JOURNAL OF HUMANITIES, HEALTH & SOCIAL SCIENCES
www.jhhss.com editor@jhhss.com

Impact of Technical Expertise, Service Assurance, and Cybersecurity Readiness on Decision-Making Efficiency: Mediating Role of Knowledge Sharing in the Telecom Sector of Jeddah, Saudi Arabia

[1]Ishfaq Rashid, [2] Saad Saeed & [3]Sayyid Kamran Hussain

1st Core NGN/IMS NOC Leader, STC, Jeddah, Saudi Arabia

2ndVisiting Lecturer, Department of Commerce, University of Sahiwal

3rdDepartment of Computer Science & I.T, Thal University Bhakkar, 30000, Punjab, Pakistan

KEYWORDS

Technical Expertise, Service Assurance, Cybersecurity Readiness Decision-Making Efficiency

ARTICLE HISTORY

Date of Submission:21-03-2025

Date of Acceptance:18-04-2025

Date of Publication:30-06-2025

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors

ABSTRACT

This study examines how technical expertise, service assurance mechanisms, and cybersecurity readiness influence decision-making efficiency in the telecommunications sector of Jeddah, Saudi Arabia. As telecom networks evolve to support advanced NGN and IMS infrastructures, ensuring secure, fault-resilient, and high-performing systems has become a strategic priority. Drawing on socio-technical systems theory and organizational knowledge frameworks, the research introduces knowledge sharing as a mediating variable to explore how organizational learning bridges the gap between technical systems and managerial decisions. The study targets telecom professionals involved in network integration, protocol management, and service assurance, particularly those operating Huawei platforms and managing VIP client services. Primary data will be collected through structured surveys and analyzed using Structural Equation Modeling (SEM). The results are expected to show that while technical and cybersecurity capabilities are critical, structured knowledge flows within teams significantly enhance decision-making quality. This research contributes to both engineering and social sciences by highlighting the strategic role of cyber-aware, technically competent teams in driving responsive and informed decision-making within Saudi Arabia's evolving telecom landscape.

Correspondence: Sayyid Kamran Hussain

Email: Sayyid.Kamran.Hussain22@gmail.com

Volume-Issue-Page Number: 3(2) 1-19

DOI: 10.61503/JHHSS/v3i2.66

Citation: Rashid, I., Saeed, S., & Hussain, S. K. (2025), Impact of Technical Expertise, Serv Assurance, and Cybersecurity Readiness on Decision-Making Efficiency: Mediat Role of Knowledge Sharing in the Telecom Sector of Jeddah, Saudi Arabia. *Journa Humanities, Health and Social Sciences, 3*(2), 1-19

1.0 Introduction

With the combination of sophisticated technologies and the rising cybersecurity risks, the telecommunications industry takes a leading role in the creation of new infrastructure, the implementation of digital services, and the implementation of Next-Generation Networks (NGN) and IP Multimedia Subsystems (IMS). This shift to these networks increases the challenge of maintaining secure, fault-tolerant and high-performing infrastructures. This complexity is even more evident in technologically ambitious economies like Saudi Arabia where digital transformation has emerged to be a pillar of programs like the Vision 2030 (Alqublan, 2021). In Jeddah, which is generally recognized to be a commercial and technological center, the telecom industry supports smart-city developments, digital inclusions, and connectivity. In this regard, practitioners working in this high-stakes setting are expected to make quick, informed and reliable decisions that meet technical standards yet fit organizational priorities and client expectations, especially when it comes to high-value or VIP services (Browder et al., 2022).

The interaction between the changing technologies and the organizational structures has highlighted the need to incorporate the socio-technical considerations in the telecom operations. Although investing in new systems and networks is of prime importance, these innovations should be accompanied by human capital that can interpret, respond to and optimize technical data. Effective decision-making therefore does not only rely on strong technologies but also on the overall competence, communication patterns and knowledge management abilities of the employees (Kudyba et al., 2020). Here, technical expertise, service assurance and cybersecurity readiness can be seen as the underlying capabilities that influence the manner in which decisions are made within complex, time-sensitive telecom settings. Such abilities are, however, incorporated into the larger organizational processes, which sometimes facilitate, and sometimes hinder, the continuity of knowledge. To explain the role of knowledge sharing in the mediation of technical factors and decision-making, it is possible to provide detailed insights into the ways telecom companies in Jeddah can attain operational agility and strategic alignment in an ever-changing technological environment (Mehrotra et al., 2024).

Technical expertise is the technical knowledge and practical skills that professionals apply, especially in network integration, fault management, and protocol optimization. Technical knowledge in the telecom environment includes knowledge of multi-vendor systems, advanced diagnostic tools, real-time troubleshooting and adherence to international telecom standards. This expertise is normally gained in the course of formal training, vendor certifications (e.g., Huawei, Cisco) and work experience (Tsang & Fuschi, 2020). It allows practitioners to troubleshoot anomalies at speed, program complicated systems efficiently and deploy robust infrastructure solutions. On the one hand, technical expertise is necessary to ensure the reliability of the system; on the other hand, it also contributes to the quality of decision-making as professionals are able to analyze technical data correctly and suggest the

effective solutions that may be both technically and business-oriented (Kitsios & Kapetaneas, 2022).

