Global Research journal of Natural Science & Technology (GRJNST)

Volume: 04 - Issue 4 (2026), 2110
ISSN P: 2790-7643 ISSN E: 2790-7651
www.grjnst.net
https://doi.org/10.53762/grjnst.04.04.01

AI Capability and Performance: The Strategic Roles of Cyber Risk Management Firm and Knowledge Management Systems in Pakistan Halal Foods

Received: 14 April 2026. Accepted: 16 May 2026. Published: 19 June 2026

Ghulam Zara
Abasyn University Islamabad Campus
zara.zafar152@gmail.com
https://orcid.org/0009-0009-3801-8461
Hassan Raza Ahsan
Federal Urdu University of Arts, Science & Technology, Islamabad, Pakistan
hassan_raza325@yahoo.com
https://orcid.org/0009-0006-1259-0660

Abstract

The fast development of digital technology has changed the way organizations operate and increased the importance of artificial intelligence capabilities, cyber risk management and knowledge management systems, in enhancing business performance. The present study examined the impact of artificial intelligence capabilities on organizational performance, and the mediating role of cyber risk management and knowledge management systems in halal food manufacturing enterprises in Pakistan. The study is based on the Resource-Based View, the Theory of Dynamic Capabilities and the Knowledge-Based View. The study has adopted a quantitative research methodology with a cross-sectional survey design. Data was collected from 300 management workers working in halal food production companies in Pakistan using a standardised questionnaire. The collected data were analyzed using SPSS and SmartPLS. Results show that artificial intelligence capabilities have a significant positive effect on corporate performance, cyber risk management and knowledge management systems. In addition, the cyber risk management and knowledge management systems contribute greatly to the performance of the organization. The results also reveal that the proposed model possesses adequate explanatory power, predictive relevance, reliability and validity. The study contributes to the existing literature on digital transformation and organizational performance by providing real findings from the halal food manufacturing industry of Pakistan. The results suggest that organizations should spend money on AI technology, cybersecurity measures and knowledge management systems to enhance operational efficiency, organizational resilience and sustained competitive advantage.

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

Keywords: *AI Capability, Cyber Risk Management, Knowledge Management System, Firm Performance*

Introduction

The fast development of digital technologies has changed the operational environment of today's organizations, especially of the manufacturing industry. In recent years, organizations have increasingly adopted artificial intelligence (AI), cybersecurity measures, and knowledge management systems to enhance operational efficiency and organizational competitiveness (Olan et al., 2022; Leoni et al., 2022). The development of industry 4.0 has made easier the application of intelligent technology in the business processes. This gives organizations a chance to automate operations, improve resource allocation and increase strategic performance. Among these technical breakthroughs, AI competence has become a critical organizational resource to improve productivity and competitiveness (Shao et al. 2026). Neiroukh et al., (2025) also showed that organizations with high AI capabilities have better speed of decision making, operational efficiency and organizational performance.

Furthermore, artificial intelligence competence refers to an organization's ability to successfully implement, integrate, and use artificial intelligence technology, infrastructure, technical knowledge, and analytical abilities in order to achieve strategic

goals (Mikalef et al., 2023). In addition, solutions that are powered by artificial intelligence improve predictive analytics, automate processes, provide intelligent forecasting, and monitor customer behavior, all of which contribute to an increase in organizational efficiency. According to Islam et al. (2024), artificial intelligence technologies are increasingly used in the manufacturing sector to improve production quality, inventory management, supply chain operations, and product innovation. The growing use of artificial intelligence has had a significant influence on businesses operating in specialized environments, such as the manufacture of halal products, where compliance with laws, quality control, operational transparency, and consumer trust are of the utmost importance.

Although there are strategic benefits to using AI, companies are also facing increasing security dangers and digital vulnerabilities. The digital revolution in industrial processes has heightened the organizational dependence on interrelated technologies, cloud infrastructures, and data-driven operations, which, in turn, increases the susceptibility to cyber-attacks (Areghan, 2025). Vidović et al. (2025) mention that cybersecurity incidents, data breaches, ransomware attacks, and operational disruptions may have a considerable influence on firm reputation, financial stability and customer confidence. As a result, managing cyber risk has emerged as a vital organizational capability to protect digital assets, ensure business continuity, and enhance organizational resilience. Research like Kure et al. (2018) and Fernando et al. (2023) suggests that effective management of cyber risks provides a substantial contribution to improve company performance via the reduction of operational uncertainty and the improvement of information system reliability.

Cyber risk management is the process of identifying, assessing, monitoring, and managing cybersecurity threats that might influence the organization's operations (Parsola, 2022). Organizations with excellent cybersecurity management systems are more likely to preserve intellectual property, ensure customer data safety, and maintain stakeholder confidence in digital, linked business environments. Cyber risk management is equally important in halal food production as integrated supply chain systems, digital certification procedures and online transaction platforms depend on secure information management and operational integrity. Poor management of cyber risks leads to poor corporate performance (Okoye, 2017), disruption of business continuity and loss of client trust in halal products.

Besides AI capabilities and cyber risk management, knowledge management systems (KMS) have become an important organizational resource that significantly affects corporate performance. Knowledge management systems are the technological and organizational structures used to create, store, distribute, transmit and apply knowledge within enterprises (Mohammad et al., 2024). Organizational knowledge is recognised as a significant intangible asset in information-dense, technology-driven organizational settings, enhancing inventive ability, operational efficiency and strategic flexibility. Knowledge management systems (KMS) are able to support organizational learning, assist in decision-making, and develop employee collaboration, and finally affect organizational performance (Jia et al., 2024). Recent empirical studies have shown that

knowledge management systems are important for enhancing organizational productivity, innovativeness, and performance (Lai et al., 2022). Knowledge management systems help manufacturing organisations effectively gather and use critical company knowledge to optimise processes, improve quality, foster product innovation, and make strategic decisions. Halal manufacturing companies utilize knowledge management systems to improve compliance with halal principles, product consistency and best practices in operations.

