InternexT

INTERNATIONAL BUSINESS AND MANAGEMENT REVIEW

v.20, n. 3, e847, 2025| e-ISSN: 1980-4865 | http://internext.espm.br

THE IMPACT OF TECHNOLOGICAL AND ECONOMIC FACTORS ON CYBERSECURITY MANAGEMENT AND MSME PERFORMANCE

Muslim Najeeb Zaidan[1]* & Aram Hanna Massoudi[2]

[1]Cihan University-Erbil, Department of Public Administration – Kurdistan Region, Iraq.

[2]Cihan University-Erbil, Department of Business Administration – Kurdistan Region, Iraq.

ARTICLE DETAILS

Received:
January 16, 2025

Accepted:
July 22, 2025

Available online:
September 30, 2025

Double Blind Review System

Editor in Chief
Priscila Rezende da Costa

ABSTRACT

Objective: This study applies the Protection Motivation Theory (PMT) as a theoretical framework to explore how technological and economic factors influence the performance of micro, small, and medium-sized enterprise (MSME) employees in Iraq, with a particular focus on the mediating role of cybersecurity management. **Method:** A quantitative research design was employed, involving the collection of data from 384 MSME employees through both online and in-person questionnaires. **Main Results:** The analysis reveals that cybersecurity management is significantly affected by both technological and economic factors. In turn, effective cybersecurity management positively impacts MSMEs performance. Furthermore, cybersecurity management acts as a key mediator in the relationship between these external factors and enterprise success. **Theoretical / Methodological Contributions:** This study offers both theoretical and practical contributions. Theoretically, it expands the application of PMT to the context of cybersecurity and MSME performance. Methodologically, it provides a robust framework for evaluating mediating effects in this domain. Practically, the research offers actionable insights for policymakers and business owners, emphasizing the importance of affordable cybersecurity strategies and targeted support programs to improve enterprise resilience and reduce vulnerability to cyber threats.

Keywords: Cybersecurity Management, Micro, small, and medium-sized enterprises, Technological Factors, Economic Factors, and Protection Motivation Theory.

O IMPACTO DOS FATORES TECNOLÓGICOS E ECONÔMICOS NA GESTÃO DA CIBERSEGURANÇA E NO DESEMPENHO DAS MICRO, PEQUENAS E MÉDIAS EMPRESAS

DETALHES DO ARTIGO

Recebido:
16 jan., 2025

Aceito:
22 Jul., 2025

Disponível online:
30 Set., 2025

Sistema de revisão "Double blind review"

Editora Chefe:
Priscila Rezende da Costa

RESUMO

Objetivo: Este estudo aplica a teoria da motivação para a proteção como arcabouço teórico para explorar como fatores tecnológicos e econômicos influenciam o desempenho de micro, pequenas e médias empresas no Iraque, com foco específico no papel mediador da gestão da segurança cibernética. **Método:** Foi utilizado um delineamento de pesquisa quantitativa, envolvendo a coleta de dados de 384 funcionários de micro, pequenas e médias empresas por meio de questionários *online* e presenciais. **Principais Resultados:** A análise revelou que a gestão da segurança cibernética é significativamente afetada por fatores tecnológicos e econômicos. Por sua vez, uma gestão eficaz da segurança cibernética impacta positivamente o desempenho das micro, pequenas e médias empresas. Além disso, a gestão da segurança cibernética atua como um mediador fundamental na relação entre esses fatores externos e o sucesso empresarial. **Contribuições Teóricas / Metodológicas:** Este estudo oferece contribuições teóricas e práticas. Teoricamente, expande a aplicação da teoria da motivação para a proteção ao contexto da segurança cibernética e do desempenho de micro, pequenas e médias empresas. Metodologicamente, fornece uma estrutura robusta para avaliar os efeitos mediadores nesse domínio. Na prática, a pesquisa oferece *insights* práticos para formuladores de políticas e proprietários de empresas, enfatizando a importância de estratégias de segurança cibernética acessíveis e programas de suporte direcionados para melhorar a resiliência empresarial e reduzir a vulnerabilidade a ameaças cibernéticas.

Palavras-chave: Gestão de Segurança Cibernética, Micro, Pequenas e Médias Empresas, Fatores Tecnológicos, Fatores Econômicos e Teoria da Motivação da Proteção.

*Corresponding author: muslim.najeeb@cihanuniversity.edu.iq

https://doi.org/10.18568/internext.v20i3.847

INTRODUCTION

In recent years, micro, small, and medium-sized enterprises (MSMEs) around the world have depended more on digital technologies to improve their operations and reach more individuals as technology is developing so quickly (Massoudi & Birdawod, 2023). The digital world is spreading swiftly in Iraq. This is excellent news for MSMEs because it means they may connect with more people and develop. As of the beginning of 2024, about 36.22 million individuals in Iraq were online, which is 78.7% of the population. In addition, roughly 31.95 million people, or 69.4% of the total, were active on social networking platforms. Many small and medium-sized enterprises (SMEs) in Iraq have been adopting mobile-based solutions to enhance their operations and communicate with clients (DataReportal, 2024), as the country boasts 46 million cell phones, representing 100% of the population. But even with this technology, it is very difficult for SMEs in Iraq, and the telecommunications companies that support these businesses, to maintain information security as they move into the technology age. According to Sayeed et al. (2024), this leaves these organizations susceptible to cyberattacks since they do not have any of the technical expertise or resources available to them for protection. In the end, this can impact their work and reflect badly on them. To make sure this challenge is met, it is pertinent to analyze how economic and technological facets influence the management of cybersecurity and how these components leverage business expansion and security.

Despite the growing recognition of cybersecurity threats faced by MSMEs, much of the existing literature remains disproportionately focused on large organizations in developed economies. This leaves a significant gap in understanding how MSMEs in developing and fragile contexts, such as Iraq, navigate cybersecurity challenges. Furthermore, previous studies often overlook the intersection of macro-environmental factors, such as economic instability and technological infrastructure limitations, in shaping cybersecurity behaviors within these enterprises.

Another critical gap lies in the limited application of theoretical frameworks to explain cybersecurity adoption and its impact on firm performance in MSMEs. While some research references technology acceptance models or general risk frameworks, few employ behavioral theories such as protection motivation theory (PMT) to elucidate how perceived threats and coping mechanisms influence cybersecurity practices and business outcomes.

This study aims to apply PMT to a non-Western MSME context, offering a behavioral lens through which to understand cybersecurity decision-making. Also, it focuses on the mediating role of cybersecurity management, providing empirical insights into how technical and economic pressures are translated into performance outcomes via cyber resilience. The study contributes context-specific evidence from Iraq, a country characterized by unique economic and technological constraints, thus enhancing the geographic and contextual diversity of the cybersecurity literature. In addition, the study delivers practical implications for policy and practice by emphasizing cost-effective and scalable cybersecurity measures suited for resource-constrained MSMEs. By doing so, the study not only fills theoretical and empirical gaps but also offers actionable guidance tailored to the realities of MSMEs operating in high-risk and under-resourced environments.