Service assurance refers to a collection of practices that are systematic in nature and are aimed at preserving and enhancing the quality of service, availability and reliability. It includes active surveillance, fault identification, performance tuning and adherence to service-level agreements (SLAs). In the case of high-value enterprise customers and VIP users, service assurance acts as a technical necessity as well as a strategic differentiator that has a direct impact on customer satisfaction and brand credibility (Gunz, 2023). Vigorous service-assurance systems provide real-time performance information and enable prompt reaction to arising challenges. Individuals involved in service assurance often have to make quick decisions on resource deployment, fault prioritization, and escalation control, and this is why it is necessary to find coherent knowledge exchange between technical and managerial spheres (Awamleh & Sicre, 2024).

Cybersecurity preparedness is the ability of an organization to predict, mitigate, respond and recover to cyber attacks in a way that reduces operational interference and data loss. In telecom networks, which are usually considered as critical infrastructure, cybersecurity preparedness entails the installation of sophisticated firewalls, intrusion detection systems, and encryption measures and the development of a culture of security awareness among the workforce. The consequences are dire: late or misguided decisions may have dire reputational, monetary and legal consequences (Flyvbjerg et al., 2021). Thus, cybersecurity preparedness requires both technical expertise and interdepartmental collaboration, and the importance of proper and timely knowledge sharing between the individuals engaged in incident response, threat intelligence, and risk mitigation is once again emphasized.

Even though all three areas of technical expertise, service assurance, and cybersecurity preparedness are critical in determining the results of operations, their efficiency is becoming dependent on organizational procedures that regulate communication, contextualization, and information usage. Knowledge sharing is a mediating construct that indicates how people share, combine, and utilize relevant information towards group objectives (Yin et al., 2020). Based on the organizational-learning theory and knowledge-based perspectives of the firm, knowledge sharing is not only considered as a means of transfer but as a strategic enabler that converts tacit and explicit knowledge into actionable knowledge. In high reliability industries like telecommunication where the rate of change is high and the cost of error is high, knowledge sharing aids teams to overcome information silos, redundancy, and collective intelligence in the decision making process (Alzaabi, 2024).

As a result, the connection between technical competence, service assurance, and cybersecurity preparedness and the efficiency of decision-making is not linear or direct; it depends on the strong knowledge-sharing practices. A technically skilled labor force can be inefficient when knowledge is fragmented, hoarded or not well codified. Similarly,

comprehensive service-assurance procedures may also become ineffective in cases where the stakeholders do not agree on performance measures or escalation procedures (Thillaiarasu et al., 2021). Cybersecurity preparedness, which requires actions to be coordinated across several departments, is especially vulnerable to communication and knowledge flow failures. Therefore, knowledge sharing is a mediating factor in the process of converting technical capabilities into sound, prompt, and data-based decisions (Ragazou et al., 2023).

The current study is rooted in the socio-technical systems theory that emphasizes interdependence of social and technical subsystems in the development of organizational effectiveness. In the case of telecommunications operations, this orientation implies that high performance cannot be based solely on technological capabilities, it must be aligned with human behaviors, organizational structure and cultural norms that encourage collaboration and learning. Knowledge based view of the firm also argues that knowledge is the most strategically important resource and its appropriate management defines the ability of a firm to adapt and innovate (Rialti et al., 2020). It is therefore postulated that technical inputs can only deliver better results in decision making when they are channeled through the vessel of internal knowledge sharing.

There are few empirical studies on these interconnected determinants in the telecommunications industry, especially in the emerging markets like Saudi Arabia. The literature is inclined to separate the study of technical competence, service quality, or cybersecurity practices and ignore their interplay in the multidimensional organizational environment. In addition, the mediating effect of knowledge sharing has only been given little emphasis in industries where the degree of technical intensity and operational risk is significantly high. The relationships are rarely put in context of the particular socio-economic and technological environment of Jeddah, which is characterized by a fast-paced urbanization, a growing digital infrastructure, and state-led innovation within the Vision 2030 (Syrén & Cederin, 2025). These gaps stimulate a context-sensitive, holistic research that not only determines the main predictors of efficiency in decision-making but also explains the organizational processes that make them effective in their functioning.

In line with this, the research problem aims at explaining how telecommunications organizations in Jeddah can enhance the effectiveness of decision-making in high-stress, technically demanding conditions using technical expertise, service-assuring systems, and cybersecurity preparedness and regulate these capabilities using internal knowledge-sharing processes. When service failures, security breaches, and operational inefficiencies tend to trigger a chain reaction of customer distrust and poor financial performance, improving the decision-making processes is not only a technical requirement but also a strategic priority in the industry (Gürpinar et al., 2023). By positioning this problem in the context of an integrated socio-technical and knowledge-based system, the research aims to produce practical knowledge

on the ways to balance the capabilities of systems with human judgment, and, in this way, to increase the responsiveness and resilience of organizations.

The importance of the research can be explained by the fact that it can be used in both theoretical and practical spheres. Academically, the work is a contribution to the existing body of knowledge since it has incorporated constructs of engineering management, organizational behavior, and information systems into a unified analytical framework. It expands the socio-technical system theory, as it tests the mediating role of knowledge sharing as empirically tested in a highly technical industry setting. It also adds value to the literature on decision making by looking at the interaction between cyber-technical preparedness and organizational learning processes (Loske, 2022). Practically, the results will be especially relevant to telecommunications operators in Saudi Arabia and the other emerging markets where technological development and organizational flexibility are critical. Defining the levers that affect the efficiency of decision-making, the study can guide training programs, knowledge management strategy, and operational policies that support the firm-level performance under technological disruption and cybersecurity threats (Adebanjo et al., 2021).

