

ROLE OF DIGITAL TECHNOLOGIES BASED ON CYBERSECURITY AWARENESS IN ENHANCING FIRMS' PERFORMANCE: DIGITAL ACCOUNTING SYSTEMS SETTING

Bilal Nayef Zureigat¹, Hasan Alhanatleh^{2*}, Mahmoud Alghizzawi³,
Abdallah Ali Mohammad Alrifae⁴

Received 17.02.2025.

| Sent to review 05.03.2025. | Accepted 09.08.2025.

Original article



¹ Amman Arab university, accounting department, business faculty, Amman, Jordan

² Applied Science Private University, Management Information Systems, faculty of Business, Amman, Jordan

³ Applied Science Private University, Digital Marketing, faculty of Business, Amman, Jordan

⁴ Middle East University, Human Resource Management, faculty of Business, Amman, Jordan

*Corresponding Author:
Mahmoud Alghizzawi

Email:
dr.alghzawi87@gmail.com

JEL Classification:
G32, L21, L25, M15, M41, O32, O33

Doi: 10.2478/eoik-2025-0070

UDK: 004.738.5:[336.711.6:657.631.6

ABSTRACT

Managing cybersecurity policies and procedures within organizations suggests increasing the efficiency of digital accounting systems and, eventually, the overall performance among Small-Medium Enterprises (SMEs). Therefore, this study aims at exploring the role of cybersecurity awareness and its priors in improving the quality of digital accounting systems and ultimately reinforcing the overall performance SMEs in Jordan. Using a quantitative approach, 435 employees from Jordanian SMEs were surveyed to determine the purpose of this study. Utilizing a structural equation model based on AMOS software, the results of this study indicate that employees' cybersecurity awareness is significantly affected by their priors (Strategies Adopted, Legal Consequences, Proactive, and Information Security). Additionally, the results of this study indicate that employees' cybersecurity awareness significantly influences their adoption of digital accounting systems. Furthermore, the results of this research reveal that the adoption of digital accounting systems significantly influences organizational performance. The results of this research contribute to the related literature through integrating Human-Organization-Technology Theory and Diffusion of Innovations Theory to reinforce SMEs' performance. Finally, the primary practical insight of this study outcomes is that policymakers in SMEs are encouraged to employ assertive policies and procedures regarding cybersecurity settings to obtain digital accounting quality and enhance overall business performance.

Keywords: Cybersecurity awareness, Digital accounting systems, Organization Performance, information security, Intention to use, SMEs.

1. INTRODUCTION

As digital transformation technologies play a critical role in enhancing organizational competitiveness in the market, management accounting systems and innovation capabilities can bolster the productivity of an organization (Ahmad et al., 2024). Among SMEs environments, the usage of accounting information systems plays a primary role in SMEs' sustainability and success of SMEs as accounting information systems strongly enhance the effectiveness of management control processes (Al-Hattami & Kabra, 2024). Additionally, accounting information systems can provide sufficient information and reports that assist policymakers and managers in decision-making processes (Salehi, 2024). Developing accounting information systems offers a positive correlation

with organization performance, Al-Okaily (2024) discovered that well implementation of accounting information systems based on various attributes such as information, system, and services quality, individual performance, and workgroup performance indicate a positive impact on firm performance among listed firms of Jordan. However, there is a consensus that enhancing accounting information systems can improve organizational performance (Elmaasrawy Tawfik, 2024).

Security is a challenge, accounting information is considered a sensitive resource for organizations, and unauthorized access to accounting information can lead to undesirable consequences (Tao et al., 2019). In this digital era, integrating cybersecurity algorithms with digital technologies such as blockchain, big data, cloud computing, and artificial intelligence has the ability to reinforce the adoption of digital technologies among accounting information systems in organizations (Saputra & Paranoan, 2024). As accounting and financial information are targets for attackers, cybersecurity algorithms have become a real alternative for avoiding unauthorized access, accounting information attacks, and financial information crimes (Alhanatleh et al., 2024; Alghizzawi et al., 2024). In this setting, users of accounting information systems play a critical role in protecting personal and accounting information by increasing their knowledge toward the cybersecurity attack types.

The modern resources of cyber risks, rules, and regulations lay companies under robust pressure to create information security measures and offer guarantees to regulators immediately (Yigit Ozkan & Spruit, 2023). Based on this, organizations should provide sufficient policies for accounting information systems users to improve their cybersecurity awareness and clarify the significant role of information confidentiality and integrity regarding accounting and financial information (Anyanwu et al., 2024). SMEs can enhance their information security measures by employing various measurements and standards (Bosanac et al., 2025). Investing in cybersecurity technologies has been an endeavor in various business domains, purposing to provide robust tools for securing business information and resources. Cybersecurity capabilities play a considerable role in the successful implementation of digital transformation technologies (e.g., artificial intelligence, cloud computing, blockchain, and various others) among accounting information systems in organizations, as adopting the quality of cybersecurity tools can assist in the ongoing deployment of digital transformation infrastructure (Alhanatleh et al., 2023; Rabie, 2024; Priambodo et al., 2025). Recent trends in information technology industries have indicated that cybersecurity algorithms provide significant implications in enhancing digital technology development and cyber-attackers have the ability to damage digital information systems and technology infrastructure (Vestad & Yang, 2023). For instance, artificial intelligence capabilities enhance the effectiveness and efficiency of digital accounting systems through cybersecurity among industrial companies in Jordan (Alrfai et al., 2023). Supporting employees with last updates on cybersecurity threats is the most important procedure that organizations should systematically conduct, leading to reinforce a staff culture toward risk management (Cram et al., 2023). Studies in relevant literature have demonstrated that cybersecurity awareness and digital accounting information systems provide critical perspectives to enhance organizational performance (Thamae et al., 2024; Soomro et al., 2024).

The main objective of this study is to explore the critical influence of cybersecurity awareness and digital technologies on industrial firms' performance. This study establishes a new connection between cybersecurity awareness and its priors with digital accounting information systems and firms' performance through applying both Human-Organization-Technology Theory and Diffusion of Innovations Theory. Therefore, searching for these factors suggests new insights to reinforce firms' performance, particularly within emerging nations such as Jordan. The interaction between model constructs provides valuable practical implications for managers of SMEs in industry settings in Jordan in terms of empowering employees with cybersecu-

rity awareness and knowledge, reinforcing the post-adoption of digital accounting information systems, and offering new directions to enhance overall performance.

2. LITERATURE REVIEW

2. 1. STUDY THEME BACKGROUND

Advancements in accounting information systems improve individual, workgroup, and overall organizational performance (Idris et al., 2018; Magboul et al., 2024). Maintaining a high reputation image in the marketplace is considered a strategic key for most organizations, as digital accounting systems can redesign and restructure compliance processes that minimize the potential risk of reputational damage (Ahmad, 2024). Moreover, digital technologies among accounting systems play a considerable role in reducing cost in organizations that digitally change the frames of accounting procedures and practices, leading to cost savings for firms and improving overall firm performance (Jackson & Allen, 2024). Moreover, improving innovation quality among firms is a major factor in reinforcing firms' performance, as the quality of accounting information systems can drive, boost, and motivate firm innovation (Zhang et al., 2024). Accounting information systems offer a high degree of innovation efficiency by adjusting and monitoring firm resources, fostering overall performance.

Recent empirical examinations have asserted that the quality measurements of accounting information systems provide great opportunities to achieve organizational objectives and goals. Hattami et al. (2024) conducted research on accounting information systems using an information success model to evaluate the role of the quality measurements of accounting information systems on SMEs in emerging nations and discovered that high quality accounting information systems offer various advantages for SMEs, such as maximizing the net benefit of employees and managers, facilitating transactions, increasing throughputs, and earning a competitive advantage. In the same vein, Pereira et al. (2024) stated that the quality measurements of accounting information systems have the ability to increase the degree and efficiency of SMEs investments, leading to an enhancement in the decision-making process to ensure SMEs' growth. The authors discovered that a high degree of accounting information system quality enables SMEs to conduct more future investments, making SMEs' performance more active.