Prior research has studied the effects of AI capability, cyber risk management and knowledge management systems on organizational outcomes separately, but there is a paucity of research on these factors altogether in a comprehensive framework, especially in the context of halal product manufacturing companies. The present study is based on general manufacturing industries, service organizations and technical companies, although factual data from halal manufacturing sectors are scarce. Additionally, previous studies have mostly concentrated on the direct relationships between technology capabilities and business performance, overlooking the interdependent roles of AI capability, cybersecurity management, and knowledge management systems in boosting organizational performance.

Literature review

Theoretical Foundation

The study is mainly based on the Resource-Based View (RBV) which argues that companies may achieve sustained competitive advantage and superior performance via

the efficient use of valuable, rare, distinctive and non-substitutable organizational resources (Barney, 1991). AI capabilities, cyber risk management and knowledge management systems are seen as important organizational assets for the contemporary digital corporation to boost operational efficiency, innovation potential, organizational resilience and decision making quality. The RBV has clearly defined the importance of technical and administrative capabilities in boosting the performance of halal product production firms.

In addition, the study is supported by the Dynamic Capabilities Theory which defines the ability of the organization to integrate, reconfigure and transform internal competences to meet the changing technology and market circumstances (Teece et al., 1997). AI capabilities may increase digital transformation and operational intelligence. Cyber risk management can improve the organization's resistance to cybersecurity threats and knowledge management systems can support organizational learning and knowledge utilization. Recent studies like Zheng (2024) reveal that organizations with sophisticated digital capabilities and competent knowledge-based resources display more innovation, strategic agility, and economic success. Thus, the integration of Resource-Based View and Dynamic Capabilities Theory provides a strong theoretical foundation to understand the combined effect of AI capability, cyber risk management and knowledge management systems on organizational performance in the halal manufacturing industry.

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

Hypothesis development

The effectiveness of artificial intelligence has turned into kind of a vital organizational asset that helps companies boost operational efficiency, sharpen strategic choices , encourage innovation and get a clearer edge over competitors. AI competency is basically how capable an organization is at rolling out, embedding, and putting AI technologies into practice, including the infrastructure, technical know-how, and analytical skills needed to push corporate objectives forward and create measurable value (Mikalef et al., 2023). As AI technology keeps spreading through manufacturing, it has shifted ordinary, routine operating procedures into more intelligent, data oriented systems , which in turn can lift organizational efficiency and overall performance. If you look at it through the Resource-Based View (RBV), AI capacity is treated as a strategic organizational asset that supports long lasting competitive advantage and better business outcomes. The Resource-Based View suggests that firms with valuable resources and hard-to-duplicate technical skills are more likely to achieve stronger results (Barney, 1991).

Recent empirical research does, in a general sense, strongly back up the idea that higher AI capacity links with stronger organizational performance. Neiroukh et al. (2025) showed that AI capabilities actually can improve organizational performance not just "a little" but noticeably, mainly because decision making gets more efficient and the organization becomes more strategically responsive, in practice. Wahyudi et al. (2026) noted the same pattern too, companies that use AI technology tend to see higher

operational efficiency , stronger innovation performance, and better organizational competitiveness. In industrial contexts, AI capabilities support process automation , predictive maintenance, quality control, and even supply chain optimisation, so overall organizational performance tends to rise. And for specialized sectors, like halal product manufacturing, the potential advantage can be even more meaningful since intelligent systems can help with halal compliance monitoring, raise operational transparency, and boost production efficiency. So in the end, firms that build up stronger AI capabilities are expected to reach improved organizational performance, relatively faster perhaps, depending on how they implement it.

HI: *Artificial intelligence capability has a positive and significant relationship with firm performance.*

The swift digital shift within firms has, sort of, increased their exposure to cybersecurity attacks, so cyber risk management has become a serious corporate matter. Cyber risk management, in general, is about identifying, assessing, monitoring, and mitigating cybersecurity threats that could disrupt organizational systems, digital infrastructure, and day-to-day operational continuity (Parsola, 2022). At the same time, artificial intelligence has become a key technical enabler, strengthening corporate cybersecurity readiness and the overall performance of cyber risk management. Dynamic Capabilities Theory suggests that companies with stronger technical expertise can deal more effectively with environmental uncertainty and digital hazards, because they stay engaged

in ongoing adaptation and innovation (Teece et al., 2016). In practice, AI capabilities let organizations employ machine learning methods, predictive analytics, vigilant monitoring tools, and automated threat detection approaches, which all together improve cybersecurity management and organizational resilience.

Recent studies show that AI technologies can significantly improve cybersecurity operations, in that anomaly detection improves, cyber threat identification becomes more precise, and incident response speeds up. Ravikumar (2025) argued that AI-enhanced cybersecurity approaches make it easier for an organisation to spot and respond to complex cyber threats in real time. Likewise, Mızrak (2023) found that companies relying on intelligent digital systems tend to improve their cybersecurity readiness and overall ability to mitigate risk. In practice, AI-driven cybersecurity systems can sift through vast amounts of organizational data, detect anomalous or out-of-pattern behaviour, and even surface likely vulnerabilities before real operational disruption occurs. In industrial settings, digitalisation, along with integrated operational technologies, can exacerbate cybersecurity vulnerabilities, especially those related to cloud services, IoT devices, and supply chain networks. Halal product manufacturing firms are increasingly relying on digital certification systems, production monitoring platforms, and interconnected information systems, making the need for AI-enhanced cybersecurity measures more urgent. So overall, organizations that have stronger AI capabilities tend to build more solid cyber risk management frameworks and, in turn, improve cybersecurity resilience.

H2: *Artificial intelligence capability has a positive and significant relationship with cyber risk management.*

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

Knowledge management systems (KMS) are basically organizational frameworks meant to improve the generation, storage, exchange, transfer, and practical use of organizational information (Kumar & Gupta, 2012). In this digital age, AI capabilities have become a key technical asset, as they strengthen corporate knowledge management by accelerating information processing, enabling advanced analytics, and supporting learning mechanisms. How exactly AI capabilities tie in with knowledge management systems can be understood through the Knowledge-Based View (KBV), because it argues that information is a critically crucial organizational resource for achieving ongoing competitive advantage. With AI capabilities in place, an organization can better collect, evaluate, structure and distribute useful information among its divisions, which then really helps knowledge generation and knowledge application (Olan et al., 2023).