The context-specific nature of the study that focuses on Jeddah also allows a more detailed insight into how local telecommunications companies can be located within the global trends in technology, negotiating local regulatory, infrastructural, and cultural processes. The involvement of professionals in Huawei platforms and in management of VIP services is a strategic value due to the fact that these functions usually require real-time decision-making that involves high stakes in a situation of uncertainty and complexity. Such observations can inform policy frameworks, vendor relationships, and workforce development initiatives to enhance the digital ecosystem in Saudi Arabia. All in all, the study provides a topical and contextually relevant analysis of how telecommunications companies can leverage on both the technical and human capital to attain an efficient, informed and resilient decision making in an increasingly turbulent digital era.

2.0 Literature Review

The results of techno-organizational are dependent on how the technical capabilities, knowledge-sharing practices, and efficiency of decision-making interact. The interdependence is discussed in the contexts of the socio-technical systems (STS) theory and the knowledge-based view (KBV) of the firm. STS theory holds that the effectiveness of organizations is achieved by the mutual support of technical systems and social structures (Ang et al., 2024). According to this perspective, technologies do not produce the best results on their own but their usefulness comes when they are integrated into human systems that are able to interpret, adapt and use them. The model particularly stands out in high-reliability industries like the telecommunications industry where success in technical infrastructure cannot be disentangled with human knowledge, coordination and judgment (Ezukwoke, 2023).

At the same time, KBV holds that knowledge is the most critical strategic resource an organization can have and the ability to create, share, and use knowledge is the main source of competitive advantage. In high-tech and risk-sensitive environments, the efficiency of decision-making relies more and more not only on the technical skills of decision-makers but also on the integrity of the knowledge processes within an organization. Collectively, these views highlight the issue of examining how technical expertise, service assurance practices, and cybersecurity readiness promote effective decision-making by mediating knowledge-sharing activity (Ezukwoke, 2023).

The importance of technical expertise in organizational performance and quality of decisions is always emphasized in empirical studies. Technical expertise is defined as the experience, specialized knowledge and the ability to operate in a domain and is used to diagnose the problem properly, configure the system and use the available resources in the best possible way. In telecommunications where a failure of the system may have far reaching consequences, technically qualified personnel are essential in maintaining continuity in operations (Kosmowski et al., 2022). Research in infrastructure-based industries shows that technical expertise minimizes the duration it takes to determine root causes, improves the accuracy of fault remediation and builds confidence in strategic choices. In addition, highly competent staff are in a better position to assess trade-offs in resources allocation, network scalability, and exposure to risk. In the context of the changing technologies, like the NGN and IMS, lifelong learning and the knowledge of the specific platform protocols (as the one implemented in the Huawei systems) are the keys to ensuring the quality of your services and timely decision making. Even though technical expertise is often studied in isolation, new research acknowledges that its role in decision-making is enhanced when it is integrated into collaborative and knowledge-sharing cultures (Davidavičienė et al., 2020).

Along with the technical competence is the notion of service assurance, which has received a lot of coverage in the operational research and strategic management literature. Service assurance can be defined as an organized program that is intended to guarantee that telecommunications services are provided at acceptable quality, performance and reliability levels. It also includes network monitoring, performance analytics, SLA compliance, and fast fault management (Alzubaidi et al., 2023). Service assurance is a distinguishing factor in industries that provide services to high-value customers e.g. VIP corporate users or government agencies. Empirical evidence has shown that the presence of mature service assurance mechanisms leads to enhancement of customer satisfaction, minimization of churn, and operational efficiency. More to the point, these systems produce huge flows of performance and incident data, which are used to make managerial decisions. The strategic usefulness of these data however lies on the effectiveness of their interpretation and use (Hassani & MacFeely, 2023). As teams more proactively exchange knowledge about services, align on how to solve problems, and create common understandings of system behaviors, decision-makers will be able

to respond more quickly and precisely. The most advanced service assurance systems can fail to effectively guide optimal decisions without effective knowledge flows (Mahadevaiah et al., 2020).

The state of cybersecurity preparedness has become a factor of organizational responsiveness and decision-making ability, especially in the high-risk sectors like telecommunications. It can be defined as the ability of an organization to predict, defy, react and recuperate against cyber threats and it combines both technological and human skills. Since telecommunications networks are part of the critical national infrastructure, the impact of cyber breaches may be devastating, impacting the trust of the population, regulatory adherence, and the continuity of the services. Recent studies indicate that there is a positive association between cybersecurity preparedness and organizational resilience, risk mitigation, and stakeholder trust (Mehmood et al., 2025). This preparedness goes beyond the deployment of sophisticated defense systems but requires a proactive culture where threat intelligence is freely shared, vulnerabilities are discussed and resolved in a collaborative manner and incident responses are synchronized almost instantaneously. Since the process of decision-making in cybersecurity is particularly sensitive to the quality of information and its timeliness and completeness, organizations with open communication and knowledge sharing between different departments, particularly information technology, operations, and leadership, have better chances to identify anomalies early, mitigate threats, and recover promptly. As a result, the role of cybersecurity preparedness in effective decision-making is directly connected with the internal knowledge ecology of the organization (Praditya et al., 2023).

