Social capital and Artificial intelligence readiness: the mediating role of cyber resilience and value construction of SMEs in resource-constrained environments

ODE, Egena, AWOLOWO, Ifedapo Francis <http://orcid.org/0000-0003-0172-0846>, NANA, Rabake and OLAWOYIN, Femi

Citation:

Copyright and re-use policy

Social Capital and Artificial Intelligence Readiness: The Mediating Role of Cyber Resilience and Value Construction of SMEs in Resource-Constrained Environments

Egena Ode[1] · Ifedapo Francis Awolowo[2] · Rabake Nana[3] · Femi Stephen Olawoyin[2]

Abstract

Drawing on social capital theory, this study explores the antecedents of AI readiness in Small and Medium-sized Enterprises (SMEs) operating in resource-constrained environments, emphasising capabilities that mitigate cyber risks, and foster value construction in SMEs. Specifically, the study examines how structural, cognitive, and relational social capital fosters cyber resilience and contributes to proactive value construction, enhancing SMEs' AI readiness and enabling them to construct and sustain value while safeguarding against potential cyber threats. The study adopts a Covariance-based Structural Equation Modelling (CB-SEM) approach to analyse 589 valid responses. A multi-wave data strategy with an interval cross-lagged design was implemented to reduce the risk of common method bias. The findings reveal that structural and relational capital significantly drive AI readiness, while cognitive social capital enhances cyber resilience, which is pivotal in constructing and protecting organisational value. Moreover, cyber resilience mediates the relationship between cognitive social capital and AI readiness, and enabling value construction amid cyber-related disruptions. SMEs with robust social capital networks are better equipped to leverage AI technologies for innovation and growth, construct new value streams, and defend against cyber risks, securing value in dynamic digital environments. This study contributes to the growing discourse on cybersecurity and digital transformation by offering insights into how SMEs can bolster digital innovation and construct sustainable value in the face of mounting cyber risks.

Keywords Social capital · Cyber resilience · AI readiness · Value construction

1 Introduction

Globally, Small and Medium-sized Enterprises (SMEs) are vital for job creation, economic growth, and development. As most economies' backbone, SMEs contribute significantly to innovation, employment, and social stability. However, the rapid pace of digital evolution presents both opportunities and challenges for SMEs. Digital adoption can enhance competitiveness, support sustainable development, and drive the customisation of products and services. For instance, adopting digital technologies such as Artificial Intelligence (AI), offers SMEs significant opportunities for innovation, operational efficiency, and market competitiveness (Mitsa & Lyakh, 2023; Paul et al., 2023). Previous studies have argued that AI can improve product personalisation, customer engagement, internal processes, and decision-making (Abrokwah-Larbi & Awuku-Larbi, 2023; Wang et al., 2021).

However, SMEs face barriers such as high costs, infrastructure challenges, and other risks such as data security concerns (Iftikhar & Nordbjerg, 2021; Oldemeyer et al., 2024). In addition, SMEs often face significant obstacles before and after digitisation, including a lack of skilled personnel, cybersecurity vulnerabilities, and difficulties in implementing digital strategies (Melo et al., 2023; Philbin et al., 2022; Rupeika-Apoga & Petrovska, 2022). Moreover, organisational factors such as business strategy, leadership,

✉ Ifedapo Francis Awolowo
    i.f.awolowo@shu.ac.uk

1   Centre for Enterprise, Department of Strategy, Enterprise and Sustainability, Manchester Metropolitan University, Lower Ormond Street, Manchester M15 6BX, UK

2   Sheffield Business School, Sheffield Hallam University, Howard Street, Sheffield S1 1WB, UK

3   School of Business, Education and Law, University of Huddersfield, Huddersfield HD1 3DH, UK

and management are critical in facilitating digital adoption. When supported by skilled employees, robust IT infrastructure, and clear digital strategies, digitisation can positively impact SMEs' performance, financial outcomes, and value construction (Eller et al., 2020; Melo et al., 2023).

Value construction refers to the process by which firms create, enhance, and sustain value for stakeholders through strategic activities and resource utilisation (Lepak et al., 2007). For SMEs, value construction involves leveraging digital technologies and organisational capabilities to improve operational efficiency, develop innovative products and services, and achieve sustainable growth. In the digital economy, value construction is essential for competitiveness and resilience. It requires SMEs to manage risks, including cybersecurity threats, and proactively and effectively harness internal and external resources. However, digital adoption such as AI increases exposure to cyber threats such as phishing, malware, and data breaches (Benjamin et al., 2024). These risks are exacerbated by resource constraints and limited cybersecurity expertise (Bagheri et al., 2023; Punt et al., 2023). Cyber incidents can lead to financial losses, reputational damage, and operational disruptions, hindering value construction. Therefore, SMEs must develop robust networks and strategies to protect their digital assets and ensure business continuity.

Strong social networks can mitigate cybersecurity vulnerabilities by facilitating the exchange of critical information, best practices, and resources. SMEs' ability to acquire capabilities and apply knowledge is crucial for success, competitiveness, and value construction (Eller et al., 2020; Ramdani et al., 2021). Engagement with business networks and stakeholders, including other firms, financial institutions, and government agencies, is essential for accessing scarce resources and finding innovative solutions. Social capital, defined as the network of relationships that provide access to resources (Nahapiet & Ghoshal, 1998), fosters collaboration, knowledge sharing, and the collective development of cybersecurity capabilities. Leveraging these networks allows SMEs to build cybersecurity resilience proactively, safeguarding against cyber risks while constructing and sustaining value in the digital economy. Structural social capital enhances information flow, relational capital builds trust for sharing cybersecurity knowledge, and cognitive capital fosters a proactive cybersecurity culture. These dimensions enable SMEs to pool resources, reduce costs, and develop capabilities supporting cyber resilience and value construction (Ali-Hassan, 2009; Baycan & Öner, 2023).

Kanini and Muathe (2019) argue that SMEs with strong social capital are better equipped to navigate market challenges and seize new opportunities. Social network theory further emphasises that both bonding (strong internal ties) and bridging (external connections) social capital are critical for resource access and value construction (Kalra et al.,

2020). Despite its importance, research on how social capital mitigates cyber risks and fosters value construction in SMEs, particularly in resource-constrained environments, remains limited. While digital adoption can automate operations and reduce costs with SMEs (Giguashvili, 2024), limited research has examined how SMEs in resource-constrained environments build AI readiness to drive value construction.

This study extends the literature on AI readiness by exploring how structural, relational, and cognitive social capital enhances cyber resilience and AI readiness and value construction in resource-constrained environments. While previous studies have examined AI adoption in SMEs, majority of the research has focused on organisational factors, key challenges, and technological factors (Abrokwah-Larbi & Awuku-Larbi, 2023; Hibban & Abhishek, 2024; Karuppiah et al., 2023; Rasaputhra, et al., 2024; Schönberger, 2023). Our study moves beyond these perspectives by illustrating the role of social capital dimensions in fostering AI readiness through cyber resilience. Specifically, we demonstrate that different dimensions of social capital influence AI readiness through distinct mechanisms. For instance, structural and relational social capital are direct enablers of AI readiness while cognitive social capital, while not directly linke to social capital, fosters cyber resilience, which in turn enhances AI readiness and value construction.