This study is organized into five sections: Introduction: Outlines the theoretical foundation (PMT) and highlights the contextual challenges faced by MSMEs in Iraq. Literature Review and Theoretical Framework: Reviews prior research on cybersecurity in MSMEs, technological and economic challenges, and the application of PMT in organizational contexts. It also presents the conceptual model and hypotheses. Research Methodology: Details the quantitative research design, data collection process, sample characteristics, and measurement instruments used in the study. Results and Analysis: Presents the data analysis, including descriptive statistics, validity tests, and structural equation modeling (SEM) results used to test the hypothesized relationships. Conclusion: Interprets the findings in light of the theoretical framework and existing literature. It also discusses practical implications for policymakers and MSME practitioners, outlines the study's limitations, and suggests directions for future research.

1. LITERATURE REVIEW

1.1. MSME performance

MSMEs are vital to Iraq's economy due to their capacity to produce employment opportunities and serve different industries (Agha et al., 2023). Neverthe-

less, they experience obstacles in offering services due to their poor financial resources, concerns surrounding cybercrime, inadequate digital skills, and regulatory limits. As a result of the solid digital infrastructure, all 46 million Iraqis will have access to mobile phones by the beginning of 2024 (DataReportal, 2024). Additionally, 31.95 million individuals, or 31.95% of the population, were using the Internet, whereas 36.22 million individuals, or 78.7% of the population, were online. Despite the fact that MSMEs use digital tools more frequently, Charfeddine et al. (2024) discovered that they could not afford crucial security measures. As a consequence, they are prone to service outages and cyberattacks. The government's capacity to expand is also hampered by the complexity of the system, which renders it less effective. Research indicates that small and medium-sized firms may be more suited to solving issues if they have more convenient access to capital, government help, digital technologies, and stable market conditions. These can help their businesses do good in the economy through the expansion of digital infrastructure (Ali et al., 2022).

Iraq has a high share of micro, small, and medium-sized firms (Massoudi & Fatah, 2021). These businesses are the primary focus of the current work. In an estimate done by the Iraq MSME 2020 Survey, the three governorates (Nineveh, Basra, and Baghdad) host 1,186,790 MSMEs. As indicated by a previous investigation (Rasool & Al-Othman, 2023), Baghdad alone hosts a large number of MSME operations. The evidence of these enterprises can be seen from the SMEs in Baghdad that are relevant to the employment generation and economic growth. According to Nather et al. (2020), the employment generation and service provision of MSMEs are blood arteries to Iraq, along with their stability and growth. Most of the time, they can turn out to be more disadvantageous due to structural restrictions, weak infrastructure, limited supply of currency, and inefficient cybersecurity methods (Younus et al., 2022). It should be noted that MSMEs typically have trouble obtaining loans or investments owing to a lack of necessary apparatus, so it is extremely important that they gain access to financial resources.

1.2. Cybersecurity management

The statement "security management" implies the approaches, tactics, and instruments that businesses adopt to defend their digital assets, including data, networks, and systems, against cyberthreats such as intrusions, malware, and phishing assaults (AllahRakha, 2024). The following are critical components of efficient cybersecurity management: the development of secure networks, the regular updating of security software, employee training, and the attentive observation of prospective threats. In order to preserve crucial company and consumer information, it is imperative that MSMEs in Iraq employ cybersecurity management (Nazem et al., 2023).

On the other hand, a study by Massoudi et al. (2024) shows that a large number of Iraqi MSMEs cannot build proper cybersecurity, due to a lack of resources. This fragility makes them susceptible to cyberattacks that can halt operations, cause financial losses, and erode consumer trust. The efficacy of MSMEs in Iraq is considerably reliant on the administration of cyberspace (Ulupui et al., 2024). Cyber incidents can lead to operational interruptions, reputational damage, and substantial financial losses (Arroyabe et al., 2024). A data breach can impose substantial penalties from regulators on an MSME, impair its consumer services, and deprive it of essential information.

In severe instances, such impediments could lead to potential business closure, diminished revenues, and eroded client trust. Consequently, cyber threats pose a risk to the stability and growth potential of MSMEs in Iraq due to the absence of cybersecurity safeguards. A prior study has advocated for economic security measures. Rahman et al. (2024) advocate for the creation of cost-effective cybersecurity solutions tailored to the requirements of MSMEs. This strategy enables them to safeguard their assets while evading substantial liabilities. Research conducted by Al-Anbgai (2021) suggests that the Iraqi government ought to offer grants, tax incentives, or subsidies to assist MSMEs in acquiring vital cybersecurity measures. Furthermore, cybersecurity training, as outlined by Li et al. (2019), safeguards MSMEs from prevalent cyber dangers by enhancing employee awareness and mitigating detrimental online behaviors. This study indicates that the establishment of public–private partnerships among governments, technology providers, and SMEs may bolster these firms' capacity to mitigate cyberattacks by facilitating access to resources, guidance, and cost-effective cybersecurity solutions.

From the above discussion, the authors postulate the following hypothesis:

H1: Cybersecurity has a significant positive impact on MSME performance.

1.3. Technology factors

Technology integration has changed the daily activities of MSMEs. However, this has created significant safety concerns, especially for Iraqi MSMEs. The elements of technology such as availability of modern cybersecurity tools, access to the Internet, and digital skills are directly affecting the ability of businesses to manage cyber risks (Yeoh et al., 2022). In underdeveloped nations such as Iraq, adopting effective cybersecurity measures is problematic due to inconsistent Internet connectivity and inadequate bandwidth. This renders MSMEs particularly susceptible to cyber intrusions. Restricted access to cybersecurity solutions raises the chance of data breaches, leading to severe financial losses and reputational damage. Technological limits in cybersecurity management impede the overall profitability of MSMEs, resulting in lower consumer trust and lost revenue. Due to these restraints, MSMEs are also prone to cyber risks. The growth of digital technology has eased remote work for MSMEs. This has decreased operational expenses and boosted market accessibility (Hendrawan et al., 2024).

Current security software and solutions are the knowledge base for SMEs to improve their safety management. Tyagi et al. (2023) claim that this will enhance their defenses against Internet attacks. Although cloud computing may save on the cost and provide further flexibility, it could also bring extra security challenges if you do not manage the system properly. When security processes are automated, human errors are eliminated and MSMEs can respond to the assault more quickly and efficiently. But in addition to promoting illegal access for hackers, the Internet of Things (IOT) devices make the security systems more challenging (Mallick & Nath, 2024). It may increase production but needs stringent regulation to curb dangers. Cybersecurity is bolstered as technology has a major impact on the success of small- and medium-sized businesses. Hasan et al. (2021) denote that advanced technologies, particularly artificial intelligence (AI)-assisted threat monitoring and secure software systems, greatly increase organizations' capacity to protect sensitive data and deter cyber threats. Massoudi (2025) adds that a robust technology infrastructure is important for MSME growth as it ensures regulatory compliance, builds customer confidence, and improves operational efficiency. Using technology for safety helps firms reduce risks and avoid downtimes, which improves the MSMEs' productivity and operational performance. From the above, the authors proposed that:

H3: Technology factors have a significant positive impact on cybersecurity.