To enhance the usage and quality of accounting information systems, most organizations have sought to develop their accounting information systems by deploying digital technologies, providing advanced capabilities to reinforce various features such as accuracy, effectiveness, efficiency, decision-making processes, and overall performance (AlFraihat et al., 2025). In this setting, Adeyeri (2024) asserted that artificial intelligence technologies are considered a critical tool in developing accounting information systems practices, bolstering organizational performance. Therefore, Artificial intelligence tools have changed the form of accounting activities and processes based on several methods such as machine learning, robots, and deep learning, resulting in enhancing operational effectiveness and efficiency, reinforcing financial report quality, automating accounting transactions, and providing reliable and accurate financial information (Azaan & Elsa, 2024). Furthermore, the digital transformation infrastructure among accounting systems plays a primary role in SMEs' performance, which invest in artificial intelligence applications, big data science, and data analytics tools, have a considerable chance to enhance the accuracy and timeliness of accounting and financial information, reduce cost, and eventually boost the efficiency and effectiveness of decision-making (Kusumawardhani et al., 2024). Almaqtari et al. (2024) explored the role of artificial intelligence applications in increasing the usage of accounting information systems among information audit technologies in Middle Eastern nations, discovering that artificial intelligence and digital technologies, such as

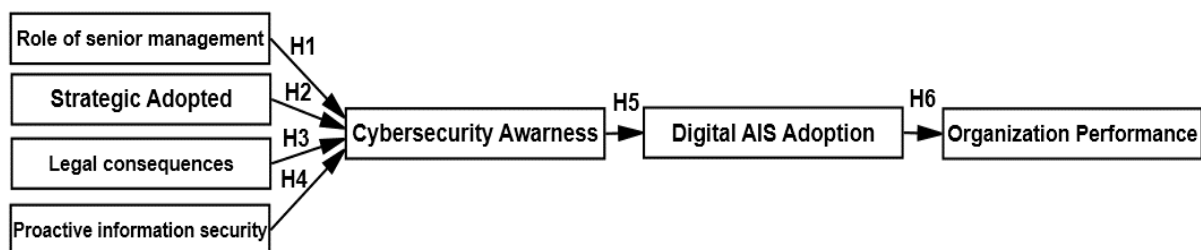
cloud computing and data mining have a critical influence on accounting information systems usage and reinforce the perceived benefits. Therefore, digital information platforms are capable to enhance the productivity of organizations, assist in allocating resources, and support to increase the usage of accounting information systems, especially in emerging nations.

Based on the adoption of modern technologies to implement effective accounting information systems, [Alharasis et al. \(2024\)](#) disclosed that technological factors (relative advantage and compatibility), Organizational factors (top management support, firm size, IT infrastructure, and employees' IT competency), and environmental factors (competitive pressure and client accounting information system complexity) positively influence accounting data quality. As a result, this can reduce user mistakes, improve financial reporting, foster financial and accounting data transparency and accessibility, and enhance decision-making processes among SMEs in Jordan, resulting in sustaining SMEs productivity. In the same context, adopting artificial intelligence technologies, cloud computing platforms, deep learning applications, and big data considerably affects the efficiency and effectiveness of accounting practices and auditing processes through the mediating role of IT governance among SMEs in emerging nations, thereby positively influencing the overall performance of accounting and audit functions ([Almaqtari, 2024](#)). In modern business, digital transformation technologies are considered a primary resource for organizations that enhance their internal and external processes. Therefore, digital transformation capabilities reduce the effort and cost of classifying, filtering, retrieving, and analyzing accounting information and assist organizations in reducing the expenses of management processes ([Ballantine & Galliers, 2017](#)). For instance, blockchain technology as new concept of data structure has changed the form of accounting and financial practices that generate a digital transaction and disseminate it between users, providing various features for accounting processes such as security, decentralization, and group consensus, which supports perceived trust in accounting transactions ([Abad-Segura et al., 2024](#)). In addition, big data applications have been deployed among organizations, offering valuable accounting information to enhance accounting management practices and overall performance ([Sun et al., 2024](#)).

2. 2. DEVELOPED RESEARCH MODEL

The theoretical framework and the hypotheses development of this study's model were well-justified based on cybersecurity setting and digital accounting system literature. Figure 1 provides the conceptual framework of this study that seeks to discover the real influence of employees' cybersecurity awareness based on its priors in enhancing digital accounting information systems and eventually measuring SMEs performance in Jordan. The primary feature of this model is to integrate Human-Organization-Technology theory and Diffusion of Innovations Theory to measure the role of cybersecurity awareness to enhance SMEs performance in Jordan. The model developed in this study considers a few frameworks applied to industrial companies in emerging countries, especially in digital accounting information systems.

Figure 1. Developed research framework



Source: Based on Literature Review

2.2.1. ANTECEDENTS OF CYBERSECURITY AWARENESS

Cybersecurity is a set of processes for providing protection to business from digital crimes that are mostly targeted at harming the physical or soft resources of organizations such as operating systems, network infrastructure, and information systems (Akter et al., 2022). As a stressor factor to enhance cybersecurity functions, cybersecurity awareness is a platform that provides users with the best practices and knowledge to deal with various types of digital threats, aiming to increase their proactive and protective behavior (Neri et al., 2024). To reinforce cybersecurity awareness among businesses, an employees' cybersecurity awareness has been influenced by multiple antecedents, leading to the maximization of employees' protection knowledge to ensure best experiences of usage (Thamae et al., 2024). It has been indicated that Human-Organization-Technology theory has an ability to enhance cybersecurity in organization and cybersecurity awareness among employees (Kumar et al., 2021). Based on Human-Organization-Technology theory that established by (Yusof et al., 2008), this study suggests that legal consequences, proactive information security, role of senior management, and strategies adopted determinants provide a significant role on enhanced cybersecurity awareness in Jordanian SMEs.

The Role of Senior Management implies that various activities of top management should be accomplished in developing organizations such as support, commitment, and participation. It has been confirmed that even though establishing a qualified cybersecurity infrastructure is a cost center, investing in cybersecurity provides positive insights toward reinforcing the information security culture and overall performance within organizations as information technology and top management managers play a critical role in this process (Pigola et al., 2024). The role of senior management has been researched as a primary key for enhancing organizational performance in various settings based on several features such as legitimacy, commitment, evaluation, and ethical leadership (Dora, et al, 2013; Kumar et al., 2021). Commitment, participation, regular evaluation, and ethical leadership of senior management in organizations can considerably improve cybersecurity levels and reinforce employees' cybersecurity awareness (Kumar et al., 2021; Xue et al., 2018).

H₁: the role of senior management has a capacity to influence employees' cybersecurity awareness among SMEs.

Strategies Adopted considered critical determinant of cybersecurity awareness that aligns with the main business strategies of a firm (Nassimbeni et al., 2012). The strategies adopted define various aspects to reinforce cybersecurity awareness. First, providing a clear vision regarding information security can foster employees' cybersecurity awareness and enrich information security knowledge and culture (Mirtsch et al., 2020). Moreover, institutionalized IT security governance is considered a critical aspect of strategies adopted by SMEs to sketch information technology governance procedures and policies to affirm information security execution and security instructions (Moulton & Coles, 2003). Kumar et al. (2021) asserted that institutionalized IT security governance substantially enhances confidentiality, integrity, authenticity, and non-repudiation of organizational information, leading to the management of cyber threats. Furthermore, risk management controls are a critical feature of strategies adopted, aiming to achieve various objectives such as identifying appropriate controls at the strategic level of the organization, determining the degree of compatibility with internet providers, and defining the degree of centralization and decentralization of these controls (Knowles et al., 2015; Van der Haar & Von Solms, 2003). Additionally, reward policy is another considerable feature of adopted strategies that argues that sanctions and rewards play a positive role in motivating employees to follow the information security protocol (Bulgurcu et al., 2010). As a result, applying organizational theories regarding reward policy among SMEs is considered a primary aspect in

forming positive employee behavior and attitudes toward cybersecurity awareness. Finally, information sharing is an influential strategy that encourages the dissemination of information regarding cyber threats and information technology risk among SMEs, which supports the culture of proactive security (Skopik et al., 2016). Information sharing about risks has been confirmed as a primary procedure for increasing employees' cybersecurity awareness (Kumar et al., 2021).

H₂: Strategic adopted has a capacity to influence employees' cybersecurity awareness among SMEs.

Legal Consequences are an additional essential determinant driving employees' cybersecurity awareness in organizations that legal platforms based on assertive sanctions have the capacity to reduce risks and cyber-attacks (Roumani et al., 2015). Informing regulatory authorities about previous cyber-crimes suggests decreasing information security risks among employees (Ratten, 2019). Additionally, using the power of law to monitor employees' behavior during information systems usage is considered a critical procedure to reinforce proactive practice in terms of protection (Samtani et al., 2017). Finally, applying local and international legislation regarding cyber-attacks within organizations can assist in avoiding potential cyber risks (Albrecht, 2016). However, empirical evidence has demonstrated that legal consequences ensure a positive interaction toward enhanced cybersecurity among organizations and reinforce employees' cybersecurity awareness degree (Kumar et al., 2021).

H₃: Legal Consequences has a capacity to influence employees' cybersecurity awareness among SMEs.

Proactive Information Security is considered a significant antecedent of cybersecurity awareness which is achieved by regularly performing frames and updating and providing programs regarding security education, training, and awareness (Sipior et al., 2018; Ekelund and Iskounjina, 2019). Proactive information security occurs by aligning the organization, information technology, and information system strategies to form the policies, procedures, and practices of information technology security (Bulgurcu et al., 2010). A literature review on proactive information security has confirmed that ongoing and proactive environmental analysis regarding cyber threats and attacks assist in addressing such cyber risks and successfully dealing with attacks successfully (Appiah et al., 2020; Kumar et al., 2021). Therefore, providing education and knowledge about possible cyber-attacks increases employees' cybersecurity awareness and security levels among organizations (Kumar et al., 2021).

H₄: Proactive Information Security has a capacity to influence employees' cybersecurity awareness among SMEs.