Previous studies have shown that AI readiness primarily depends on factors such as firm size, financial resources, and technical expertise (Mariyana et al., 2024; Paul et al., 2023; Schönberger, 2023), however this study shows the social capital-based enablers of AI readiness, by demonstrating that well-connected SMEs (structural and relational capital) can overcome technical and financial constraints. Generally, while previous studies on AI adoption has focused on technical enablers such as data infrastructure and digital literacy, this study introduces cyber resilience as a key factor, showing that cognitive social capital indirectly contributes to AI readiness by strengthening the ability of SMEs to withstand cyber threats. Moreover, studies have explored the fundamental role of cybersecurity in large organisations but have largely neglected its implications for SMEs digital transformation (Philbin et al,. 2022; Ramdani, et al., 2021). This study bridges the gap by positioning cyber resilience as a crucial mediator, demonstrating how SMEs in resource-constrained environments leverage social capital to construct value despite cyber risks. Similarly, previous research has explored the role of social capital in general innovation processes and value creation (Sulistyo & Ayuni, 2019). but has not explicitly linked it to AI readiness and cybersecurity in SMEs. This study extends the social capital theory by showing how distinct forms of social capital interact to shape AI readiness and digital resilience in SMEs. Specifically, the study extends current literature in three ways:

First, this study develops a framework positioning social capital and cyber resilience as key drivers of AI readiness, enabling SMEs to mitigate cyber risks while constructing value. This is important because resilient networks facilitate the exchange of best practices and technical knowledge for AI integration, helping SMEs overcome innovation challenges through shared resources and collective learning (Abredu et al., 2023; Boateng et al., 2020). Moreover, strong social capital also supports collaborations with AI providers and experts, fostering technological advancement and sustainable value construction (Antwi et al., 2021; Fanggidae et al., 2023). Secondly, building on social capital theory, this study demonstrates that the relationship between cyber resilience and AI readiness is significantly strengthened through the effective use of social capital (Bagheri et al., 2023; Punt et al., 2023). Despite the importance of social capital in fostering resilience and innovation, limited research examines how it drives SME AI readiness and value construction in resource-constrained environments.

Thirdly, this study provides a nuanced examination of how different dimensions of social capital—structural, relational, and cognitive social capital contribute to strengthening cyber resilience, and in turn, facilitate AI readiness in SMEs. The study explores how cyber resilience mediates the relationship between social capital and AI readiness to safeguard and construct organisational value. Structural social capital, characterised by network ties and connectivity enhances information sharing, collaborative problem-solving and access to resources which are critical to building cyber resilience. On the other hand, relational capital which involves mutual obligations, trust and norms can foster an environment where SMEs can collectively develop cybersecurity practices and exchange best practice in ways that mitigate cyber risks. Cognitive social capital, characterised by shared understanding and common language among stakeholders can ensure that SMEs align their digital transformation strategies with cyber risk management. Particularly in resource contrained environments where technological and financial limitations hinder digital adoption, this study demonstrates that social capital can become a strategic asset that can facilitate trust-based knowledge exchange, adaptive security practices and peer learning within SMEs. It also positions social capital as a foundational capability that strengthens the ability of SMEs to leverage AI and digital technologies for sustained value construction. By conceptualising cyber resilience as a mediating mechanism, this paper offer a novel perspective that explains how SMEs can simultaneously innovate and secure value in dynamic environments, thereby extending the scope of AI readiness research into the domain of cybersecurity.

The remainder of this paper is structured as follows: Section 2 reviews the literature and develops hypotheses; Section 3.1 outlines the research methodology; Section 4.1 presents the results and hypothesis testing; and Section 5.1 discusses the findings, implications, limitations, and future research directions.

2 Literature Review and Hypotheses Development

This study draws from the social capital theory (SCT) to explore how SMEs' social capital can act as a buffer against cyber vulnerabilities caused by digital adoption to enhance their competitiveness. SCT has emerged as a crucial concept highlighting the resources embedded in social networks and their potential benefits (Lin, 2017; Lin & Huang, 2023). The notion of social capital in information systems research emphasises the resources inherent in social networks, including structural, relational, and cognitive characteristics (Ali-Hassan, 2009). It offers a significant foundation for comprehending knowledge-sharing activities and cooperation in intricate, knowledge-intensive environments (Lee et al., 2019).

Ali-Hassan (2009) asserts that social capital enhances knowledge diffusion, collaboration, and influence inside networks. Thus, SCT has been used as a theoretical framework that provides insights into several areas of information systems study, such as outsourcing, knowledge management, software development, and IT-enabled inter-organisational connections (Balijepally et al., 2004). In contrast to human capital, which exists inside individuals, social capital is ingrained in relational networks, rendering it an essential asset for managing social interactions within organisational settings (Balijepally et al., 2004). Most research defines social capital as the social or economic value an individual or group derives from resources made available by social networks or interactions (Baycan & Öner, 2023). Previous studies have predominantly focused on technological solutions to cyber threats while overlooking the social dimensions that can empower SMEs in resource-constrained environments to strengthen their defences. SCT is applied in this study to explain how SMEs can develop capabilities that can exploit their social resources to improve their cyber resilience and reduce the potential risks associated with cyber threats.

2.1 Social Capital in SMEs

The complexity of social capital is reflected in its varied definitions. Bourdieu (2018) views it as a resource linked to durable networks, emphasising its instrumental value. Others focus on its societal benefits, such as fostering civic engagement (Gupta & Singh, 2023), while a resource-oriented view sees it as assets within networks that can be accessed for various purposes (Kanazawa & Savage, 2009).

These perspectives highlight social capital's individual and collective benefits.

Due to their limited resources, social capital is crucial for SMEs. Strong networks help SMEs access information, resources, and opportunities vital for growth and innovation (Kanini & Muathe, 2019). This aligns with the resource-based view (RBV), which sees unique resources like social capital as competitive advantages (Hsu & Chen, 2019). During the COVID- 19 pandemic, firms with strong networks adapted better through information sharing and resource mobilisation (Darmi et al., 2022; Ngoc & Vy, 2022).

Social network theory further explains social capital's role in SMEs. Bonding social capital (strong internal ties) fosters trust while bridging social capital (weaker external ties) provides diverse information and resources, driving innovation and adaptability (Kalra et al., 2020; Kim & Shim, 2018). Entrepreneurs with high social capital can access financial resources and market opportunities, boosting growth and profitability (Fanggidae et al., 2023; Sombolayuk & Yusuf, 2019).

Social capital also strengthens SMEs' competitive advantage. It supports innovation and entrepreneurial orientation, driving profitability and sustainable business practices (Prabandari & Yulianti, 2023; Sulistyo & Ayuni, 2019). Social networks help SMEs navigate global market complexities in internationalisation, especially in emerging economies (Khoury et al., 2020; Kontinen & Ojala, 2012).

Social capital in SMEs consists of three dimensions: structural (network size), relational (quality of relationships), and cognitive (shared understanding) (Cots, 2011). These dimensions foster innovation, knowledge sharing, and problem-solving. However, over-reliance on existing networks can limit diverse perspectives, stifling adaptability (Octasylva et al., 2023). Additionally, the impact of social capital varies by context and is influenced by geography, culture, and industry dynamics (Chumnangoon et al., 2021; Halim et al., 2015).

2.2 Social Capital and Cyber Resilience

Cyber resilience is an organisation's ability to prepare for, respond to, and recover from cyber incidents while maintaining operations (Carias et al., 2021; Uddin et al., 2023). This is critical for SMEs, which often lack the resources to combat sophisticated cyber threats, leaving them vulnerable to financial, reputational, and operational risks (Carias et al., 2020; Munusamy & Khodadi, 2023). Strong social capital can mitigate these risks by enabling information sharing on threats, best practices, and resources, strengthening individual firms and the broader business community (Bagheri et al., 2023; Punt et al., 2023).

Within social capital, the structural dimension comprising formal and informal networks is key in enhancing cyber resilience. These networks facilitate communication and collaboration, which is crucial for sharing critical cybersecurity information and strategies (Muniady et al., 2015). Diverse networks encourage innovative cybersecurity solutions by enabling knowledge exchange across sectors (Oussi & Chtourou, 2020). Access to external expertise through these networks improves SMEs' resilience while enhancing overall firm performance, particularly in supply chain responsiveness during crises (Acquah et al., 2023).

However, larger and more complex networks, especially those using digital channels, can increase SMEs' exposure to cyber risks like malware and phishing attacks (Abbasi et al., 2014; Boyes, 2015). The rise of remote work and digital operations post-COVID- 19 has further expanded these vulnerabilities (Ozanne et al., 2022). As SMEs' networks grow, their ability to monitor and secure all connections weakens, creating a trade-off between collaboration-driven innovation and security. Therefore, while structural social capital likely supports cyber resilience, its effectiveness may be moderated by the size and complexity of networks (Shan & Tian, 2022). Based on this analysis, we hypothesise that:

H1a: Structural social capital is positively associated with cyber resilience.

Relational social capital, particularly trust, promotes cooperation, reduces transaction costs, and enhances organisational performance (Saz-Gil et al., 2021). In cybersecurity, trust encourages employees to report security issues, share concerns, and collaborate on solutions without fear, fostering quick decision-making and effective threat mitigation (Marampa et al., 2023; Wilson & McDonald, 2024).

