Indus Journal of Social Sciences
Online ISSN: 2960-219X
Print ISSN: 2960-2203
Volume 3, Number 3, 2025, Pages 377 – 393
Journal Home Page
https://induspublishers.com/IJSS/about

Digital Leadership, Knowledge Management, and Cybersecurity Readiness: Building Organizational Resilience in IT and Fintech Firms

Maham Hafeez[1] & Dr. Imran Sharif[2]

[1-2]*The University of Lahore, Pakistan*

ARTICLE INFO

Article History:

Received:	*June*	*14, 2025*
Revised:	*July*	*23, 2025*
Accepted:	*August*	*03, 2025*
Available Online:	*August*	*14, 2025*

Keywords:

Digital transformational leadership, knowledge management, organizational resilience, cybersecurity readiness.

Corresponding Author:
Maham Hafeez
Email:
mahamhafeez35@yahoo.com

ABSTRACT

This study examined the impact of digital transformational leadership (DTL) on organizational resilience (ORS), directly and in the mediation role of knowledge management (KM), while the moderating role of cybersecurity readiness (CR) in Pakistan's IT services and fintech sectors. Guided by the Knowledge-Based View (KBV), the study tested a moderated mediation model using survey data from 430 managerial employees. Data were analyzed using SPSS and PROCESS Macro. Results showed that DTL positively influenced both KM and ORS, with KM partially mediating the DTL–ORS relationship. KM had a significant positive effect on ORS, and CR strengthened this relationship, indicating that resilience benefits most when knowledge processes operate alongside strong cybersecurity capabilities. These findings contribute to theory by integrating CR into KBV and offer practical guidance for developing leadership, knowledge systems, and security readiness to enhance resilience in high-risk digital environments.

Introduction

IT services and fintech organizations operate in high-risk environments. They store and process sensitive customer data. Such data attracts cybercriminals. The average global cost of a data breach reached USD 4.88 million in 2024. This represents a 10% increase from the previous year. Almost half of these incidents involved customer data (IBM, 2024). The financial and insurance sectors face particularly complex attacks. Ransomware, extortion, and breaches involving third parties are common. This reflects the sector's interconnected nature (Verizon, 2024).

Regulatory bodies have responded with stricter rules. In the European Union, the Digital Operational Resilience Act (DORA) became applicable in January 2025 (EIOPA, 2025). It sets binding requirements for incident reporting, resilience testing, and operational governance (European Banking Authority, 2025). In the United States, the National Institute of Standards and

Technology (NIST) released Cybersecurity Framework 2.0 in 2024. This update adds a "Govern" function to emphasize strategic oversight of cyber risk (NIST, 2024). Global organizations also warn of the systemic risks of cyberattacks on finance (IMF, 2024; WEF, 2024). In this environment, firms must ensure service continuity, maintain customer trust, and comply with evolving regulations after incidents.

Organizational resilience is a core capability in such contexts. It refers to the ability to anticipate, absorb, adapt to, and recover from disruption (van Assen, 2020). Scholars view resilience as a dynamic capability that develops before, during, and after a crisis (Conz & Magnani, 2020; Troilo et al., 2016). It is built on structures, culture, and routines (Bhamra et al., 2011). Leadership, situational awareness, and adaptability are key indicators (McManus et al., 2008). However, there is limited empirical work that combines leadership, knowledge management, and cybersecurity readiness in one study. This gap is particularly evident in the IT and fintech sectors.

Digital transformational leadership (DTL) is essential in digital environments. It involves creating a vision, mobilizing resources, and guiding large-scale transformation. DTL improves organizational agility and supports digital change (Ly, 2024). Research shows that agility links DTL to higher digital intensity, especially in dynamic settings (Kludacz-Alessandri et al., 2025). DTL also has a direct positive effect on resilience in turbulent conditions (Ye, 2025). In service firms, transformational leadership aligns technology, operations, and people to sustain performance across crisis phases (He et al., 2023). This suggests that DTL may influence resilience indirectly through knowledge processes.

Knowledge management (KM) plays a key role in this process. It supports decision-making and adaptability during disruption (Wang et al., 2016). Knowledge sharing and learning improve post-crisis adaptation (Evenseth et al., 2022). Evidence from small firms shows that KM capabilities increase business resilience (Zayed et al., 2022). Reviews confirm a strong link between KM and performance (Georgescu et al., 2024). These findings suggest that KM can act as a mediator between DTL and resilience.

Cybersecurity readiness (CR) may strengthen this relationship. CR includes policies, controls, technical capabilities, and skills for handling cyber threats. Higher readiness improves security performance and overall outcomes (Hasan et al., 2021). Adoption of cybersecurity capabilities boosts performance in high-threat environments (Hasani et al., 2023). Studies on SMEs also find a positive relationship between cybersecurity systems, resilience, and performance (Al-Somali et al., 2024). Frameworks like NIST CSF 2.0 and DORA offer clear guidance for operationalizing readiness. CR can enhance the ability of KM to support resilience after cyber incidents.

Three research gaps emerge from this review. First, few studies test DTL, KM, and resilience together in a moderated-mediation model. Second, the moderating role of CR in the KM–resilience link is underexplored. Third, there is a lack of context-specific evidence for IT services and fintech, despite their exposure to cyber threats and regulatory demands. This study addresses these gaps. It examines the impact of DTL on ORS directly and in the mediating role of KM, while in the moderating role of CR.

Review of Literature

Digital Transformational Leadership (DTL)

DTL is a leadership approach that applies transformational leadership principles to digital contexts. It combines vision, inspiration, and individualized support with a focus on digital tools and change (Ly et al., 2023). Leaders practicing DTL promote a clear digital vision and mobilize people and

resources to achieve it. They also encourage the use of emerging technologies to improve efficiency and innovation (Kludacz-Alessandri et al., 2025). DTL has been linked to organizational agility and adaptability. Research shows that leaders who communicate a clear digital strategy and empower employees can increase the speed of decision-making (Ly et al., 2023). This is important in industries where technological change is constant. Leaders also build a culture that accepts experimentation and learning from failure, which helps organizations respond to uncertainty (Ye et al., 2025).

