Bruno, E., Pistolesi, F., and Teti, E. (2025). Cybersecurity policy, ESG and operational risk: A Virtuous relationship to improve banks' performance. *International Review of Economics and Finance*, *99*, 104053. https://doi.org/10.1016/j.iref.2025.104053

Bueno, L. A., Sigahi, T. F. A. C., Rampasso, I. S., Leal Filho, W., and Anholon, R. (2024). Impacts of digitization on operational efficiency in the banking sector: Thematic analysis and research agenda proposal. *International Journal of Information Management Data Insights*, *4*(1), 100230. https://doi.org/10.1016/j.jjimei.2024.100230

Gatzert, N., and Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *Journal of Risk and Insurance*, *89*(3), 725–763. https://doi.org/10.1111/jori.12381

Ghosh, P., and Golder, U. (2025). Exploring the effects of FinTech adoption on traditional banking : A systematic literature review on opportunities and challenges. *Digital Business*, *6*(1), 100163. https://doi.org/10.1016/j.digbus.2026.100163

Hashem, S. D. (2025). Investigating the Cybersecurity Risks on Digital Banking System. *Lex Localis - Journal of Local Self-Government*, *23*(S6), 289–305. https://doi.org/10.52152/801774

Hidayat, R. R., Husna, J., and Akbar, S. A. (2025a). Evaluating Bank DJX's Cybersecurity Maturity Level from Indonesia's Regulatory Perspective. *Journal of Information Technology and Its Utilization*, *8*(1), 39–44. https://doi.org/10.56873/jitu.8.1.6019

Hidayat, R. R., Husna, J., and Akbar, S. A. (2025b). Evaluating Bank DJX's Cybersecurity Maturity Level from Indonesia's Regulatory Perspective. *Journal of Information Technology and Its Utilization*, *8*(1), 39–44. https://doi.org/10.56873/jitu.8.1.6019

Maréchal, L., Mermoud, A., Percia David, D., and Humbert, M. (2025). Are cybersecurity firms different? Intra-sector and cross-industry comparisons of financial performance. *Journal of Cybersecurity*, *11*(1). https://doi.org/10.1093/cybsec/tyaf032

McGregor, R., Reaiche, C., Boyle, S., and De Zubielqui, G. C. (2025). Consumer perceptions of personal cyber awareness, knowledge, and risk. *Journal of Cybersecurity*, *11*(1). https://doi.org/10.1093/cybsec/tyaf029

Metibemu, O. C. (2025). Financial Risk Management in Digital-Only Banks: Addressing Fraud and Cybersecurity Threats in a Cashless Economy. *Asian Journal of Research in Computer Science*, *18*(3), 434–455. https://doi.org/10.9734/ajrcos/2025/v18i3603

Mulyana, R., Rusu, L., and Perjons, E. (2024). Key ambidextrous IT governance mechanisms for successful digital transformation: A case study of Bank Rakyat Indonesia (BRI). *Digital Business*, *4*(2), 100083. https://doi.org/10.1016/j.digbus.2024.100083

Opoko Apendi, D. A., Li, K., Pea-Assounga, J. B. B., and Bambi, P. D. R. (2025). Investigating the impact of e-banking, employee job security, innovativeness, and productivity on organizational performance: Perspectives from South Africa. *Sustainable Futures*, *9*(April). https://doi.org/10.1016/j.sftr.2025.100605

Pea-Assounga, J. B. B., Yao, H., Mulindwa Bahizire, G., Bambi, P. D. R., and Nima Ngapey, J. D. (2024). Effect of financial innovation and stakeholders' satisfaction on investment decisions: Does internet security matter? *Heliyon*, *10*(6), e27242. https://doi.org/10.1016/j.heliyon.2024.e27242

Percia David, D., Keupp, M. M., and Mermoud, A. (2020). Knowledge absorption for cyber-security: The role of human beliefs. *Computers in Human Behavior*, *106*(November 2019), 106255. https://doi.org/10.1016/j.chb.2020.106255

Purnamasari, R., Hasanudin, A. I., Zulfikar, R., and Yazid, H. (2025). Technological infrastructure and financial resource availability in enhancing public services and government performance: The role of digital innovation adoption in Indonesia. *Social Sciences and Humanities Open*, *11*(August 2024), 101621. https://doi.org/10.1016/j.ssaho.2025.101621

Shehab, R., S.alismail, A., Almaiah, M. A., Alkhdour, T., Alwadi, B. M., and Alrawad, 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

Sulong, Z., Fuszder, M. H. R., Abdullah, M., and Abakah, E. J. A. (2025). Cybersecurity risk and bank risk-taking. *Journal of Behavioral and Experimental Finance*, *47*, 101080. https://doi.org/10.1016/j.jbef.2025.101080

Wachyuni, S. S., Namira, S., Respati, R. D., and Teviningrum, S. (2024). Fenomena Fear Out Missing Out (Fomo) Terhadap Keputusan Pembelian Restoran Viral Karen'S Diner Jakarta. *Jurnal Bisnis Hospitaliti*, *13*(1), 89–101. https://doi.org/10.52352/jbh.v13i1.1382