Recent research suggests that AI technologies substantially improve corporate learning and knowledge-sharing activities. Gao et al. (2025) found that AI capabilities help strengthen knowledge integration, boost innovation ability, and support strategic decision making, mainly because they make intelligent information handling easier while also encouraging organizational cooperation. In a similar way, Yu et al. (2017) reported that technical capabilities have a positive effect on knowledge management effectiveness and organizational learning results. AI-driven solutions offer smart data mining, automatic knowledge categorisation, and near-instant information distribution, so, overall, they improve how organisations apply knowledge and how smoothly operations run. In industrial settings, AI-enhanced knowledge systems can improve product

development, reinforce operational standardisation, strengthen quality management, and optimise processes. Halal product manufacturing companies may benefit in particular, as these tools make it easier to share halal compliance knowledge, increase operational visibility, and help organisations understand the requirements of halal manufacturing. So, companies that already have strong AI capabilities are expected to build more efficient knowledge management systems.

H3: *Artificial intelligence capability has a positive and significant relationship with knowledge management systems.*

Cyber risk management has become paramount for firms operating in technology-led, digitally interconnected business spaces. Ahmad et al. (2021) argue that as enterprises continue to adopt digital technologies, cloud computing systems, and web-based operational platforms, their exposure to cyberattacks and information security vulnerabilities has increased noticeably. Also, having solid cyber risk management helps a firm not only spot likely cyber threats but also guard digital assets, sustain day-to-day operations, and strengthen overall organizational resilience. When you look at it through the Resource-Based View, cyber risk management is treated as an essential internal capability, as it protects strategic resources and supports long-term company performance. Firms with strong cybersecurity management systems are typically better at reducing the likelihood of operational stoppages, mitigating financial harm, and minimising reputational damage from cyberattacks or data breaches.

Recent empirical studies back up, not just hint at, a positive link between cyber risk management and overall organizational results. Sukachova et al. (2025) found that firms with strong cybersecurity capabilities, kind of like a resilient shield, tend to show stronger organizational resilience and also better commercial outcomes. Althonayan and Andronache (2019) suggested that when enterprise risk management and cybersecurity measures work together, the organisation's sustainability improves significantly, as well as operational continuity and even strategic effectiveness. Effective cyber risk management builds stakeholder trust, strengthens consumer confidence, and supports long-term organizational stability. Cybersecurity management is increasingly necessary for manufacturing firms because production systems, supply chains, and operational technologies increasingly rely on interconnected digital infrastructure. For halal product manufacturing organizations, the stakes are even higher: cyber risk management is crucial so companies can protect halal certification documents, customer information, and supply chain traceability platforms. If there's a cybersecurity incident, operational dependability can be harmed, and customer confidence in halal goods may drop. So, in the end, companies that implement efficient cyber risk management techniques are more likely to reach improved performance outcomes.

H4: *Cyber risk management has a positive and significant relationship with firm performance.*

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

Knowledge management systems are widely regarded as strategic organizational tools that help organisations increase innovation capacity, enhance organizational learning, and support corporate success (Migdadi, 2022). In a similar vein, knowledge management systems (KMS) help with the collection, storage, circulation, and application of organizational information. Because of that organizations can improve the quality of decisions, raise operational efficiency, and gain a bit more strategic flexibility. The knowledge-based view argues that organizational knowledge is a major intangible asset that can strengthen competitive advantage and produce better organizational outcomes (Osobajo & Bjeirmi, 2021). When knowledge management systems are run well, they can also expand organizational learning, strengthen employee collaboration, and encourage innovative activities that, in practice, benefit firm performance. More recent empirical work also points to a clear and positive effect of KMS on organizational performance. Alrubaiee et al. (2015) found that knowledge management practices significantly improve operational efficiency, innovative capacity, and overall organizational productivity. Likewise, Rialti et al. (2020) showed that firms employing effective knowledge management systems tend to display stronger innovation performance, higher strategic adaptability, and better organizational competitiveness. Also, knowledge-sharing approaches let firms leverage human know-how in a more efficient way, reduce operational inefficiencies, and improve how quickly the organization responds to shifts in the environment.

In manufacturing contexts, Knowledge Management Systems help with process improvements, better quality outcomes, and product novelty, through more efficient knowledge sharing and a kind of collective organizational learning. In halal product

manufacturing companies, it is especially important to have knowledge management systems that work well, so they can preserve halal compliance, maintain strong quality assurance protocols, and ensure operational consistency across departments. When knowledge management is done efficiently, it also supports staff coaching, compliance awareness, and ongoing refinement tasks in halal industrial settings. So, organizations that have effective knowledge management systems are more apt to reach stronger operational results and better financial performance. Based on that, researchers put forward the following hypothesis.

H5: *Knowledge management systems have a positive and significant relationship with firm performance.*