However, excessive trust can create vulnerabilities. Employees may unknowingly fall victim to social engineering or phishing attacks by trusting seemingly legitimate internal communications without verification (Birthriya et al., 2024; Jagatic et al., 2007; Lineberry, 2007; Workman, 2007). Many cyberattacks exploit this trust to breach systems (Taib et al., 2019).

Additionally, the interaction between relational and structural social capital strengthens organisational networks, improving cross-departmental information sharing and the effectiveness of security teams (Orekhova & Zarutskaya, 2022). This synergy supports a unified approach to cyber resilience. Based on this, we propose the following hypothesis:

H1b: Relational social capital is positively associated with cyber resilience.

Cognitive social capital, defined by shared values, beliefs, and norms, fosters trust and a sense of belonging, promoting cooperation and collective action within organisations

(Prieto-Pastor et al., 2018; Ruseva et al., 2016). This shared understanding influences employees' perceptions of their roles and responsibilities, enhancing collaboration (Ahn & Kim, 2017).

Organisations with strong cognitive social capital show greater innovation and learning due to increased knowledge sharing and problem-solving (Ahn & Kim, 2017; Maurer et al., 2011). This mindset is crucial for cyber resilience, enabling adaptability and quick responses to emerging threats (Lakse & Menike, 2020). Shared mental models and common security language improve communication, aiding faster threat detection and coordinated responses (Lee et al., 2015).

However, overreliance on shared understanding can lead to overconfidence, groupthink, and blind spots, increasing vulnerability to unconventional threats (Størseth, 2017; Tuma & Van Der Lee, 2022). Thus, while cognitive social capital likely supports cyber resilience, balancing internal cohesion with external insights is essential. Based on this, we theorise that:

H1c: Cognitive social capital is positively associated with cyber resilience.

2.3 Social Capital, Cyber Resilience and SME AI Readiness

As AI becomes central to modern business strategies, SMEs must prepare for adoption while managing rising cyber threats (Varma et al., 2023). This readiness depends on technology and external networks but also on cyber resilience, which enables SMEs to withstand and recover from cyber-attacks that could hinder AI integration (Borah et al., 2022; Karuppiah et al., 2023). This study examines how social capital dimensions, particularly structural social capital, influence SME AI readiness through the mediating role of cyber resilience. Strong networks with external partners provide SMEs access to vital information, resources, and cybersecurity expertise, supporting AI adoption and digital security (Antwi et al., 2021; Fanggidae et al., 2023). Collaborative networks help SMEs share risks, pool resources, and overcome innovation barriers while strengthening defences against cyber threats (Abredu et al., 2023; Boateng et al., 2020). This is critical, especially in resource-constrained emerging economies like Nigeria, where digital breaches can severely disrupt operations (Aderibigbe et al., 2023; Badghish & Soomro, 2024). SMEs with strong structural social capital can better access cybersecurity and AI support, ensuring secure AI integration (Oldemeyer et al., 2024; Schönberger, 2023). Therefore, this study proposes that cyber resilience enables AI readiness by safeguarding SMEs against cyber disruptions. Based on this, we propose the following hypothesis:

H2a: Structural social capital is positively associated with SME AI readiness.￿￿￿￿

Relational social capital, driven by trust, fosters cooperation and knowledge sharing, which is vital for SMEs adopting AI (Lawa & E-Vahdati, 2022; Prabandari & Yulianti, 2023). Strong relational ties encourage collaboration, helping SMEs overcome knowledge gaps and implementation challenges in AI adoption (Jöhnk et al., 2020; Oldemeyer et al., 2024).

Beyond information sharing, trust-based relationships promote a culture of experimentation and innovation, motivating SMEs to explore and invest in AI despite uncertainties (Al-Somali et al., 2024; Chao & Kim, 2023; Prabandari & Yulianti, 2023). These networks also provide insights into market needs and technological trends, driving AI innovation (Antwi et al., 2021). In emerging economies with limited resources (Aderibigbe et al., 2023; Lee et al., 2025), relational networks are crucial for pooling knowledge and resources, enabling collective progress in AI adoption. Based on this, we propose the following hypothesis:

H2b: Relational social capital is positively associated with SME AI readiness.

Building on the link between relational social capital and SME AI readiness, cognitive social capital shared values and norms strengthen an organisation's ability to adopt AI technologies. A collective understanding of AI's benefits increases employee willingness to embrace new systems and aligns AI initiatives with business strategies, enhancing successful implementation (Hibban & Abhishek, 2024; Novandari et al., 2023).

Additionally, cognitive social capital supports cyber resilience during AI adoption. Shared awareness of cybersecurity risks encourages preventive actions, safeguarding digital infrastructure and ensuring secure AI integration (Ortigueira-Sánchez et al., 2020; Sugandini et al., 2020). This alignment prevents complacency and protects sensitive data and operations.

Moreover, a unified cognitive framework balances innovation and security, fostering collaboration and tailored solutions while mitigating risks (Kim & Shim, 2018; Widyawati et al., 2023). Thus, cognitive social capital positively influences SME AI readiness by integrating innovation with cyber resilience. Based on this, we theorise that:

H2c: Cognitive social capital is positively associated with SME AI readiness.

The relationship between cyber resilience and technology adoption in SMEs is complex. Organisations with strong cyber resilience are better equipped to adopt advanced

technologies, including AI, by mitigating cyber risks (Mudalige, 2022). This is especially critical in emerging markets where data security concerns and infrastructure challenges are prevalent (Aderibigbe et al., 2023). Conversely, SMEs with weak cyber resilience may hesitate to adopt new technologies due to fears of vulnerabilities and data breaches (Carias et al., 2020; Gautam & Gautam, 2023). Thus, cyber resilience is both a defensive and proactive strategy for fostering innovation and technology adoption.

Research shows that organisations with robust cyber resilience frameworks are more prepared for AI adoption, having established protocols for data security and privacy (Ahmadi-Assalemi et al., 2020). Additionally, integrating AI can enhance cyber resilience through advanced threat detection and response (Kant & Johannsen, 2022). This symbiotic relationship underscores the need for a cyber-resilient culture in SMEs, particularly in emerging economies, where resilience can offset resource and infrastructure constraints.

SMEs face dynamic cyber threats and resource limitations, making cyber resilience critical (Carias et al., 2020; Fernandez de Arroyabe et al., 2023; Soudi & Bauters, 2024). Developing resilience through anticipating, detecting, surviving, and recovering from cyber incidents is essential. While social engineering remains a major threat, AI presents opportunities and challenges in managing cyber risks (Varma et al., 2023). Strengthening cyber resilience is proposed to influence SME AI readiness positively. Based on this, we hypothesise that:

H3: Cyber resilience is positively associated with SME AI readiness.

Building on the link between cyber resilience and AI readiness, this study proposes that cyber resilience mediates the relationship between social capital and SMEs' AI readiness. The three dimensions of social capital, structural, relational, and cognitive- positively influence cyber resilience and support AI adoption. Structural social capital enhances access to cybersecurity resources and collaborative opportunities (Abredu et al., 2023; Antwi et al., 2021). Relational social capital fosters trust and cooperation, encouraging open communication and problem-solving around cybersecurity issues (Lawa & E-Vahdati, 2022; Prabandari & Yulianti, 2023). Cognitive social capital promotes a shared commitment to balancing security and innovation (Novandari et al., 2023; Sugandini et al., 2020).

Stronger cyber resilience instils confidence in SMEs to invest in AI technologies that handle sensitive data (Ahmadi-Assalemi et al., 2020; Carias et al., 2020). This is especially important for Nigerian SMEs, where social capital can help overcome cybersecurity challenges through collaboration and knowledge sharing, easing concerns about data security in AI adoption.

Research shows that cyber incidents impact SME resilience more than cybersecurity capabilities, highlighting SMEs' need for shared cybersecurity information due to vulnerability (Fernandez de Arroyabe et al., 2023; van Kranenburg et al., 2023). Therefore, we propose that:

H4: Cyber resilience mediates the relationship between social capital and SME AI readiness.

