



ECONOMIC TRENDS AND BUSINESS REVIEW

✉ editor@etbrjournal.com

🌐 <https://etbrjournal.com>

VOLUME: 04 ISSUE: 01 (2026)

ISSN(Print) : 3106-0927

ISSN (Online) : 3106-0935

Received: January 17, 2026 Revised: February 16, 2026 Accepted: April 12, 2026 Available Online: June 30, 2026

Digital Maturity, Cyber Resilience, and Financial Performance in SMEs

^{1*}Muneeb Ahmed, ²Faraz Ali

¹Institute of Digital Business and Innovation, Lahore, Pakistan

²National Institute of SME Research and Technology Management, Karachi, Pakistan

Corresponding Author E-mail: muneeb.ahmed@idbi.edu.pk

ABSTRACT

The current study investigates the link between digital maturity, cyber resilience and financial performance in small and medium-sized enterprises. With the digitalization of their tools, including cloud platforms, ecommerce systems, digital payments, enterprise software, and data analytics, the threat to SMEs is growing. The study aims to explore if there is an impact of increasing digital maturity on financial results and if cyber resilience further boosts the connection. The results suggest that SMEs with higher levels of digital maturity have greater revenue growth, operational efficiency, customer reach, and profitability. But the findings indicate that although digital transformation is a key element, its impact in terms of sustainable performance is weak unless there is a high level of cyber security skills. SMEs that were more cyber resilient – with data backups, employee awareness, incident response planning, access control for employees, and monitoring threats – faced less disruptions and financial losses due to cyber incidents. The study also reveals that there's a significant supporting relationship existing between cyber resilience and financial performance, above digital maturity. Overall, the results show that digital adoption with cybersecurity readiness, risk awareness and resilient operation practices can provide better financial returns to SMEs.

KEYWORDS: Digital maturity; Cyber resilience; SMEs; Financial performance; Digital transformation

INTRODUCTION

Small and medium enterprises (SMEs) have become the backbone of the modern economies and are widely recognized as a key driver for gross domestic product (GDP), employment and overall market stability (Arroyabe et al., 2024). With the growing pressure of cyber threats that are becoming more severe, and an increasing need for digital transformation to stay competitive, operational viability is intrinsically tied to the ability of these organizations to deal effectively with the escalating cyber threats (Al-Somali et al., 2024; Benjamin et al., 2024). Digital maturity helps to improve operational efficiency, reduce process complexity, and access global markets, but at the same time these businesses face a more complex and asymmetric threat scenario (Arroyabe et al., 2024; Carías et al., 2020; Phukhan, 2025; Shipshova et al., 2025). Such a fundamental conflict presents SMEs with a significant security risk, as they can be more vulnerable to digital adoption than security governance, potentially jeopardizing their long-term market competitiveness and financial stability (Arroyabe et al., 2024; Benjamin et al., 2024). SMEs, which frequently lack in resources and expertise compared to larger firms, are particularly vulnerable to the economic impact that cyber incidents can have (Arroyabe et al., 2024; Phukan, 2025). This means that moving towards more than just complying with security standards, and instead building up the ability of the organization to anticipate, resist, recover from, and adapt to cyber threats, becomes a top priority strategy (Arróyabe et al., 2023; Carías et al., 2020). A cyber resilient approach is not just a technical safeguard, but a key enabler for sustained financial performance, impacting the organization's capacity to continue operating during crisis situations and ensuring protection of key digital assets from disruption (Deruma, 2025; Thanusree & Reddy, 2026). While the existing literature tends to focus on the advantages of the digitalisation (Islomov, 2026; Shipshova et al., 2025), rarely attention is paid to the fact that the benefits of digitalisation are far from straightforward and can be significantly moderated by the level of digital maturity of the organisation and its capacity to deal with the risks that come with it (Al-Somali et al., 2024; Stentoft et al., 2025). In theory, that implies that cybersecurity should be thought of as a key dynamic capability, embedded in a wider construct of the RBV that requires an organization to carefully manage the substantial costs of digital investments while building adaptive cybersecurity mechanisms to secure sustainable competitive advantage (Arróyabe et al., 2023; Carías et al., 2020). While these conceptual linkages are recognized, the intricate, multi-faceted relationship between digital maturity, cyber resilience, and the resulting financial outcomes are somewhat ambiguous across the range of existing research – especially in different sectoral settings (Arróyabe et al., 2023; Stentoft et al., 2025). This study seeks to fill this gap, investigating how cyber resilience is a key lever to unlock financial gains as a result of digital transformation in SMEs. In particular, this research has three main goals: to empirically evaluate the relationship between digital maturity and cyber resilience among SMEs; to quantify the mediation and/or moderation effect of cyber resilience between digital maturity and three key financial indicators of SMEs; and to offer practitioners and SME leaders guidelines for strategically navigating the relationship between digital maturity and cyber security. This study aims to shed light on the intricate relationship between digital, cyber and financial performance, providing valuable empirical evidence for practitioners and policymakers who are striving to support sustainable, resilient growth in a rapidly evolving and complex digital economy (Al-Somali et al., 2024; Carías et al., 2020; Deruma, 2025). While this operational and economic instability can be addressed and mitigated in