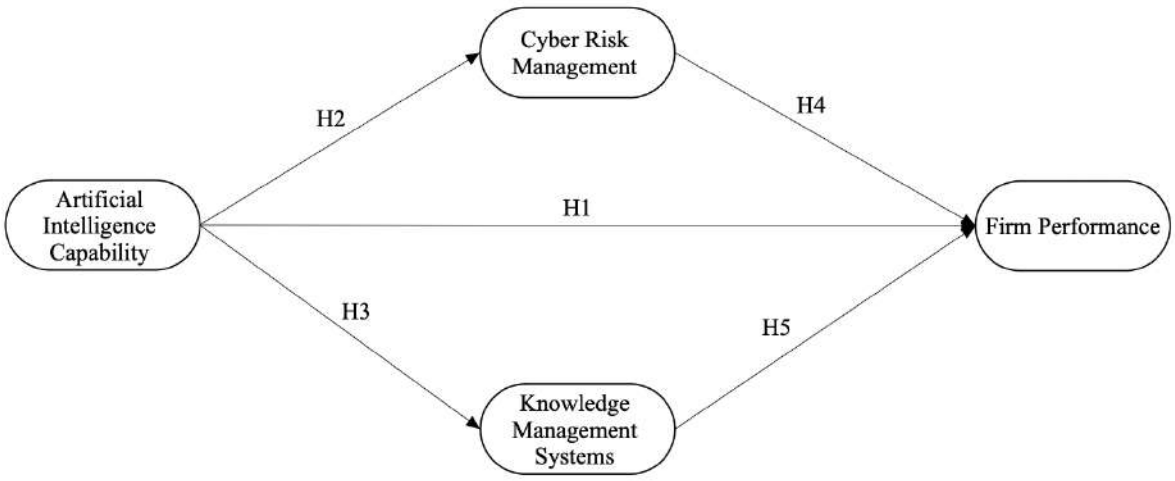

Figure 1: Research model

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

Research Methodology

Research Design

This research employs a quantitative methodology to investigate the influence of artificial intelligence capabilities, cyber risk management, and knowledge management systems on the performance of halal food manufacturing firms in Pakistan. Quantitative research is considered suitable because it enables researchers to objectively investigate correlations among variables through statistical analysis and hypothesis testing (Lim, 2025). Furthermore, the research employed a cross-sectional survey design, collecting data from participants at a single point in time. Moreover, the cross-sectional method is extensively used in organizational and management research since it allows for the efficient and systematic analysis of causal linkages among variables (Hunziker & Blankenagel, 2024).

Target population

The study's population of interest comprises halal food manufacturing companies operating in Pakistan. Similarly, the unit of study comprises managers in halal food manufacturing firms, since they hold substantial knowledge about organizational technical capabilities, cybersecurity procedures, knowledge management systems, and business performance. The participants include operations managers, production managers, IT managers, supply chain managers, quality assurance managers, and senior executives engaged in organizational decision-making processes. In addition, Pakistan is a significant setting for this research, as the halal food production sector has expanded considerably due to rising local and global demand for halal-certified goods. The

escalating digital transformation of industrial processes in Pakistan has heightened the significance of AI capabilities, cybersecurity management, and knowledge management systems in enhancing organizational performance.

Sampling Technique and Sample Size

The research employed a purposive sampling method to select participants from halal food production companies in Pakistan. A purposive sample is deemed suitable, as the research focuses on administrative personnel with relevant organizational expertise and experience in artificial intelligence, cybersecurity procedures, and knowledge management systems. The recommended sample size for structural equation modeling (SEM) investigations typically varies between 200 and 400 participants. This research aims to gather data from approximately 300 management respondents, following the guidelines of Hair et al. (2022), to ensure statistical reliability and sufficient representation of the target population.

Data Collection Method

Primary data were obtained using a standardised questionnaire sent to the management of halal food production companies in Pakistan. The questionnaire was constructed using validated measurement scales derived from earlier research. Data collection was executed using both online and physical survey methodologies to enhance response rates

and accessibility. A pilot study was performed with a small sample of respondents prior to releasing the questionnaire to assess the clarity, reliability, and validity of the survey instrument. Essential improvements were made in response to participant comments to enhance the clarity and pertinence of the questionnaire questions.

Constructs Measurement

The measuring scales employed in this study were derived from previously validated research to confirm the reliability and validity of the variables. The research assessed four primary variables: artificial intelligence capabilities, cyber risk management, knowledge management systems, and organizational performance. Each construct was assessed using five items adapted from existing literature to align with the setting of halal food manufacturing firms in Pakistan. All items were evaluated on a five-point Likert scale, with 1 denoting strong disagreement and 5 indicating strong agreement. The competency of artificial intelligence was assessed using five elements derived from Obenza et al. (2024). Cyber risk management was assessed by five items derived from Siyaya et al. (2025), focusing on cyber threat detection. Furthermore, knowledge management systems were assessed using five items derived from Ma et al. (2025). Moreover, firm performance was evaluated using five factors derived from Atobishi et al. (2024). The modification of existing scales from previous studies improves the content validity and reliability of the measuring instrument employed in the present research.

Data analysis and results

The gathered data were examined using SPSS and SmartPLS. SPSS facilitated preliminary data screening, descriptive statistics, demographic analysis, evaluation of missing values, and reliability assessment. SmartPLS was used to do Partial Least Squares Structural Equation Modeling (PLS-SEM) for hypothesis testing and structural model assessment. PLS-SEM was chosen because it is well-suited to predictive and exploratory research models involving numerous latent dimensions and intricate interactions. Moreover, PLS-SEM is suitable for research incorporating managerial and behavioral dimensions and does not need stringent assumptions about data normality.

Sample Characteristics

The demographic details of the participants in this research are shown in Table 1. The study was completed by 300 management staff members from Pakistani halal food production companies. According to the demographic analysis, male respondents comprised 72.7% (n = 218) of the sample, while female respondents comprised 27.3% (n = 82). The management makeup often seen in Pakistan's manufacturing industry is reflected in this distribution. In terms of age distribution, the majority of respondents were between 31 and 35, comprising 31.3% (n = 94) of the sample. Respondents between the ages of 36 and 40 made up 29.3% (n = 88). 18.7% (n = 56) of respondents were between the ages of 25 and 30, while 20.7% (n = 62) were above the age of 41. The findings show that the respondents had sufficient administrative experience and professional maturity regarding the variables under study.

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

Regarding educational background, 54.0% (n = 162) of respondents held a master's degree, while 30.3% (n = 91) held a bachelor's degree. Just 4.0% (n = 12) of respondents had PhD degrees, while 11.7% (n = 35) had MPhil/MS degrees. The interviewees' educational backgrounds indicate that they were professionally competent and had sufficient academic understanding of technical and management procedures. Production managers made up the largest category of management positions (24.7%, n = 74), followed by operations managers (22.7%, n = 68). IT managers made up 16.3% (n = 49), supply chain managers 18.7% (n = 56), and quality assurance managers 17.6% (n = 53). Respondents from several management departments were included, which improved the data's dependability and comprehensiveness.