2.4 SME AI Readiness and Value Construction

In a dynamic business environment, SMEs must capitalise on new opportunities to maintain a competitive edge. SMEs with high AI readiness can streamline operations, automate tasks, and optimise resources, enhancing resilience and enabling faster responses to market changes and customer demands (Medeiros & Maçada, 2021). This efficiency drives adaptability and positions SMEs as industry innovators by offering superior products, improved customer experiences, and novel business models (Sombolayuk & Yusuf, 2019). Thus, AI-ready SMEs are more agile, innovative, and capable of seizing market opportunities.

Social capital further strengthens the link between AI readiness and value construction. Strong networks promote knowledge sharing, collaboration, and collective problem-solving (Ma et al., 2021), enabling SMEs to leverage AI for innovative projects and quicker responses to emerging opportunities. This collaboration expands market awareness and enhances strategic action.

Additionally, social capital fosters internal knowledge diffusion, allowing AI-ready SMEs to develop innovative solutions tailored to their needs (Ul Zia et al., 2023). Combined with AI tools that analyse market trends in real-time, SMEs can identify and exploit market gaps ahead of competitors (Ebuka et al., 2023; Kareem et al., 2024). This synergy between AI readiness and social capital drives sustainable innovation and growth (Badghish & Soomro, 2024). Therefore, this study proposes that SMEs with higher AI readiness are better positioned to exploit market opportunities through improved efficiency, innovation, and collaboration. Based on this, the following hypothesis is proposed:

H5: SMEs with higher AI readiness are better positioned for value construction.

3 Method

3.1 Data Collection and Sample

The sample for this study comprises registered small and medium-sized enterprises (SMEs) in Nigeria, employing between 10 and 249 employees. In stage 1, SMEs were

identified through business directories, chambers of commerce, industry associations, databases of registered companies and networks of SME associations. Some of the list was drawn from the Corporate Affairs Commission of Nigeria and the Small and Medium Enterprises Development Agency of Nigeria (SMEDAN). In stage 2, a stratified random sampling was applied to ensure adequate representation of industries, geographic regions and firm sizes. The stratification helped the researchers ensure diversity while maintaining generalisability within the SME population. Regarding respondents' selection, the survey was sent to decision-makers directly involved in strategic decision-making and familiar with AI readiness and social capital dynamics. Multiple contacts were made to encourage participation and reduce the risk of non-response bias. To mititage potential selection bias, the data collection process ensured representation across different SME sectors, including retail, manufacturing and digital services. To mititage selection bias, we focused on SMEs that have engaged in digital adoption efforts within the last three years. The study also stratified the sample based on industry type and business size to avoid over-repreenting technology-focused SMEs which may already have higher AI readiness in comparison to non-tech sectors.

This study implemented a multi-wave data strategy using a 6-month interval cross-lagged design to reduce the risk of common method bias (Podsakoff et al., 2003). The six-month interval was chosen for the three-wave design because previous research indicates that it can provide adequate observation to accurately capture the perceived impact of social capital on AI readiness within SMEs. The interval approach is in accordance with the existing literature (Xie et al., 2023). The survey, which included links to the questionnaire, was shared with leaders of various SME associations. For the SMEs we identified, we sent emails to the SMEs containing the URLs to the survey, the participant information document, and the informed consent forms. The participants were initially invited to evaluate their use of digital technology and provide demographic data, including education, age, involvement with innovation activities, and other demographic information, during time 1 (T1). The participants were requested to assess their cyber resilience and social capital during time 2 (T2). Lastly, the respondents were requested to assess their capacity to capitalise on opportunities and AI readiness in time 3 (T3). In T1, a total of 681 responses were received. The questionnaire was disseminated to 681 SMEs in T2, and 613 had completed it. The questionnaire was distributed to 613 SMEs in T3. In total, 589 usable responses were obtained and analysed using Covariance-Based Structural Equation Modelling (CB-SEM). A time-lagged approach was used to mirror real-world organisational processes, considering that the development of capabilities such as resilience and the

ability to exploit opportunities unfold over time (Khurana et al., 2022). Also, the research reduced concerns regarding reverse causality by measuring the antecedent, such as social capital and cyber resilience, before measuring value construction (Podsakoff et al., 2003).

Two factors influenced our choice. First, temporal separation for causal examination. First,this method diminishes the likelihood that the data collection procedure influences the observed correlations among variables, therefore properly reflecting authentic organisational dynamics (Podsakoff et al., 2003). Secondly, alignment with real-world processes: the three-wave architecture reflects actual organisational processes, wherein skills such as cyber resilience and the leveraging of social capital often develop following the creation of foundational conditions, such as AI readiness. This technique corresponds with research methodologies suitable for evolving organisational environments, such as the resource-constrained environment of our study.

However, further checks were carried out to ensure the data was suitable for further analysis. Consequently, Harman's single-factor test was performed to test for Common Method Bias (CMB). To compute CMB, all items were loaded into an exploratory factor analysis to examine if a single factor explained most of the variance. The analysis results indicate that the first factor accounted for 22.73% of the variance, below the recommended 50% ((Podsakoff et al., 2003). This suggests that CMB is not a major concern in this study. Thus, it does not affect the validity of the relationships examined in this study. Thus, procedural remedies and statistical tests confirm the robustness of the reported results.

3.2 Measures

Social capital was measured using 12 items across three dimensions: structural (4-items), relational (4-items) and cognitive social capital (4-items). The scale was adopted from Seo (2020). AI readiness scale was adopted from a measurement scale from Baabdullah et al. (2021). The scale measures the readiness of firms to adopt new technologies like AI across three dimensions – awareness (4 items), technicality (4 items) and infrastructure (3 items). The scale assesses whether SMEs know AI's existence, their capacity to use AI technologies, and whether they have the infrastructure to adopt AI technology, such as IT components, integrated web applications and databases. Cyber resilience scale was measured using a 10-item scale adapted from Martín-Rojas et al., (2023). Value construction, which measures an SME's capacity to identify and capture opportunities, was measured using a 5-item opportunity recognition scale adopted from Kuckertz et al.

Table 1 Research items

Variables	Items	Factor loading	α
Structural social capital (Seo, 2020)	The formal exchange of industrial and/or market information among partners	0.55	0.79
	Periodical meetings to share ideas and/or technological knowledge with partners	0.85	
	Active use of informal communication channels to enhance the networks of the partnership	0.74	
	High accessibility among partners regardless of geographical limitation	0.61	
Relational social capital (Seo, 2020)	Avoidance to make decisions that may damage partners' concerns	0.72	0.77
	A strong belief that partners keep their word to others	0.75	
	Constructive negotiations with partners to solve conflicts or coordinate interests	0.69	
	Goodwill to support each other in the partnership	0.46	
Cognitive social capital (Seo, 2020)	Partners' mutual understanding of common goals and motives for the partnership	0.62	0.79
	Development of a common identity to reduce cultural distance among partners	0.82	
	Shared interpretations of different meanings among partners	0.88	
	Shared norms to discourage undesirable behaviour against common goals	0.47	
Cyber resilience (Martín-Rojas, et al., 2023)	My organisation has documented procedures to deal with whatever follows from cyber-attack disruption	0.59	0.88
	My organisation has tried to see the humorous side of problems and has taken advantage of them following a cyber disruption	0.65	
	Coping with the stress generated by cyber threats has strengthened my organisation	0.64	
	My organisation has tended to bounce back from difficulties or hardships caused by cyber-attacks	0.72	
	My organisation has been able to achieve goals despite obstacles generated by cyber threats	0.71	
	My organisation has been able to stay focused under the pressure caused by cyber-attacks	0.71	
	My organisation has not been easily discouraged by failures generated by cyber-attacks and has been able to handle unstable and unpleasant situations	0.77	
	My organisation has been more successful after a cyber-attack disruption	0.71	
	My organisation has not succumbed to problems and has remained strong during cyber threats	0.68	
Value Construction (Kuckertz, et al., 2017)	I have set up an organisation to pursue a business opportunity I perceived	0.78	0.86
	Based on a business opportunity I perceived, I have developed a new market	0.88	
	I have put together an entrepreneurial team to pursue a business opportunity I perceived	0.74	
	I have approached investors (e.g. business angels or venture capitalists) to acquire funding for a business opportunity	0.66	
AI Awareness (Baabdullah, et al., 2021)	We know about AI applications	0.60	0.71
	We have received enough information about the benefits of using AI applications	0.84	
	We have received enough information on how to use AI applications	0.54	
	We have received information about the security system of AI applications	0.81	
AI Technicality (Baabdullah, et al., 2021)	It would be easy to use the AI applications technically	0.83	0.80
	It would be easy to operate the AI applications	0.58	
	It would not take much time to become familiar with the AI applications	0.51	
	It does not look difficult to use the AI applications	0.76	
AI Infrastructure (Baabdullah, et al., 2021)	Our firm has a good AI-based infrastructure including all IT components	0.93	0.74
	There are integrated Web applications encompassing different functional areas	0.63	
	Our firm shares the databases for various applications, rather than having a separate database for each application	0.74	

(2017). Table 1 Shows the factor loadings and the Cronbach alpha for each construct.