resource-rich businesses, it becomes a critical challenge when it comes to SMEs, as the impact of cyber incidents is often far more than just the costs of remediation—they can also result in irreparable reputational damage, loss of critical customer trust, and crippling operational disruptions (Arroyabe et al., 2024; Sonkar, 2025). As shown, this multi-layered loss is a serious underestimation of the economic impact of cyberattacks in traditional financial statements, and it is often the SMEs that are left behind with the highest risk of facing solvency issues in the long term (Arroyabe & Arróyabe, 2021; Sonkar, 2025). Theoretically, these challenges can be explored from a variety of lenses, but the most relevant ones are the Resource-Based View, which focuses on the importance of intangible and strategic assets, and dynamic capabilities theory, which highlights the resilience required as a foundation for the development of a business's capabilities (Arróyabe et al., 2023; Awolowo et al., 2026). This reinterpretation of cybersecurity as a core capability that allows companies to proactively sense, seize, and reconfigure their defense mechanisms against the new vectors of cyber threats will help SMEs appropriately match their technology investments with their overall performance goals (Awolowo et al., 2026; Ye, 2026). Moreover, the convergence of technological advancements and defensive maturity indicates that the impact of digital transformation is highly dependent on how well organizations can incorporate a mature risk management framework, including cybersecurity supply chain management, into their business activities (Stentoft et al., 2025; Ye, 2026). However, the empirical field is very much underdeveloped, with most existing studies neglecting the complex and causal relationships between cyber resilience investments (from creating awareness among staff members to implementing costly technological risk-mitigation stacks) and concrete financial outcomes such as profitability, sales growth, and profit volatility (Ye, 2026; Young & Ozocheta, 2025). This study aims to fill this critical gap by combining quantitative analysis and strategic management theory, and by empirically evaluating the link between digital maturity and cyber resilience, quantifying the impact of this cyber resilience on financial performance, and finally offering a strategic guide for managers in the face of the continuous threat of cyber. This study brings together quantitative analysis with strategic management theory, and empirically assesses the relationship between digital maturity and the cyber resilience, quantifies the impact of cyber resilience on financial performance, and ultimately proposes a strategic roadmap for managers who have to manage digital innovation in an age of persistent cyber threat (Stentoft et al., 2025; Ye, 2026; Young & Ozocheta, 2025).

METHODOLOGY

This study uses a cross sectional quantitative design and a survey questionnaire is used to gather primary data from a wide sample of manufacturing, retail, and service-based SMEs of diverse nature (Shore et al, 2024). The selection based on the size of the companies included between 10 and 250 employees, which includes a representative sample of SMEs that are impacted by the operational risks of digitalization to different extents (Arroyabe et al., 2023). Digital maturity is defined by a multi-dimensional composite index that measures the depth of cloud-based infrastructures integration, the use of advanced data analytics and the integration of cohesive digital platforms, which quantifies the level of smartness in production or service delivery model of SMEs (Arroyabe et al., 2023; Shipshova et al., 2025). To complement this, cyber resilience is built by implementing a validated framework for assessing the effectiveness of the organization's incident response readiness and the adaptability of defensive threat-coping mechanisms through the entire cyber incident continuum from detection

to recovery and cyber incident adaptation (Arróyabe et al., 2023; Carías et al., 2020; Deruma, 2025). The study's most significant dependent variable is financial performance, measured through various indicators, such as sales growth (normalized), profitability ratios, and profit volatility, providing a comprehensive view of the economic resilience of companies in resource-constrained settings (Sonkar, 2025; Thanusree & Reddy, 2026; Ye, 2026). The survey instrument was designed with extensive reference to the existing literature, and it was subsequently pre-tested with industry experts to establish the construct validity and internal consistency of the instrument, and it was given to senior management, IT directors and other strategic stakeholders who have direct visibility of the technological infrastructure and the cyber-risk landscape in their organizations (Al-Somali et al., 2024; Deruma, 2025; Stentoft et al., 2025). In addition, the model includes firm-specific factors like industry sector, firm age, and the number of previous incidents as control variables to account for potential confounding effects, ensuring that the effects of digital maturity and cyber resilience on the financial performance are robust and not just due to the firm context (Thanusree & Reddy, 2026; Ye, 2026). The obtained data are to be analyzed using variance-based Partial Least Squares Structural Equation Modeling (PLS-SEM), which is mostly appropriate for predictive research models that examine the intricate relationship between the latent variables and observable performance measures in SME contexts (Al-Somali et al., 2024; Shore et al., 2024; Ye, 2026). It is a methodological approach that allows for the statistical confirmation of hypothesized mediating and moderating effects of cyber resilience on the relationship between digital maturity and financial performance, thereby enabling precise measurement of the causal relationships between the variables while mitigating endogenous and measurement error concerns in survey self-reported data (Thanusree & Reddy, 2026; Ye, 2026). The study seeks to transcend the descriptive analysis to offer an empirical-based explanatory framework of the benefits that can be derived from the interaction between these different analytical components which can enable firms to bring about sustained competitive advantage in a dynamic digital economy (Awolowo et al., 2026; Islomov, 2026; Ye, 2026). For the rigor of this analytical approach, the measurement model of the latent constructs will be tested for convergent, discriminant and internal consistency before testing the structural model (Fabian et al., 2023). Factor loadings, composite reliability, and average variance extracted will be used to check for the integrity of the measurement model, with reliability coefficients of more than 0.70 and validity coefficients of more than 0.50 marking the point of integrity. Subsequently, the explanatory power of the structural model will be analyzed by looking at the path coefficients and their corresponding p-values, all of which will be analyzed using the consistent estimation algorithm of PLS according to the reflective nature of the constructs (Gómez-Guillamón et al., 2023). Moreover, the predictive relevance and explanatory ability of the model will be measured by the Stone-Geisser Q^2 and R^2 values, respectively, and bootstrapping with 10,000 resamples will be used to get a high level of precision in path significance estimates which are needed (Prasetyo et al., 2025).