Studies highlight the connection between DTL and innovation. DTL fosters the development of new products, services, and processes through the integration of digital solutions (Kraus et al., 2021). This innovation orientation improves competitiveness in turbulent markets (Suwanto et al., 2022). In public sector cases, DTL has been found to improve service delivery by aligning digital transformation with policy goals (Boussaidi & Korbi, 2025). In crisis conditions, DTL supports resilience by guiding technology use and ensuring alignment between systems, processes, and people (Awad & Martín-Rojas, 2024). This integration allows organizations to maintain operations even during disruptions. Research also suggests that DTL affects resilience indirectly through mediating factors such as knowledge management, digital skills, and organizational learning (Kryvovyazyuk et al., 2023).

Overall, the literature positions DTL as a driver of change, adaptability, and innovation. However, most studies focus on direct effects. There is less empirical work on how DTL interacts with other organizational factors such as knowledge management and cybersecurity readiness to influence resilience, especially in IT services and fintech firms. This gap offers an important avenue for research.

Knowledge Management (KM)

KM refers to the processes of creating, storing, sharing, and applying knowledge to achieve organizational goals (Nonaka, 2009). Effective KM enables employees to access relevant information when needed. It also ensures that critical knowledge is retained and transferred, even when staff turnover occurs (Cegarra-Navarro et al., 2016). In dynamic environments, KM enhances decision-making speed and quality (Andreeva & Kianto, 2012). KM supports adaptability during disruptions. Organizations with structured KM processes can learn from past incidents and apply lessons quickly (Evenseth et al., 2022). This capability is essential for resilience because it reduces recovery time and limits operational losses (Bolisani & Bratianu, 2017). KM also fosters innovation by combining diverse knowledge sources into new solutions (Martínez-Peláez et al., 2024).

Several studies link KM to performance outcomes. Evidence from SMEs shows that KM practices improve business resilience and competitiveness (Zayed et al., 2022). In large organizations, KM increases operational efficiency and reduces duplication of effort (Georgescu et al., 2024). Research in digital transformation contexts finds that KM mediates the relationship between leadership and organizational performance (Kryvovyazyuk et al., 2023). This suggests that KM can translate leadership vision into practical, coordinated action. KM effectiveness depends on both technology and culture. Digital tools such as intranets, collaboration platforms, and databases facilitate knowledge storage and retrieval (Alavi & Leidner, 2001). However, without a culture of trust and knowledge sharing, these systems may be underused (Wang & Noe, 2010). Leaders play a role in fostering openness and rewarding knowledge-sharing behaviors (Donate & de Pablo, 2015).

In cybersecurity contexts, KM can integrate threat intelligence, incident reports, and best practices. This integration allows organizations to respond faster to new attacks and maintain continuity (Hasan et al., 2021). Despite these advantages, few empirical studies explore KM's mediating role between leadership and resilience, particularly in IT services and fintech firms. This gap warrants further investigation.

Organizational Resilience (ORS)

ORS refers to the ability of a firm to anticipate, absorb, adapt to, and recover from disruptions (Duchek, 2020). It is a dynamic capability that develops before, during, and after crises (Conz & Magnani, 2020). ORS enables organizations to maintain operations under stress and to return to normal or improved states afterward (Annarelli & Nonino, 2016). Scholars emphasize that resilience is built through leadership, culture, and routines. Leadership provides direction and commitment during uncertainty (Bhamra et al., 2011). Culture fosters trust and collaboration, which are essential for coordinated responses (Ortiz-de-Mandojana & Bansal, 2016). Routines, such as risk assessments and scenario planning, improve preparedness (McManus et al., 2008).

ORS is increasingly linked to organizational performance. Firms with high resilience recover faster from disruptions and suffer less financial loss (Kantur & İşeri-Say, 2012). In high-technology sectors, resilience supports continuous innovation and market competitiveness (Somers, 2009). Research also finds that resilience enhances employee well-being by reducing uncertainty during crises (Sharma & Sharma, 2020). The drivers of resilience include resource flexibility, information flow, and adaptive capacity (Lengnick-Hall et al., 2011). Resource flexibility ensures that organizations can reallocate assets when conditions change. Information flow allows decision-makers to respond quickly. Adaptive capacity involves learning from disruptions and integrating lessons into future planning (Duchek, 2020).

In digital environments, resilience depends heavily on the ability to manage knowledge and respond to cyber threats. IT service and fintech firms require rapid recovery from incidents to avoid customer loss and reputational harm (Hasan et al., 2021). Regulatory frameworks such as the Digital Operational Resilience Act highlight the importance of ORS in safeguarding financial stability. Although the literature offers extensive conceptual frameworks, empirical studies that integrate leadership, knowledge management, and cybersecurity readiness as predictors of ORS remain limited. This creates an opportunity for research in high-risk digital service sectors.

Cybersecurity Readiness (CR)

CR refers to the ability to prevent, detect, respond to, and recover from cyber incidents. It includes governance, technical controls, skilled personnel, and tested response plans (Al-Somali et al., 2024). CR is not only a technology issue. It is an organizational capability that requires policies, culture, and continuous improvement (Cram et al., 2017). Standards and frameworks define its core elements. ISO/IEC 27001 sets requirements for information security management systems. It covers risk assessment, controls, and continual improvement (Malatji, 2023). NIST CSF 2.0 adds a "Govern" function. It links security to enterprise risk and board oversight (NIST, 2024).

Empirical studies link CR to outcomes. Higher levels of readiness associate with stronger security performance and better organizational results (Hasan et al., 2021). Adoption of cybersecurity capabilities predicts performance in high-threat settings (Hasani et al., 2023). Employee behavior is central to readiness. Policy design and deterrence mechanisms improve compliance with security rules (Herath & Rao, 2009). Social and cognitive factors also shape compliance, which affects incident likelihood and impact. Awareness programs help, but they need careful design to change behavior in practice (Bada et al., 2019).