Some items, such as "goodwill' under relational social capital, showed low factor loadings (< 0.4). Such items with consistently low factor loadings were flagged and considered for removal from the final analysis. Also, content validity was revisited, and items were revised or dropped if they failed to align conceptually with the latent constructs. Also, the reliability was computed after item adjustments with Cronbach's alpha and composite reliability values exceeding acceptable thresholds.

4 Results

The CFA and path analysis were performed using AMOS 29. The method described by Fornell and Larcker (1981) is employed to test convergent and discriminant validity. Cronbach alpha was used to evaluate a construct's reliability. As shown in Table 1, it ranged from 0.71 to 0.88.

4.1 Sample Characteristics

The characteristics of the respondents and their firms are presented in Table 2 reveals that 80.8 per cent of the firms employ between 11 and 200 employees, while 84.4 per cent of the firms have never exported their products or services. As can be seen in Table 2, 51.4 per cent of the firms have developed new products and services, while 48.6 per cent have filed patents.

Table 2 Sample characteristics

Highest Education	Freq	%	Age	Freq	%
PhD	17	2.9	*20–29 years*	141	23.9
Masters	129	21.9	*30–39 years*	200	34.0
Degree/HND	347	58.3	*40–49 years*	186	31.6
O'Level	96	16.3	*> 50 years*	62	10.5
Work experience			**Firm size**		
1–5 years	171	29.0	*1–10*	113	19.2
6–10 years	298	50.6	*11–50*	357	60.6
11–15 years	118	20.0	*50–200*	119	20.2
> 16 years	2	3			
Industry/Sector			**Digital Tech used**		
Services	181	30.7	*Cloud computing*	58	9.6
Retail	81	13.8	*E-commerce*	196	33.3
Technology	162	27.5	*CRM software*	67	11.4
Others	165	28	*Others*	268	45.5
Innovation activities			**Exporting activities**		
New product/service development	303	51.4	*Yes*	92	15.6
Patents filed	286	48.6	*No*	497	84.4

4.2 Measurement Model

A confirmatory factor analysis (CFA) was used to examine the convergent and discriminant validity to test for reliability and validity (Table 3). The Average Variance Extracted (AVE) and Composite Reliability (CR) values were assessed for each construct to assess the convergent validity. According to the Fornell and Larcker (1981) criterion, the AVE scores for each construct should be above 0.50, while the CR values should be above 0.70 to demonstrate sufficient internal consistency. As indicated in Table 3, the AVE values range between 0.50 and 0.59, suggesting sufficient convergent validity. Similarly, the CR values range from 0.79 to 0.90, demonstrating a strong internal consistency among the variables. Discriminant validity was also assessed using the Fornell-Larcker Criterion. This method compares the square root of the AVE for each construct and its correlation with other constructs. As shown in Table 3, Discriminant validity is confirmed when the square root of each variable's AVE is higher than its correlation with other constructs (Fornell & Larcker, 1981). Table 1 shows that discriminant validity was confirmed for all the constructs. Table 3 also shows the means and standard deviation for each construct. Since the criteria for convergent and discriminant validity thresholds were met, a path analysis was used to test the hypotheses.

To prepare the data for further analysis, CFA was performed to evaluate the measurement model. The measurement model was assessed by evaluating the observed normed χ^2 (χ^2/df), Comparative fit index (CFI), Goodness of fit (GFI), root mean square of approximation (RMSEA), root mean square of residual (RMR), Adjusted goodness of fit (AGFI), Normed fit index (NFI) for all constructs and the overall model. All the constructs were evaluated in the CFA to confirm their unidimensionality and ensure that the factor structure holds. The analysis revealed that structural capital χ^2 (χ^2/df) = 0.457, CFI = 1.00, GFI = 1.00, RMSEA = 0.000, RMR = 0.004, AGFI = 0.996, and NFI = 0.999, p = 0.499, relational capital = χ^2 (χ^2/df) = 4.276, CFI = 0.995, GFI = 0.996, RMSEA =, RMR = 0.012, AGFI = 0.964, and NFI = 0.993, p = 0.039, cognitive capital χ^2 (χ^2/df)

Table 3 Correlations, Reliability and Validity

Variables	M	SD	C.R	AVE	1	2	3	4	5	6
(1) Structural capital	4.469	.602	.823	.56	**0.748**	**				
(2) Relational capital	3.052	.369	.795	.50	.639**	**0.707**			*	
(3) Cognitive capital	2.997	.439	.785	.50	.404**	.517**	**0.707**	*		
(4) Cyber resilience	4.959	.617	.899	.51	.051	.094*	.131**	**0.714**	.057	
(5) Value construction	4.826	.799	.829	.55	.316**	.303**	.277**	.057	**0.742**	
(6) AI Readiness	5.700	.685	.875	.59	.387**	.461**	.321**	.178**	.308**	**0.768**
MSV					.408	.408	.267	.032	.100	.212

** Correlation is significant at the 0.01 level (2-tailed), * Correlation is significant at the 0.05 level (2-tailed). n = 589. Diagonal values (in bold) are the square roots of AVE for each construct

= 1.658, CFI = 0.999, GFI = 1.00, RMSEA = 0.033, RMR = 0.000, AGFI = 0.986, and NFI = 0.998, $p = 0.198$ and AI readiness = $\chi 2$ ($\chi 2/df$) = 2.967, CFI = 0.966, GFI = 0.973, RMSEA = 0.058, RMR = 0.055, AGFI = 0.945, and NFI = 0.950 exhibit a good fit as reported in the fit indices. Similarly, cyber resilience = $\chi 2$ ($\chi 2/df$) = 2.797, CFI = 0.985, GFI = 0.980, RMSEA = 0.055, RMR = 0.022, AGFI = 0.954, and NFI = 0.977 and value construction = $\chi 2$ ($\chi 2/df$) = 1.846, CFI = 0.998, GFI = 0.996, RMSEA = 0.038, RMR = 0.015, AGFI = 0.981, and NFI = 0.995, $p = 0.136$ also exhibited a good fit. To simplify the model for the subsequent path analysis and reduce the potential for multicollinearity, item parcelling was employed. Parcelling involved combining individual items into smaller number of parcels which are then treated as indicators of the laten constructs. This approach was adopted because it simplifies the model complexity whilst maintaining the integrity of the measurement structure. After the item parcelling, a path analysis was performed to test the hypothesises relationships among the latent variables. As shown in Table 4, the overall model fit indices for the measurement model meets the criteria for the recommended thresholds for fit indices. Thus, it can be concluded that the model fits the data well and can be used for testing the hypotheses.