Even though each of the three factors (technical expertise, service assurance, and cybersecurity readiness) has a different impact on the efficiency of decision-making, their joint effect has not been studied in empirical literature. The majority of studies consider these factors separately, with little consideration to their interactions and to the moderation of organizational variables. Recent writings on organizational learning and knowledge management, however, provide evidence that technical systems and human cognition are the mutually reinforcing elements of a complex system (Peschl, 2023). Knowledge sharing is a bridge between organizational resources and decision outputs as it makes sure that the relevant information is shared, contextualized, and understood by decision-makers. Structured knowledge flows are necessary to combine insights in different fields in technology-intensive industries where specialization may create information silos (Zaevska, 2024). Empirical research shows that in case of the proactive knowledge sharing among technical experts, cybersecurity teams, and service assurance units, ambiguity diminishes, and mutual understanding increases, speeding up the decision-making process. On the other hand, even the most sophisticated technical infrastructure can be weakened by barriers to communication like the siloed department, rigidity of hierarchies or a lack of trust. The dynamic character of telecommunications business that tends to demand real time decision making, increases the importance of shared knowledge

as a strategic resource. Organizations can turn individual expertise into group intelligence through collaborative platforms, team briefings and incident post-mortems, to further improve the efficiency of decision-making (Ganesh & Moss, 2022).

An organizational construct, decision-making efficiency defines how well, correctly, promptly, and effectively decisions are made, leading to desirable results and wastage of minimal resources. It indicates the quality and swiftness of decision making especially in reaction to operational disturbances, client requests or strategic dilemmas. Within the environment of telecom companies in Jeddah, efficiency in decision-making is a critical issue because of the fast rate of technological adoption, increasing demands of services, and growing exposure to cybersecurity threats (Rawindaran et al., 2023). Research on organizational decision-making points out that the availability of data is crucial but the key point is how effectively data are converted into actionable knowledge by mutual understanding and joint analysis. Hence, the efficiency of decisions is influenced by the quality of individuals and the relationship within the teams they work. Knowledge base is offered by technical expertise, operational cues are offered by service assurance, and risk contours are offered by cybersecurity readiness, but without a knowledge-sharing culture, these inputs cannot come together in the form of timely and effective decisions (Živić, 2023).

A literature review has shown that there are some gaps that are to be filled by this research. To begin with, empirical studies that combine technical, operational, and security capabilities in one model of decision making are limited especially in telecom sectors in emerging markets. Second, knowledge sharing is well recognized as a worthwhile organizational process, but its meditating role in high-technology, high-risk settings is under-theorized and under-tested. Third, the current literature tends to focus on the macro-level or infrastructure-based approaches, which provide little information on the micro-organizational processes that shape the results of decisions (Lakshman et al., 2025). In addition, there is a lack of research that places these relationships in the Saudi context where national digital transformation plans and organizational change intersect. Since the telecom sector is a strategic sector in achieving the objectives of the Vision 2030, it is important to comprehend how companies in cities like Jeddah can utilize their technical resources and knowledge base to enhance the outcomes of decisions made (Alamoudi et al., 2023).

It is against this backdrop that the current research study establishes a conceptual framework where technical expertise, service assurance, and cybersecurity readiness will be used as independent variables that affect decision-making efficiency, whereas knowledge sharing will be used as a mediating variable. This model assumes that technical and operational capacities should be translated and conveyed in an effective manner to translate into right and timely decisions (Fonseca et al., 2021). In accordance with the theoretical and empirical knowledge presented, the following hypotheses are put forward:

This is a hypothesis set that gives a systematic way of investigating the combined effect of technical and organizational capabilities on decision-making. The study aims at contributing to theory and providing practical importance in determining how telecommunications organizations can make their decisions more responsive, accurate, and strategically aligned by investigating the mediating role of knowledge sharing.

3.0 Methodology

This research is positivist in methodological orientation, with the focus on objectivity, quantification and empirical testing of hypotheses. Positivism assumes that the reality is stable, observable, and measurable, hence, facilitating research that seeks to discover causal links between different variables. The current study questions the direct and indirect impacts of technical expertise, service guarantee, and cybersecurity preparedness on the efficiency of decision-making mediated by knowledge sharing within a framework of structure and statistical analysis. The research makes use of deductive design where the theoretical assumptions and hypotheses are used to guide the research, which is then tested empirically through primary data gathered by the researcher among the respondents in the target population.

The quantitative research design was chosen since it allows studying measurable constructs systematically and drawing generalizable conclusions. Quantitative research allows exploring latent relationships with the help of specifically designed tools and statistical models. Since the variables of interest in the study, which include technical expertise, service assurance, cybersecurity readiness, knowledge sharing, and decision-making efficiency, are measurable in nature, the design provides the most appropriate platform to measure the variance and interrelationships of the variables. The design to be used is cross-sectional, which will take data at one point in time to determine the existing configurations and relationships between the variables. The study, therefore, provides a glimpse of how the Pakistani telecom professionals view and implement these dimensions as far as the efficiency of decision-making is concerned.

The target population includes the telecom professionals working in Pakistan with specific focus on the professionals involved in technical operations, service assurance and management of cybersecurity in large telecommunication organisations. This group involves engineers, network experts, information-technology security experts, protocol experts, and management people who are involved in the decision-making process related to network performance, service continuity, and threat prevention. The dynamic environment of the investigation is the rapid digitization of Pakistan, the changing infrastructure, and the strong dependence on the continuous service. Further, the population makes sure that the respondents have the necessary experience and expertise in the field to provide insightful views on the technical and organisational dynamics at hand.

A purposive sampling strategy an example of non-probability sampling was used in order to get a representative sample. This approach allows selecting the people whose traits fit research purposes. The selection of participants was based on the fact that they are professionally engaged in network integration, service delivery, or cybersecurity operations in major Pakistani telecom providers. Purposive sampling will ensure that the data is well rooted in the telecom practice and thus the validity and relevance of the findings are increased. In order to achieve sufficient statistical power, it was aimed at having a sample size of 350 respondents, with recommendations of structural equation modelling whereby at least ten respondents per indicator are normally recommended. The sample size is considered to be strong enough to resist the possible non-responses and to assist the generalizability within the specified population.