Incident response capability is a major component of CR. Organizations with defined roles, playbooks, and post-incident reviews recover faster (Bartnes et al., 2016). Evidence from incident management research shows that coordinated detection, containment, and learning reduce repeat events (Ahmad et al., 2012). Sector guidance reinforces these findings. The Financial Stability Board sets effective practices for response and recovery in financial institutions (FSB, 2020). The European Union's DORA turns many of these practices into binding requirements for financial entities.

CR matters for resilience. It enables continuity of operations, limits customer harm, and supports regulatory compliance after attacks. For IT services and fintech, readiness must address supply chain risk, third-party access, and data protection at scale (Verizon, 2024). Readiness also relies on sound knowledge flows. Integrating threat intelligence, incident lessons, and best practices into daily routines strengthens adaptive capacity and supports recovery (Hasan et al., 2021). The literature therefore positions CR as a moderator that can amplify the effect of knowledge management on resilience in data-intensive services.

Digital Transformational Leadership and Knowledge Management

The Knowledge-Based View (KBV) sees knowledge as the most important resource for competitive advantage (Stoian et al., 2024). Leaders shape how knowledge is created, shared, and applied. In digital environments, leadership style influences both the culture and systems that support knowledge management. Digital transformational leadership combines a strong vision with the ability to inspire people to use digital tools effectively (Ly et al., 2023). Under KBV, such leaders act as architects of knowledge processes, guiding how organizational knowledge is structured and mobilized.

Empirical evidence shows that transformational leaders foster trust, openness, and learning conditions that encourage knowledge sharing (Donate & de Pablo, 2015). In digital contexts, leaders also select and promote the use of collaborative platforms, analytics tools, and knowledge repositories (Chen et al., 2023). These actions increase knowledge accessibility and quality. In Pakistani IT and fintech firms, leaders must manage large volumes of sensitive customer data and rapidly changing technical knowledge. The sector is also under pressure from global competition and regulatory changes. Leaders who can set a clear digital vision and support its execution can improve KM practices by aligning people, processes, and technology. This is consistent with KBV's focus on leveraging internal knowledge for strategic advantage. The hypothesis therefore predicts that DTL will have a positive and significant impact on KM in such organizations (see figure 1).

H1: *Digital transformational leadership has a positive and significant effect on knowledge management.*

Knowledge Management and Organizational Resilience

KBV argues that firms with superior knowledge assets can respond more effectively to change. Knowledge management ensures that valuable information is captured, organized, and used in decision-making (Grant, 2015). When disruptions occur, such as cyber incidents, knowledge about prior responses, technical solutions, and best practices becomes essential for rapid recovery (Evenseth et al., 2022). Empirical research supports this link. Structured KM processes improve adaptability and reduce downtime during crises (Cegarra-Navarro et al., 2016). Resilience is strengthened when organizations can quickly access knowledge about threats, responses, and mitigation strategies (Zayed et al., 2022). This fits KBV's view that knowledge, when effectively applied, is a strategic capability that enhances survival.

In Pakistani IT and fintech firms, resilience is critical due to the sensitivity of customer data and the financial impact of service interruptions. KM can integrate cyber threat intelligence, compliance requirements, and client communication protocols into daily operations. This improves the organization's ability to maintain operations during disruptions and to adapt to new risks. The hypothesis predicts that effective KM will positively and significantly influence organizational resilience in these contexts.

H2: *Knowledge management has a positive and significant effect on organizational resilience.*

Digital Transformational Leadership and Organizational Resilience

From a KBV perspective, leadership determines how knowledge is harnessed to adapt and recover. Digital transformational leadership fosters a culture of learning, innovation, and adaptability (Ly et al., 2023). These qualities are essential for resilience, which depends on rapid access to relevant information and coordinated action (Duchek, 2020). Empirical studies indicate that transformational leaders enhance organizational resilience by motivating employees, supporting innovation, and aligning technology with strategy (Ye et al., 2025). In digital contexts, leaders facilitate the use of information systems and analytics to monitor threats and identify response options (Awad & Martín-Rojas, 2024). These actions improve preparedness and recovery capacity. For Pakistani IT and fintech organizations, where digital infrastructures are core to operations, leadership plays a direct role in resilience. Leaders must ensure that teams are ready for disruptions and have the resources and skills to respond. While KM can mediate this link, DTL can also directly enhance resilience by setting priorities, mobilizing support, and maintaining morale during crises. The hypothesis predicts a positive and significant effect of DTL on resilience in such organizations.

H3: *Digital transformational leadership has a positive and significant effect on organizational resilience.*

Mediation Role of Knowledge Management

KBV emphasizes that knowledge processes translate strategic intent into operational capability. DTL provides vision and resources, but KM is the mechanism that embeds this vision into routines and responses (Grant, 2015). Without strong KM systems, leadership's influence on resilience may be weakened. Studies support this mediating role. Leadership improves resilience indirectly through its effect on knowledge sharing and learning (Evenseth et al., 2022). Chen et al. (2023) found that digital leadership enhanced performance through KM practices. This aligns with KBV, which argues that knowledge must be organized and applied to generate strategic outcomes. In Pakistani IT and fintech firms, leaders face complex digital ecosystems with high cybersecurity demands. They can inspire and direct teams, but resilience depends on the ability to store, retrieve, and use relevant information under pressure. KM bridges this gap. It captures threat intelligence, incident reports, and recovery strategies, making them available when needed. The hypothesis predicts that KM mediates the relationship between DTL and organizational resilience in such firms.