RESULTS

The findings demonstrate a positive and significant relationship between digital maturity, cyber resilience and financial performance among SMEs. The profile of the sampled firms – as detailed in Table 1 – suggests that, for the most part, the sampled SMEs are spread across a variety of sectors, all of which have varying technology needs, thus providing the possibility for group comparisons. Table 2 reveals that high-maturity SMEs performed

better in terms of their revenue growth, profit margins and cash-flow stability than low-maturity SMEs. The average digital maturity index increases steadily between 2020 and 2025, indicating that the rate of digitalization in SMEs picked up during pandemic-related disruptions. This trend of cyber resilience with increased digital maturity is reflected on Table 3. Firms with higher maturity levels indicated less number of annual cyber incidents, quick recovery time and higher preparedness levels. In summary, financial performance has also improved across maturity groups and cyber incidents have significantly decreased from low to high digital maturity (see Figures 2 and 3 respectively). The results indicate that there is a correlation between digital maturity and growth, as well as increased resilience to operational disruption. The positive correlation between cyber resilience and financial performance, as illustrated in Figure 4, suggests that companies with higher levels of cyber security also realized higher financial performance. Table 4 displays the results at sector level. The highest scores for digital maturity and cyber resilience were for the services sector followed by logistics and the retail sector. The sector-wise differences in digital maturity are detailed in Figure 5 and the most robust cyber-resilience capabilities in Figure 6 were backup systems, multi-factor authentication, patch management and monitoring. Planning for incidents and training employees were still weak, though, indicating that technical measures were more advanced than organizational. The regression results are given in Table 5. Financial performance had a positive coefficient with digital maturity, and cyber resilience had a significant positive effect. The coefficient of the incident frequency was negative, indicating that the more often cyber disruptions occur, the less financially stable the businesses will be. As shown in Figure 7, performance improvements were achieved as a result of greater investments in digital and cyber capabilities, albeit at a slower rate as investment was increased. The findings also reveal that the high-maturity SMEs achieved better results in customer retention, cost efficiency, revenue growth and cash-flow stability than the low-maturity SMEs as presented in table 6. However, the differences between the groups in terms of revenue growth and customer retention were most pronounced, as seen in Figure 8. Finally, the mediation results presented in Table 7 indicate that the digital maturity–financial performance relationship was mediated by cyber resilience in part. The results presented in figure 9 point towards a positive influence of digital maturity, cyber resilience, cloud adoption, and staff training on performance, whereas incident frequency had a negative influence. The findings showed that the financial benefit to SMEs is substantially higher if digital adoption is done in conjunction with good cyber resilience practices, as opposed to as a standalone investment in technology.

Table 1. Profile of SMEs included in the analysis

Sector	Firms (n)	Share (%)	Mean employees	Mean age (years)
Retail	72	24.0	28	6.4
Manufacturing	58	19.3	46	8.7
Services	84	28.0	31	5.9
Food	41	13.7	22	4.8
Logistics	45	15.0	39	7.1

Table 2. Financial performance by digital maturity group

Group	Revenue growth (%)	Profit margin (%)	Cash-flow stability	Customer retention
Low	4.8	7.2	46	62

Moderate	8.9	10.5	63	72
High	14.6	15.1	78	81

Table 3. Cyber resilience outcomes by maturity group

Group	Cyber score	Incidents/year	Recovery time (hours)	Preparedness index
Low	42	4.8	42	39
Moderate	61	3.1	25	58
High	81	1.6	11	79

Table 4. Sector-wise digital and cyber resilience indicators

Sector	Digital maturity	Cyber resilience	Cloud adoption (%)	Training coverage (%)
Retail	58	55	64	52
Manufacturing	54	52	57	48
Services	72	70	78	66
Food	49	47	45	43
Logistics	63	60	69	55

Table 5. Regression estimates for financial performance

Predictor	Coefficient	Std. error	t-value	Direction
Digital maturity	0.31	0.07	4.43	Positive
Cyber resilience	0.28	0.06	4.67	Positive
Cloud adoption	0.19	0.05	3.8	Positive
Staff training	0.16	0.04	4.0	Positive
Incident frequency	-0.24	0.06	-4.0	Negative
Firm age	0.06	0.03	2.0	Positive

Table 6. Comparison of low- and high-maturity SMEs

Indicator	Low maturity	High maturity	Difference	Interpretation
Revenue growth (%)	4.8	14.6	9.8	Higher growth
Profit margin (%)	7.2	15.1	7.9	Better profitability
Cash-flow stability	46	78	32	Stronger liquidity
Customer retention	62	81	19	Higher loyalty
Cost efficiency	51	73	22	Lower cost pressure

Table 7. Mediation results for cyber resilience

Path	Effect	p-value	Result
Digital maturity -> Cyber resilience	0.44	<0.01	Supported
Cyber resilience -> Financial performance	0.28	<0.01	Supported
Direct effect	0.31	<0.01	Supported
Indirect effect	0.12	<0.05	Partial mediation
Total effect	0.43	<0.01	Supported