2. 2. 2. ROLE OF CYBERSECURITY AWARENESS ON DIGITAL ACCOUNTING SYSTEMS USAGE

Cybersecurity attacks have a considerable role in organizational performance as a high degree of cybersecurity procedures reinforces a high rate of performance, improves business value models, increases revenue, and influences organizational reputation, especially among accounting information systems (Alzghoul et al., 2024; Berkman et al., 2018; Curtis et al., 2018). As employees' cybersecurity awareness is a vital element in this context, providing appropriate knowledge and understanding regarding the fundamentals and activities of cybersecurity affirmatively influences employees' behavior toward cyber-attacks during performing accounting and financial practices in digital accounting systems (Hossain & Johora, 2024). In addition, ongoing assessments of cyber threats are considered a critical process that provides employees with the last updates for mitigating risks as regular training is essential for increasing their cybersecurity awareness during digital accounting system usage (Stefanska & Al-Dawod, 2021).

Moreover, it has been disclosed that fostering employees' cybersecurity awareness strongly enhances the protection degree of organization's digital accounting assets (Oroni & Xianping, 2023) and internal processes (Hasani et al., 2023). Recent empirical confirmations in accounting systems literature have asserted that cybersecurity awareness mightily maximizes the degree of dependability in performing accounting and financial transactions based on digital accounting systems, fostering an organization's culture regarding digital accounting information assets (Hasan et al., 2021). Furthermore, empirical validations in the relevant literature have emphasized that employees' cybersecurity awareness considers decisive factors that reinforce the efficiency and effectiveness of digital accounting systems (Alrfai et al., 2023).

H₅: cybersecurity awareness has a capacity to influence digital accounting system use among SMEs.

2. 2. 3. ROLE OF DIGITAL ACCOUNTING SYSTEMS ADOPTION ON ORGANIZATION PERFORMANCE

Based on the diffusion of innovation theory, adoption behavior is a critical determinant employed to discover users' attitudes and future trends toward adopting or utilizing digital technologies (Rogers, 1975). In the context of digital technologies adopted in the accounting field, cloud-based accounting information systems have been adopted to improve the efficiency of accounting information systems among companies (Moudud-Ul-Huq et al., 2020). Advancements in cloud-based accounting information systems have reinforced the capabilities of accounting information resources and company performance (Alshirah et al., 2021). In addition, utilizing artificial intelligence applications within accounting domains assists in increasing the quality of computational accounting transactions, thereby enhancing the decision-making process (Hamza et al., 2024; Masa'deh et al., 2025; Kakizhanova et al., 2025). It has been emphasized that artificial intelligence has an ability to enhance accounting, auditing, and financial operations through handling massive volume of data, enabling robust analysis, risk evaluations, and future predictions (Thottoli, 2024). The use of artificial intelligence tools in accounting plays a significant role in gaining a competitive advantage among companies by boosting operational practice efficiency and adding considerable value to employees and businesses (Shakdwipee et al., 2023). Moreover, employing blockchain technology in accounting domains assists in restructuring accounting and financial data in shared ledgers, supporting various features such as immutability, security, decentralization, traceability, and shared resources (Akter et al., 2024; Masa'deh et al., 2024). The use of blockchain accounting in companies enhances the management of accounting information and overall business performance by filtering and classifying transactions across blockchain accounting (Pflueger et al., 2024; Jiang, 2024). Finally, the use of big data provides another perspective for organizing and managing large amounts of accounting and financial transactions in companies (Sun et al., 2024). It has been disclosed that adopting big data in accounting scopes has an ability to improve accounting management practices and sustain firms' performance (Abdelhalim, 2024).

Overall, deploying digital technologies within the accounting scope benefits organizations by enhancing performance. Empirical validations have supported that adopting digitalization among accounting domains affects the best decision-making practices due to digital technology capabilities in reinforcing the quality of accounting information (Abu Huson et al., 2024; Vărzaru et al., 2022). Among businesses, utilizing digital technologies within accounting improves strategic performance and influences growth and performance (Nassani et al., 2023). Moreover, digital technologies based on cybersecurity adoption reinforce SMEs performance by advancing accounting and financial resources, consumer orientations, interior business processes, and organizational growth and learning (Alrfai et al., 2023; Hasani et al., 2023).

H₆: Digital accounting systems adoption has a capacity to influence organization performance among SMEs.

3. METHODOLOGY

This study is quantitative in nature by discovering the interactions between exogenous and endogenous factors of the developed model to explore the real insights of cybersecurity awareness based on its priors on digital accounting information systems and organizational performance among industrial companies from the employees' perspective. Quantitative analyses were performed at various stages. First, establishing a relative literature review of accounting domains, cybersecurity awareness, and digital transformation technologies is essential. Next, the research model was developed to integrate the model constructs. The sampling technique, data collection methods, analysis procedures, and analysis software were used to obtain the outcomes of this study. Additionally, the results of this study are in accordance with prior studies. Finally, research insights regarding the findings are presented.

The model of this study consists of seven constructs: cybersecurity awareness and its priors (four constructs), digital accounting information systems, and organizational performance. The instrument items of the seven constructs were adapted from the well-justified relevant literature in the study field. First, the items of cybersecurity awareness antecedents were adapted from (Kumar et al., 2021) as the role of senior management was measured based on four items, strategies adopted were measured based on three items, legal consequences were measured based on five items, and proactive information security was measured based on five items. Moreover, the items of the cybersecurity awareness construct were adapted based on 4-items from (Khando et al., 2021; Oroni & Xianping, 2023). Furthermore, the items of the digital accounting systems were adapted based on 5-items from (Tan et al., 2009). Finally, the items of organizational performance were adapted based on 5-items from (Rawat et al., 2019; Oroni & Xianping, 2023). Therefore, the responses of SMEs employees were gradually ranked utilizing a Five-point Likert scale categorizing from "Totally disagree" describing the lowest level of SMEs performance to "Totally agree" describing the highest level of SMEs performance. After developing the research instrument's items, four linguistic experts were invited to translate the items into Arabic because of the nature of the research population, as this process has the capacity to provide reliable responses (Alhanatleh et al., 2022). Next, a pilot study was conducted by selecting 25 digital accounting information system employees to complete the new version of the study instrument. The outcomes show that all constructs' items had a strong factor loading (>.60) and some items were modified and rephrased for enhancing their clarity based on pilot study respondents. As a result, the internal consistency of model constructs and items' content validity were strongly improved.

Listed SMEs in the Jordanian Chamber of Industry (JCI) were used to determine the population and sample size of this study. The total number of SMEs is 15571 the total number of employees is 264198 (JCI, 2023). However, the population of the current study comprised employees who deal with digital accounting information systems among SMEs in Jordan (accountants, accounting heads of departments, accounting managers, information technology employees, information technology managers, and managers in top management). The probability sampling method was employed to determine the required sample, as this approach can support a common bias and generalize the study's outcomes. Based on this method, a random sample technique was used to choose 550 employees who deal with digital accounting systems in SMEs in Jordan. After generating an electronic survey based on Google Form, the link was disseminated to reach the selected sample. The current research was approved by the Amman Arab University research ethics committee, which is established by the deans' council, as the official document number is (39/2021-2022), Decision No.: 70, Date: 20/07/2022, Rev. d). Ethical matters were

completely issued in data collection process and the present study obligated to all principles of informed consent, confidentiality, and harm. Therefore, only 483 responses were returned after the questionnaire was completed. Only 435 responses were used for the analysis, as this number is appropriate for accomplishing analysis procedures (Awang, 2018). The data collection stages began on April 22, 2024, and finished on June 6, 2024.

4. RESULTS

Two popular analysis software packages, SPSS and AMOS Version 22, were employed to evaluate the findings of this research. The AMOS program has the ability to generate reliable and accurate findings, especially among multi-construct models, such as the current study model (Ringle et al., 2020). The analysis stages of this research followed methodological procedures (Sarstedt et al., 2021). First, the dataset of responses was prepared using the SPSS program by performing various statistical methods such as coding, missing values, outliers, skewness, and normally distributed data. Second, the reliability and validity of this study model were confirmed using the AMOS program through a confirmatory factor analysis approach, using various statistical methods such as model fit indices, construct reliability, convergent reliability, and discernment validity. Finally, sophisticated hypotheses findings were retrieved using AMOS by employing the structural equation model technique.

4.1. MITIGATION OF COMMON METHOD BIAS

To ensure the common method bias of the study model constructs, Harman's single-factor evaluations were employed through using Exploratory Factor Analysis (EFA). The required cut-off value to judge the common method bias is that the total variance of first component should be < 50% as proposed by Podsakoff et al. (2003). Therefore, all constructs' items (29 items) of this study's model were subjected to EFA as a single construct. Table 1 provides that the total variance of first component is (39.962%) which indicates that common method bias is not a critical matter regarding the model constructs of this study.

Table 1. The obtained outcomes of common method bias.

Components	Total	Percentage of variance	Cumulative Percentage
1	11.589	39.962	39.962
2	4.079	14.065	54.027
3	2.744	9.463	63.490
4	1.127	3.885	67.375
5	.942	3.248	70.623
6	.869	2.996	73.619
7	.716	2.468	76.087

Source: Based on SPSS Software.