H5: Technology factors have a significant indirect impact on MSME performance through cybersecurity.

1.4. Economic factors

Economic variables strongly influence cybersecurity management methods in MSMEs in Iraq (Salim, 2022). Limited financial resources, high costs of cybersecurity solutions, and fluctuations in markets in Iraq lower the priority of cybersecurity for MSMEs, thereby increasing the possibility of cyberattacks. Due to low money, they are more at risk of security incidents, economic damage, and disruptions to client confidence (Hassan & Ahmed, 2023). Moreover, the unreasonably high cost of cybersecurity solutions such as firewalls, encryption software, and intrusion detection systems renders them increasingly unavailable to MSMEs. Employing qualified cybersecurity professionals presents financial challenges, leading to a reactive approach to cybersecurity. The economic volatility and market fluctuations in Iraq considerably impact the capacity of MSMEs to adequately manage cybersecurity (Mehchy et al., 2023). The Iraqi government should provide financial incentives, establish public–private partnerships, implement awareness campaigns, and offer low-interest loans to enhance cybersecurity in Iraqi MSMEs. These measures will promote investment in robust security systems, educate businesses, and enhance their resilience in the digital economy.

Limited budgets, high costs of cybersecurity technologies, and low government support are the most important economic challenges for the cybersecurity of MSMEs and their performance in Iraq. According to studies, the financial prudence of MSMEs labels them more likely to prioritize the not-so-important operations over keeping themselves protected from cyber

threats, making them vulnerable to attacks. Hedging these are the costs for cybersecurity tools and skills, which stalls the deployment of the required safety measures for countless small businesses and for MSMEs; the precariousness of the economy means prioritizing immediate needs over long-term safety investments (Simpson, 2024). Thus, in the face of little government support, MSMEs are not granted subsidies or incentives that would decrease expenditure on cybersecurity, and this creates additional problems. Therefore, the financial threat aspect plays a significant role in amplifying the other cybersecurity threats that MSMEs encounter, which in turn affect their operational stability and customer loyalty.

Economic factors also considerably affect the cybersecurity governance of MSMEs and, hence their performance. A proper budget can support investments in critical cybersecurity infrastructure, increase resilience, and reduce costs related to breaches (Vegesna, 2024). MSMEs are at risk, as the high cost of cybersecurity technology sometimes hinders access to advanced protection (Maulana, 2024). When the return on investment is favorable, MSMEs are more likely to spend more on cybersecurity projects, which, in turn, reinforces consumers' trust (Cartwright et al., 2023).

Moreover, economic stability and access to financing, which reduces risk exposure, aids long-term cybersecurity planning (Erondu & Erondu, 2023). For economic instability, the authors suggest policy-level interventions, such as establishing financial safety nets or stabilization funds to support MSMEs during macroeconomic shocks. With regard to financing constraints, we propose alternative financing mechanisms including digital micro-lending platforms, government-backed loan guarantee schemes, and partnerships with fintech firms to improve MSMEs' credit access.

Comprehensive cybersecurity measures are thus essential to retain a competitive edge in highly competitive markets (Charoenrat & Harvie, 2021). Furthermore, the digital economy also requires the implementation of robust cybersecurity policies to protect consumer information and digital assets (Akter et al., 2025). Nonetheless, the high cybersecurity insurance costs may keep MSMEs from getting uncovered, thereby increasing the monetary dangers in the hours of cyber catastrophes (Ayinde-Olawale et al., 2023). These economic factors directly influence the stability and growth potential of MSMEs, making the cybersecurity hygiene of MSMEs heavily reliant on these factors.

H2: Economic factors have a significant positive impact on cybersecurity.

H4: Economic factors have a significant indirect impact on MSME performance through cybersecurity.

1.5. Theoretical framework

This work employs another useful analysis framework, PMT, relevant for the evaluation of MSMEs' security behavior in terms of perceived risks and the employed coping strategies (Norman et al., 2015) (Figure 1). The PMT describes the factors that affect protective behavior through two main appraisals: threat appraisal that consists of perceived severity and susceptibility, and coping appraisal that encompasses response efficacy, self-efficacy, and response costs. The literature on cybersecurity and organizational performance has largely centered on large enterprises in stable, developed economies, with limited attention paid to MSMEs operating in fragile and volatile environments such as Iraq. This neglect is critical, as Iraqi MSMEs face unique challenges—including limited access to technology, low cybersecurity awareness, economic instability, and political uncer-

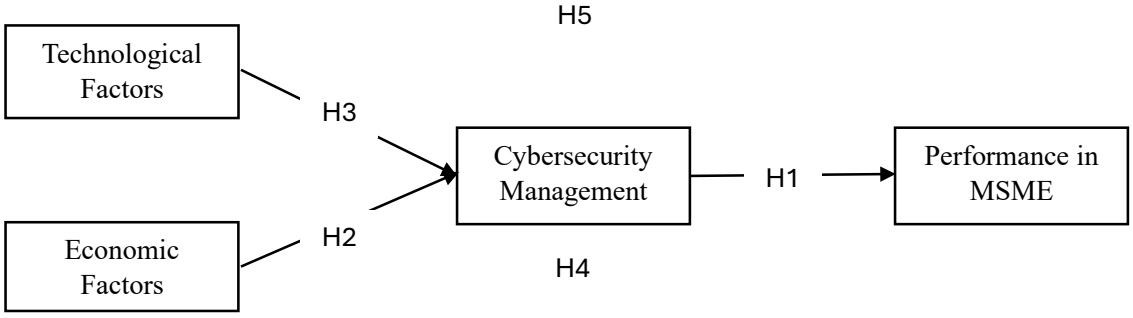

Figure 1. Theoretical framework.

tainty—that significantly affect their ability to adopt effective cybersecurity practices.

Furthermore, while existing studies have identified various technical and economic barriers to cybersecurity adoption, they often lack a robust theoretical framework to explain the behavioral motivations behind cybersecurity decision-making in MSMEs. PMT, which emphasizes threat appraisal and coping appraisal processes, offers a valuable lens for addressing this gap. Yet, its application to cybersecurity in MSMEs—particularly in conflict-affected economies—remains underexplored.