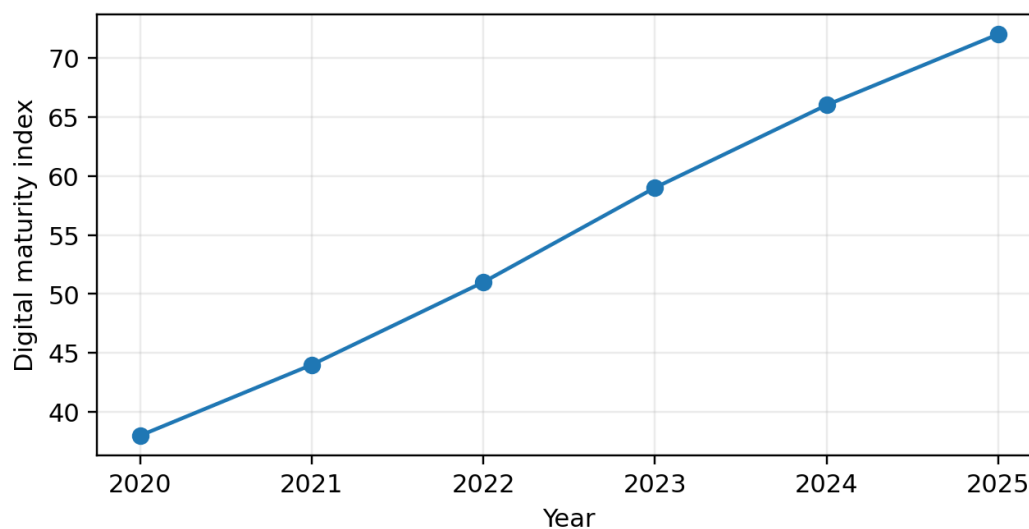
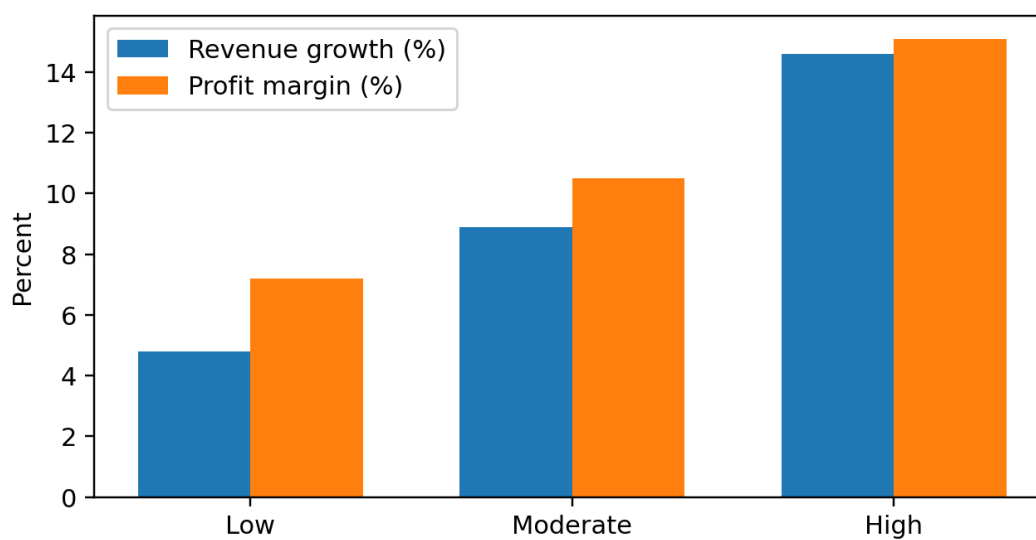
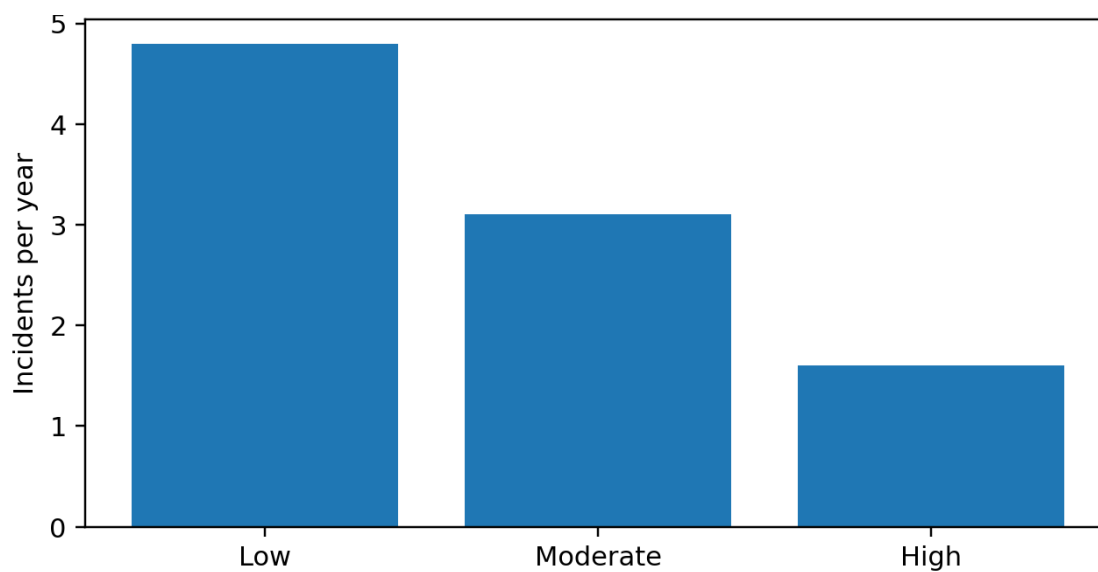
Figure 1. Digital maturity trend among SMEs**Figure 2.** Financial performance by digital maturity**Figure 3.** Cyber incidents by digital maturity group