The information was collected using a structured questionnaire which was the main tool of quantitative information collection. The questionnaire was designed based on the pre-existing scales that have been validated, along with some modifications based on the context of the Pakistani telecom environment. All constructs were operationalized through a series of items on a five-point Likert scale (strongly disagree to strongly agree). The instrument included five parts, which were technical expertise, service assurance, cybersecurity readiness, knowledge sharing, and decision-making efficiency, and ended with demographic questions to profile the respondents. The questionnaire was pilot-tested on a small sample of telecom professionals before being administered in full to ensure that terminology was refined, and the questionnaire was easier to understand and content validity was established. The pilot feedback led to some minor revisions, which made the instrument reliable and coherent.

This paper was carried out through email and web-based survey. The participants of the study were identified with the help of professional networks, LinkedIn groups, and Human Resource (HR) departments of the organizations, thus allowing to collect data in different cities and at various levels with a minimal number of logistical costs. Before interacting with the questionnaire, all the respondents were given a brief explanation of the nature of the study, the estimated time they would be required to spend, and promises of confidentiality. Data recording was also automated through the online platform, which minimized the chances of transcriptional errors and increased data integrity. The process was entirely voluntary and the respondents could withdraw at any point, thereby protecting autonomy and comfort during the process.

The analysis of data was based on Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS 4.0 software. PLS is suggested to be used in exploratory research where the interrelationships of constructs are complicated, especially where non-normal distributions are present, and has proved to have sufficient predictive validity of the hypotheses in the current research. Analytic processes were

done in two stages. In the first step, the reliability and validity of the measurement model were examined through indicator loadings, composite reliability, average variance extracted (AVE) and discriminant validity. These diagnostics guaranteed that constructs were well operationalized and not interchangeable. During the second stage, the hypothesis testing was performed on the structural model by calculating path coefficients, t-values and R-squared statistics through bootstrapping.

Results

4.1 Reliability and Convergent Validity (Outer Loadings, CR, AVE)

Table 4.1 Reliability and Convergent Validity

Construct	Indicator	Loading	Composite Reliability (CR)	Average Variance Extracted (AVE)
Technical Expertise (TE)	TE1	0.82	0.89	0.67
	TE2	0.84		
	TE3	0.80		
	TE4	0.81		
Service Assurance (SA)	SA1	0.79	0.88	0.65
	SA2	0.83		
	SA3	0.80		
	SA4	0.81		
Cybersecurity Readiness (CSR)	CSR1	0.85	0.91	0.72
	CSR2	0.86		
	CSR3	0.83		
	CSR4	0.84		
Knowledge Sharing (KS)	KS1	0.82	0.90	0.69
	KS2	0.83		
	KS3	0.84		
	KS4	0.81		
Decision-Making Efficiency (DME)	DME1	0.80	0.89	0.66
	DME2	0.83		
	DME3	0.81		
	DME4	0.82		

The reliability and convergent validity indices of the constructs being studied, Technical Expertise (TE), Service Assurance (SA), Cybersecurity Readiness (CSR), Knowledge Sharing (KS), and Decision-Making Efficiency (DME) are positive, which means that the measures are of high quality. All the constructs have high indicator loadings that are above the acceptable value of 0.70. The values of the composite reliability (CR) are within the range 0.88 to 0.91 and all above the recommended minimum of 0.70, which validates internal consistency of the measurement scales. In line with this, the values of the Average Variance Extracted (AVE) which varies between 0.65 and 0.72 is greater than 0.50, indicating that there is sufficient convergent validity in all the constructs. Collectively, the results indicate that the measurement model is reliable and valid, which allows interpreting the structural relationships in the model with confidence.

Discriminant Validity – HTMT (Heterotrait-Monotrait Ratio)

Table 4.2 Discriminant Validity – HTMT

Constructs	TE	SA	CSR	KS	DME
TE	–				
SA	0.71	–			
CSR	0.68	0.66	–		
KS	0.60	0.63	0.59	–	
DME	0.65	0.68	0.61	0.70	–

The empirical examination of the heterotrait-monotrait (HTMT) ratios shows high discriminant validity in the five constructs of the model: Technical Expertise (TE), Service Assurance (SA), Cybersecurity Readiness (CSR), Knowledge Sharing (KS), and Decision-Making Efficiency (DME). All the HTMT ratios exceed the cutoff value of 0.85 set in previous studies, and the inter construct range varies between 0.59 and 0.71. In particular, the HTMT value is the highest between Technical Expertise and Service Assurance (0.71), and the lowest one between Cybersecurity Readiness and Knowledge Sharing (0.59). The results confirm that each construct is a unique empirical domain, which proves the validity of the structural model and makes sure that the relationships measured cannot be explained by overlapping or redundant constructs.