H4: *Knowledge management mediates the relationship between digital transformational leadership and organizational resilience.*

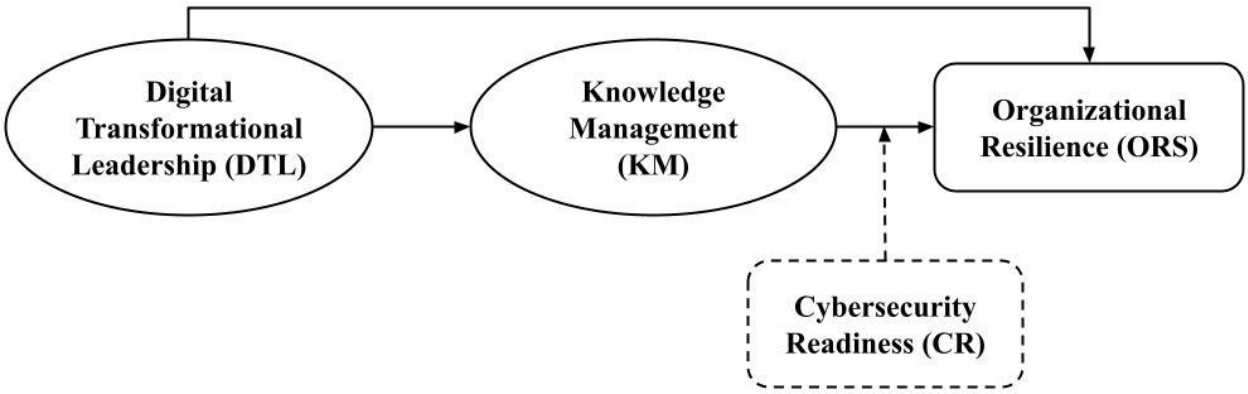

Figure 1. Conceptual Framework | *Source:* Author

Moderating Role of Cybersecurity Readiness

From a KBV lens, knowledge alone is not enough; it must be supported by the right capabilities. Cybersecurity readiness (CR) enhances the value of KM by ensuring that knowledge about threats and responses can be applied effectively. CR includes tools, skills, and protocols for detecting and managing incidents (Von Solms & Von Solms, 2018). Empirical evidence shows that organizations with higher CR respond faster and suffer less damage from cyber incidents (Hasan et al., 2021). CR ensures that knowledge is integrated into monitoring systems, incident response plans, and recovery strategies (Hove & Tårnes, 2013). This alignment increases the impact of KM on resilience. In Pakistani IT and fintech sectors, where cyber threats are frequent and complex, CR is essential for operational continuity. High CR means that KM outputs, such as threat intelligence and best practices, are acted upon quickly and effectively. When CR is low, even well-structured knowledge may remain unused or misapplied. The hypothesis predicts that CR will strengthen the KM–resilience relationship in such organizations.

H5: *Cybersecurity readiness positively moderates the relationship between knowledge management and organizational resilience, such that the relationship is stronger when cybersecurity readiness is high.*

Methods

Research Design

The study targeted managerial-level employees in the Pakistani IT services and fintech sectors. These sectors were chosen because they handle sensitive customer data and face high exposure to digital disruptions and cybersecurity risks. Managers were selected as the unit of analysis due to their involvement in strategic decision-making, knowledge management processes, and resilience planning. This choice aligns with the KBV, which emphasizes the role of managerial capabilities in leveraging organizational knowledge resources (Grant, 2015). The population comprised managers from registered IT services and fintech firms operating in major business hubs such as Karachi, Lahore, and Islamabad. These cities host the majority of Pakistan's technology and financial innovation companies, making them appropriate for the study's context. To ensure diversity, firms of varying sizes, service portfolios, and market segments were included. The sampling frame was drawn from professional networks, LinkedIn groups, and industry directories. Purposive sampling was employed, consistent with other leadership and KM studies in specialized sectors (Podsakoff et al., 2003).

Measures

All constructs were measured using previously validated scales to ensure content validity and comparability with prior research. Each construct was assessed on a 5-point Likert scale ranging from 1 ("strongly disagree") to 5 ("strongly agree"). Digital transformational leadership was measured using six items adapted from Chen and Chang (2013) and (Podsakoff et al., 1996), consistent with Ly (2023). The scale captures leaders' ability to inspire, guide, and engage teams toward digital transformation goals. Knowledge management was measured with 23 items adapted from Almashari et al. (2002), (Kulkarni & St Louis, 2003), and Lee et al. (2005), consistent with (Rašula et al., 2012). The items cover knowledge acquisition, sharing, and application across three dimensions: knowledge, information technology, and organization. Organizational resilience was measured using a four-item scale adapted from (Ambulkar et al., 2015). The scale assesses the organization's capacity to adapt and respond to disruptions while maintaining operational performance. Finally, cybersecurity readiness was measured using a 10-item scale adapted from Liu et al. (2018) and Hasan et al. (2021). The scale covers four dimensions: prevention capability, detection capability, response capability, and recovery capability.

Data Collection

An online survey method was employed due to the geographical dispersion of respondents and the ease of reaching technology professionals through digital platforms. This approach also reduced administrative costs and data entry errors (Dillman et al., 2014). The survey was distributed via email and LinkedIn, with a cover letter explaining the study's purpose, assuring confidentiality, and requesting voluntary participation. Screening questions ensured that respondents met the inclusion criteria of being managers with a minimum of a bachelor's degree and at least one year of experience in their current organization. Multiple reminders were sent to increase response rates, a strategy shown to improve participation in organizational surveys (Baruch & Holtom, 2008). Data was collected over eight weeks, allowing sufficient time for follow-ups and for respondents to complete the survey without time pressure.

A total of 600 online survey invitations were distributed. From these, 450 responses were received, resulting in a response rate of 75%. After data screening for missing values, outliers, and inconsistent responses, 430 valid responses were retained for analysis. This sample size exceeds the minimum threshold suggested by (Kline, 2023) for structural equation modeling (SEM) and provides adequate statistical power for hypothesis testing. During data collection, the respondents were informed that their participation is voluntary, and they can withdraw at any time without any intimation. Also, they were ensured that their responses will be kept confidential and data will only be used for this study purposes.