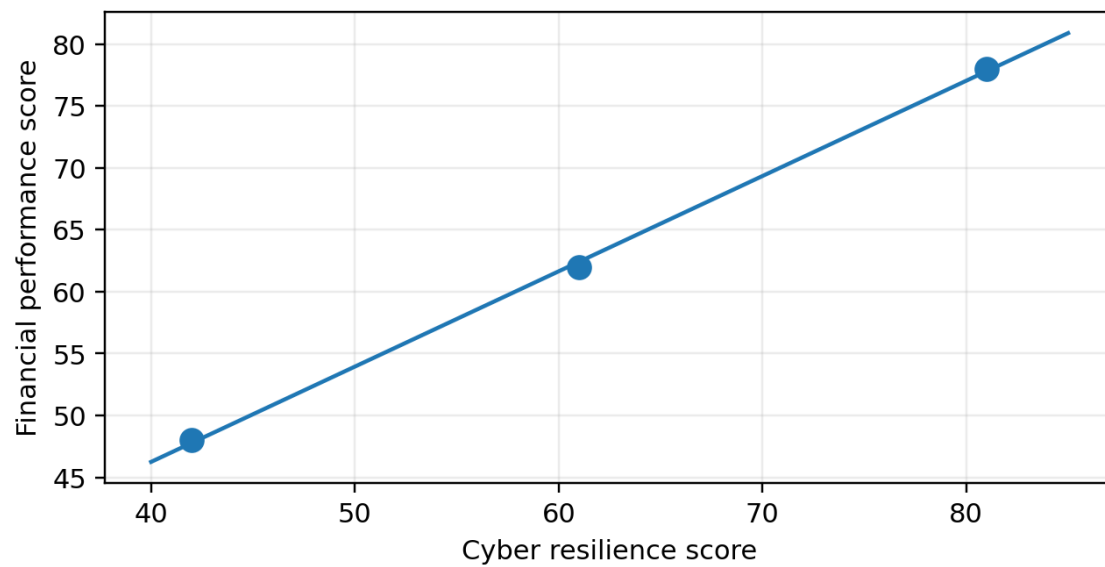
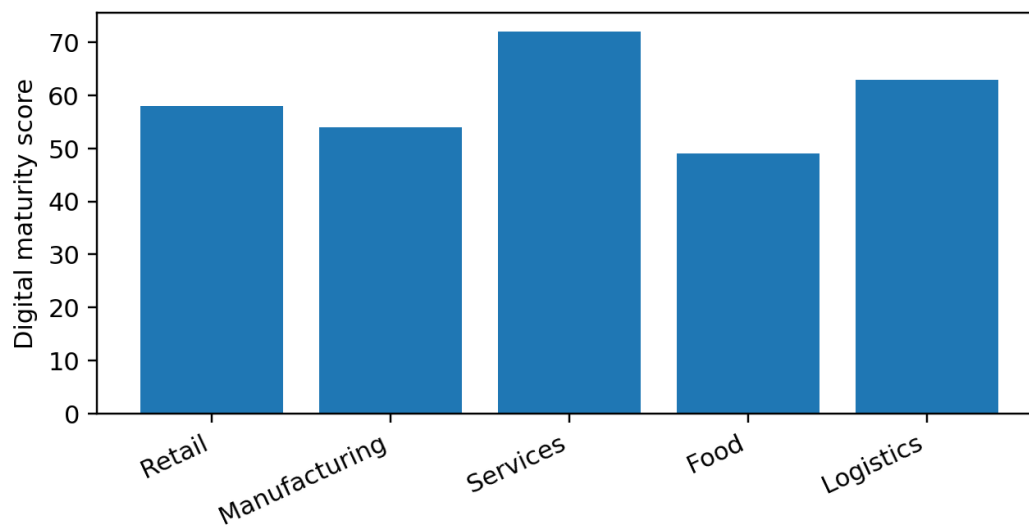
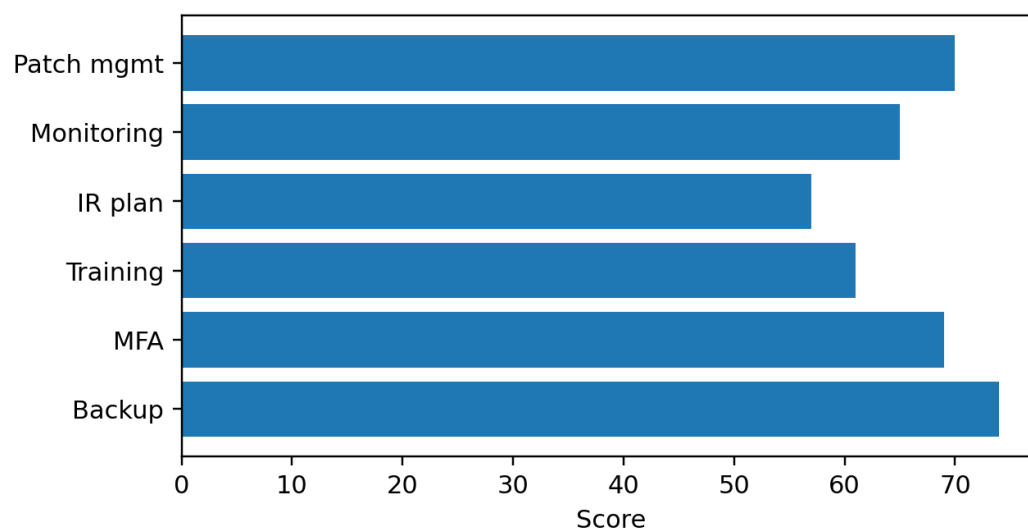
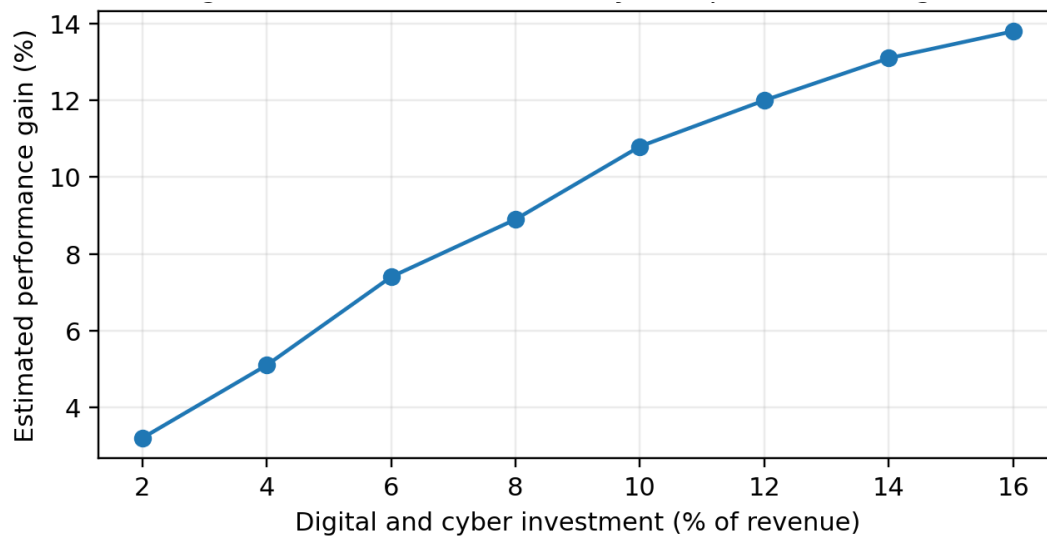
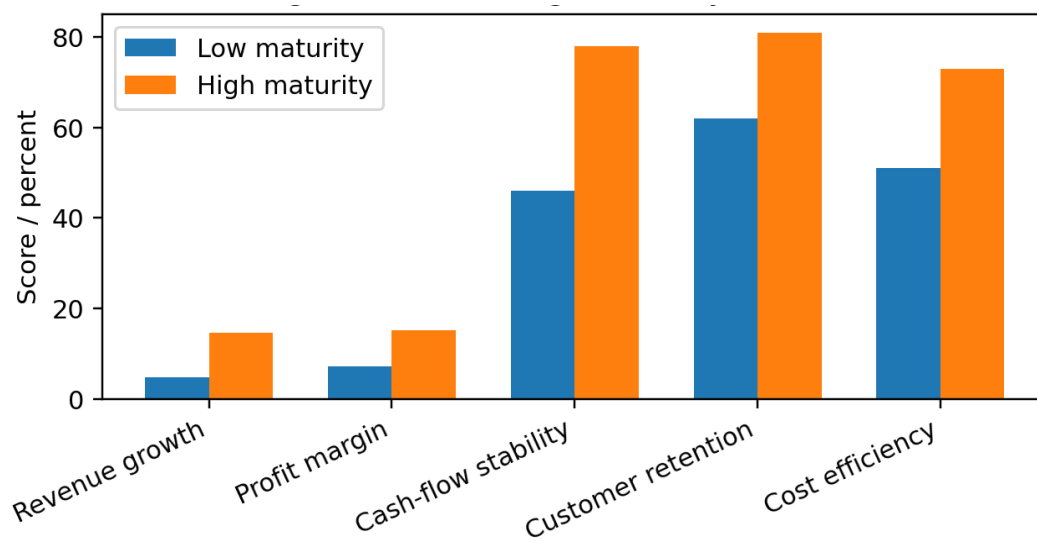