This study explicitly applies PMT to understand how MSMEs in Iraq perceive and respond to cyber threats. In a context where cyber risks are often underestimated and resources are scarce, PMT provides a framework for analyzing how MSME managers evaluate the perceived severity and vulnerability of cyber threats amid Iraq's limited digital infrastructure and growing digitalization. It also considers the costs of action or inaction, which are heightened by Iraq's economic volatility and lack of institutional support.

2. METHOD

2.1. Research design

The research examined the impact of technology and the economy on Iraqi SMEs and formulated cybersecurity management strategies. A quantitative research methodology was employed, as this approach is well-suited for investigating the influence of various factors in business and information technology (Younus & Zaidan, 2022). Within the framework of this investigation, these elements were designated as independent variables. The performance of MSMEs was the dependent variable, while risk management acted as the intermediary via which the independent variables were linked. To gather data, structured questionnaires were administered to a sample of 384 MSMEs, as indicated in Morgan's table.

Utilizing Morgan's table, it was revealed that the total number of answers, 384, adequately represents the entire community, as stated by Morgan (1965). The objective was to ensure that the results are reliable and significant from a statistical perspective. To guarantee appropriate representation for all, we employed stratified random selection. To do this, the population was initially divided into groups based on company types or geographical regions, followed by the random selection of individuals from each category. This multi-dimensional stratification ensures a representative sample that captures the diversity within the MSME population. These strata were informed by national business registry data and relevant statistical classifications provided by the Ministry of Planning, Central Statistical Organization. Furthermore, potential biases arising from the dual-mode (physical and online) data collection approach were addressed by considering demographic and contextual differences between respondents. For example, those more likely to complete physical surveys (e.g., rural, low-digital-literacy areas) versus those responding online (e.g., urban, tech-savvy businesses).

The questionnaire items were adapted from established and validated scales in the existing literature on PMT, cybersecurity, and MSME performance. To ensure content validity and contextual relevance, the initial draft was reviewed by a panel of five experts, including two cybersecurity professionals, two academic researchers, and one MSME manager. Based on their feedback, several items were reworded for clarity and contextual fit.

A pilot test was then conducted with 20 MSME employees not included in the final sample. This pretest helped assess item clarity, internal consistency, and completion time. Minor revisions were made to improve comprehensibility and cultural appropriateness of the items.

2.2. Data analysis

This study analyzed data from 384 MSME respondents to assess the impact of technology and the economy on the performance and risk management of MSMEs. Statistical methods were applied to guarantee the accuracy and reliability of the findings.

During the main analysis, partial least squares-structural equation modeling (PLS-SEM) was employed to evaluate the measurement model. The following criteria were used:

Internal consistency was confirmed using Cronbach's alpha and composite reliability (CR), both exceeding the threshold of 0.70.

Convergent validity was established through average variance extracted (AVE), with all constructs achieving AVE values above 0.50.

Discriminant validity was assessed using the Heterotrait-Monotrait (HTMT) ratio, ensuring that each construct was distinct from the others.

2.3. Common method bias

The study implemented several procedural and statistical controls: Anonymity and confidentiality were assured to participants, reducing pressure to provide socially desirable responses. Also, reverse-coded items were included to detect inconsistent answering patterns. Finally, Harman's single-factor test was conducted to check for common method variance. The results indicated that no single factor accounted for the majority of the variance, suggesting that common method bias (CMB) was not a serious concern. These steps collectively enhanced the rigor of the data collection and analysis process, increasing the reliability of the findings and ensuring they are robust and contextually grounded.

2.4 Measurement

To measure the effects of the elements in the study, the researcher used Likert scales (1= strongly disagree; 2= disagree; 3= neutral; 4= agree; and 5= strongly agree). The questionnaire used in the present study comprised two sections, where the first one gathered demographic data and the second one included items regarding the variables in the study. Economic factor was explored with four items adapted from Sekhar and Radha (2019) and cybersecurity management with three items adapted from Takács and Pogátsnik (2024). Three items were used for MSME performance, adapted from Purwanto et al. (2022). Finally, three were used for technological factors, adapted from Marsudi et al. (2024). Specifically, these were created to confirm the validity and reliability of the data collection process involved in testing the role of different variables in our conceptual model.

3. RESULT AND DISCUSSION

3.1. Demographics of respondents

Table 1 presents an overview of the demographic characteristics of the 384 individuals who participated in the survey, reflecting common features found in MSME-related studies.

Table 1. Demographic variables.

Demographic variables	Category	Frequency	Percentage (%)
Gender	Male	268	69.8
	Female	116	30.2
Age group (years)	18–25	58	15.1
	26–35	140	36.5
	36–45	110	28.6
	46–55	56	14.6
	Above 55	20	5.2
Education level	High school	90	23.4
	Diploma	130	33.9
	Bachelor's degree	120	31.3
	Postgraduate	44	11.4
Business size	Micro (1–9)	140	36.5
	Small (10–49)	172	44.8
	Medium (50–249)	72	18.8
Business sector	Trade	134	34.9
	Services	168	43.8
	Manufacturing	82	21.4

The authors noted that male-dominated ownership or leadership in MSMEs may correlate with different risk perceptions or decision-making styles regarding cybersecurity investments, as suggested in prior literature. We also note that education level likely plays a role in shaping digital literacy and cybersecurity awareness. Respondents with higher education did exhibit greater understanding and willingness to adopt cybersecurity practices, which could affect both perceived usefulness and intention to adopt technologies.

3.2. Reliability and validity indicators

Hair et al. (2024) provide evidence for good measurement properties for every study construct, with high values for reliability and validity metrics (Cronbach's alpha, rho_A, CR, and AVE), as shown in Table 2, where the internal consistency and convergent validity are significant. Cronbach's alpha coefficients greater than 0.9 suggest excellent internal consistency of constructs, meaning that items in each construct, namely "Cybersecurity" and "Economic Factors," measure the same underlying construct reliably. Rho_A values that vary from 0.914 to 0.965 support the soundness of each construct in assuring measurement precision in a PLS-SEM ground. CR values greater than 0.94 indicate substantial shared variance of items in each construct with insignificant measurement error and support internal coherence of the constructs. AVE values (all exceed 0.83) indicate that each construct's indicators account for a large proportion of variance. 'These results demonstrate strong convergent validity, indicating that each construct is well-represented by its indicators and distinct from others. The findings confirmed that the constructs' reliability and validity are significant for precisely evaluating the impact of technology and economic forces on cybersecurity practices and MSME performance in Iraqi companies.

Following Hair et al. (2024), factor loadings above 0.7 were considered strong, as they confirm the items' reliability in measuring their respective constructs. All loadings met this criterion, indicating good indicator reliability. Each item loaded highly on its intended construct, demonstrating strong convergent validity and suggesting that the constructs are distinct from one another (discriminant validity).