Data Analysis

Data was analyzed using SPSS version 26 and PROCESS Macro (Hayes, 2018). Before hypothesis testing, data cleaning was performed. For missing values' identification, frequency distribution was utilized; however, Mahalanobis Distance test was employed for identifying outliers. Normality was checked through skewness and kurtosis statistics. Common method bias was assessed using Harman's single-factor test (Podsakoff et al., 2003). Reliability was assessed using Cronbach's alpha. Hypotheses were tested using PROCESS Macro, Model 4 for mediation (H4) and Model 14 for moderated mediation (H5). Bootstrapping with 5,000 resamples was employed to obtain bias-corrected confidence intervals for indirect and interaction effects. The significance of direct effects (H1, H2, H3) was examined through regression coefficients, with p-values less than 0.05 considered significant. The choice of PROCESS Macro was justified by its ability to estimate complex mediation and moderation models within the same framework (Hayes, 2018).

Results and Findings

Data Cleaning

The dataset of 430 responses collected was examined for quality before statistical analysis. Missing values were first assessed through frequency distribution. This method allows the identification of unanswered items or irregular patterns in responses (Hair Jr et al., 2019). The analysis showed no missing value in the dataset, confirming that all participants completed the survey items in full. This ensures that no bias was introduced from data imputation or case deletion. Outliers were then examined using the Mahalanobis Distance Test. This multivariate technique detects unusual response patterns that deviate significantly from the centroid of all responses (Tabachnick & Fidell, 2013). No significant outliers were identified, indicating that all cases fell within the acceptable range for inclusion in the analysis. The absence of outliers reduces the likelihood of distortion in regression estimates and effect sizes (Aguinis et al., 2013).

Common method bias (CMB) was assessed because all variables were measured using self-reported survey data, which can inflate correlations if bias is present (Podsakoff et al., 2003). Harman's single-factor test was used, in which all items are entered into an unrotated exploratory factor analysis to see if a single factor accounts for most of the variance. The first factor explained 21.7% of the variance, which is well below the 50% threshold suggested by Podsakoff et al. (2003). This result suggests that CMB was not a significant concern in this study. Data normality was tested through skewness and kurtosis values for each variable. Skewness measures asymmetry in the distribution, while kurtosis assesses the peakedness relative to a normal distribution (Field, 2018). According to Kline (2023), skewness values between -3 and +3 and kurtosis values between -10 and +10 are acceptable for SEM or regression analysis. All variables in Table 2 had skewness values ranging from -0.45 to -0.36 and kurtosis values from -0.55 to -0.47, which are well within acceptable limits. These results indicate that the data met the assumption of normality required for regression-based analyses, including the PROCESS Macro used in this study. The data were therefore suitable for further hypothesis testing.

Demographic Profile

The sample consisted of 430 managerial-level employees from IT services and fintech organizations in Pakistan. The majority were male (81.4%), with females representing 18.6%. Most respondents were between 26 and 35 years old (44.2%), followed by 36–45 years (32.6%), indicating a relatively young and mid-career managerial workforce. In terms of education, nearly half held a master's degree (46.5%), while 34.9% had a bachelor's degree, 14% had an MPhil, and 4.7% held a PhD or higher qualification. This reflects a highly educated sample, consistent with the knowledge-intensive nature of the industry.

Regarding professional experience, 27.9% had 10–13 years, 25.6% had 2–5 years, and 24.4% had more than 14 years of experience, suggesting a balanced representation of mid- and senior-level managers. Only 1.2% had less than one year of experience, ensuring that most participants had substantial exposure to organizational processes, leadership, and cybersecurity challenges. This demographic composition supports the reliability of the responses in reflecting informed managerial perspectives.

Table 1. Demographic Characteristics

		Frequency	Percent
Gender	Male	350	81.4
	Female	80	18.6
	Total	430	100
Age	≤25	20	4.7
	26-35	190	44.2
	36-45	140	32.6
	46-55	65	15.1
	56 and above	15	3.5
	Total	430	100
Qualification	Bachelor	150	34.9
	Master	200	46.5
	MPhil	60	14
	PhD or above	20	4.7
	Total	430	100
Experience	≤1	5	1.2
	2-5	110	25.6
	6-9	90	20.9
	10-13	120	27.9
	14 and above	105	24.4
	Total	430	100

Descriptive Statistics

Descriptive statistics provide an overview of the central tendency and variability of the variables measured. As shown in Table 2, the mean scores ranged from 3.75 to 3.85 on a five-point Likert scale, indicating generally positive perceptions of DTL, KM, ORS, and CR. The highest mean was for DTL (3.85), suggesting that respondents perceived their leaders as actively engaging in digital transformation initiatives. The lowest mean was for CR (3.75), indicating slightly lower but still positive perceptions of readiness to address cyber threats. Standard deviation values ranged from 0.70 to 0.74, showing moderate variability in responses. This suggests that while overall perceptions were favorable, there were differences among respondents in the extent to which these practices and capabilities were present in their organizations. These variations are important for examining relationships among the study's variables.

Table 2. Descriptive Statistics

				Skewness		Kurtosis	
	Cronbach's Alpha	Mean	SD	Statistic	SE	Statistic	SE
Digital Transformational Leadership	0.91	3.85	0.72	-0.45	0.12	-0.55	0.24
Knowledge Management	0.94	3.78	0.7	-0.38	0.12	-0.49	0.24
Organizational Resilience	0.89	3.80	0.74	-0.4	0.12	-0.5	0.24
Cybersecurity Readiness	0.92	3.75	0.71	-0.36	0.12	-0.47	0.24

Reliability

Reliability refers to the internal consistency of measurement items, indicating the degree to which they consistently measure a construct (Bell et al., 2022). In this study, Cronbach's alpha was used to assess reliability. According to Nunnally and Bernstein (1994), alpha values above 0.70 are acceptable for research purposes, with values above 0.80 considered good and above 0.90 considered excellent. As shown in Table 2, all constructs demonstrated high reliability: DTL (α = 0.91), KM (α = 0.94), ORS (α = 0.89), and CR (α = 0.92). These values exceed the recommended thresholds, indicating that the items within each scale were highly consistent in measuring their respective constructs. This high reliability supports the validity of subsequent regression, mediation, and moderation analyses.