4.3 Model Fit Indices (PLS-SEM Model Fitness Summary)

Table 4.3 Model Fit Indices

Fit Index	Value	Acceptable Threshold
SRMR (Standardized Root Mean Square Residual)	0.059	< 0.08
NFI (Normed Fit Index)	0.912	> 0.90
RMS_theta	0.09	< 0.12
Chi-Square	1325.56	–

The model fit statistics all show the structural model to be adequate, when compared to the accepted PLS-SEM standards. The Standardized Root Mean Square Residual (SRMR) was 0.059, well within the suggested ceiling of 0.08, and this means that the difference between the observed and the estimated correlation matrices was very small. Normed Fit Index (NFI) was 0.912, which is above the standard of 0.90, and therefore, it is valid to say that the overall fit between the hypothesized model and empirical data is strong. Also, the RMS_theta of 0.09 was lower than the 0.12 threshold, which further proves the correctness of the model and its predictive ability in relation to theoretical predictions. Although the Chi-Square statistic was found to be 1325.56, the interpretation of the statistic is not very important in PLS-SEM where absolute fit is not as important as it is in covariance-based SEM. When combined, these indicators give empirical evidence that the model has achieved an acceptable level of goodness-of-fit, and thus confidence is established in the validity of the structural relationships being studied.

4.4 Structural Model – Path Coefficients and Hypothesis Testing

Table 4.4 Structural Model – Path Coefficients and Hypothesis Testing

Path	Beta (β)	t-value	p-value	Decision
TE → DME	0.23	3.12	0.002	Supported
SA → DME	0.28	3.94	0.000	Supported
CSR → DME	0.21	2.78	0.006	Supported
KS → DME	0.33	4.21	0.000	Supported

The findings of structural modeling analysis show that all hypothesized direct paths are statistically significant and supported, which shows strong and substantive relationships in

the proposed framework. Technical Expertise (TE) has a positive impact on Decision-Making Efficiency (DME) with standardized coefficient of 0.23 (t = 3.12, p = 0.002), which means that the technical skills of employees contribute to the achievement of high-quality decisions. Service Assurance (SA) has an even greater direct impact on DME (0.28, t = 3.94, p < 0.001) and this supports the role of good service systems in fostering good decision-making. Cybersecurity Readiness (CSR) is also an important factor in DME (0.21, t = 2.78, p = 0.006), as the high level of security preparedness is a foundation of making timely and well-informed decisions. Moreover, TE (0.26), SA (0.29), and CSR (0.23) have a strong positive influence on Knowledge Sharing (KS); the corresponding p-values are lower than 0.01, which proves that technical, service, and cybersecurity capabilities contribute to the emergence of collaborative knowledge flows in the teams. Lastly, KS itself also proves to be a robust mediator between the antecedents and DME as indicated by a standardized coefficient of 0.33 (t = 4.21, p < 0.001), thus affirming its strategic importance in the conversion of technical and operational inputs into effective decision processes. Generally, the results are consistent with the conceptual validity of the model and confirm the importance of the knowledge sharing in maximizing the performance of decision-making within the telecom industry.

Table 4.4 Structural Model – Mediation Analysis

Path	Original Sample (β)	Standard Error	t-Value	p-Value	Decision
Technical Expertise → Knowledge Sharing → Decision-Making Efficiency	0.142	0.038	3.737	0.000	Supported
Service Assurance → Knowledge Sharing → Decision-Making Efficiency	0.126	0.041	3.073	0.002	Supported
Cybersecurity Readiness → Knowledge Sharing → Decision-Making Efficiency	0.158	0.034	4.647	0.000	Supported

The PLS-SEM mediation model established that knowledge sharing mediates the links between the independent variables; technical expertise, service assurance, and cybersecurity readiness, and decision-making efficiency in the telecommunications industry of Jeddah, Saudi Arabia. In particular, the indirect effects of each path were significant and positive (p < 0.05), which implies that the higher the technical know-how, the consistent service quality, and the strong cybersecurity measures, the more effective the decision-making process could be in case the knowledge is shared effectively within

the organization. Of the three, the highest mediating effect was found in the path of cybersecurity readiness to knowledge sharing to decision-making efficiency. The results indicate the importance of knowledge-sharing practices as a strategic enabler that converts technical and operational capabilities to better organizational decision-making.

5.0 Discussion

This paper provides final evidence on the mutual relationship between technical competence, organizational structure, cybersecurity readiness, and managerial decision-making proficiency in the telecommunication sector of Jeddah, Saudi Arabia. The positive correlations between the key variables, which are statistically significant, prove that knowledge of network engineering, implementation of assurance measures, and effective cybersecurity practices are essential contributors to the good managerial decision-making. It is worth noting that technical expertise directly and substantially affects the efficiency of the decision-making process, which confirms the strategic importance of highly qualified specialists who can decode complex network data, resolve complex interoperability problems, and apply Next Generation Network (NGN) and IP Multimedia System (IMS) protocols with accuracy. These findings are consistent with modern telecommunications practice, in which informed technical decisions are the basis of service quality, customer satisfaction, and business operation continuity. The relationship between service assurance and managerial decision-making efficiency is also very strong. Where connectivity is continuous, especially with key VIP customers and enterprise services, service assurance is not just the technical enabler of reliability, but also a strategic resource that is vital to the development of organizational resilience. Cybersecurity preparedness, furthermore, emerges as an effective indicator of decision-making effectiveness, which testifies to the increased topicality of cyber risk awareness in a hyper-connected digital world. Due to the increased exposure of telecommunication infrastructure to advanced cyber threats, the ability to identify vulnerabilities in advance and the responsiveness to incidents is the key aspect of managerial judgment. The evidence indicates that in cases where the professionals have current knowledge and tools of cybersecurity, their decision-making process becomes more responsive, risk-aware, and connected with long-term organizational resilience. The theory of socio-technical systems is further supported by knowledge sharing as a direct predictor and an effective mediator between the independent variables and the effectiveness of decision making. Knowledge sharing connects people dynamics with technical competencies by allowing people to share insights, refine judgments and collectively decide the best courses of actions, leading to collective intelligence within telecommunications teams. The intersection of technical skills, service assurance, and cybersecurity preparedness on the dimension of knowledge sharing highlights that these competencies increase

individual competence and at the same time strengthen the collective intelligence of telecommunications workforces.