4.2. THE VALIDITY AND RELIABILITY OF MODEL CONSTRUCTS

After completing data preparation, ensuring construct validity and reliability is a required process that is established by evaluating three major measurements (convergent validity, composite reliability, and discriminant validity), as recommended by (Rex, 2011). To do so, all construct items of this study model were subjected to confirmatory factor analysis assessments. Therefore, the first step in the validity and reliability measurements is to ensure the values of items' loading factors and covariance correlation between all constructs model achieved their cut-off values ($\geq .50$ and $\leq .85$, respectively), leading to a model fit adequacy, as confirmed by (Raza & Awang, 2021). The model fit adequacy was evaluated by statistically computing vari-

ous indices based on their threshold values, as supported by (Awang, 2018; Talwar et al., 2019). Table 2 shows the cut-off values and the retrieved index values regarding this study's model, which strongly support the adequacy of the model fit, as this guides the analysis of this research to conduct the validity and reliability measurements.

Table 2. The retrieved findings of Model Fit indices

Indices	CMIN/DF	GFI	NFI	CFI	AGFI	TLI	RMSEA
Cut-off values	< 5 or < 3	$\geq .90$ or $\geq .85$	$\geq .90$ or $\geq .85$	$\geq .90$ or $\geq .85$	$\geq .90$ or $\geq .85$	$\geq .90$ or $\geq .85$	< 0.08
Retrieved results	2.478	.892	.901	.938	.865	.928	.057

Source: Based on Literature and AMOS Software

In the setting of convergent validity and construct reliability assessments, Hermida (2015) affirmed that the convergent validity measurement computed based on the cut-off values of the factor loading approach and Average Variance extracted technique (AVE) as suggested cut-off values for both measurements was $\geq .50$. Brown (2015) ensured that the construct reliability measurements were computed based on the cut-off values of composite reliability evaluations (CR) and Cronbach's alpha measurements (α), as the proposed cut-off values for both measurements was $\geq .70$. Table 3 shows the concluded outcomes regarding the construct validations, which noticeably confirm the statistical evidence of convergent validity and construct reliability.

Table 3. Findings Matrix regarding convergent validity and construct reliability (N=435)

Constructs	Coding Items	Factor Loading $\geq .60$	AVE	CR	α
Legal consequences	LCO.1	.771	0.545	0.780	0.774
	LCO.2	.637			
	LCO.3	.796			
Proactive information security	PIS.1	.802	0.639	0.842	0.840
	PIS.2	.823			
	PIS.3	.773			
Role of senior management	RSM.1	.790	0.661	0.886	0.885
	RSM.2	.872			
	RSM.3	.829			
	RSM.4	.756			
Strategies adopted	STA.1	.656	0.516	0.841	0.836
	STA.2	.696			
	STA.3	.845			
	STA.4	.638			
	STA.5	.597			
Cybersecurity awareness	CYA.1	.806	0.622	0.868	0.862
	CYA.2	.780			
	CYA.3	.740			
	CYA.4	.828			
Adoption of Digital accounting systems	ADA.1	.705	0.545	0.856	0.851
	ADA.2	.752			
	ADA.2	.798			
	ADA.4	.744			
	ADA.5	.731			
Organization Performance	OGP.1	.600	0.673	0.910	0.902
	OGP.2	.866			
	OGP.3	.906			
	OGP.4	.887			
	OGP.5	.809			

Source: Based on AMOS Software

To finalize the constructs' validation measurements, **Awang (2018)** emphasized that discernment validity measurements are an essential aspect. Therefore, discernment validity measurements are computed based on the proposed equation: AVE's square root of all model constructs (bold font) are $>$ AVE's absolute values of interior correlations, as asserted by **Dijkstra and Henseler (2015)**. Table 4 clarifies the conclusions of the discernment validity measurements, which significantly indicate statistical evidence regarding the discernment validity of the current model constructs. Based on the above-mentioned statistical computations, the validity and reliability of this study model were accomplished and received further empirical proof to conduct the next analysis stage.

Table 4. Findings Matrix regarding discernment validity measurements

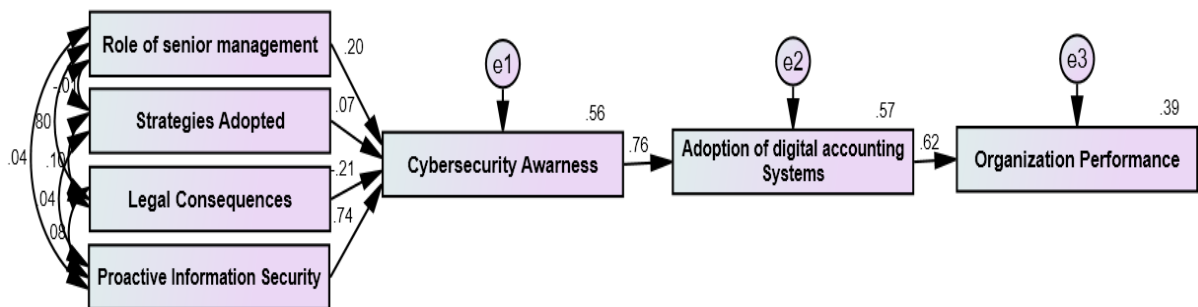
	1	2	3	4	5	6	7
Adoption of Digital accounting systems	0.738						
Legal consequences	0.037	0.738					
Proactive information security	0.521	0.072	0.800				
Role of senior management	0.135	0.712	0.034	0.813			
Strategies adopted	0.050	0.092	0.037	-0.023	0.718		
Cybersecurity awareness	0.687	0.007	0.662	0.053	0.065	0.789	
Organization Performance	0.568	0.073	0.602	0.095	0.093	0.797	0.821

Source: Based on AMOS Software

4. 3. STRUCTURAL EQUATION MODEL FOR HYPOTHESES FINDINGS

After confirming the validity and reliability of the model constructs, a new dataset was generated using the regression imputation method. Based on this, the interactions between model constructs were implemented using the structural equation model approach to estimate the hypotheses' findings. Therefore, Figure 2 and Table 5 indicate the findings of the developed hypotheses regarding the present study, summarizing that all the hypotheses received significant support. At the outset, squared multiple correlations (R^2) were evaluated to determine the total variance effect of the exogenous factors on the endogenous factors, as shown in Figure 2. The outcome of the computed (R^2) of cybersecurity awareness is about 0.563, clarifying that the exogenous factors (role of senior management, strategies adopted, legal consequences, and proactive information security) have the ability to predict 56.3% of the total variance effect on cybersecurity awareness. Furthermore, the computed (R^2) of adoption of digital accounting is nearly 0.573, explaining that the exogenous factor (cybersecurity awareness) has the ability to predict 57.3% of the total variance influence on the adoption of digital accounting. Finally, the computed (R^2) of organizational performance is roughly 0.390, indicating that the exogenous factor (adoption of digital accounting) has the ability to predict 39% of the total variance influence on organizational performance.

Figure 2. The structural equation model estimations of the study model



Source: Based on estimations of SEM in AMOS Software

Table 5 presents the estimated findings for the current research hypotheses. First, the findings reveal that the role of senior management offers a significant and positive influence on cybersecurity awareness among employees in Jordanian SMEs ($\beta=0.220^{***}$), as the first hypothesis receives empirical evidence. Furthermore, the findings indicate that the confirmed strategies offer a significant and positive influence on cybersecurity awareness among employees in Jordanian SMEs ($\beta=0.088^*$), as the second hypothesis receives empirical evidence. Additionally, the findings affirmed that legal consequences have a significant influence on cybersecurity awareness among employees in Jordanian SMEs ($\beta= -0.272^{***}$), as the third hypothesis received empirical evidence. Moreover, the findings emphasize that proactive information security has a significant and positive influence on cybersecurity awareness among employees in Jordanian SMEs ($\beta=0.852^{***}$), as the fourth hypothesis receives empirical evidence. In addition, the findings revealed that cybersecurity awareness has a significant and positive influence on the Adoption of Digital accounting among employees in Jordanian SMEs ($\beta=0.634^{***}$), as the fifth hypothesis receives empirical evidence. Finally, the findings reveal that the Adoption of Digital accounting asserts a significant and positive influence on organizational performance among employees in Jordanian SMEs ($\beta=0.537^{***}$), as the sixth hypothesis receives empirical evidence.

Table 5. The statistical evaluations of hypotheses findings

Hypothesis	β	S.E.	C.R.	P
Role of senior management $\rightarrow$ Cybersecurity awareness	.220	.057	3.858	***
Strategies adopted $\rightarrow$ Cybersecurity awareness	.088	.037	2.377	.017
Legal consequences $\rightarrow$ Cybersecurity awareness	-.272	.066	-4.094	***
Proactive information security $\rightarrow$ Cybersecurity awareness	.852	.036	23.938	***
Cybersecurity awareness $\rightarrow$ Adoption of Digital accounting systems	.634	.026	24.780	***
Adoption of Digital accounting systems $\rightarrow$ Organization Performance	.537	.031	17.080	***

Notes: $*p < 0.05$; $**p < 0.01$; $***p < 0.001$

Source: Based on AMOS Software evaluations

5. DISCUSSION

The main objective of this study was to empirically estimate the role of cybersecurity based on its antecedents in digital accounting systems and, eventually, overall organizational performance among SMEs in Jordan from employees' perspectives. The findings of this study show that all the developed hypotheses receive empirical support. The findings of (R^2) indicate that cybersecurity awareness based on priors and digital accounting systems can predict the overall performance of SMEs in Jordan.