Hypotheses Testing

Hypothesis testing was conducted using SPSS and PROCESS Macro, with bootstrapping for confidence intervals. Direct, indirect, and moderating effects were assessed to evaluate the proposed relationships.

The direct effect of DTL on KM was positive and significant (β = 0.62, t = 12.40, $p < 0.001$, LLCI = 0.52, ULCI = 0.72). A positive coefficient indicates that higher levels of digital transformational leadership are associated with higher levels of knowledge management. This supports KBV's assertion that leadership plays a central role in enabling knowledge creation, sharing, and application (Grant, 1996). Since the confidence interval does not include zero, H1 is accepted.

The effect of KM on ORS was also positive and significant (β = 0.54, t = 9.00, $p < 0.001$, LLCI = 0.42, ULCI = 0.66). This means organizations with stronger KM practices tend to have greater resilience. The result aligns with previous studies highlighting KM as a driver of adaptive capacity during disruptions (Cegarra-Navarro et al., 2016); hence, H2 is therefore accepted.

DTL had a direct, positive effect on ORS (β = 0.38, t = 5.43, $p < 0.001$, LLCI = 0.24, ULCI = 0.52). This indicates that leaders who champion digital transformation also enhance organizational resilience, even without the mediating role of KM. This supports earlier findings that leadership directly influences resilience by aligning resources and motivating adaptive responses (Ye et al., 2025); hence, H3 is accepted.

Table 3. Direct Effects

Hypotheses		Coeff.	se	t	p	LLCI	ULCI
H1:	DTL → KM	0.62	0.05	12.4	0.000	0.52	0.72
H2:	KM → ORS	0.54	0.06	9.00	0.000	0.42	0.66
H3:	DTL → ORS	0.38	0.07	5.43	0.000	0.24	0.52

The indirect effect of DTL on ORS via KM was significant (β = 0.34, SE = 0.04, $p < 0.001$, LLCI = 0.26, ULCI = 0.42). Since the confidence interval excludes zero, KM is confirmed as a mediator. This means part of the effect of DTL on ORS operates through enhanced knowledge processes. This supports KBV's claim that leadership shapes resilience primarily by enabling effective use of organizational knowledge; hence, H4 is accepted.

Table 4. Indirect Effects

Hypotheses		Coeff.	se	p	LLCI	ULCI
H4:	DTL → KM → ORS	0.34	0.04	0.000	0.26	0.42

The interaction effect of KM and CR on ORS was positive and significant (β = 0.11, t = 3.67, p = 0.003, LLCI = 0.05, ULCI = 0.17). This suggests that the positive relationship between KM and ORS is stronger when cybersecurity readiness is high. Under KBV, this indicates that the value of knowledge is amplified when supported by strong cyber capabilities that ensure its secure and timely application (Hasan et al., 2021). This result supports H5.

Table 5. Moderating Effects

	Hypotheses	Coeff.	se	p	LLCI	ULCI
H5:	KM × CR → ORS	0.11	0.03	0.003	0.05	0.17

Overall, all hypotheses were supported. The results confirm that in Pakistani IT services and fintech organizations, digital transformational leadership fosters resilience both directly and indirectly through knowledge management, and that cybersecurity readiness strengthens the KM–resilience link. This integrated model offers both theoretical support for KBV and practical guidance for resilience-building in high-risk digital sectors.

Discussion and Conclusion

Discussion

The results confirm that DTL has a significant and positive effect on KM and ORS. The strong link between DTL and KM aligns with the Knowledge-Based View, which emphasizes leadership's role in shaping how knowledge is created, shared, and applied (Grant, 1996). This is consistent with earlier research by Donate and de Pablo (2015) and Chen et al. (2023), who found that transformational leaders promote knowledge sharing and foster a culture of learning. In the Pakistani IT and fintech context, leaders who articulate a clear digital vision and enable the use of technology were found to enhance KM effectiveness, likely because these sectors rely heavily on timely and secure knowledge flows.

The positive relationship between KM and ORS supports previous findings that structured knowledge processes improve adaptability and recovery from disruptions (Cegarra-Navarro et al., 2016; Zayed et al., 2022). In this study, KM appears to be a critical capability that allows IT and fintech firms to integrate threat intelligence, operational experience, and recovery strategies. Given the high stakes of customer data protection, KM provides both the content and the processes needed to maintain performance under pressure.

The direct impact of DTL on ORS confirms that leadership also drives resilience without necessarily passing through KM. This supports the view of Duchek (2020) and Ye et al. (2025) that leaders play a role in mobilizing resources, maintaining morale, and coordinating responses during disruptions. In practice, this means that effective digital leaders in Pakistan's IT and fintech sectors can prepare teams for unforeseen challenges by instilling confidence and clarity in times of uncertainty.

The mediation analysis showed that KM partially mediates the relationship between DTL and ORS. This is consistent with the idea that while leadership sets the strategic direction and creates enabling conditions, it is through knowledge processes that these intentions are translated into

coordinated, informed, and adaptive action (Evenseth et al., 2022). In this study's context, leaders' influence on resilience is amplified when they ensure that knowledge resources are accessible, relevant, and updated to meet changing cyber and market conditions.

The moderation results indicate that cybersecurity readiness strengthens the KM–ORS link. This aligns with findings by Hasan et al. (2021) and Liu et al. (2018), showing that readiness in prevention, detection, and recovery enhances the value of knowledge by ensuring it can be applied securely and effectively. In Pakistani IT and fintech firms, where cyber risks are both frequent and complex, high CR means that knowledge about threats and responses can be acted upon quickly, reducing the risk of service disruption and reputational damage. This suggests that KM systems should not be developed in isolation from cybersecurity capabilities, as their combined strength produces higher resilience outcomes.

Overall, these findings present an integrated view where leadership, knowledge processes, and cybersecurity readiness jointly contribute to resilience. The results not only reinforce the KBV's emphasis on knowledge as a strategic resource but also highlight the enabling role of security readiness in translating knowledge into operational continuity.