4.3 Structural Model

First, this study examined the direct association between structural capital, relational capital, cognitive social capital, cyber resilience and SME AI readiness. The results, as shown in Table 2 and Fig. 1, Support the direct association between cognitive social capital and cyber resilience ($\beta = 0.115$, $p = 0.017$). Still, the relationship between structural social capital ($\beta = -0.031$, $p = 0.568$), relational social capital ($\beta = 0.055$, $p = 0.339$) and cyber resilience was not supported. Based on these findings, H1c is accepted, while H1a and H1b are rejected. Furthermore, the results demonstrate that all three dimensions of social capital are significantly and positively related to SME AI readiness. Structural social capital ($\beta = 0.149$, $p = 0.001$), relational social capital ($\beta = 0.311$, $p < 0.001$) and cognitive social capital ($\beta = 0.083$, $p = 0.049$) are significantly associated with SME AI readiness. This finding supports H2a, H2b and H2c. Also, the results for hypothesis 3 (H3) show that cyber resilience is positively and significantly associated with SME AI readiness ($\beta = 0.131$, $p < 0.001$). H5 explored the link between AI readiness and value construction among SMEs. The results (See Table 1) show that SMEs that are AI ready are better positioned for value construction ($\beta = 0.181$, $p < 0.001$). This provides support for H5 (Table 5).
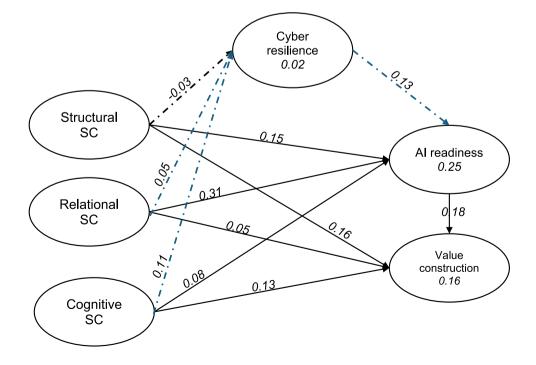
Table 4 Fit Indices

Fit indices	Recommended threshold	Fit model
CMIN/DF	< 3.0	.016
CFI	>.90	.998
GFI	>.80	1.00
RMSEA	<.08	.000
RMR	<.08	.001
AGFI	>.80	1.00
NFI	>.90	.999

Fig. 1 Path Analysis

Table 5 Test of hypotheses

Variables			β	S.E	C.R	P	Remark
Structural capital	→	Cyber resilience	-.031	.055	-.571	.568	*NS*
Relational capital	→	Cyber resilience	.055	.095	.955	.339	*NS*
Cognitive capital	→	Cyber resilience	.115	.067	2.391	.017	*Supported*
Cyber resilience	→	AI Readiness	.131	.040	3.622	***	*Supported*
Relational capital	→	AI Readiness	.311	.093	6.222	***	*Supported*
Structural capital	→	AI Readiness	.149	.053	3.187	.001	*Supported*
Cognitive capital	→	AI Readiness	.083	.066	1.970	.049	*Supported*
AI Readiness	→	Value construction	.181	.051	4.195	***	*Supported*
Relational capital	→	Value construction	.049	.118	.899	.369	*NS*
Structural capital	→	Value construction	.163	.066	3.266	.001	*Supported*
Cognitive capital	→	Value construction	.127	.081	2.848	.004	*Supported*

Figure 1 presents the path analysis showing the relationship between social capital, cyber resilience, SME AI readiness and value construction.

The findings indicate that structural and relational capital do not significantly influence cyber resilience. While this result diverges from expectations based in traditional SCT theory's argument that stronger network ties and social ties are often assumed to enhance information flow and collective resilience (Ahn & Kim, 2017; Ali-Hassan, 2009; Claridge, 2018), the results presented here suggests that cybersecurity preparedness is not only a function of strong network ties. Rather, the results show that it depends on firms cognitive capacity to internalise and apply cybersecurity practices. This divergence is particularly relevant in resource-constrained environments where SMEs usually lack in-house cybersecurity expertise but rather rely on external interventions instead of peer-driven resilience building mechanisms.

4.3.1 Mediation Analysis

A mediation analysis was performed to assess the mediating role of cyber resilience in the relationship between social capital and SME AI readiness. The analysis used 2000 bootstrapping samples with a bias corrected 95% confidence interval. To conduct the mediation analysis, the three dimensions of social capital were combined and transformed into a single construct of social capital. The method of transformation is consistent with previous

literature (Ul zia et al., 2023). The results (See Table 2) revealed a significant indirect effect of social capital on SME AI readiness (β = 0.130, t = 6.842, p < 0.05). The total effect of social capital on SME AI resilience was significant (β = 0.364, t = 7.745, p < 0.001), with the inclusion of the mediator, the effect of social capital on SME Ai readiness was still significant (β = 0.351, t = 7.630, p < 0.001). These results demonstrate that cyber resilience partially mediates the relationship between social capital and SME AI readiness. Hence, H4 is supported (Table 6).

However, to examine each social capital dimension separately, further mediation analysis was conducted using the PROCESS macro using 5000 bootstrap samples (Hayes, 2022) to examine whether cyber resilience mediates the relationship between dimensions of social capital and AI readiness. The results for Cognitive social capital CC) revealed a statistically significant relationship with AI readiness b = 0.500, SE = 0.061, t(587) = 8,209, p < 0.001, 95% CI [0.381, 0.620]. The path between CC and CR, CR and AI Readiness and between CC and AI readiness were all statistically significant. The results show that the indirect effect of cognitive social capital on AI readiness through cyber resilience was statistically significant (b = 0.018, BootSE = 0.012, 95% Bootstrapped CI [0.003 0.073]. The analysis revealed that cyber resilience partially mediates the relationship between cognitive social capital and AI readiness. The model explained 12.2% of the variance in AI Readiness (See Table 7).

For structural social capital (SC), the total effect of SC on AI readiness was statistically significant (b = 0.441, SE

Table 6 Mediation Analysis

Total effect SC → AI readiness			Direct effect SC → AI readiness			Indirect effect Social capital → Cyber resilience → AI Readiness					Percentile bootstrap 95% confidence interval	
β	t	*p*	β	t	*p*		β	S.E	t	*p*	Lower	Upper
.364	7.745	.000	.351	7.630	.000	H4	.130	.019	6.842	.028	.001	.038

S.E. Standard Error, *SC* Social capital

Table 7 Mediation Analysis with PROCESS macro

Social Capital Dimension	Path	Effect (b)	SE	t-value	p-value	95% CI	Significance
Structural	X → M	0.052	0.042	1.231	0.219	[− 0.031, 0.135]	*Not significant*
	M → Y	0.177	0.042	4.233	< 0.001	[0.095, 0.258]	*Significant*
	Total Effect (X → Y)	0.441	0.043	10.181	< 0.001	[0.356, 0.526]	*Significant*
	Direct Effect (X → Y)	0.432	0.043	10.098	< 0.001	[0.348, 0.516]	*Significant*
	Indirect Effect (X → M → Y)	0.009	0.009	—	—	[− 0.008, 0.030]	*Not significant*
Relational	X → M	0.158	0.069	2.298	0.022	[0.023, 0.293]	*Significant*
	M → Y	0.151	0.040	3.735	< 0.001	[0.072, 0.230]	*Significant*
	Total Effect (X → Y)	0.855	0.068	12.584	< 0.001	[0.721, 0.988]	*Significant*
	Direct Effect (X → Y)	0.831	0.067	12.312	< 0.001	[0.698, 0.964]	*Significant*
	Indirect Effect (X → M → Y)	0.024	0.018	—	—	[− 0.002, 0.070]	*Not significant*
Cognitive	X → M	0.184	0.057	3.195	0.001	[0.071, 0.297]	*Significant*
	M → Y	0.154	0.043	3.552	< 0.001	[0.069, 0.239]	*Significant*
	Total Effect (X → Y)	0.500	0.061	8.209	< 0.001	[0.381, 0.620]	*Significant*
	Direct Effect (X → Y)	0.472	0.061	7.754	< 0.001	[0.353, 0.592]	*Significant*
	Indirect Effect (X → M → Y)	0.028	0.018	—	—	[0.003, 0.073]	*Significant*

= 0.043, t(587) = 10,181, p < 0.001, 95% CI [0.356, 0.526], suggesting that structural social capital explains a significant proportion of the variance in AI readiness (R2 = 0.150). Similarly, when controlling for CR, the direct effect of SC on AI Readiness remained significant (b = 0.432, SE = 0.043, t(586) = 10,098, p < 0.001, 95% CI [0.348, 0.516]. However, the indirect effect of SC on AI Readiness through CR was not statistically significant (b = 0.009, BootSE = 0.009, 95% Bootstrapped CI [− 0.008 0.030]. The confidence interval includes zero which indicates that there is no significant mediation effect of CR in the link between SC and AI Readiness. The mediation results for relational social capital (RC) was also examined using PROCESS macro. The total effect for RC on AI readiness (b = 0.855, SE = 0.068, t(587) = 12,584, p < 0.001, 95% CI [0.721, 0.988], was statistically significant, same as the relationship between RC and CR (b = 0.158, SE = 0.069, t(587) = 2,298, p < 0.022, 95% CI [0.23, 0.293]. The direct effect of RC on AI readiness while controlling for CR was also statistically significant (b = 0.831, SE = 0.067, t(586) = 12,312, p < 0.001, 95% CI [0.698, 0.964]. However, the indirect effect of RC on AI Readiness through CR was not statistically significant (b = 0.024, BootSE = 0.018, 95% Bootstrapped CI [0.002, 0.070]. These results suggest that while SC, RC and CR independently predicts AI readiness, CR does not mediate the relationship. The mediation analysis for the mediating role of CR in the relationship between the three dimensions of SC and value construction reveals that, while the SC predicts value construction directly, CR does not mediate the relationship between all the dimensions and VC. This suggests that the SC capabilities are crucial for identifying and taking advantage of business opportunities however, CR may play a different role in the relationship.