The findings of H_1 indicate that the role of senior management has a positive and significant influence on cybersecurity awareness, which is congruent with prior studies (Pigola et al., 2024; Kumar et al., 2021; Xue et al., 2018). This empirical validation suggests that establishing an adequate information security culture among SMEs in Jordan can enhance employees' cybersecurity awareness and lead to applicable cybersecurity objectives. Ongoing evaluation of the cybersecurity level is a required process that managers should conduct to continuously improve cybersecurity goals. The findings of H_2 reveal that strategic adoption ensures a positive and significant influence on cybersecurity awareness, which is congruent with prior studies in existing literature (Skopik et al., 2016; Kumar et al., 2021). This empirical evidence suggests that senior managers in SMEs in Jordan may always seek to enhance their strategic vision regarding information security, leading to practical information technology security purposes. Adopting

appropriate information security risk management controls assists in reducing cybersecurity threats and reinforces employee cybersecurity awareness. Sharing analyzed information and knowledge about cybersecurity threats with other SMEs in Jordan suggests that it bolsters information security goals and increases employees' cybersecurity awareness.

The findings of H_3 found that legal consequences are a considerable determinant of cybersecurity awareness, which is congruent with prior studies in the existing literature (Ratten, 2019; Samtani et al., 2017; Kumar et al., 2021). The negative value of the relationship indicates that increasing legal consequences framework decreases employees' cybersecurity awareness. The potential explanation of negative relationship is that assertive legal consequences may lead to decrease employees' engagement with cybersecurity among SMEs in Jordan. In addition to, overreliance on legal consequences platforms may provide employees with a fake security feeling, supporting that the responsibilities of cybersecurity awareness assign to SMEs in Jordan, leading to believe that legal consequences can prevent cybersecurity risks without an effective employee participating. Furthermore, employees of SMEs in Jordan may consider legal consequences as perceived irrelevance, leading to reduce their responsibilities about threats and accountability. However, this empirical validation suggests that complying with law-enforced surveillance approaches is a required procedures for SMEs in Jordan, assisting in increasing the protection rate against various sources of cyber threats. Reporting prior cybersecurity attacks to regulatory authorities is a necessary process that helps reinforce information protection and positively influences employees' cybersecurity awareness. The findings of H_4 reveal that proactive information security is critical prior to cybersecurity awareness, which is congruent with prior studies in the existing literature (Appiah et al., 2020; Kumar et al., 2021). This empirical evidence indicates that senior managers of information technology security should revise and update the policies of internet services among SMEs in Jordan. In addition, having qualified training programs on security issues suggests maximizing the rate of employees' cybersecurity awareness.

The findings of H_5 emphasize that cybersecurity awareness strongly influences the adoption of digital accounting systems, which is congruent with prior studies in existing literature (Oroni & Xianping, 2023; Alrfai et al., 2023). This empirical evidence suggests that SMEs in Jordan should support their employees with sufficient knowledge and experience toward cybersecurity awareness policies, leading to enhanced digital accounting system usage. Preparing comprehensive training programs on employees' cybersecurity awareness, including managerial practices, cyber risks, security policies, and compliance, suggests an increase in the adoption rate of digital accounting systems among SMEs in Jordan. The findings of H_6 support the idea that the adoption of digital accounting systems has a significant influence on organizational performance, which is congruent with prior studies in existing literature (Pflueger et al., 2024; Jiang, 2024). This empirical evidence confirms that adopting digital accounting systems robustly enhances the value, competitiveness, and overall performance of SMEs in Jordan. Therefore, SMEs in Jordan should carefully choose adequate digital technologies to implement effective accounting systems to serve accounting practices and ultimately enhance organizational performance.

6. RESEARCH IMPLICATIONS

6.1. THEORETICAL IMPLICATIONS

This study provides new theoretical insights into relevant literature. Firstly, this study explores factors influencing SMEs performance through integrating Human-Organization-Technology theory and Diffusion of Innovations theory to enhance overall performance among organizations. The current study differs from previous investigations by interacting model constructs to predict SMEs performance, especially in developing nations. By integrating previous theories,

the retrieved results of (R^2) by the SMEs performance construct were 39%. The most likely explanation is that employees who have better knowledge and understanding of cybersecurity policies could be more realized regarding the riskiness of cyber-attacks, while employees who have sufficient skills to use digital accounting systems could positively affect organizational performance. Second, the outcomes of this research confirm that the Human-Organization-Technology theory support that the alignment between SMEs components (employees, organizational, and information technology) provides a strong chance for successful digital accounting information systems implementation and quality. In addition to, the outcomes of this study ensure that extending the Human-Organization-Technology theory by combining Diffusion of Innovations theory has an ability to offer a comprehensive overview about the dynamic changes affecting each dimension of Human-Organization-Technology model. Thirdly, to the best of the authors' knowledge and experience, this study considers the first research of its kind, which explores the role of cybersecurity awareness based on the role of senior management, strategies adopted, legal consequences, and proactive information security on digital accounting systems to estimate overall performance among SMEs in developing nations. Finally, the findings of this research ensure that increasing employees' cybersecurity awareness can drive the process of adopting digital accounting systems and significantly influence overall performance among SMEs in Jordan.

6. 2. PRACTICAL IMPLICATIONS

Moreover, this study offers several practical implications. Cyber risks in developing countries are considered a great defiance to employees, businesses, and digital accounting systems. From a research point of view, the findings of this work concentrate on the necessity to conduct further scientific research into the determinants affecting cybersecurity awareness. Furthermore, it explores how cybersecurity awareness influences the adoption of digital accounting systems, and ultimately, overall organizational performance. The findings of this research indicate that the role of senior management, strategies adopted, legal consequences, and proactive information security in digital accounting systems as determinants have the ability to form employees' cybersecurity awareness. Therefore, enhancing these determinants will positively affect employees' behavior toward cybersecurity awareness. Moreover, SMEs may prioritize employees' cybersecurity awareness based on their priors in order to reinforce digital accounting system usage. By doing so, SMEs can affirm a secure workplace environment, particularly during digital accounting system usage to conduct accounting and financial transactions. Additionally, implementing an adequate and effective digital accounting systems depending on cybersecurity measures can protect accounting and financial assets and significantly impact SMEs performance in Jordan. Subsequently, senior managers, policymakers, information technology, and accounting managers among SMEs in Jordan could establish the following practical insights:

- Continually analyze and classify various cyber threats to reform and update cybersecurity policies. Therefore, applying an adequate cybersecurity framework can support SMEs to systematically perform segmentation of cyber-attack resources that greatly enhances employees' cybersecurity awareness and quick responses to reduce the negative impact of cyber-risks. This process can support SMEs readiness to mitigate different type of risks.
- Continuous to evolve new regulations, principles, and instructions can assist SMEs to report cyber-attacks and enhance threat detection strategies.
- SMEs may use several tools to improve cyber-attacks monitoring such as employees' behavior analytics that allow SMEs to quickly detect various resources of dubious practices. Using proactive detection methodologies has an ability to support a quick re-

sponse and contain emerging cyber-attacks.

- Providing employees with practical skills and knowledge regarding cybersecurity awareness through qualified workshops and training. To provide a quick response, using digital marketing tools such as short video approach may help SMEs to provide a quick training for employees.
- Develop an infrastructure of digital accounting systems in accordance with safety and security policies to offer quality outcomes regarding accounting and financial practices and eventually strengthen SMEs performance. Improving digital accounting systems infrastructure can enhance the efficiency and effectiveness of SMEs as upgrading with high-quality servers, adopting new digital platform like cloud-based accounting systems, and ensuring security of data enable SMEs to perform their core functions and timely execute accounting transactions. These enhancements help SMEs to increase the quality of accounting and financial functions, resulting in fostering SMEs performance.