According to the work experience analysis, 38.7% (n = 116) of the respondents had 6 to 10 years of professional experience, while 24.3% (n = 73) had 11 to 15 years of experience. 23.7% (n = 71) of participants had one to five years of experience, while 13.3% (n = 40) had more than fifteen years of experience. This distribution shows that most respondents had significant industrial experience related to company performance and organizational technical capabilities. Lastly, in terms of company size, the largest percentage of participating companies was medium-sized businesses (45.7%; n = 137), followed by big businesses (28.3%; n = 85) and small businesses (26.0%; n = 78). The study's results are more broadly applicable to Pakistan's halal food production industry thanks to the involvement of companies with varying organizational sizes.

Table 1: Respondents' data

Demographic	Category	Frequency	Percentage	Total

Variable		(n)	(%)	
Gender	Male	218	72.7	100
	Female	82	27.3	
Age	25–30 Years	56	18.7	100
	31–35 Years	94	31.3	
	36–40 Years	88	29.3	
	41 Years and Above	62	20.7	
Educational Qualification	Bachelor's Degree	91	30.3	100
	Master's Degree	162	54.0	
	MPhil/MS	35	11.7	
	PhD	12	4.0	
Managerial Position	Operations Manager	68	22.7	100
	Production Manager	74	24.7	
	IT Manager	49	16.3	
	Supply Chain Manager	56	18.7	
	Quality Assurance Manager	53	17.6	
Work Experience	1–5 Years	71	23.7	100
	6–10 Years	116	38.7	
	11–15 Years	73	24.3	

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

	Above 15 Years	40	13.3	
Type of Firm	Small Enterprise	78	26.0	100
	Medium Enterprise	137	45.7	
	Large Enterprise	85	28.3	

Measurement model

The measurement model was tested to check the reliability and validity of the constructs employed in this research, i.e. artificial intelligence capabilities, cyber risk management, knowledge management systems, and business performance. The reflective measurement model was assessed using SmartPLS, following the suggestions of Hair et al. (2022). The indicator's dependability was assessed using factor loadings, and all item loadings exceeded the suggested cut-off of 0.70, indicating adequate reliability. Cronbach's alpha (CA) and composite reliability (CR) were used to assess internal consistency. The results indicated that all constructs were above the acceptable threshold of 0.70, indicating high internal consistency. Convergent validity was tested using average variance extracted (AVE). AVE values for all constructs were over 0.50, indicating that the constructs satisfactorily explained the variance in their indicators. Additionally, the Fornell–Larcker criteria and the Heterotrait–Monotrait ratio (HTMT) were used to test discriminant validity. The findings showed that the square root of each construct's AVE exceeded its correlations with other constructs, and HTMT values were below the required threshold of 0.85, indicating appropriate discriminant validity for the constructs. The results indicate that the measurement model has sufficient reliability and validity and is adequate for future examination of the structural model and hypothesis testing (Henseler et al., 2016).

Construct the reliability and validity of the study

We checked construct reliability and validity to verify the consistency, accuracy, and sufficiency of the measuring scales employed in the present study. The reliability of the constructs was examined using Cronbach's alpha (CA) and composite reliability (CR). All constructs' values were above the required threshold value of 0.70, suggesting excellent internal consistency reliability. CR values ranging between 0.70 and 0.95 indicate adequate construct reliability in PLS-SEM (Hair et al., 2022). Convergent validity was tested using factor loadings and average variance extracted (AVE). All indicator loadings exceeded 0.70, and all AVE values exceeded 0.50, indicating that the constructs explained more than 50% of the variance in their respective indicators.

Table 2 shows good construct reliability and validity for all the variables in the research. All measurement items had factor loadings above the suggested level of 0.70, indicating high internal reliability. All constructs had Average Variance Extracted (AVE) values over 0.50, thereby demonstrating sufficient convergent validity. Also, the values of Composite dependability (CR) and Cronbach's Alpha were above the acceptable value of 0.70, which indicates good internal consistency dependability for all constructions. Therefore, the measurement model has adequate reliability and validity to proceed with structural model analysis and hypothesis testing, as recommended by Hair et al. (2022).

Table 2: Constructs reliability and validity

Constructs	Item Codes	Loadings	AVE	CR	Cronbach's Alpha
AI Capability	AIC1	0.812	0.681	0.914	0.883
	AIC2	0.845			
	AIC3	0.836			
	AIC4	0.801			
	AIC5	0.824			
Cyber Risk Management	CRM1	0.821	0.667	0.909	0.875
	CRM2	0.843			
	CRM3	0.798			
	CRM4	0.815			
	CRM5	0.822			
Knowledge Management System	KMS1	0.832	0.689	0.917	0.889
	KMS2	0.851			
	KMS3	0.814			

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

	KMS4	0.826			
	KMS5	0.839			
Firm Performance	FP1	0.841	0.702	0.922	0.894
	FP2	0.857			
	FP3	0.824			
	FP4	0.836			
	FP5	0.845			

Discriminant Validity

Discriminant validity was tested to evaluate the extent to which a variable in the research was statistically unique from other variables. Furthermore, discriminant validity in PLS-SEM refers to the degree to which a construct measures phenomena not measured by other constructs in the model. Discriminant validity was assessed using the Fornell–Larcker criteria and Heterotrait–Monotrait ratio (HTMT) as recommended by Hair et al. (2022). The Fornell–Larcker criteria showed that the square root of the Average Variance Extracted (AVE) of each construct was larger than the construct's correlations with other constructs, which indicates sufficient discriminant validity. Furthermore, the

HTMT values for all construct pairings were below the required threshold value of 0.85, which again supports the uniqueness of the constructs. Henseler et al. (2023) have written that HTMT is among the most reliable methods for testing discriminant validity in variance-based SEM research. The results consequently demonstrate that artificial intelligence capabilities, cyber risk management, knowledge management systems and company performance are statistically different entities. The result is that the measurement model has good discriminant validity.