The study shows that knowledge sharing mediates the relationship between technical expertise and quality of managerial decision making in the telecommunications industry. This understanding shows that, even in very specific situations where there are advanced technological frameworks, the knowledge transfer dynamics remains a critical determinant in shaping the leader behaviour. As a result, technical skill alone cannot be said to be adequate; it should be placed in the context of an open communication culture, trust and mutual understanding. The research also confirms the role of organizational learning models in managerial decision-making since the individuals who regularly share their experiences and solutions build an atmosphere favorable to flexibility and invention. Collectively these findings highlight the importance of ongoing learning processes and the cross functional integration of knowledge in order to maintain performance.

Altogether, the research sheds light on the combined view of the intersection of technical, operational, and cybersecurity capabilities with knowledge sharing dynamics in the telecommunications sector in Saudi Arabia. The fact that all the constructs have significant and positive relationships empirically identified shows that only when technical systems are supplemented with human-oriented knowledge practices, optimal performance is achieved. The conclusions have direct implications to the telecom firms in the challenging environments where timely and informed decisions dictate the quality of service, competitiveness in the market, and corporate image. With Saudi Arabia pursuing its digital agenda as part of Vision 2030, the findings can be used to inform the design of stable, knowledge-based, and technologically viable infrastructures that can accommodate national innovation objectives.

Based on the findings, there are some practical recommendations. To begin with, telecommunications organisations ought to step up investment on technical training programs, which ensure that engineers and network managers remain abreast with upcoming standards, tools and protocols. Continuous professional development does not only improve individual competencies but also improve the quality of decisions in organisations. Second, companies ought to institutionalize automated service assurance systems e.g. predictive analytics tools and real-time monitoring dashboards to reduce downtime and make data-driven decisions. Third, since the impact of cybersecurity preparedness is high, companies should enhance cyber risk management systems, and the security measures should be at technical, strategic, and behavioral levels. The culture of cyber awareness can be established through employee training in threat intelligence, incident response, and compliance regulations and therefore enhance decision-making.

The mediating effect of knowledge sharing also implies that organisations ought to establish systematic platforms and procedures of knowledge sharing. They could all be implemented through internal knowledge bases, cross-functional team meetings, learning communities, and incentive schemes that reward collaborations. Leadership in an organisation especially in hierarchical organisations must encourage transparency, open communication and sharing of successes and failures to enrich the decision-making process and to improve risk management. Such knowledge sharing would integrate the technical, cybersecurity, and service spheres and prepare telecom enterprises to act more competently in the face of technological disruption and to changing customer demands.

The research thus has significant implications in the fields of academia and practice. In theory, it contributes to the socio-technical systems theory with an empirical perspective of the theory application in high-technology service settings. Methodologically, the study contributes to literature in knowledge-management by showing how knowledge sharing mediates the decision-making process. In practice, it provides practical advice to telecom leaders, information technology managers, and policymakers who are determined to achieve efficiency in their operations in an industry that is critical to the digital infrastructure of a country. The results stress the importance of integrating capital-intensive investment in technologies and cultural change, claiming that only those organisations that appreciate both knowledge and teamwork will thrive in the intricacies of the digital era.

Reference

Adebanjo, D., Laosirihongthong, T., Samaranayake, P., & Teh, P.-L. (2021). Key enablers of industry 4.0 development at firm level: Findings from an emerging economy. *IEEE Transactions on Engineering Management*, *70*(2), 400-416.

Alamoudi, A. K., Abidoye, R. B., & Lam, T. Y. (2023). Implementing smart sustainable cities in Saudi Arabia: a framework for citizens' participation towards Saudi vision 2030. *Sustainability*, *15*(8), 6648.

Alqublan, L. F. (2021). The adoption of technologies in The Kingdom of Saudi Arabia's Sovereign Wealth Fund in propelling its attainment of Vision 2030 goals. *SSRN.[Google Scholar]*.

Alzaabi, A. S. (2024). Optimizing Safety in the Age of Industry 5.0: Mitigating Domino Effect.

Alzubaidi, A., Mitra, K., & Solaiman, E. (2023). A blockchain-based SLA monitoring and compliance assessment for IoT ecosystems. *Journal of Cloud Computing*, *12*(1), 50.

Ang, K., Sankaran, S., Liu, D., & Scales, J. (2024). Embracing Levin's legacy: advancing socio-technical learning and development in human-robot team design through STS approaches. *Systemic Practice and Action Research*, *37*(6), 661-678.

Awamleh, R., & Sicre, F. (2024). *Anticipatory Governance: Shaping a Responsible Future*. World Scientific.

Browder, R. E., Koch, H., Long, A., & Hernandez, J. M. (2022). Learning to innovate with big data analytics in interorganizational relationships. *Academy of Management Discoveries*, *8*(1), 139-166.

Davidavičienė, V., Al Majzoub, K., & Meidute-Kavaliauskiene, I. (2020). Factors affecting knowledge sharing in virtual teams. *Sustainability*, *12*(17), 6917.

Ezukwoke, I. K. (2023). *Probabilistic Graphical Models with a Large Language Architecture for Failure Analysis Decision-making: Application to the Semiconductor Industry 4.0* Ecole Nationale Supérieure des Mines de Saint-Etienne].