6. 3. LIMITATIONS AND FUTURE RESEARCH

Similar to prior empirical investigations, this study has various challenges, limitations, and potential future work. At the outset, the study findings need to be generalized. Future work may be conducted in various fields to maximize the sample size and generalize the outcomes. Next, even though this study uses some techniques to mitigate common method bias and causal inference issues, there is risks to generalize and mislead hypotheses claims. To reduce these issues, conducting research from multiple sources has an ability to mitigate common method bias matters and performing longitudinal research design can minimize causal inference matters. Additionally, this study focuses on employees' perspectives as human behavior that considers a complex to be measured due to multiple internal and external factors affecting their behavior and attitude. Future trends could investigate the same model based on a time-series approach that is expected to provide considerable insights into the current study area. The organization size also suggests to be a stressor factor as the type of training and cybersecurity infrastructure distinguishes among large and small businesses. Future works may consider organization size as primary key to increase organization performance. In addition to, focusing on how legal consequences framework opens critical opportunities to conduct further investigations to highlight factors increasing cybersecurity awareness and SMEs performance such as employee engagement, trust, psychological mechanisms, and perceived fairness. Moreover, the mediating role of cybersecurity awareness and digital accounting systems has not yet been estimated. Future studies may make additional contributions by examining these directions. Furthermore, organization type and age as moderator factors suggest a deep understanding toward SMEs performance in Jordan, as they could be evaluated. Besides, adding other factors to the current study's model is expected to offer a comprehensive overview of its objectives. As widely investigated in relevant literature, adding cybersecurity knowledge may drive cybersecurity awareness and reinforce digital accounting system usage. Finally, future trends may employ various theoretical backgrounds to confirm the relationship between cybersecurity awareness and business performance. Resource-Based View, Institutional Theory, and Contingency Theory have an ability to clarify the nexus between cybersecurity awareness and business performance.

7. CONCLUSION

Owing to the rapid development of digital business, there is a large demand to reinforce the performance level among organizations and employees. Cybersecurity awareness, as a major stressor, is influenced by various factors such as human factors, organizational capabilities, and technology factors. This study investigates the role of cybersecurity awareness based on

its priors in enhancing the capabilities of digital accounting systems and increasing SMEs performance in Jordan. The outcomes of this study assert that the role of senior management, strategies adopted, legal consequences, and proactive information security play a critical role in increasing the knowledge and vision of employees' cybersecurity awareness to safeguard themselves from cyber threats among SMEs in Jordan. SMEs in Jordan can establish powerful cybersecurity strategies to positively affect employees' behavior and knowledge of using digital accounting systems. Thus, SMEs reinforce a secure business environment that likely maximizes the adoption rate of digital accounting systems and enhances the overall performance of SMEs in Jordan. The outcomes of this study also affirm that senior managers of SMEs in Jordan can take pre-action measures based on the interplay between model constructs to increase employees' cybersecurity awareness to enhance digital accounting system functions, resulting in fostering companies' performance. Therefore, this research distinguishes from prior works by contributing to relevant literature through confirming the role of the Human-Organization-Technology model and Diffusion of Innovations theory, especially among SMEs in a developing economy. The combination between these theories is firstly ensured in this study that addresses the understanding of the complex interplay between cybersecurity awareness and SMEs performance in Jordan.

REFERENCES

- Abad-Segura, E., Infante-Moro, A., González-Zamar, M. D., & López-Meneses, E. (2024). Influential Factors For A Secure Perception Of Accounting Management With Blockchain Technology. *Journal of Open Innovation: Technology, Market, and Complexity*, 100264. <https://doi.org/10.1016/j.joitmc.2024.100264>
- Abdelhalim, A. M. (2024). How management accounting practices integrate with big data analytics and its impact on corporate sustainability. *Journal of Financial Reporting and Accounting*, 22(2), 416-432. <https://doi.org/10.1108/JFRA-01-2023-0053>
- Abu Huson, Y., Sierra-García, L., & Garcia-Benau, M. A. (2024). A bibliometric review of information technology, artificial intelligence, and blockchain on auditing. *Total Quality Management & Business Excellence*, 35(1-2), 91-113. <https://doi.org/10.1080/14783363.2023.2256260>
- Adeyeri, T. B. (2024). Automating Accounting Processes: How AI is Streamlining Financial Reporting. *Journal of Artificial Intelligence Research*, 4(1), 72-90. <https://thesciencebrigade.com/JAIR/article/view/166>
- Ahmad, A. Y. B. (2024). Firm Determinants that Influences Implementation of Accounting Technologies in Business Organizations. *WSEAS Transactions on Business and Economics*, 21, 1-11. <https://doi.org/10.37394/23207.2024.21.1>
- Ahmad, A., El-Dalameh, S., Al-Shakri, K., Alkhawaldeh, B., & Alsmadi, L. (2024). The link between management accounting information systems and firm competitiveness: The mediating role of innovation capabilities. *Uncertain Supply Chain Management*, 12(3), 1781-1790. <https://doi.org/10.5267/j.uscm.2024.3.004>
- Akter, M., Kummer, T. F., & Yigitbasioglu, O. (2024). Looking beyond the hype: The challenges of blockchain adoption in accounting. *International Journal of Accounting Information Systems*, 53, 100681. <https://doi.org/10.1016/j.accinf.2024.100681>
- Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Annals of operations research*, 1-26. <https://doi.org/10.1007/s10479-022-04844-8>
- Albrecht, J. P. (2016). How the GDPR will change the world. *European Data Protection Law Review*, 2, 287. <https://doi.org/10.21552/EDPL/2016/3/4>
- Alghizzawi, M., Ezmigna, I., Ezmigna, A. A. R., Alhawamdeh, Z. M., Hammouri, M. A., Alawneh, E., & Al-Gasawneh, J. A. (2024). The Big Data Analysis and Digital Marketing. In *Opportunities and Risks in AI for Business Development: Volume 2*, 1-10. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-65207-3_1
- Alhanatleh, H., Alghizzawi, M., Habes, M., Tahat, K., & Tahat, D. N. (2023, November). The Impact of Digital Marketing Through the TikTok Application on Purchase Intent. In *2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS)*, 1-6. IEEE. <https://doi.org/10.1109/SNAMS60348.2023.10375451>
- Alhanatleh, H., Khaddam, A., & Abousweilem, F. (2022). Mobile government public value model for assessing the public institution's services: evidence through the context of Jordan. *International Journal of Data and Network Science*, 6(4), 1295-1308. <https://doi.org/10.5267/j.ijdns.2022.6.005>
- Alhanatleh, H., Khaddam, A., Abudabaseh, F., Alghizzawi, M., & Alzghoul, A. (2024). Enhancing the public value of mobile fintech services through cybersecurity awareness antecedents: A novel framework in Jordan. *Investment Management and Financial Innovations*, 21(1), 417-430. [https://doi.org/10.21511/imfi.21\(1\).2024.32](https://doi.org/10.21511/imfi.21(1).2024.32)
- Alharasis, E. E., & Alkhwalidi, A. F. (2024, June). The Implementation of Advanced AIS and the Accounting Data Quality: The Case of Jordanian SMEs. In *International Conference on Human-Computer Interaction*, 149-173. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-61318-0_11
- Al-Hattami, H. M., & Kabra, J. D. (2024). The influence of accounting information system on management control effectiveness: The perspective of SMEs in Yemen. *Information Development*, 40(1), 75-93. <https://doi.org/10.1177/02666669221087184>

- Al-Hattami, H. M., Senan, N. A. M., Al-Hakimi, M. A., & Azharuddin, S. (2024). An empirical examination of AIS success at the organizational level in the era of COVID-19 pandemic. *Global Knowledge, Memory and Communication*, 73(3), 312-330. <https://doi.org/10.1108/GKMC-04-2022-0094>
- Almaqtari, F. A. (2024). The Role of IT Governance in the Integration of AI in Accounting and Auditing Operations. *Economies*, 12(8), 199. <https://doi.org/10.3390/economies12080199>
- Almaqtari, F. A., Farhan, N. H., Al-Hattami, H. M., Elsheikh, T., & Al-dalaien, B. O. A. (2024). The impact of artificial intelligence on information audit usage: Evidence from developing countries. *Journal of Open Innovation: Technology, Market, and Complexity*, 10(2), 100298. <https://doi.org/10.1016/j.joitmc.2024.100298>
- Al-Okaily, M. (2024). Assessing the effectiveness of accounting information systems in the era of COVID-19 pandemic. *VINE Journal of Information and Knowledge Management Systems*, 54(1), 157-175. <https://doi.org/10.1108/VJKMS-08-2021-0148>
- Alrfai, M. M., Alqudah, H., Lutfi, A., Al-Kofahi, M., Alrawad, M., & Almaiah, M. A. (2023). The influence of artificial intelligence on the AISs efficiency: Moderating effect of the cyber security. *Cogent Social Sciences*, 9(2), 2243719. <https://doi.org/10.1080/23311886.2023.2243719>
- Alshirah, M., Lutfi, A., Alshirah, A., Saad, M., Ibrahim, N. M. E. S., & Mohammed, F. (2021). Influences of the environmental factors on the intention to adopt cloud based accounting information system among SMEs in Jordan. *Accounting*, 7(3), 645-654. <https://doi.org/10.5267/j.ac.2020.12.013>
- Alzghoul, A., Alhanatleh, H., Alnajdawi, S., Alghizzawi, M., & mohammad Al Htibat, A. (2024, December). Actual Role of Cybersecurity Awareness and Knowledge to Drive Digital Technology Adoption for Enhance Sustainable Development: Engineering Industry Setting. In *2024 International Conference on Decision Aid Sciences and Applications (DASA)*, 1-5. IEEE. <https://doi.org/10.1109/DASA63652.2024.10836494>
- Anyanwu, A., Olorunsogo, T., Abrahams, T. O., Akindote, O. J., & Reis, O. (2024). Data confidentiality and integrity: a review of accounting and cybersecurity controls in superannuation organizations. *Computer Science & IT Research Journal*, 5(1), 237-253. <https://doi.org/10.51594/csitrj.v5i1.735>
- Appiah, G., Amankwah-Amoah, J., & Liu, Y. L. (2020). Organizational architecture, resilience, and cyberattacks. *IEEE Transactions on Engineering Management*, 69(5), 2218-2233. <https://doi.org/10.1109/TEM.2020.3004610>
- AlFraihat, S. F. A., Ali, A. M., Hodaifa, G., & Alghizzawi, M. (2025). The Impact of Digital Content Marketing on Brand Defence: The Mediating Role of Behavioural Engagement and Brand Attachment. *Administrative Sciences*, 15(4), 124. <https://doi.org/10.3390/admsci15040124>
- Awang, P. (2018). Pendekatan Mudah SEM (Structural Equation Modeling). *MPWS Rich Resources*. <http://eprints.unisza.edu.my/id/eprint/3865>
- Azaan, S., & Elsa, J. (2024). The Rise of Automated Accounting: Navigating the Digital Landscape, No. 12113. *EasyChair*. <https://easychair.org/publications/preprint/G7b5>
- Ballantine, J., & Galliers, R. D. (2017). New developments in information technology: A call for action. In *The Routledge Companion to Accounting Information Systems*. 292-301. Routledge. <https://doi.org/10.4324/9781315647210>
- Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, 37(6), 508-526. <https://doi.org/10.1016/j.jaccpubpol.2018.10.003>
- Bosanac, K., Ivančić, I., & Dragičević, D. (2025). Contemporary needs of animation programmes in business tourism. *Oeconomica Jadertina*, 15(1), 55-68. <https://doi.org/10.15291/oec.4562>
- Brown, T. A. (2015). Confirmatory factor analysis for applied research. *Guilford publications*. <https://www.guilford.com/books/Confirmatory-Factor-Analysis-for-Applied-Research/Timothy-Brown/9781462515363>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548. <https://www.jstor.org/stable/25750690>