3.3. Model interpretation

This study investigated the interrelationships between technological variables, economic factors, cybersecurity, and the performance of MSMEs through a structural equation modeling (PLS-SEM) path model (Figure 2). Hair et al. (2024) assert that PLS-SEM is highly advantageous for predictive research, notably in the formulation of theoretical frameworks like cybersecurity in MSMEs. A multitude of indicators with substantial loadings was employed to assess

Table 2. Reliability and validity measures of constructs.

Construct			Cronbach's alpha	Rho_A	Composite reliability	(AVE)
Cybersecurity	CYB1	0.939	0.922	0.922	0.950	0.865
	CYB2	0.930				
	CYB3	0.921				
Economic factors	ECO1	0.940	0.933	0.965	0.952	0.833
	ECO2	0.941				
	ECO3	0.931				
	ECO4	0.835				
MSME performance	MSME1	0.948	0.905	0.914	0.941	0.841
	MSME2	0.889				
	MSME3	0.914				
Technology factors	TEC1	0.942	0.906	0.914	0.941	0.841
	TEC2	0.892				
	TEC3	0.916				

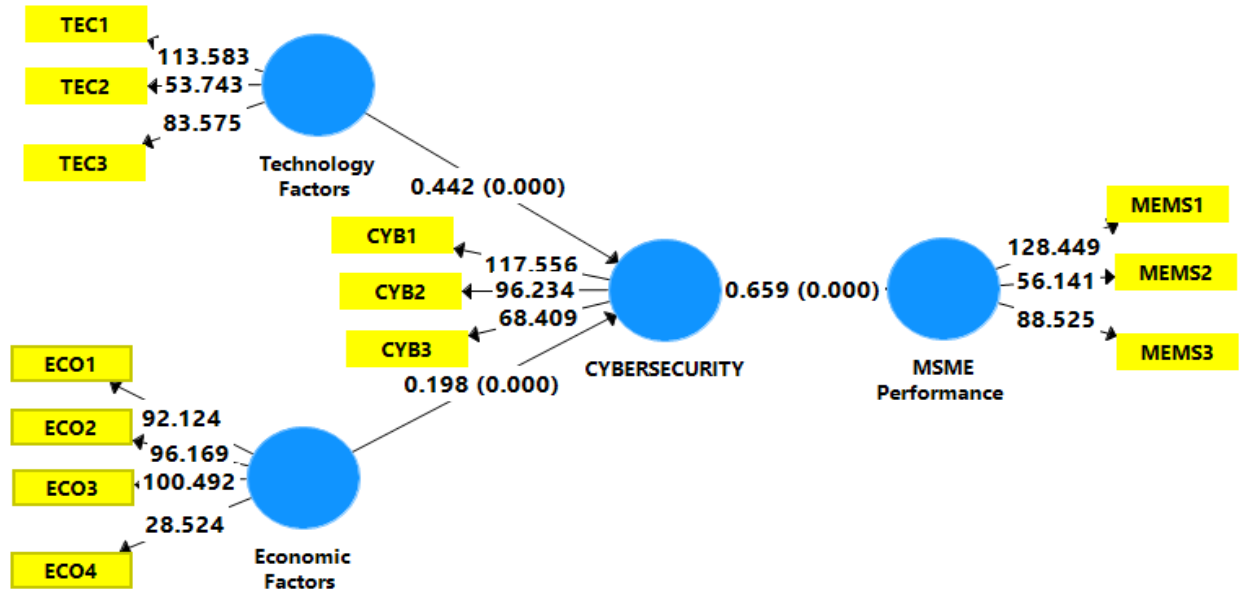

Figure 2. Structural model.

each construct, signifying a high degree of reliability. The path coefficients indicated that technological variables exert a fairly beneficial influence on cybersecurity (0.442), but economic factors have a lesser impact (0.198). The performance of MSMEs was significantly improved by cybersecurity, as indicated by a coefficient of 0.659. The R-squared values demonstrated that technological and economic factors constitute 25.5% of the variance in cybersecurity, but cybersecurity accounts for 43.4% of the variance in MSME performance. This indicates that cybersecurity possesses considerable explanatory power.

The authors added 95% bias-corrected and accelerated (BCa) confidence intervals for all path coefficients, derived through bootstrapping (5,000 samples), to provide greater transparency regarding the statistical significance and precision of the estimates. With regard to model fit, the authors included the standardized root mean square residual (SRMR) as an approximate fit index. The reported SRMR value (< 0.08) confirmed acceptable model fit.

In the zero-order SEM path analysis, the effects of the "technology factor" and the "economic factor" on "cybersecurity" as a mediating variable on "MSME performance" as the dependent variable were examined. As stated by Hair et al. (2024), the path coefficients (e.g., 0.442 and 0.198) showed the strength and significance of relationships between constructs (2024). The p-values, provided in brackets, support statistical significance. It was clear that the ideas of reliability and validity were correct because technological factors (TEC1, TEC2, and TEC3) and economic factors (ECO1, ECO2, ECO3, and ECO4) had big impacts on the latent variables that they were linked to. It turned out that the path coefficient of 0.659 indicates that cybersecurity significantly affects the performance of MSMEs. As such, this model, along with other studies, demonstrated the critical role of cybersecurity on MSME performance by moderating the effects of technological and economic inputs on MSME performance.

Hair et al. (2024) state that R-squared (R^2) values in PLS-SEM indicate the extent to which independent factors account for the variance in dependent variables. Cybersecurity exhibits an R^2 of 0.255, indicating that technology and economic factors account for approximately 25.5% of the variation in the cybersecurity practices of MSMEs. An R^2 value of 0.434 for MSME performance indicates that cybersecurity and other factors account for 43.4% of the variance. The data indicates a moderate capacity for explanation, particularly regarding MSME success.

3.4. Correlation matrix of constructs

The relationship matrix (Table 3) showed the connections between cybersecurity, economic factors, and MSME performance along with technological

Table 3. Correlation matrix of constructs (HTMT).

Constructs	Cybersecurity	Economic factors	MSME performance	Technology factors
Cybersecurity	1.000			
Economic factors	0.261	1.000		
MSME performance	0.718	0.278	1.000	
Technology factors	0.506	0.128	0.563	1.000

factors, which was a significant insight seen in the relationship matrix, according to Hair et al. (2024) and other studies. A significant correlation (r= 0.718) between cybersecurity and MSME performance indicated a positive association between good cybersecurity practices and boosted performance for MSMEs. This reinforced the belief that strong security protocols reduce operational risks. Cybersecurity limiting efficiency had a fair-to-moderate correlation with technological parameters (r= 0.506), indicating a general gap of technological readiness. Such a finding is set within a broader context of existing research, reminding us that a technology underpinning is a prerequisite for successful cybersecurity efforts. The findings suggested that there is a moderate and positive relationship between economic considerations and cybersecurity (r= 0.261), meaning that while financial resources have an impact on cybersecurity, they are not the sole factor leading to effective security. The moderate correlation (r= 0.563) observed between MSME performance and technological parameters showed that technological capabilities are positively linked to operational efficiency and resilience, thereby enhancing performance. The weak correlation of MSME performance with economic factors (r= 0.278) suggested that, while economic resources have a positive impact on MSME performance, their effect is less compared to other variables. The correlations emphasized the crucial role technology and security investments play in significantly improving the performance of small firms, particularly within resource-limited contexts like Iraq, while also signifying the importance of cybersecurity and technology for the resilience of MSMEs.