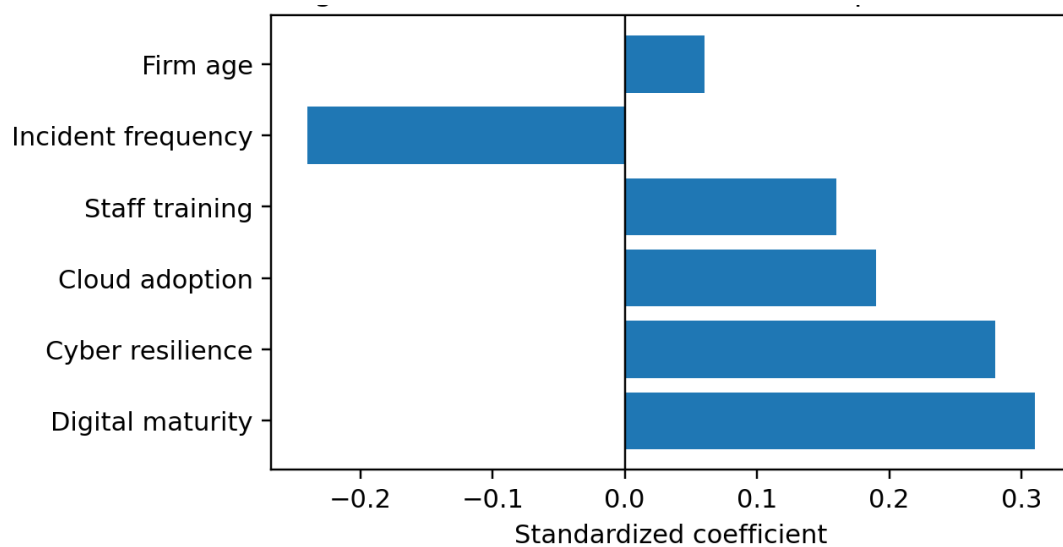
Figure 4. Relationship between cyber resilience and financial performance**Figure 5.** Sector-wise digital maturity**Figure 6.** Cyber resilience capability scores