Table 3: Discriminant Validity (Fornell–Larcker Criteria)

Constructs	AI Capability	Cyber Risk Management	Knowledge Management System	Firm Performance
AI Capability	**0.825**			
Cyber Risk Management	0.612	**0.817**		
Knowledge Management System	0.648	0.635	**0.830**	
Firm Performance	0.701	0.664	0.678	**0.838**

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

The discriminant validity of the measurement model was assessed using the Fornell–Larcker criteria Table 3 and the Heterotrait–Monotrait ratio (HTMT) in Table 4, as suggested by Hair et al. (2022) and Henseler et al. (2023). The Fornell–Larcker test results reveal that the square root of each construct's AVE (bolded numbers on the diagonal) exceeds the correlations among the constructs, supporting discriminant validity for artificial intelligence capability, cyber risk management, knowledge management systems, and firm performance. Similarly, the HTMT values for all pairwise construct combinations are below the threshold of 0.85, indicating that the constructs are empirically distinct and assess separate theoretical notions. The latest methodological development in PLS-SEM uses HTMT as a more conservative criterion for the establishment of discriminant validity, and the findings of this research clearly support the uniqueness of all constructs in the model.

Table 4: Discriminant Validity (HTMT Criteria)

Constructs	AI Capability	Cyber Risk Management	Knowledge Management System	Firm Performance
AI Capability	0.831			
Cyber Risk	0.731	0.778		

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

Management				
Knowledge Management System	0.754	0.742	0.790	
Firm Performance	0.801	0.768	0.783	—

Structural model

The structural model was evaluated to investigate the proposed links among artificial intelligence capabilities, cyber risk management, knowledge management systems, and firm performance using SmartPLS. In accordance with the recommendations of Hair et al. (2021), the assessment of the structural model included analysing path coefficients (β), t-values, p-values, coefficient of determination (R^2), and predictive relevance (Q^2). The importance of the proposed correlations was evaluated using the bootstrapping method with 5,000 resamples. In PLS-SEM, path coefficients (β) signify the magnitude and orientation of links between constructs, with elevated positive β values indicating greater positive associations. Hair et al. (2021) assert that a link is deemed statistically significant when the t-value exceeds 1.96 at the 95% confidence level, and the p-value is below 0.05. Additionally, p-values < 0.01 indicate very significant correlations between constructs, and path coefficients (β) are -+1. The structural model findings revealed positive and significant correlations among the study variables, indicating that artificial intelligence capability positively affects cyber risk management, knowledge management systems, and firm performance, and that cyber risk management and knowledge management systems also positively affect firm performance. The coefficient of

determination (R^2) values further demonstrated the model's efficacy in elucidating the variation in endogenous constructs. The results of the structural model substantiate the provided hypotheses and validate the appropriateness of the theoretical framework for elucidating company performance in halal food manufacturing enterprises in Pakistan (Sarstedt et al., 2014).

The hypothesis results of this study, as shown in Table 5, demonstrate that all presented hypotheses are statistically significant and strongly positively confirmed. The correlation between artificial intelligence capabilities and firm performance ($\beta = 0.412$, $t = 7.103$, $p < 0.001$) indicates that AI capability substantially improves organizational outcomes. Likewise, AI capability demonstrates a robust and significant influence on cyber risk management ($\beta = 0.468$, $t = 8.667$, $p < 0.001$) and knowledge management systems ($\beta = 0.501$, $t = 9.635$, $p < 0.001$), suggesting that organizations with enhanced AI capability are inclined to exhibit superior cybersecurity and knowledge management practices.

Moreover, cyber risk management has a substantial and significant influence on business performance ($\beta = 0.297$, $t = 4.869$, $p < 0.001$), indicating that proficient cybersecurity measures enhance organizational efficiency, resilience, and overall performance. Similarly, knowledge management systems significantly affect organizational

performance ($\beta = 0.354$, $t = 6.211$, $p < 0.001$), underscoring the significance of information exchange, storage, and application in enhancing organizational results. All t-values are above the essential threshold of 1.96, and all p-values are below 0.05, so affirming that all hypotheses are statistically significant at the 95% confidence level, in accordance with structural equation modelling standards (Hair et al., 2022).

Table 5: Hypotheses results

Hypothesis	Paths	β-value	STD	t-values	p-values	Result
H1	AI Capability → Firm Performance	0.412	0.058	7.103	0.000	Supported
H2	AI Capability → Cyber Risk Management	0.468	0.054	8.667	0.000	Supported
H3	AI Capability → Knowledge Management System	0.501	0.052	9.635	0.000	Supported
H4	Cyber Risk Management → Firm Performance	0.297	0.061	4.869	0.000	Supported
H5	Knowledge Management System → Firm Performance	0.354	0.057	6.211	0.000	Supported

Table 6 shows the coefficient of determination (R 2) and the predictive relevance (Q 2) for the endogenous constructs of the research, namely cyber risk management, knowledge management system, and business performance. The R2 values demonstrate the model's explanatory power and the variance of the dependent constructs explained by the independent variable (artificial intelligence capabilities). The findings demonstrate that the R2 value of cyber risk management is 0.438, indicating that the artificial intelligence capabilities can account for 43.8% of the variation, which is a reasonable level of explanatory power. The knowledge management system has the same R2 value of 0.501, which means 50.1% of the variation is explained. This shows a good level of explanatory power. An R2 value of 0.627 for firm performance indicates that 62.7% of the variation in firm performance is explained collectively by artificial intelligence capabilities, cyber risk management, and the knowledge management system, indicating the good explanatory power of the structural model.

Table 6: R^2 and Q^2

Construct	R^2	Q^2
Cyber Risk Management	0.438	0.312
Knowledge Management System	0.501	0.346
Firm Performance	0.627	0.401

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

Table 6 shows the effect size (f^2) values, which assess the individual contribution of each exogenous construct to the endogenous variables in the structural model. The findings reveal that the artificial intelligence capability has a significant effect on cyber risk management (f2 = 0.421) and knowledge management systems (f2 = 0.503), suggesting that the AI capability plays a robust role in improving cybersecurity practices and knowledge management processes in halal food manufacturing firms. The medium effect size (f^2 = 0.318) of cyber risk management on firm performance and the large effect (f^2 = 0.376) of knowledge management system indicate that both constructs are important for the organizational performance improvement, with a greater impact of knowledge management. Finally, the capacity for artificial intelligence has a medium direct influence on firm performance (f^2 = 0.289), indicating that AI enhances performance both directly and indirectly through other organizational capacities. Finally, the findings support the argument that AI competence is a critical driver of organizational capabilities and that knowledge management systems and cyber risk management are essential drivers of firm success.