3.5. Hypothesis testing

The path analysis results clarified the effects of cybersecurity, economic factors, and technology factors on MSME performance (Table 4). All direct effects were statistically significant, with T-values above the criterion of 1.96 (Hair et al., 2024), thus providing strong support for all hypotheses. The relationship between cybersecurity and MSME performance (O= 0.659, p< 0.001) had a very strong positive impact, which indicates that enhanced implementation of cybersecurity measures significantly influences MSME performance. It was observed that economic factors affect cybersecurity (O= 0.198, p< 0.001), while technological aspects have a strong positive impact on cybersecurity (O= 0.442, p< 0.001). This means both economic and technological preparedness are key to improving cybersecurity protocols. It should be noted that indirect pathways (economic factors→cybersecurity→MSME performance and technology factors→cybersecurity→MSME performance) detail how cybersecurity mediates links between the factors and MSME performance. The findings corroborated previous studies, highlighting robust cybersecurity as an enabler to improve MSMEs' economic and technological factors for organizational performance.

3.6. Discussion

The purpose of this study was to analyze the variables that affect MSME performance through cybersecurity by using a structural equation model to test five hypotheses. The results prove that cybersecurity plays a very important role in MSME performance (R^2= 0.659, p= 0.000), proving that this is an absolute instrument to improve the stability and resilience of this type of enterprise. This is in agreement with the results of Ahmed et al. (2022) in their investigations on SMEs in emerging markets. As concluded by Kiganda (2022), the success of MSMEs depends on applying strong cybersecurity frameworks. Such frameworks not only boost performance by

Table 4. Path analysis results.

Path	Original sample	Sample mean	Standard deviation	T statistics	P values	Support
Cybersecurity-> MSME performance	0.659	0.659	0.038	17.125	0.000	Yes
Economic factors-> cybersecurity	0.198	0.199	0.043	4.566	0.000	Yes
Technology factors-> cybersecurity	0.442	0.444	0.049	9.076	0.000	Yes
Economic factors-> cybersecurity-> MSME performance	0.130	0.131	0.030	4.273	0.000	Yes
Technology factors-> cybersecurity-> MSME performance	0.291	0.293	0.038	7.588	0.000	Yes

instilling consumer confidence and safeguarding against cybersecurity threats but also help organizations align their actions with their words. The notable positive impact of economic factors on security (β= 0.198, p= 0.000) supports the findings of Jang and Kim (2022). This means that MSMEs should have enough finance to spend on cybersecurity infrastructure. Al-Hawamleh's (2024) findings are supported by a significant improvement in cybersecurity associated with technical aspects (β= 0.442, p= 0.000). These results provide a foundation for evaluating the effectiveness of cybersecurity practices implemented under conditions of technical readiness. The performance of SMEs is indirectly impacted by economic factors through cybersecurity (R^2= 0.130, p= 0.000), confirming Hasani et al.'s (2023) assertion that stable economies enable new methods of high-level security to be used, ultimately improving business outcomes. This tells us that security-oriented economic investments not only safeguard MSMEs but also facilitate their expansion. The direct effect of technical aspects on MSME performance (p= 0.000, R^2= 0.291) through cybersecurity support aligns with Singh & Singla's (2024) statement that organizational results are improved through the reinforcement of the security systems. By improving cybersecurity, technology therefore has an indirect effect on promoting the growth of MSMEs in a more digitalized environment. The results confirm all anticipated relationships, showing that both economic and technological components directly and indirectly impact MSME performance through cybersecurity. The relevance of having an integrated strategy that encompasses the economic, technological, and security components to improve MSME performance is also aligned with the latest literature, published after 2020. These findings demonstrate that cybersecurity is as critical a driver of outcomes as economic and technological drivers, thus enhancing our understanding of MSME performance.

CONCLUSION

This study was designed to study technology and the economics of MSMEs regarding the management of cybersecurity and its effectiveness in Iraq. This study has provided a better understanding of quantitative research methodology using PLS-SEM and contributed beneficial knowledge related to the effect of these attributes on MSME performance. The findings reveal that technological factors exert a stronger influence on cybersecurity adoption than economic factors, such as access to finance or macroeconomic stability. While both are statistically significant, the relatively weaker impact of economic considerations (β= 0.198) reflects the constraints faced by Iraqi MSMEs in a resource-limited, post-conflict environment where immediate operational concerns often outweigh long-term strategic investments. The moderate explanatory power of the model (R^2= 0.255 for cybersecurity adoption and R^2= 0.434 for MSME performance) underscores the complexity of the adoption landscape. Importantly, the findings suggest that technological readiness and awareness are more immediate enablers of cybersecurity implementation than economic incentives alone. This insight is particularly relevant given Iraq's ongoing digital transformation efforts amidst infrastructure gaps and limited institutional support.

These results emphasize the need for maintaining a stable economy and technology development to ensure effective cybersecurity management and, thereby, positively affect the overall organizational performance. These findings have tangible consequences for policymakers, MSME owners, and other stakeholders looking to strengthen cybersecurity and adapt to the changing digital landscape.

Practical implications and theoretical implications

The findings of this study offer several actionable insights for both MSME managers and government decision-makers, particularly in fragile and resource-constrained environments like Iraq. The study demonstrates that technological and economic factors significantly influence cybersecurity management, which in turn enhances enterprise performance. MSME managers should therefore prioritize even modest investments in cybersecurity tools, training, and awareness programs, recognizing cybersecurity not as a cost center but as a strategic asset that drives operational resilience and performance. By applying PMT, the study reveals how perceptions of cyber threat severity and response efficacy shape behavior. MSME leaders should foster a culture of risk awareness and proactive coping strategies—such as implementing clear security protocols, conducting regular risk assessments, and engaging employees in cybersecurity practices.

For government decision-makers, the findings highlight the mediating role of cybersecurity management in driving performance. Government agencies should provide targeted assistance to MSMEs such as tax incentives for cybersecurity adoption, subsidized access to training programs, or the creation of national cybersecurity advisory services focused on SMEs. In addition, governments should invest in public awareness campaigns and education initiatives that emphasize the growing threat of cyberattacks to small businesses, using culturally appropriate messaging that resonates with local business owners and managers.