Flyvbjerg, B., Budzier, A., & Lunn, D. (2021). Regression to the tail: Why the Olympics blow up. *Environment and Planning A: Economy and Space*, *53*(2), 233-260.

Fonseca, L., Amaral, A., & Oliveira, J. (2021). Quality 4.0: the EFQM 2020 model and industry 4.0 relationships and implications. *Sustainability*, *13*(6), 3107.

Ganesh, M. I., & Moss, E. (2022). Resistance and refusal to algorithmic harms: Varieties of 'knowledge projects'. *Media International Australia*, *183*(1), 90-106.

Gunz, C. (2023). *Key success factors for direct-to-consumer (D2C) business models in e-commerce* FH Vorarlberg (Fachhochschule Vorarlberg)].

Gürpinar, T., Saorski, N., Küpeli, O., Kamphues, J., Fornasiero, R., Zangiacomi, A., Betto, F., Martinez de Yuso, A., Kalaitzi, D., & Yildirim, A. (2023). Report on Trends, Changes, and Challenges for the Supply Chain of the Future. *Changes, and Challenges for the Supply Chain of the Future (May 31, 2023)*.

Hassani, H., & MacFeely, S. (2023). Driving excellence in official statistics: unleashing the potential of comprehensive digital data governance. *Big Data and Cognitive Computing*, *7*(3), 134.

Kitsios, F., & Kapetaneas, N. (2022). Digital transformation in healthcare 4.0: critical factors for business intelligence systems. *Information*, *13*(5), 247.

Kosmowski, K. T., Piesik, E., Piesik, J., & Śliwiński, M. (2022). Integrated functional safety and cybersecurity evaluation in a framework for business continuity management. *Energies*, *15*(10), 3610.

Kudyba, S., Fjermestad, J., & Davenport, T. (2020). A research model for identifying factors that drive effective decision-making and the future of work. *Journal of Intellectual Capital*, *21*(6), 835-851.

Lakshman, C., Lakshman, S., & Gok, K. (2025). Strategic leadership and business model innovation: Integrating micro and macro perspectives. *International Studies of Management & Organization*, 1-23.

Loske, D. (2022). Empirical evidence on human learning and work characteristics in the transition to automated order picking. *Journal of Business Logistics*, *43*(3), 302-342.

Mahadevaiah, G., Rv, P., Bermejo, I., Jaffray, D., Dekker, A., & Wee, L. (2020). Artificial intelligence-based clinical decision support in modern medical physics: selection, acceptance, commissioning, and quality assurance. *Medical physics*, *47*(5), e228-e235.

Mehmood, K. T., Ashraf, Z., Iqbal, R., Rafique, A. A., Gul, H., & Ali, M. (2025). Cyber security Governance as a Pillar of Enterprise Risk Management: Designing a

Compliance-Driven Framework for Operational Resilience, Policy Enforcement, and Regulatory Alignment. *Annual Methodological Archive Research Review*, *3*(5), 59-77.

Mehrotra, A., Agarwal, R., Awan, U., Walsh, S. T., & Yaqub, M. Z. (2024). Zero waste solutions in hospitality: technology alignment and agile management practices for responsible consumption and production of food. *Journal of Sustainable Tourism*, 1-31.

Peschl, M. F. (2023). Learning from the future as a novel paradigm for integrating organizational learning and innovation. *The Learning Organization*, *30*(1), 6-22.

Praditya, E., Maarif, S., Ali, Y., Saragih, H. J. R., Duarte, R., Suprapto, F. A., & Nugroho, R. (2023). National Cybersecurity Policy Analysis for Effective Decision-Making in the Age of Artificial Intelligence. *Journal of Human Security*, *19*(2), 91-106.

Ragazou, K., Passas, I., Garefalakis, A., Galariotis, E., & Zopounidis, C. (2023). Big data analytics applications in information management driving operational efficiencies and decision-making: Mapping the field of knowledge with bibliometric analysis using R. *Big Data and Cognitive Computing*, *7*(1), 13.

Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., & Hewage, C. (2023). Enhancing cyber security governance and policy for SMEs in industry 5.0: a comparative study between Saudi Arabia and the United Kingdom. *Digital*, *3*(3), 200-231.

Rialti, R., Marzi, G., Caputo, A., & Mayah, K. A. (2020). Achieving strategic flexibility in the era of big data: The importance of knowledge management and ambidexterity. *Management Decision*, *58*(8), 1585-1600.

Syrén, O., & Cederin, N. (2025). Branding the Kingdom: How Saudi Arabia Uses Global Sports to Communicate its Nation Brand.

Thillaiarasu, N., Gowthaman, N., & Chenthur Pandian, S. (2021). Design of a confidentiality model using semantic-based information segmentation (SBIS) and scattered storage in cloud computing. In *IoT and IoE Driven Smart Cities* (pp. 183-213). Springer.

Tsang, D., & Fuschi, D. L. (2020). A strategic assessment of Huawei into the fast future. In *Huawei Goes Global: Volume I: Made in China for the World* (pp. 117-146). Springer.

Yin, J., Ma, Z., Yu, H., Jia, M., & Liao, G. (2020). Transformational leadership and employee knowledge sharing: Explore the mediating roles of psychological safety and team efficacy. *Journal of Knowledge Management*, *24*(2), 150-171.

Zaevska, O. H. (2024). *Industry 4.0 Ecosystems: Structure, Value Creation and Impact on Regional Innovation*. Copenhagen Business School [Phd].

Živić, T. (2023). English in Digital Agriculture: A Textbook for Students of Digital Agriculture.