5 Discussion

This study draws from SCT to examine the role of social capital and how it shapes SMEs' AI readiness and their capacity to exploit opportunities in resource-constrained environments. Building upon the foundational work of Tsai and Ghoshal (1998), this study examines the role of social capital within SMEs, particularly focusing on its relational and cognitive dimensions and their impact on AI readiness and value construction. Tsai and Ghoshal (1998) underscored how intrafirm networks facilitate exchange and combination of resources, thereby fostering innovation and value construction. This findings in this study extend this perspective to the realm of AI adoption in SMEs, demonstrating that robust social capital not only enhances internal knowledge sharing but also equips firms to effectively navigate the complexities of digital transformation. A replication study by Lester (2013) further illustrates the significance of social capital in firm value construction. The findings of this study corroborates the findings of Lester (2013) that the positive relationship between social capital and resource exchange, whilst emphasising that social interaction and trust are critical in facilitating innovation and value construction. The findings in this study extends these findings to the context of SMEs to demonstrate how internal and external networks characterised by trust and shared understanding can effectively shape how they adopt and manage AI technologies, in

ways that can lead to value construction. The findings make three important contributions.

First, the significant relationship between cognitive social capital and cyber resilience underscores the essential role that shared goals, values, and communication play in strengthening SMEs' ability to withstand and recover from cyber threats. This finding is consistent with previous studies, such as Tsai and Ghosahl (1998), who argued that cognitive social capital fosters collective action and coordination. In the cybersecurity context, shared trust and understanding among SME employees can create an environment that possesses the capacity to detect threats early through a coordinated response. Johnson et al. (2013) assert that common mental models and situational assessment indicators are essential for cyber defence. These cognitive attributes are associated with the efficacy of team communication and adaptability in cyber defence operations. Nonetheless, social support behaviours often diminish under high-stress circumstances, highlighting the necessity for intentional modifications to sustain team resilience (Johnson et al., 2013).

The lack of significance between structural social capital and relational capital with cyber resilience indicates that access to trust-based relationships and networks alone is insufficient to enhance resilience in resource-constrained environments. While previous studies (e.g. Ul zia et al., 2023) found that network ties can foster resilience and innovation, the findings in this study suggest that SMEs may not have the technical proficiency or the formalised processes required to convert resources from their networks into tangible cybersecurity outcomes. Although Narooz and Child (2017) have noted that the lack of institutional support in developing countries often poses a limitation to SMEs'ability to leverage external resources effectively, Torkkeli et al. (2019) however, argues that SMEs in developing countries often rely on networking to navigate institutional deficiencies.

Secondly, the findings show that all three dimensions of social capital (structural, relational and cognitive) were significantly associated with SME AI readiness. This aligns with the arguments of social capital, which state that social networks provide access to essential resources, including collaborative opportunities, technical expertise, and information. Specifically, the strong positive relationship between relational capital and AI readiness suggests that mutual obligations and trust are critical ingredients that enable SMEs to adopt AI technologies. This aligns with Claridge's (2018) finding that relational social capital can enhance the free flow of information, which is essential for innovation and technology adoption. Moreover, the significant relationship between structural social capital and AI readiness suggests that having a close-knit network configuration can provide resources for SMEs willing to integrate AI into their operations. Agostini and Filippini

(2019) and Pérez-Luño et al. (2011) argue that inter-organisational networks facilitate access to technical knowledge, which is essential for digital transformation. The positive effects of cognitive social capital with AI readiness also illustrate how shared goals and vision can strategically influence SMEs willing to adopt and implement AI solutions. Wasko and Faraj (2005) established that having a shared understanding within organisations can foster an environment conducive to adopting complex technologies. These findings align with Ul Zia et al. (2023), which found that the three components of social capital—structural, relational, and cognitive are associated with Industry 4.0 readiness. While Cooke and Clifton, (2004) investigated the regional disparities of social capital across SMEs, indicating that high-performance regions generally have businesses that effectively utilise social capital, this finding suggests that social capital also strongly influences AI readiness in resource-constrained environments.

Thirdly, the findings that cyber resilience is significantly associated with AI readiness in SMEs add to the growing body of literature on the intersection between digital transformation and cybersecurity. This is particularly relevant because AI systems, although offering significant benefits, are vulnerable to cyber risks, and firms that have low resilience may experience security breaches. Chatterjee (2021) illustrates the need to integrate cybersecurity strategies with AI adoption, and this is supported by our findings, which demonstrate that cyber resilience plays an essential role in enabling SMEs'readiness to adopt AI solutions. Cavelty et al. (2023) justify the need to consider the role of social capital in enhancing cyber resilience because it is a sociotechnical issue that involves integrating social considerations with technological solutions.

This is because more than focusing on technical aspects is needed to disregard the diverse societal values and the different ways firms experience and deal with cyber threats (Cavelty et al., 2023). De Arroyabe et al. (2023) confirm this by suggesting that firms investing in cybersecurity are better positioned to exploit and deploy digital technologies in a way that enhances their full potential. This aligns with the results of Sutrisno et al. (2022) that adaptability and innovation, frequently enabled by AI, are essential for the survival of SMEs during crises. Furthermore, the significant relationship between SME AI readiness and value construction in SMEs indicates that SMEs that are AI-ready are in a better position to explore new markets, create value and innovate. This aligns with Agostini and Filippini (2019)'s findings that AI adoption can empower firms to harness data-driven insights, develop innovative solutions and improve organisational efficiency. Particularly in resource-constrained environments, AI-ready SMEs possess a distinct advantage because they can deploy and use digital tools to overcome their limitations and compete in the market effectively.

The findings also showcase the differentiated mediating role of cyber resilience in the relationship between social capital and AI readiness. The findings demonstrate that while cyber resilience partially mediates the relationship between cognitive social capital and AI readiness, it did not mediate the relationship between structural social capital, relational social capital and AI readiness. The findings suggest that higher levels of shared norms, understanding and trust enhance an SME's ability to adopt AI both directly and indirectly by improving the resilience to cyber risks (Novandari et al., 2023; Rasaputhra et al., 2024). Thus, cognitive, social capital provides the foundation SMEs require for collective problem-solving and trust, which is likely to foster the adoption of cyber resilience strategies (Ortigueira-Sánchez et al., 2020; Sugandini et al., 2020).

These strategies can potentially prepare SMEs to adopt AI by mitigating potential technological vulnerabilities (Sugandini et al., 2020). The results also show that network ties and relational components such as trust and reciprocity directly influence AI readiness but are not mediated by cyber resilience. While these dimensions of social capital are fundamental for resource mobilisation and collaboration, they may not directly lead to the organisational practices required for cyber resilience (Ortigueira-Sánchez et al., 2020; Widyawati et al., 2023). This finding extends the SCT by highlighting the importance of intermediary capabilities in translating the potential of social capital, especially cognitive factors, into practical outcomes such as AI-ready firms. This is particularly true of resource-constrained environments where the formal resources are scarce. Thus, cyber resilience can enable firms to protect and apply the knowledge and resources acquired via their social networks (Polyviou et al., 2019).

This aligns with the findings of Cohen and Levinthal's (1990) absorptive capacity framework, which suggests that external knowledge must be absorbed and efficiently applied to produce meaningful outcomes. The partial mediation effect of cognitive social capital demonstrates that while, on the one hand, social capital can provide the necessary access to resources, building cyber resilience can help safeguard and protect these resources throughout the digital transformation process. This is consistent with the findings of Bernier and Meinzen-Dick (2014) and De Arroyabe et al. (2023) that cyber resilience can enhance an organisation's capacity to adapt and exploit digital technologies through adaptive, coping and transformative capacities, especially in resource-constrained environments with heightened risks.