This study contributes to the theoretical implication by expanding the application of PMT beyond its traditional use in individual health behavior and consumer research, demonstrating its relevance in an organizational context, specifically within MSMEs in developing economies. By showing how MSME decision-makers appraise threats (cyber risks) and coping mechanisms (cybersecurity measures), the study validates PMT as a robust behavioral framework for understanding cybersecurity adoption at the enterprise level. Also, by conceptualizing cybersecurity management as a mediating construct between external factors and firm performance, the study provides a theoretical mechanism through which external conditions influence organizational outcomes. This mediational pathway contributes to the growing literature on dynamic capabilities and risk management by highlighting how threat appraisal and response strategies can transform external pressure into performance-enhancing capabilities.

While the study is based in Iraq, its insights are highly transferable to other developing or conflict-affected countries with similar socioeconomic and technological conditions. Many MSMEs in regions such as sub-Saharan Africa, South Asia, or the Middle East face limited access to advanced digital infrastructure, high levels of economic uncertainty, and low awareness of cybersecurity threats. Therefore, the model and findings presented here can inform cross-national policy design and comparative research. Future studies can test the framework in these settings to further validate its generalizability and refine context-specific interventions.

Research limitations

This study was completed in October 2023, and in the intervening time, there have been many important developments, some of which are reported in this issue. Statistical sample sizes may by no means cover all the MSMEs in Iraq, particularly in rural or conflict-affected regions. Response bias can occur when individuals fill in self-reported questionnaires, providing responses that they deem socially valid. Cross-sectional studies differ from other research methodologies by virtue of the fact that they survey a collection of data at a given point in time. This complicates predictions about how technological and economic forces will affect performance and safety in the long run. People will likely remedy these shortcomings in the future with longitudinal studies, larger sample sizes, and a combination of different research methodologies.

REFERENCES

Agha, A. M., Massoudi, A. H., & Zaidan, M. N. (2023). The influence of individual, environmental, technology, and manufacturing factors on Iraqi gas and oil companies. *Cihan University-Erbil Journal of Humanities and Social Sciences*, *7*(1), 136-147. https://doi.org/10.24086/cuejhss.v7n1y2023.pp136-147

Ahmed, A., Bhatti, S. H., Gölgeci, I., & Arslan, A. (2022). Digital platform capability and organizational agility of emerging market manufacturing SMEs: The mediating role of intellectual capital and the moderating role of environmental dynamism. *Technological Forecasting and Social Change*, *177*, 121513. https://doi.org/10.1016/j.techfore.2022.121513

Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2025). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Annals of Operations Research*, *350*, 673-698. https://doi.org/10.1007/s10479-022-04844-8

Al-Anbgai, H. A. (2021). The impact of taxation accounting of value-added-tax in the engineering of the Iraqi economy. *Studies of Applied Economics*, *39*(11), 1-12. https://doi.org/10.25115/eea.v39i11.5910

Al-Hawamleh, A. (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. *International Journal of Computing and Digital Systems*, *15*(1), 1315-1331. https://doi.org/10.12785/ijcds/150193

Ali, M. H., Abd, M., Abdulnabi, S. M., Basheer, Z. M., Wafqan, H. M., Al_Lami, G. K., Alwan, A. N., & Mohammad, T. A. (2022). Mediating impact of supply chain management capabilities among the relationship of digital innovation, technology innovation and corporate sustainable performance of manufacturing firms in Iraq. *International Journal of Operations and Quantitative Management*, *28*(1), 316-334.

AllahRakha, N. (2024). Cybersecurity regulations for protection and safeguarding digital assets (data) in today's worlds. *Lex Scientia Law Review*, *8*(1), 405-432. https://doi.org/10.15294/lslr.v8i1.2081

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*, *78*, 102670. https://doi.org/10.1016/j.techsoc.2024.102670

Ayinde-Olawale, A. E., Ogunyemi, I. T., & Cirella, G. T. (2023). Economic shocks from COVID-19 and the assessment of micro-, small-, and medium-sized enterprises emergence of insurance coverage in urban south-west, Nigeria. In G. T. Cirella (Ed.), *Uncertainty shocks in Africa: Impact and equilibrium strategies for sound economic and social development* (pp. 45-63). Springer International Publishing.

Cartwright, A., Cartwright, E., & Edun, E. S. (2023). Cascading information on best practice: cybersecurity risk management in UK micro and small businesses and the role of IT companies. *Computers & Security*, *131*, 103288. https://doi.org/10.1016/j.cose.2023.103288

Charfeddine, L., Umlai, M. I., & El-Masri, M. (2024). Impact of financial literacy, perceived access to finance, ICT use, and digitization on credit constraints: evidence from Qatari MSME importers. *Financial Innovation*, *10*(1), 15. https://doi.org/10.1186/s40854-023-00557-4

Charoenrat, T., & Harvie, C. (2021). Analysis of the impact of COVID-19 on micro, small and medium-sized enterprises (MSMEs) in Thailand from competition policy and market access perspectives.

DataReportal (2024). *Digital 2024*. Retrieved from https://datareportal.com/reports/digital-2024-iraq

Erondu, C. I., & Erondu, U. I. (2023). The role of cyber security in a digitalizing economy: a development perspective. *International Journal of Research and Innovation in Social Science*, *7*(11), 1558-1570. https://doi.org/10.47772/IJRISS.2023.7011121

Hair, J. F., Sharma, P. N., Sarstedt, M., Ringle, C. M., & Liengaard, B. D. (2024). The shortcomings of equal weights estimation and the composite equivalence index in PLS-SEM. *European Journal of Marketing*, *58*(13), 30-55. https://doi.org/10.1108/EJM-04-2023-0307

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cybersecurity 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

Hassan, A., & Ahmed, K. (2023). Cybersecurity's impact on customer experience: an analysis of data breaches and trust erosion. *Emerging Trends in Machine Intelligence and Big Data*, *15*(9), 1-19.

Hendrawan, S. A., Chatra, A., Iman, N., Hidayatullah, S., & Suprayitno, D. (2024). Digital transformation in MSMEs: Challenges and opportunities in technology management. *Jurnal Informasi dan Teknologi*, 141-149. https://doi.org/10.60083/jidt.v6i2.551

Jang, J., & Kim, B. (2022). The impact of potential risks on the use of exploitable online communities: The case of South Korean cybersecurity communities. *Sustainability*, *14*(8), 4828. https://doi.org/10.3390/su14084828

Kiganda, M. (2022). *An Assessment of the factors affecting cyber resilience in microfinance institutions in Kenya* (Doctoral dissertation, Strathmore University).

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Mallick, M. A. I., & Nath, R. (2024). Navigating the cybersecurity landscape: a comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, *190*(1), 1-69.

Marsudi, D. F., Firmansyah, A. A., Censano, R., Dwiyanti, R. R., & Prasetyo, D. (2024). Key factors influencing the success of MSMEs in the digital era: A study in Jakarta City. *Modern Advances in Business, Economics, and Finance*, *1*(1), 1-10.