Implications

Theoretically, this study extends the KBV by demonstrating that the path from leadership to resilience is both direct and mediated through KM. It also shows that the KM–resilience link is contingent upon CR, adding a contextual layer to the KBV by integrating security readiness into the framework. This aligns with calls for more nuanced models that include boundary conditions in knowledge–performance relationships (Wang et al., 2014). The moderated mediation design strengthens the argument that KM alone is insufficient without robust capabilities to protect and apply it.

Practically, the results suggest that IT and fintech firms should invest in leadership development programs that emphasize digital vision, change management, and technology adoption skills. KM systems should be designed with both accessibility and security in mind, ensuring that employees can access critical information when needed without compromising data protection. CR should be embedded into organizational routines, including regular training, incident simulations, and continuous monitoring, to ensure that knowledge can be acted upon during crises. Senior leaders should treat KM and CR not as separate initiatives but as interconnected pillars of resilience planning.

Limitations and Future Indications

This study relied on cross-sectional survey data, which limits causal inference. Longitudinal studies could better capture how leadership, KM, and CR evolve over time. The research focused on Pakistani IT and fintech sectors; results may differ in other cultural or industry contexts. Future studies could compare across industries or explore additional moderators, such as organizational culture or digital maturity. Including objective performance metrics alongside perceptions could also strengthen validity.

References

1. Aguinis, H., Gottfredson, R. K., & Joo, H. (2013). Best-practice recommendations for defining, identifying, and handling outliers. *Organizational research methods*, *16*(2), 270-301.

2. Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). Organizational cybersecurity systems and sustainable business performance of small and medium enterprises (SMEs) in Saudi Arabia: The mediating and moderating role of cybersecurity resilience and organizational culture. *Sustainability*, *16*(5), 1880.
3. Alavi, M., & Leidner, D. E. (2001). Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS quarterly*, 107-136.
4. Almashari, M., Zairi, M., & Alathari, A. (2002). An empirical study of the impact of knowledge management on organizational performance. *Journal of Computer Information Systems*, *42*(5), 74-82.
5. Ambulkar, S., Blackhurst, J., & Grawe, S. (2015). Firm's resilience to supply chain disruptions: Scale development and empirical examination. *Journal of operations management*, *33*, 111-122.
6. Andreeva, T., & Kianto, A. (2012). Does knowledge management really matter? Linking knowledge management practices, competitiveness and economic performance. *Journal of Knowledge Management*, *16*(4), 617-636.
7. Annarelli, A., & Nonino, F. (2016). Strategic and operational management of organizational resilience: Current state of research and future directions. *Omega*, *62*, 1-18.
8. Awad, J. A., & Martín-Rojas, R. (2024). Digital transformation influence on organisational resilience through organisational learning and innovation. *Journal of Innovation and Entrepreneurship*, *13*(1), 69.
9. Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.
10. Bartnes, M., Moe, N. B., & Heegaard, P. E. (2016). The future of information security incident management training: A case study of electrical power companies. *Computers & Security*, *61*, 32-45.
11. Baruch, Y., & Holtom, B. C. (2008). Survey response rate levels and trends in organizational research. *Human relations*, *61*(8), 1139-1160.
12. Bell, E., Bryman, A., & Harley, B. (2022). *Business research methods*. Oxford university press.
13. Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: the concept, a literature review and future directions. *International Journal of Production Research*, *49*(18), 5375-5393.
14. Bolisani, E., & Bratianu, C. (2017). The elusive definition of knowledge. In *Emergent knowledge strategies: Strategic thinking in knowledge management* (pp. 1-22). Springer.
15. Boussaidi, A., & Korbi, K. (2025). The role of transformational leadership in promoting digital transformation through employee engagement in public administration. *International Journal of Public Leadership*.
16. Cegarra-Navarro, J.-G., Soto-Acosta, P., & Wensley, A. K. (2016). Structured knowledge processes and firm performance: The role of organizational agility. *Journal of Business Research*, *69*(5), 1544-1549.
17. Chen, Y.-S., & Chang, C.-H. (2013). The determinants of green product development performance: Green dynamic capabilities, green transformational leadership, and green creativity. *Journal of business ethics*, *116*, 107-119.
18. Conz, E., & Magnani, G. (2020). A dynamic perspective on the resilience of firms: A systematic literature review and a framework for future research. *European Management Journal*, *38*(3), 400-412.
19. Cram, W. A., Proudfoot, J. G., & D'arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, *26*(6), 605-641.

20. Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). Internet, phone, mail, and mixed-mode surveys: The tailored design method. *Indianapolis, Indiana*, *17*.
21. Donate, M. J., & de Pablo, J. D. S. (2015). The role of knowledge-oriented leadership in knowledge management practices and innovation. *Journal of Business Research*, *68*(2), 360-370.
22. Duchek, S. (2020). Organizational resilience: a capability-based conceptualization. *Business Research*, *13*(1), 215-246.
23. EIOPA. (2025). *Digital Operational Resilience Act (DORA)*. European Insurance and Occupational Pensions Authority (EIOPA). Retrieved 28 July from https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
24. European Banking Authority. (2025). *Digital Operational Resilience Act*. European Banking Authority. Retrieved 3 August from https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act
25. Evenseth, L. L., Sydnes, M., & Gausdal, A. H. (2022). Building organizational resilience through organizational learning: A systematic review. *Frontiers in Communication*, *7*, 837386.
26. Georgescu, I., Bocean, C. G., Vărzaru, A. A., Rotea, C. C., Mangra, M. G., & Mangra, G. I. (2024). Enhancing organizational resilience: The transformative influence of strategic human resource management practices and organizational culture. *Sustainability*, *16*(10), 4315.
27. Grant, R. M. (2015). Knowledge-Based View. *Wiley encyclopedia of management*, 1-2.
28. Hair Jr, J., Page, M., & Brunsveld, N. (2019). *Essentials of business research methods*. Routledge.
29. Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*, 102726.
30. Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, *3*(5), 97.
31. Hayes, A. F. (2018). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. Guilford publications.
32. He, Z., Huang, H., Choi, H., & Bilgihan, A. (2023). Building organizational resilience with digital transformation. *Journal of Service Management*, *34*(1), 147-171.
33. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.
34. Hove, C., & Tårnes, M. (2013). *Information security incident management: an empirical study of current practice* Institutt for telematikk].
35. IBM. (2024). *Cost of a Data Breach*. IBM. Retrieved 1 August from https://wp.table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf
36. IMF. (2024). *Global Financial Stability Report*. International Monetary Fund (IMF). Retrieved 2 August from https://www.elibrary.imf.org/display/book/9798400257704/9798400257704.xml
37. Kantur, D., & İşeri-Say, A. (2012). Organizational resilience: A conceptual integrative framework. *Journal of management & organization*, *18*(6), 762-773.
38. Kline, R. B. (2023). *Principles and practice of structural equation modeling*. Guilford publications.