Table 6: Effect size (f^2)

f^2 Effect Size	Interpretation
0.421 (AI Capability → CRM)	Large
0.503 (AI Capability → KMS)	Large
0.318 (CRM → FP)	Medium

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

0.376 (KMS → FP)	Large
0.289 (AI → FP)	Medium

Conclusions and Discussions

This research investigated the influence of artificial intelligence capabilities, cyber risk management, and knowledge management systems on the performance of halal food manufacturing enterprises in Pakistan. The results indicate that all provided predictions are validated, demonstrating that AI capability is crucial in enhancing organizational systems and performance outcomes. AI capabilities significantly enhance cyber risk management and knowledge management systems, thereby enhancing overall business performance. The findings align with the theoretical frameworks of the Resource-Based View, which assert that organizations gain a competitive advantage by developing and integrating key technologies and organizational skills. The research further substantiates that cyber risk management and knowledge management systems have substantial beneficial impacts on organizational performance. This indicates that enterprises in digitally connected settings, especially within the halal food production industry, must emphasize cybersecurity resilience and efficient information exchange to guarantee operational efficiency, compliance, and innovation. The findings demonstrate that AI capacity directly enhances business performance and indirectly contributes via improved cyber risk management and knowledge management systems, underscoring the need for integrated digital capability development.

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

Implication of the study

This research offers several theoretical, practical, and managerial insights for halal food production companies in Pakistan. This study theoretically enhances the literature on digital transformation by including artificial intelligence capabilities, cyber risk management, and knowledge management systems into a unified research framework to elucidate business performance. The results substantiate the Resource-Based View, Dynamic Capabilities Theory, and Knowledge-Based View by illustrating that technical and knowledge-based capabilities constitute significant strategic resources that augment organizational competitiveness and performance. The report underscores the need for managers and policymakers to invest in AI technology, enhance cybersecurity measures, and establish robust knowledge management systems to augment operational efficiency, foster innovation, and bolster organizational resilience. The results indicate that halal food production companies must use intelligent systems and digital security measures to ensure halal compliance, optimize decision-making processes, and augment supply chain transparency. The report provides essential insights for government bodies and industry regulators to formulate digital transformation strategies and cybersecurity frameworks that facilitate the sustainable development of Pakistan's halal manufacturing sector. The research enhances academic understanding and management practice by highlighting the strategic significance of AI-driven organizational capabilities in attaining better organizational performance.

Limitations and future recommendations

Although this study is a significant contributions, this research has numerous shortcomings that need acknowledgment. The study used a cross-sectional research design, collecting data at a single time point, which limited the ability to demonstrate long-term causal linkages among artificial intelligence capabilities, cyber risk management, knowledge management systems, and company performance. Future studies may use longitudinal designs to more effectively investigate temporal changes and causal relationships. The research examined only halal food manufacturing enterprises in Pakistan, which may limit the generalizability of the results to other sectors or nations. Future researchers are urged to repeat the study across other economic sectors and foreign settings to improve external validity. Third, the research depended on self-reported data from management respondents, potentially introducing common method bias and subjective interpretation. Subsequent research may use diverse data sources or mixed-method strategies to enhance data precision and reliability. The present research only investigated direct correlations among the variables. Future studies may investigate mediating and moderating factors, including organizational culture, digital innovation, technology preparedness, and environmental unpredictability, to enhance understanding of organizational performance. Future research may explore upcoming technologies, like blockchain, big data analytics, and Industry 4.0 techniques, in conjunction with AI capabilities to enhance the literature on digital transformation and organizational performance within the halal manufacturing industry.

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

Reference:

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in iot-based cloud computing: A comprehensive survey. *Electronics*, *11*(1), 16.

Alrubaiee, L., Alzubi, H. M., Hanandeh, R. E., & Al Ali, R. (2015). Investigating the relationship between knowledge management processes and organizational performance the mediating effect of organizational innovation. *International Review of Management and business research*, *4*(4), 989-1009.

Althonayan, A., & Andronache, A. (2019). Resiliency under strategic foresight: The effects of cybersecurity management and enterprise risk management alignment. In *2019 International conference on cyber situational awareness, data analytics and assessment (Cyber SA)* (pp. 1-9). IEEE.

Areghan, E. (2025). Cyber Resilience in Digital Twin and Smart Manufacturing Environments: Challenges, Strategies, and Future Direction. *Journal of Computational Analysis and Applications*, *34*(8), 573-593.

Atobishi, T., Moh'd Abu Bakir, S., & Nosratabadi, S. (2024). How do digital capabilities affect organizational performance in the public sector? The mediating role of the organizational agility. *Administrative Sciences*, *14*(2), 37.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of management*, *17*(1), 99-120.

Fernando, Y., Tseng, M. L., Wahyuni-Td, I. S., de Sousa Jabbour, A. B. L., Chiappetta Jabbour, C. J., & Foropon, C. (2023). Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in Malaysia. *Journal of Industrial and Production Engineering*, *40*(2), 102-116.

Gao, Y., Liu, S., & Yang, L. (2025). Artificial intelligence and innovation capability: A dynamic capabilities perspective. *International Review of Economics & Finance*, *98*, 103923.

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., Danks, N. P., & Ray, S. (2021). *Partial least squares structural equation modeling (PLS-SEM) using R: A workbook*. Springer international publishing.

Hair, J., & Alamer, A. (2022). Partial Least Squares Structural Equation Modeling (PLS-SEM) in second language and education research: Guidelines using an applied example. *Research methods in applied linguistics*, *1*(3), 100027.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2016). Testing measurement invariance of composites using partial least squares. *International marketing review*, *33*(3), 405-431.