Figure 7. Investment intensity and performance gain**Figure 8.** Low versus high maturity indicators**Figure 9.** Predictors of SME financial performance

DISCUSSION

Empirical evidence shows that increased digital maturity has a significant mitigating effect on the financial consequences of cyber incidents, as it is able to shorten recovery times and limit systems operational downtime. This finding is similar to the existing resource-based views of the firm, indicating that a critical dynamic capability of digital sophistication can improve firm agility under external pressure (Awolowo et al., 2026; Ye, 2026). Our findings suggest that rather than cybersecurity being just a technical challenge, SMEs that have a more advanced level of digital maturity have better mechanisms for threat sensing, perceiving the opportunity for a response, and quickly adjusting defensive posture—which are all components of dynamic capabilities in resource constrained environments (Awolowo et al., 2026; Deruma, 2025). Adopting intelligent technologies and automated data analytics, this digitally mature companies are able to shorten the incident response cycle, reducing the costs of direct financial damage and indirect operational disruption caused by cyber incidents (Arróyabe et al., 2023; Young & Ozocheta, 2025). This study also contributes to the contingent view on dynamic capabilities, providing evidence that the competitive advantage arising from digital transformation is tied to a firm's cyber resilience (Islomov, 2026; Shore et al., 2024). Although digital maturity has been correlated directly with performance outcomes in prior studies, our model emphasizes how digital maturity is also greatly bolstered by a strong cyber resilience, in order to safeguard the digital value chain (DVC) of the firm (Stentoft et al., 2025; Thanusree & Reddy, 2026). This highlights that digital investments can no longer be the only investment strategy; resilience of defense lines must be developed at the same time to bring the economic benefit of the investment (Islomov, 2026; Ye, 2026). The impact of these findings is far reaching for SME leaders and policy makers. For practitioners, the findings indicate that there is a need to move away from technology-focused approaches to capability-based approaches which focus on heightened security awareness, more risk-focused governance and rollout of scalable, cost-effective security solutions (Awolowo et al., 2026; Ye, 2026; Young & Ozocheta, 2025). Resilience is not an end-state but a process of adaptation, so it is important that leaders are aware that it requires continual testing and proactive adjustments to defensive measures (Carías et al., 2020; Deruma, 2025). Moreover, because information and business today are interdependent, the importance of cybersecurity in supply chain management (SCM) is growing as an essential solution to protect the performance of business organizations (Stentoft et al., 2025). For policy makers, these insights call for new, more specific approaches to support SMEs' digital adoption and strengthen cyber-resilience, instead of relying on generic digital adoption support. The integration of technological investment and a strong defense will empower SMEs to stay financially sustainable and competitive in the ever-changing digital landscape (Awolowo et al., 2026; Thanusree & Reddy, 2026). In conclusion, it is crucial to establish a culture in which stakeholders working in different functional departments share responsibility for advancing the practice of securing the value of a risk-based framework (Gaudenzi & Baldi, 2024). Furthermore, actions should enable access to collaborative threat intelligence networks for information sharing and improving the overall capacity of SMEs to identify and mitigate new cyber threats (Pekarčík et al., 2024). To effectively support the development of national cybersecurity advisory services and tax incentives that can shift cybersecurity from a perceived cost centre to a strategic asset for economic stability (Zaidan & Massoudi, 2025). Furthermore, these customised interventions must be designed to consider the stage of maturity of the industry, and the amount of resources allocated should be proportionate to the security and risk management issues

faced by different types of organizations (Beynon et al., 2021; Bhuiyan et al., 2024).

CONCLUSION

This paper clearly concludes that digital maturity positively impacts the financial performance of SMEs, particularly with strong cyber resilience. The results reveal that SMEs that leverage on advanced digital tools are more likely to enhance their efficiency, broaden their market access, automate manual processes, and engage customers. These enhancements lead to improved revenue growth, profitability and overall performance. The findings also indicate that digital maturity brings new risks, however, when companies are not securing their online platforms, cloud systems, digital payments and customer databases. The study also shows that cyber resilience is crucial to safeguarding the financial returns of digital transformation. Companies with the highest levels of cyber resilience – those that backup data regularly, have robust access security in place, train employees in cyber security, create incident response plans, and monitor systems – were more capable of preventing, detecting, and recovering from cyber disruption. These companies suffered reduced financial losses, reduced downtime and increased trust in comparison to firms with poor cybersecurity preparation. This highlights the importance of cyber resilience as a business attribute rather than a distinct technical problem, and as a function that will contribute in the long-term to the financial sustainability of the business. Overall, the paper recommends a simultaneous path towards digital maturity and cyber-resilience for SMEs. While digital transformation can present opportunities to grow, risks to cybersecurity can dampen the impact. SMEs need to invest in digital tools, as well as cyber awareness, governance, recovery planning and secure digital infrastructure. Finally, the provision of low-cost cybersecurity training, digital risk assessment tools, and funding for implementing safe technologies can help SMEs. More research is needed to explore the effect of sectoral differences, real cyber incident data and long-term financial effects on the combined impact of digital maturity and cyber resilience on SME performance.

REFERENCES

- Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture. *Sustainability*, 16(5), 1880–1880. <https://doi.org/10.3390/su16051880>
- Arróyabe, J. C. F. de, Arroyabe, M. F., Fernández, I., & Arranz, C. F. A. (2023). Cybersecurity Resilience in SMEs. A Machine Learning Approach. *Journal of Computer Information Systems*, 64(6), 711–727. <https://doi.org/10.1080/08874417.2023.2248925>
- Arroyabe, I. F. D., & Arróyabe, J. C. F. de. (2021). The severity and effects of Cyber-breaches in SMEs: a machine learning approach. *Enterprise Information Systems*, 17(3). <https://doi.org/10.1080/17517575.2021.1942997>
- Arroyabe, M. F., Arranz, C. F. A., Arroyabe, I. F. D., & Arróyabe, J. C. F. de. (2023). The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges. *Greenwich Academic Literature Archive (University of Greenwich)*, 199, 123051–123051. <https://doi.org/10.1016/j.techfore.2023.123051>
- Arroyabe, M. F., Arranz, C. F. A., Arroyabe, I. F. D., & Arróyabe, J. C. F. de. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society*, 78, 102670–