39. Kludacz-Alessandri, M., Hawrysz, L., Żak, K., & Zhang, W. (2025). The impact of digital transformational leadership on digital intensity among primary healthcare entities: a moderated mediation model. *BMC Health Services Research*, *25*(1), 117.
40. Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N. (2021). Digital transformation: An overview of the current state of the art of research. *Sage Open*, *11*(3), 21582440211047576.
41. Kryvovyazyuk, I., Britchenko, I., Smerichevskyi, S., Kovalska, L., Dorosh, V., & Kravchuk, P. (2023). Digital transformation and innovation in business: the impact of strategic alliances and their success factors.
42. Kulkarni, U., & St Louis, R. (2003). Organizational self assessment of knowledge management maturity.
43. Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human resource management review*, *21*(3), 243-255.
44. Ly, B. (2024). The interplay of digital transformational leadership, organizational agility, and digital transformation. *Journal of the Knowledge Economy*, *15*(1), 4408-4427.
45. Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001: 2022. 2023 International conference on cyber management and engineering (CyMaEn),
46. Martínez-Peláez, R., Escobar, M. A., Félix, V. G., Ostos, R., Parra-Michel, J., García, V., Ochoa-Brust, A., Velarde-Alvarado, P., Félix, R. A., & Olivares-Bautista, S. (2024). Sustainable digital transformation for SMEs: A comprehensive framework for informed decision-making. *Sustainability*, *16*(11), 4447.
47. McManus, S., Seville, E., Vargo, J., & Brunsdon, D. (2008). Facilitated process for improving organizational resilience. *Natural hazards review*, *9*(2), 81-90.
48. NIST. (2024). *The NIST Cybersecurity Framework 2.0*. Retrieved 27 July from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
49. Nonaka, I. (2009). The knowledge-creating company. In *The economic impact of knowledge* (pp. 175-187). Routledge.
50. [Record #392 is using a reference type undefined in this output style.]
51. Ortiz-de-Mandojana, N., & Bansal, P. (2016). The long-term benefits of organizational resilience through sustainable business practices. *Strategic management journal*, *37*(8), 1615-1631.
52. Podsakoff, P. M., MacKenzie, S. B., & Bommer, W. H. (1996). Transformational leader behaviors and substitutes for leadership as determinants of employee satisfaction, commitment, trust, and organizational citize. *Journal of management*, *22*(2), 259-298.
53. Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology*, *88*(5), 879.
54. Rašula, J., Bosilj Vukšić, V., & Indihar Štemberger, M. (2012). The impact of knowledge management on organisational performance. *Economic and business review*, *14*(2), 3.
55. Sharma, S., & Sharma, S. K. (2020). Probing the links between team resilience, competitive advantage, and organizational effectiveness: Evidence from information technology industry. *Business Perspectives and Research*, *8*(2), 289-307.
56. Somers, S. (2009). Measuring resilience potential: An adaptive strategy for organizational crisis planning. *Journal of contingencies and crisis management*, *17*(1), 12-23.
57. Stoian, M.-C., Tardios, J. A., & Samdanis, M. (2024). The knowledge-based view in international business: A systematic review of the literature and future research directions. *International Business Review*, *33*(2), 102239.

58. Suwanto, S., Sunarsi, D., & Achmad, W. (2022). Effect of transformational leadership, servant leadershi, and digital transformation on MSMEs performance and work innovation capabilities. *Central European Management Journal*, *30*(4), 751-762.
59. Tabachnick, B. G., & Fidell, L. S. (2013). Using multivariate statistics (6. Baskı). *MA: Pearson*.
60. Troilo, M., Bouchet, A., Urban, T. L., & Sutton, W. A. (2016). Perception, reality, and the adoption of business analytics: Evidence from North American professional sport organizations. *Omega*, *59*, 72-83.
61. van Assen, M. F. (2020). Empowering leadership and contextual ambidexterity–The mediating role of committed leadership for continuous improvement. *European Management Journal*, *38*(3), 435-449.
62. Verizon. (2024). *Data Breach Investigation Report*. Verizon. Retrieved 28 July from https://www.verizon.com/business/resources/Tb2/infographics/2024-dbir-finance-snapshot.pdf
63. Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where? *Information & Computer Security*, *26*(1), 2-9.
64. Wang, S., & Noe, R. A. (2010). Knowledge sharing: A review and directions for future research. *Human resource management review*, *20*(2), 115-131.
65. Wang, W. Y., Pauleen, D. J., & Zhang, T. (2016). How social media applications affect B2B communication and improve business performance in SMEs. *Industrial marketing management*, *54*, 4-14.
66. WEF. (2024). *Global Cybersecurity Outlook*. World Economic Forum. Retrieved 2 August from https://www.weforum.org/publications/global-cybersecurity-outlook-2024/
67. Ye, Q. (2025). Digital leadership enhances organizational resilience by fostering job crafting: the moderating role of organizational culture. *Scientific Reports*, *15*(1), 24640.
68. Zayed, N. M., Edeh, F. O., Islam, K. M. A., Nitsenko, V., Polova, O., & Khaietska, O. (2022). Utilization of knowledge management as business resilience strategy for microentrepreneurs in post-COVID-19 economy. *Sustainability*, *14*(23), 15789.