- Cram, W. A., Wang, T., & Yuan, J. (2023). Cybersecurity research in accounting information systems: A review and framework. *Journal of Emerging Technologies in Accounting*, 20(1), 15-38. <https://doi.org/10.2308/JETA-2020-081>
- Curtis, S. R., Carre, J. R., & Jones, D. N. (2018). Consumer security behaviors and trust following a data breach. *Managerial Auditing Journal*, 33(4), 425-435. <https://doi.org/10.1108/MAJ-11-2017-1692>
- Dijkstra, T. K., & Henseler, J. (2015). Consistent partial least squares path modeling. *MIS Quarterly*, 39(2), 297-316. <https://www.jstor.org/stable/26628355>
- Dora, M., Kumar, M., Van Goubergen, D., Molnar, A., & Gellynck, X. (2013). Operational performance and critical success factors of lean manufacturing in European food processing SMEs. *Trends in food science & technology*, 31(2), 156-164. <https://doi.org/10.1016/j.tifs.2013.03.002>
- Ekelund, S., & Iskoujina, Z. (2019). Cybersecurity economics—balancing operational security spending. *Information Technology & People*, 32(5), 1318-1342. <https://doi.org/10.1108/ITP-05-2018-0252>
- Elmaasrawy, H. E., & Tawfik, O. I. (2024). The impact of using the Internet of Things on the development of the accounting information system in the health sector. In *Artificial Intelligence, Big Data, Blockchain and 5G for the Digital Transformation of the Healthcare Industry*, 253-270. Academic Press. <https://doi.org/10.1016/B978-0-443-21598-8.00006-3>
- Hamza, R. A. E. M., Ahmed, N. H., Mohamed, A. M. E., Bennaceur, M. Y., Elhefni, A. H. M., & Elshaabany, M. M. (2024). The Impact of Artificial Intelligence (AI) on the Accounting System of Saudi Companies. *WSEAS Transactions on Business and Economics*, 21(January), 499-511. <https://doi.org/10.37394/23207.2024.21.42>
- Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58, 102726. <https://doi.org/10.1016/j.jisa.2020.102726>
- Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, 3(5), 97. <https://doi.org/10.1007/s43546-023-00477-6>
- Hermida, R. (2015). The problem of allowing correlated errors in structural equation modeling: concerns and considerations. *Computational Methods in Social Sciences*, 3(1), 5-17. <https://www.cceol.com/search/article-detail?id=417198>
- Hossain, M. Z., & Johora, F. T. (2024). Cybersecurity in Accounting: Protecting Financial Data in the Digital Age. Available at SSRN 4868132. [https://doi.org/10.59324/ejaset.2024.2\(6\).06](https://doi.org/10.59324/ejaset.2024.2(6).06)
- Idris, M. I., Siam, Y. I. A., & Ahmad, A. L. (2018). The impact of external auditor size on the relationship between audit committee effectiveness and earnings management. *Investment Management and Financial Innovations*, 15(3), 122-130. [http://dx.doi.org/10.21511/imfi.15\(3\).2018.10](http://dx.doi.org/10.21511/imfi.15(3).2018.10)
- Jackson, D., & Allen, C. (2024). Enablers, barriers and strategies for adopting new technology in accounting. *International Journal of Accounting Information Systems*, 52, 100666. <https://doi.org/10.1016/j.accinf.2023.100666>
- JCI, 2023. https://www.aci.org.jo/Publication_Details.aspx?id=4104 . Accessed by the Internet in (17 March, 2021).
- Jiang, L. (2024). The use of blockchain technology in enterprise financial accounting information sharing. *Plos one*, 19(2), e0298210. <https://doi.org/10.1371/journal.pone.0298210>
- Kakizhanova, T., Utepaliyeva, K., Zeinolla, S., Aben, A., & Ilyashova, G. (2025). Impact of Digitalization, Economic Growth and Birth Rate on Female Labor Force: Evidence from Kazakhstan. *ECONOMICS - Innovative and Economics Research Journal*, 13(2), 95-110. <https://doi.org/10.2478/eoik-2025-0032>
- Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, 106, 102267. <https://doi.org/10.1016/j.cose.2021.102267>

- Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection*, 9, 52-80. <https://doi.org/10.1016/j.ijcip.2015.02.002>
- Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management*, 34(6), 1597-1629. <https://doi.org/10.1108/JEIM-06-2020-0240>
- Kusumawardhani, F., Ratmono, D., Wibowo, S., Darsono, D., Widyatmoko, S., & Rokhman, N. (2024). The impact of digitalization in accounting systems on information quality, cost reduction and decision making: Evidence from SMEs. *International Journal of Data and Network Science*, 8(2), 1111-1116. <https://doi.org/10.5267/j.ijdns.2023.11.023>
- Masa'deh, R. E., Almajali, D. A., & Alsmadi, L. A. (2025). Acceptance of Artificial Intelligence in a Jordanian Firm: An Overview. *The Role of Artificial Intelligence Applications in Business*, 1-10. <https://doi.org/10.1108/978-1-83662-518-620251001>
- Magboul, I., Jebreel, M., Shawtri, F., Qabajeh, M., Shanti, A., Alqudah, M., & Abu Huson, Y. (2024). Factors influencing accounting information system usage by oil companies & performance outcomes. *Cogent Business & Management*, 11(1), 2369211. <https://doi.org/10.1080/23311975.2024.2369211>
- Masa'deh, R. E., Warrad, L. H., Jahmani, K., Almajali, D., Majali, S. A., & Al-Radaideh, A. T. (2024). Antecedents of adoption blockchain: Empirical study in Jordanian firms. *International Journal of Data and Network Science*, 8 (2024) 2601–2614. <https://doi.org/doi:10.5267/j.ijdns.2024.4.017>
- Mirtsch, M., Kinne, J., & Blind, K. (2020). Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis. *IEEE Transactions on Engineering Management*, 68(1), 87-100. <https://doi.org/10.1109/TEM.2020.2977815>
- Moudud-Ul-Huq, S., Asaduzzaman, M., & Biswas, T. (2020). Role of cloud computing in global accounting information systems. *The Bottom Line*, 33(3), 231-250. <https://doi.org/10.1108/BL-01-2020-0010>
- Moulton, R., & Coles, R. S. (2003). Applying information security governance. *Computers & Security*, 22(7), 580-584. [https://doi.org/10.1016/S0167-4048\(03\)00705-3](https://doi.org/10.1016/S0167-4048(03)00705-3)
- Nassani, A. A., Yousaf, Z., Grigorescu, A., Oprisan, O., & Haffar, M. (2023). Accounting information systems as mediator for digital technology and strategic performance interplay. *Electronics*, 12(8), 1866. <https://doi.org/10.3390/electronics12081866>
- Nassimbeni, G., Sartor, M., & Dus, D. (2012). Security risks in service offshoring and outsourcing. *Industrial Management & Data Systems*, 112(3), 405-440. <https://doi.org/10.1108/02635571211210059>
- Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment. *Information & Computer Security*, 32(1), 38-52. <https://doi.org/10.1108/ICS-05-2023-0084>
- Oroni, C. Z., & Xianping, F. (2023). Structural evaluation of management capability and the mediation role of cybersecurity awareness towards enterprise performance. *Journal of Data, Information and Management*, 5(4), 345-361. <https://doi.org/10.1007/s42488-023-00108-7>
- Pereira, C., Castro, B., Gomes, L., & Canha, H. (2024). Firms' Investment Level and (In) Efficiency: The Role of Accounting Information System Quality. *International Journal of Financial Studies*, 12(1), 9. <https://doi.org/10.3390/ijfs12010009>
- Pflueger, D., Kornberger, M., & Mouritsen, J. (2024). What is blockchain accounting? A critical examination in relation to organizing, governance, and trust. *European Accounting Review*, 33(4), 1139-1164. <https://doi.org/10.1080/09638180.2022.2147973>
- Pigola, A., Da Costa, P. R., Ferasso, M., & da Silva, L. F. C. (2024). Enhancing cybersecurity capability investments: Evidence from an experiment. *Technology in Society*, 76, 102449. <https://doi.org/10.1016/j.techsoc.2023.102449>
- Priambodo, A., Anwar, N., & Suharno, S. (2025). Does Digital Literacy Mediate the Relationship between ICT and Regional Own-Source Revenue? *ECONOMICS - Innovative and Economics Research Journal*, 13(2), 203–222. <https://doi.org/10.2478/eoik-2025-0037>