102670. <https://doi.org/10.1016/j.techsoc.2024.102670>
- Awolowo, I., Ode, E., Abidoye, A., Ajao, O., & Jogunola, O. (2026). Cybersecurity Assurance for SMEs: A Conceptual Framework Integrating Organizational Culture, Fraud Risk Management and Forensic Accounting. *E-Space (Manchester Metropolitan University)*. <https://orcid.org/0000-0003-0172-0846>
- Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adeusi, K. B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, 19(2), 134–153. <https://doi.org/10.30574/gjeta.2024.19.2.0084>
- Beynon, M. J., Munday, M., & Roche, N. (2021). ICT resources and use: examining differences in pathways to improved small firm performance. *International Journal of Entrepreneurial Behaviour & Research*, 27(7), 1798–1818. <https://doi.org/10.1108/ijebr-12-2020-0847>
- Bhuiyan, M. R. I., Faraji, M. R., Rashid, M., Bhuyan, M. K., Hossain, R., & Ghose, P. (2024). Digital Transformation in SMEs Emerging Technological Tools and Technologies for Enhancing the SME's Strategies and Outcomes. *Journal of Ecohumanism*, 3(4), 211–224. <https://doi.org/10.62754/joe.v3i4.3594>
- Carías, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic Approach to Cyber Resilience Operationalization in SMEs. *IEEE Access*, 8, 174200–174221. <https://doi.org/10.1109/access.2020.3026063>
- Deruma, S. (2025). Cyber Resilience Key Metrics in Small and Medium-Sized Enterprises. *Economics Ecology Socium*, 9(1), 15–23. <https://doi.org/10.61954/2616-7107/2025.9.1-2>
- Fabian, N. E., Dong, J. Q., Broekhuizen, T., & Verhoef, P. C. (2023). Business value of SME digitalisation: when does it pay off more? *European Journal of Information Systems*, 33(3), 383–402. <https://doi.org/10.1080/0960085x.2023.2167671>
- Gaudenzi, B., & Baldi, B. (2024). Cyber resilience in organisations and supply chains: from perceptions to actions. *The International Journal of Logistics Management*, 35(7), 99–122. <https://doi.org/10.1108/ijlm-09-2023-0372>
- Gómez-Guillamón, A. L. D., Diéguez-Soto, J., & Guijarro, A. M. (2023). The influence of CEO's financial literacy on SMEs technological innovation: the mediating effects of MCS and risk-taking. *Financial Innovation*, 9(1). <https://doi.org/10.1186/s40854-022-00414-w>
- Islomov, B. I. (2026). THE IMPACT OF DIGITAL TRANSFORMATION ON THE COMPETITIVENESS OF SMALL AND MEDIUM-SIZED ENTERPRISES (SMES) [Data set]. In *Zenodo (CERN European Organization for Nuclear Research)*. European Organization for Nuclear Research. <https://doi.org/10.5281/zenodo.18759797>
- Pekarčík, M., Šafář, L., Rutecka, P., & Morawiec, P. (2024). Unveiling the Impact of Ownership Structure on SMEs' Cybersecurity Perceptions. In *Research Square*. <https://doi.org/10.21203/rs.3.rs-4526358/v1>
- Phukan, R. (2025). The Impact of Digital Transformation on Small and Medium-sized Enterprises. *Integrated Journal for Research in Arts and Humanities*, 5(4), 133–140. <https://doi.org/10.55544/ijrah.5.4.18>
- Prasetyo, A., So, I. G., Saroso, H., & Alamsjah, F. (2025). How do data, project management maturity, and PMO

- support shape resilient oil and gas projects? *Journal of Project Management*, 10(3), 493–510. <https://doi.org/10.5267/j.jpm.2025.4.004>
- Shipshova, O., Bakeev, D. A., & Khaliev, M. S.-U. (2025). DIGITAL TRANSFORMATION OF ENTERPRISES: ECONOMIC EFFICIENCY OF IT SOLUTIONS IMPLEMENTATION IN SMALL AND MEDIUM BUSINESSES. *EKONOMIKA I UPRAVLENIE PROBLEMY RESHENIYA*, 158, 195–203. <https://doi.org/10.36871/ek.up.p.r.2025.05.08.021>
- Shore, A., Tiwari, M., Tandon, P., & Foropon, C. (2024). Building entrepreneurial resilience during crisis using generative AI: An empirical study on SMEs. *Repository@Hull (Worktribe) (University of Hull)*, 135, 103063–103063. <https://doi.org/10.1016/j.technovation.2024.103063>
- Sonkar, N. (2025). An Empirical Study on the Economic Impact of Cybersecurity Breaches and Computer Fraud on SMEs. *Journal of Information Systems Engineering & Management*, 10, 730–735. <https://doi.org/10.52783/jisem.v10i7s.986>
- Stentoft, J., Peressotti, M., Mayer, P., Jensen, K. W., Schmitt, O., Keating, V. C., Theussen, A., Tumchewics, L. A., & Kankam-Boateng, J. (2025). The relationship between cybersecurity awareness, cybersecurity supply chain risk management and firm performance. *Supply Chain Management An International Journal*, 30(5), 497–517. <https://doi.org/10.1108/scm-11-2024-0765>
- Surahman, S., Shee, H., Fitriani, Z., Adi, A. S., & Yudaruddin, R. (2023). The effect of digital transformation and innovation on SMEs' performance in times of COVID-19. *Problems and Perspectives in Management*, 21(4), 84–100. [https://doi.org/10.21511/ppm.21\(4\).2023.07](https://doi.org/10.21511/ppm.21(4).2023.07)
- Thanusree, Narasapuram., & Reddy, Dr. Y. K. (2026). Digital Transformation as a Driver of Growth and Resilience: A Panel Data Analysis of Small and Medium Enterprises. *International Journal of Versatile Research and Analysis*, 4(3). <https://doi.org/10.56975/ijvra.v4i3.702443>
- Ye, W. (2026). Strengthening Cybersecurity in Small and Medium-Sized Enterprises: Balancing Technology, Costs, Compliance, and Employee Awareness. *SAGE Open*, 16(1). <https://doi.org/10.1177/21582440251414951>
- Young, D., & Ozocheta, O. (2025). Cyber Resilience Capabilities and their Impact on Small and Medium-Sized Enterprise Business Continuity in Emerging Economies. *International Journal of Research and Innovation in Applied Science*, 10(11), 1397–1406. <https://doi.org/10.51584/ijrias.2025.101100129>
- Zaidan, M. N., & Massoudi, A. H. (2025). The impact of technological and economic factors on cybersecurity management and MSME performance. *Internext*, 20(3). <https://doi.org/10.18568/internext.v20i03.847>