Massoudi, A. (2025). Predicting the power of entrepreneurial orientation in improving the level of product innovation. Business education as a mediator. *Journal of Management and Business Education*, *8*(1), 58-73. https://doi.org/10.35564/jmbe.2025.0004

Massoudi, A. & Birdawod, H. (2023). Applying knowledge management processes to improve institutional performance. *Cihan University-Erbil Journal of Humanities and Social Sciences*, *7*(1), 1-10. https://doi.org/10.24086/cuejhss.v7n1y2023.pp1-10

Massoudi, A. H., & Fatah, S. J. (2021). Advancing small and medium-size enterprises' performance by adopting marketing and service innovation. *International Journal of Procurement Management*, *14*(6), 742-758.

Massoudi, A. H., Fatah, S. J., & Jami, M. S. (2024). The role of artificial intelligence application in strategic marketing decision-making process. *Cihan University-Erbil Journal of Humanities and Social Sciences*, *8*(1), 34-39. https://doi.org/10.24086/cuejhss.v8n1y2024.pp34-39

Maulana, I. (2024). The position of MSME in the discourse of platform capitalism. In T. Fizzanty & I. Maulana (Eds.), *The digitalization of Indonesian small and medium enterprises: human capital, inclusivity and platform capitalism* (pp. 67-90). Springer Nature Singapore.

Mehchy, Z., Turkmani, R., & Gharibah, M. (2023). The role of MSMEs in Syria in poverty reduction and peacebuilding: challenges and opportunities. Peace and Conflict Resolution Evidence Platform, University of Edinburgh.

Morgan, H. L. (1965). The generation of a unique machine description for chemical structures-a technique developed at Chemical Abstracts Service. *Journal of Chemical Documentation*, *5*(2), 107-113. https://doi.org/10.1021/c160017a018

Nather, I. T., Burhanuddin, M. A., Sek, Y. W., & Ali, S. M. (2020). An investigation of crucial factors that influences the adoption of E-Commerce in small and medium enterprises in Iraq. *European Journal of Molecular and Clinical Medicine*, *7*(6), 813-828.

Nazem, S. N., Abid, M. M., Gdheeb, S. H., Altememy, H. A., Al Jouani, I. S. H., Mohsen, K. S., Abdulaal, A. H., Hamzah, A. K., & Rasol, M. A. (2023). Cybersecurity determinants in iraq's digital workplace: attitude, policy, and compliance roles. *International Journal of Cyber Criminology*, *17*(2), 1-19.

Norman, P., Boer, H., Seydel, E. R., & Mullan, B. (2015). Protection motivation theory. In M. Conner & P. Norman (Eds.), *Predicting and changing health behaviour: research and practice with social cognition models* (Vol. 3, pp. 70-106). Open University Press.

Purwanto, A. H. D., Nashar, M., Jumaryadi, Y., Wibowo, W., & Mekaniwati, A. (2022). Improving medium small micro enterprise'(MSME) performance. *International Journal of Advanced and Applied Sciences*, *9*(5), 37-46. https://doi.org/10.21833/ijaas.2022.05.005

Rahman, A., Indrajit, E., Unggul, A., & Dazki, E. (2024). Implementation of zero trust security in MSME enterprise architecture: challenges and solutions. *Sinkron*, *8*(3), 2077-2087. https://doi.org/10.33395/sinkron.v8i3.13949

Rasool, A. J. A., & Al-Othman, S. (2023). Entrepreneurship and facing challenges in Iraqi society market (an analytical prospective study on entrepreneurship in the governorates of Iraq). *International Research Journal of Innovations in Engineering and Technology*, *7*(9), 43-62. https://doi.org/10.47001/IRJIET/2023.709005

Salim, A. M. (2022). *The moderating roles of digital marketing and e-commerce on the relationship between business alignment factors and SME performance in Baghdad City of Iraq* (Doctoral dissertation, Universiti Tun Hussein Onn Malaysia).

Sayeed, S. A., Rahman, M. M., Alam, S., & Kshetri, N. (2024). FSCsec: Collaboration in Financial Sector Cybersecurity--Exploring the Impact of Resource Sharing on IT Security. *arXiv preprint arXiv*, 2410.15194.

Sekhar, S. C., & Radha, N. (2019). Impact of globalization on MSME: prospects, challenges and policy implementation on economic growth. *International Journal of Trend in Scientific Research and Development*, *3*(6), 536-541.

Simpson, D. C. (2024). *Understanding the importance of information security for small businesses* (Doctoral dissertation, National University).

Singh, V. J., & Singla, A. R. (2024). A systematic review of technological adoption factors and their impact on business intelligence implementation in MSMEs for uncertainty management. *Library Progress International*, *44*(3), 26492-26504. https://doi.org/10.48165/bapas.2024.44.2.1

Takács, J. M., & Pogátsnik, M. (2024). A comprehensive study on cybersecurity awareness: adaptation and validation of a questionnaire in hungarian higher technical education. *Acta Polytechnica Hungarica*, *21*(10), 533-552.

Tyagi, V. K., Gahlawat, R., Singla, T., & Gupta, M. (2023). Impact of emerging technologies on the disparity between micro, small, medium, and large businesses: an exploratory study. *International Conference on Financial Markets & Corporate Finance* (pp. 289-306). Springer Nature Singapore.

Ulupui, I. G. K. A., Zairin, G. M., Musyaffi, A. M., & Sutanti, F. D. (2024). Navigating uncertainties: a tri-factorial evaluation of risk management adoption in MSMEs. *Cogent Business & Management*, *11*(1), 2311161. https://doi.org/10.1080/23311975.2024.2311161

Vegesna, V. V. (2024). Cybersecurity of critical infrastructure. *International Machine Learning Journal and Computer Engineering*, *7*(7), 1-17.

Yeoh, W., Wang, S., Popovič, A., & Chowdhury, N. H. (2022). A systematic synthesis of critical success factors for cybersecurity. *Computers & Security*, *118*, 102724. https://doi.org/10.1016/j.cose.2022.102724

Younus, A. M., & Zaidan, M. N. (2022). The influence of quantitative research in business & information technology: An appropriate research methodology philosophical reflection. *American Journal of Interdisciplinary Research and Development*, *4*, 61-79.

Younus, A. M., Zaidan, M. N., & Shakir Mahmood, D. (2022). The effects of quality management practices on organizational performance in Malaysian small and medium-sized enterprises. *European Multidisciplinary Journal of Modern Science*, 137-157.

How to cite this article:

Zaidan, M., & Massoudi, A. H. (2025). The impact of technological and economic factors on cybersecurity management and MSME performance. *Internext*, *20*(3), e847. https://doi.org/10.18568/internext.v20i3.847