- Rabie, H. (2024). The Mediating Role of Cybersecurity on the Relationship between Internal Control and the Implementation of Cloud-Based Enterprise Resource Planning Systems in Jordanian Commercial Banks. *Kurdish Studies*, 12(2), 2921-2936. <https://pdfs.semanticscholar.org/2968/7110671b863d86b9b6a155537bb702e06ad4.pdf>
- Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology*, 88(5), 879. <https://doi.org/10.1037/0021-9010.88.5.879>
- Ratten, V. (2019). The effect of cybercrime on open innovation policies in technology firms. *Information Technology & People*, 32(5), 1301-1317. <https://doi.org/10.1108/ITP-03-2018-0119>
- Rawat, D. B., Doku, R., & Garuba, M. (2019). Cybersecurity in big data era: From securing big data to data-driven security. *IEEE Transactions on Services Computing*, 14(6), 2055-2072. <https://doi.org/10.1109/TSC.2019.2907247>
- Raza, I., & Awang, Z. (2021). Knowledge-sharing practices in higher educational institutes of Islamabad, Pakistan: an empirical study based on theory of planned behavior. *Journal of Applied Research in Higher Education*, 13(2), 466-484. <https://doi.org/10.1108/JARHE-03-2020-0068>
- Rex B. Kline. (2011). Principles and Practice of Structural Equation Modeling. In The Guilford Press (3rd ed.). The Guilford Press. <http://ndl.ethernet.edu.et/bitstream/123456789/74702/1/35.pdf>
- Ringle, C. M., Sarstedt, M., Mitchell, R., & Gudergan, S. P. (2020). Partial least squares structural equation modeling in HRM research. *The international journal of human resource management*, 31(12), 1617-1643. <https://doi.org/10.1080/09585192.2017.1416655>
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change¹. *The Journal of Psychology*, 91(1), 93-114. <https://doi.org/10.1080/00223980.1975.9915803>
- Roumani, Y., Nwankpa, J. K., & Roumani, Y. F. (2015). Time series modeling of vulnerabilities. *Computers & Security*, 51, 32-40. <https://doi.org/10.1016/j.cose.2015.03.003>
- Salehi, A. K. (2024). Critical review of the role of accounting in the decision-making process. *Journal of Islamic Accounting and Business Research*, 15(2), 244-264. <https://doi.org/10.1108/JIABR-12-2021-0310>
- Samtani, S., Chinn, R., Chen, H., & Nunamaker Jr, J. F. (2017). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *Journal of Management Information Systems*, 34(4), 1023-1053. <https://doi.org/10.1080/07421222.2017.1394049>
- Saputra, K. A. K., & Paranoan, S. (2024). Do Cyber security, Digitalisation and Data Visualisation Affect the Quality of Internal Environmental Audits?. *Australasian Accounting, Business and Finance Journal*, 18(2), 158-174. <https://doi.org/10.14453/aabfj.v18i2.10>
- Sarstedt, M., Ringle, C. M., & Hair, J. F. (2021). Partial least squares structural equation modeling. In *Handbook of market research*, 587-632. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-57413-4_15
- Shakdwipee, P., Agarwal, K., Kunwar, H., & Singh, S. (2023, August). Artificial Intelligence in Finance and Accounting: Opportunities and Challenges. In *International Conference on ICT for Sustainable Development*, 165-177. Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-99-5652-4_17
- Sipior, J. C., Bierstaker, J., Borchardt, P., & Ward, B. T. (2018). A ransomware case for use in the classroom. *Communications of the Association for Information Systems*, 43(1), 32. <https://doi.org/10.17705/1CAIS.04332>
- Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, 60, 154-176. <https://doi.org/10.1016/j.cose.2016.04.003>
- Soomro, R. B., Memon, S. G., Dahri, N. A., Al-Rahmi, W. M., Aldriwish, K., A. Salameh, A., ... & Saleem, A. (2024). The Adoption of Digital Technologies by Small and Medium-Sized Enterprises for Sustainability and Value Creation in Pakistan: The Application of a Two-Staged Hybrid SEM-ANN Approach. *Sustainability*, 16(17), 7351. <https://doi.org/10.3390/su16177351>

- Stefanska, B., & Al-Dawod, F. L. (2021). The importance of risk awareness in cybersecurity among companies : A perspective on the role of top management (Dissertation). <https://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-177218>
- Sun, Y., Li, J., Lu, M., & Guo, Z. (2024). Study of the Impact of the Big Data Era on Accounting and Auditing. *arXiv preprint arXiv:2403.07180*. <https://doi.org/10.48550/arXiv.2403.07180>
- Talwar, S., Dhir, A., Kaur, P., Zafar, N., & Alrasheedy, M. (2019). Why do people share fake news? Associations between the dark side of social media use and fake news sharing behavior. *Journal of retailing and consumer services*, 51, 72-82. <https://doi.org/10.1016/j.jretconser.2019.05.026>
- Tan, K. S., Chong, S. C., Lin, B., & Eze, U. C. (2009). Internet-based ICT adoption: Evidence from Malaysian SMEs. *Industrial Management and Data Systems*, 109(2), 224–244. <https://doi.org/10.1108/02635570910930118>
- Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting ample data security and privacy. *Future Generation Computer Systems*, 98, 660-671. <https://doi.org/10.1016/j.future.2019.03.042>
- Thamae, R., Abdullah, H., & Mujinga, M. (2024, April). Enhancing Cybersecurity Policy Awareness Programs in the Financial Sector: A Comprehensive Framework and Assessment of Effectiveness. In *International Conference on Business and Technology*, 48-57. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-67444-0_5
- Thottoli, M. M. (2024). Leveraging information communication technology (ICT) and artificial intelligence (AI) to enhance auditing practices. *Accounting Research Journal*, 37(2), 134-150. <https://doi.org/10.1108/ARJ-09-2023-0269>
- Van der Haar, H., & Von Solms, R. (2003). A model for deriving information security control attribute profiles. *Computers & Security*, 22(3), 233-244. [https://doi.org/10.1016/S0167-4048\(03\)00311-0](https://doi.org/10.1016/S0167-4048(03)00311-0)
- Vărzaru, A. A., Bocean, C. G., Mangra, M. G., & Simion, D. (2022). Assessing users' behavior on the adoption of digital technologies in management and accounting information systems. *Electronics*, 11(21), 3613. <https://doi.org/10.3390/electronics11213613>
- Vestad, A., & Yang, B. (2023, July). Adoption of Cybersecurity Innovations—A Systematic Literature Review. In *The International Conference on Cybersecurity, Situational Awareness and Social Media*, 285-304. Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-99-6974-6_16
- Xue, B., Xu, F., & Warkentin, M. (2018). Critical role of ethical leadership on information security climate and employee ISP violation behavior. *WISP 2018 Proceedings*. 16. <https://aisel.aisnet.org/wisp2018/16>
- Yigit Ozkan, B., & Spruit, M. (2023). Adaptable security maturity assessment and standardization for digital SMEs. *Journal of Computer Information Systems*, 63(4), 965-987. <https://doi.org/10.1080/08874417.2022.2119442>
- Yusof, M. M., Kuljis, J., Papazafeiropoulou, A., & Stergioulas, L. K. (2008). An evaluation framework for Health Information Systems: human, organization and technology-fit factors (HOT-fit). *International journal of medical informatics*, 77(6), 386-398. <https://doi.org/10.1016/j.ijmedinf.2007.08.011>
- Zhang, C., Li, Z., Xu, J., & Luo, Y. (2024). Accounting information quality, firm ownership and technology innovation: Evidence from China. *International Review of Financial Analysis*, 93, 103118. <https://doi.org/10.1016/j.irfa.2024.103118>