Hunziker, S., & Blankenagel, M. (2024). Cross-sectional research design. In *Research design in business and management: A practical guide for students and researchers* (pp. 187-199). Wiesbaden: Springer Fachmedien Wiesbaden.

Islam, M. K., Ahmed, H., Al Bashar, M., & Taher, M. A. (2024). Role of artificial intelligence and machine learning in optimizing inventory management across global industrial manufacturing & supply chain: A multi-country review. *International Journal of Management Information Systems and Data Science*, *I*(2), 1-14.

Jia, S., Khassawneh, O., Mohammad, T., & Cao, Y. (2024). Knowledge-oriented leadership and project employee performance: the roles of organizational learning capabilities and absorptive capacity. *Current Psychology*, *43*(10), 8825-8838.

Kumar, S., & Gupta, S. (2012). Role of knowledge management systems (KMS) in multinational organization: An overview. *International Journal of Advanced Research in computer science and software engineering*, *2*(2).

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, *8*(6), 898.

Lai, J. Y., Wang, J., Ulhas, K. R., & Chang, C. H. (2022). Aligning strategy with knowledge management system for improving innovation and business performance. *Technology Analysis & Strategic Management*, *34*(4), 474-487.

Leoni, L., Ardolino, M., El Baz, J., Gueli, G., & Bacchetti, A. (2022). The mediating role of knowledge management processes in the effective use of artificial intelligence in manufacturing firms. *International Journal of Operations & Production Management*, *42*(13), 411-437.

Lim, W. M. (2025). What is quantitative research? An overview and guidelines. *Australasian Marketing Journal, 33*(3), 325-348.

Ma, L., Ali, A., Shahzad, M., & Khan, A. (2025). Factors of green innovation: the role of dynamic capabilities and knowledge sharing through green creativity. *Kybernetes, 54*(1), 54-70.

Migdadi, M. M. (2022). Knowledge management processes, innovation capability and organizational performance. *International journal of productivity and performance management, 71*(1), 182-210.

Mikalef, P., Islam, N., Parida, V., Singh, H., & Altwaijry, N. (2023). Artificial intelligence (AI) competencies for organizational performance: A B2B marketing capabilities perspective. *Journal of Business Research, 164*, 113998.

Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management, 10*(3), 98-108.

Mohammad, M. F. N., Abdullah, R., Jabar, M. A., Nor, R. N. H., & Nur, N. M. (2024). A theoretical framework of knowledge management systems on quality management systems. *JOIV: International Journal on Informatics Visualization, 8*(4), 2163-2172.

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

Neiroukh, S., Emeagwali, O. L., & Aljuhmani, H. Y. (2025). Artificial intelligence capability and organizational performance: unraveling the mediating mechanisms of decision-making processes. *Management Decision*, *63*(10), 3501-3532.

Obenza, B. N., Salvahan, A., Rios, A. N., Solo, A., Alburo, R. A., & Gabila, R. J. (2024). University students' perception and use of ChatGPT: Generative artificial intelligence (AI) in higher education. *International Journal of Human Computing Studies*, *5*(12), 5-18.

Okoye, S. I. (2017). *Strategies to minimize the effects of information security threats on business performance*. Walden University.

Olan, F., Arakpogun, E. O., Suklan, J., Nakpodia, F., Damij, N., & Jayawickrama, U. (2022). Artificial intelligence and knowledge sharing: Contributing factors to organizational performance. *Journal of Business Research*, *145*, 605-615.

Osobajo, O. A., & Bjeirmi, B. (2021). Aligning tacit knowledge and competitive advantage: a resource-based view. *International Journal of Knowledge Management Studies*, *12*(3), 203-226.

Parsola, J. (2022). Cybersecurity risk assessment and management for organizational security. *NeuroQuantology*, *20*(5), 5330.

Ravikumar, N. (2025). AI-Supported Cybersecurity Monitoring in Enterprise Environments: Enhancing Threat Detection and Response. *Emerging Frontiers Library for The American Journal of Engineering and Technology*, *7*(11), 55-64.

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.

Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European business review*, *26*(2), 106-121.

Shao, S., Shao, Z., & Xiong, Y. (2026). The influence of AI capability on enterprise competitive advantage: the mediating effect of business model innovation. *Journal of Enterprise Information Management*, 1-25.

Siyaya, M. C., Dubihlela, J., & Sibanda, M. (2025). A literature review of internal auditing involvement in cybersecurity risk management of the organization. *Journal of Contemporary Management*, *22*(si1), 89-115.

Sukachova, S., Gorodianska, L., Burmaka, M., Yanenkova, I., & Tkach, I. (2025). Strategies to strengthen cybersecurity for business resilience in the digital age. *Periodicals of Engineering and Natural Sciences*, *13*(1), 263-280.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic management journal*, *18*(7), 509-533.

Teece, D., Peteraf, M., & Leih, S. (2016). Dynamic capabilities and organizational agility: Risk, uncertainty, and strategy in the innovation economy. *California management review*, *58*(4), 13-35.

GRJNST, Volume: 04 - Issue 4 (2026) / ISSN P: 2790-7643
Article ID: 2110
https://doi.org/10.53762/grjnst.04.04.01

Vidović, N., Cvetković, V. M., Beriša, H., & Milašinović, S. (2025). Understanding Ransomware Through the Lens of Disaster Risk: Implications for Cybersecurity and Economic Stability. *International Journal of Disaster Risk Management*, *7*(1), 247-264.

Wahyudi, I., Atmoko, G. D. P., Nurdin, F., & Santoso, T. N. (2026). Optimizing Business Competitiveness Through Artificial Intelligence: A Framework for Digital Innovation and Operational Efficiency. *Advances in Business and Management Research*, 100002.

Yu, C. P., Zhang, Z. G., & Shen, H. (2017). The effect of organizational learning and knowledge management innovation on SMEs' technological capability. *Eurasia Journal of Mathematics, Science and Technology Education*, *13*(8), 5475-5487.

Zheng, X. (2024). How does a firm's digital business strategy affect its innovation performance? An investigation based on knowledge-based dynamic capability. *Journal of Knowledge Management*, *28*(8), 2324-2356.