5.1 Theoretical Implications

This study offers theoretical novelty and distinct advancements. The findings provide a novel integration of social capital theory and cyber resilience in AI readiness research. Previous studies have examined these concepts separately, but the findings in this study presents a comprehensive framework that links these perspectives within SMEs digital transformation efforts. The study also provides a refined understanding of the role of social capital in AI readiness. While previous studies identified the role of social capital and how it facilitates innovation, this study demonstrated how different dimensions play distinct roles. For instance, the paper shows that structural and relational capital drives AI readiness directly, while cognitive capital influences AI readiness indirectly through cyber resilienve. Unlike previous studies that focus on the benefits of AI adioption alone, this paper demonstrates how SMEs in resource-constrained environments must simultaneously innovate and defend their digital assets to sustain value.

This study makes several key contributions to the existing literature. First, it is the first to establish a direct link between social capital, cyber resilience, and value construction in SMEs. This advances social capital theory by illustrating how structural, relational, and cognitive social capital interacts with organisational capabilities, specifically cyber resilience, to influence AI readiness and value construction in SMEs operating in resource-constrained environments. While social capital theory traditionally highlights the role of networks in fostering collaboration, trust, and knowledge sharing (Nahapiet & Ghoshal, 1998), this study demonstrates how these mechanisms collectively enable SMEs to adopt advanced technologies like AI.

Second, this study extends the social capital theory to the domain of AI readiness by highlighting the critical role of cognitive social capital in fostering organisational resilience and adopting complex technologies in resource-constrained settings. Cognitive social capital focuses on shared values, communication, and collective vision and aligns organisational strategies with digital transformation efforts (De Carolis & Saparito, 2006). The findings reveal that SMEs with shared goals and a unified understanding are better positioned to adopt new technologies and safeguard against digital threats. This underscores the importance of social capital in overcoming resource limitations, an area previously underexplored in AI readiness and digital transformation literature (Sheng & Hartmann, 2019).

Third, the study provides empirical evidence for cyber resilience's mediating role, contributing to understanding how social capital influences firm outcomes in dynamic digital environments. By positioning cyber resilience as an intermediary capability, this research integrates organisational resilience into social capital theory, explaining how social networks translate into tangible outcomes like AI readiness. This extension of Cohen and Levinthal's (1990) absorptive capacity framework demonstrates that the impact of social capital on AI readiness depends on an SME's ability to protect digital assets and sustain digital initiatives.

Finally, this study offers context-specific insights into how social capital operates in resource-constrained environments where institutional support and resources are limited. While prior studies have focused on social capital within well-resourced organisations in developed economies (Maurer & Ebers, 2006; Maurer et al., 2011), this study shows that in resource-limited settings, social capital becomes a critical substitute for missing resources. It enables SMEs to extract value and knowledge from external networks, facilitating digital transformation. This contribution broadens the understanding of how social networks drive the digital evolution of SMEs, particularly in emerging economies.

5.2 Practical Contributions and Implications for SMEs and Policymakers

This study offers valuable practical insights into SMEs' digital transformation and AI readiness, particularly in resource-constrained environments. It highlights the crucial role of social capital in facilitating the adoption of digital technologies. While previous research has acknowledged the importance of social capital in driving innovation, this study empirically demonstrates its direct impact on AI readiness. This finding underscores the need for SMEs to invest in developing cognitive social capital by fostering shared values, goals, and effective communication within their networks. Building well-structured, trust-based networks alone is not enough; SMEs must cultivate the internal capacity to leverage these relationships, especially to address cybersecurity challenges fully.

Beyond its organisational implications, the study has significant economic and technological ramifications. Strengthening cyber resilience is not just a security measure but an economic imperative. SMEs that proactively build cyber resilience can better protect their digital assets, reduce financial losses associated with cyber threats, and improve business continuity. This enhanced resilience also increases investor and consumer confidence, making SMEs more attractive to potential partners and funding opportunities. Moreover, AI readiness can drive economic competitiveness by enabling SMEs to automate processes, improve efficiency, and expand into digital markets, ultimately contributing to regional and national economic growth.

From a technological perspective, the study underscores the critical need for SMEs to integrate scalable and cost-effective cybersecurity and AI solutions. Cyber resilience fosters a safer digital environment where SMEs can confidently adopt emerging AI-driven tools, such as predictive analytics, machine learning-based risk assessment, and automated decision-making systems. However, SMEs in resource-constrained settings often face barriers to accessing these technologies. To bridge this gap, industry stakeholders must promote affordable AI and cybersecurity solutions tailored to SMEs' needs. Collaborative initiatives between governments and the private sector can facilitate access to AI-powered cybersecurity systems, such as real-time threat detection, multi-factor authentication, and automated data protection measures.

The findings also carry significant implications for policymakers and SME support organisations. There is a clear need for targeted programs that help SMEs build and sustain social capital while enhancing their cybersecurity readiness. Such initiatives are particularly critical for SMEs operating in environments with limited resources. By understanding these dynamics, policymakers can create more effective strategies to support sustainable digital transformation.

To translate these insights into action, SMEs should actively engage in industry associations and collaborative platforms to access knowledge of shared cybersecurity and AI technologies. Policymakers can support this collaborative approach through networking events and industry partnerships. Regular cybersecurity training for employees is equally vital, ensuring staff can identify and mitigate threats like phishing and malware. Government agencies can play a role by offering subsidised or free cybersecurity workshops tailored to SMEs.

Moreover, SMEs need to implement comprehensive cyber resilience strategies, including conducting risk assessments, developing incident response plans, and establishing business continuity frameworks. Policymakers can encourage this by providing incentives, such as grants or tax relief, for adopting internationally recognised cybersecurity standards like ISO 27001. Embracing scalable cybersecurity tools, such as multi-factor authentication, firewalls, and AI-driven threat detection systems, further strengthens SMEs' security posture. Collaboration between governments and the private sector can make these tools more accessible through affordable cybersecurity and AI readiness toolkits. By integrating these strategies, SMEs can enhance their resilience, optimise their digital transformation efforts, and contribute to economic growth in the digital age.

6 Limitations and Future Research

While this study makes several contributions, some limitations must be highlighted. First, this study provides valuable insights into SMEs in resource-constrained environments, offering a nuanced understanding of how social capital, cyber resilience, and AI readiness interact in these contexts. While the findings are tailored to SMEs, future research can explore how these relationships manifest in different organisational settings, such as larger firms or businesses operating in resource-rich environments. Investigating variations in mechanisms and implementation strategies across different contexts could further enrich the broader applicability of

these findings. Secondly, the study combines three dimensions of social capital into a single variable for the mediation analysis. This may not reveal the nuances of how each of the three dimensions of social capital acts as a mediator. Future studies can explore these three dimensions and how they influence cyber resilience, AI readiness, and value construction capability in SMEs. Finally, although the study used a lagged cross-sectional lagged approach, longitudinal studies could provide deeper insights into the mechanisms and evolution of social capital and cyber resilience over time and their long-term impacts. Future studies can examine other mediating factors, such as absorptive capacity and organisational learning, in the link between social capital and AI readiness.

Data Availability The data supporting the findings of this study are available from the corresponding author upon reasonable request.

Declarations

Ethics Approval and Consent to Participate Ethical approval for this study was obtained from Benue State University before data collection began. The survey design incorporated informed consent from participants. Respondents were required to complete the consent section of the questionnaire before gaining access to the subsequent sections.

Consent for Publication All authors consent to this work being published in Information Systems Frontiers.

Competing interests There are no competing interests from any of the authors.

References

Abbasi, A., Wigand, R. T., & Hossain, L. (2014). Measuring social capital through network analysis and its influence on individual performance. *Library & Information Science Research, 36*(1), 66–73. https://doi.org/10.1016/j.lisr.2013.08.001

Abredu, P., Li, C., Essien, F. K., & Adegoke, I. A. A. (2023). Unleashing potential: Overcoming bottlenecks and catalyzing innovations in intellectual capital intellectualization of small and medium-sized enterprises in Jiangsu during the post-industrial era. *SAGE Open, 13*(4). https://doi.org/10.1177/21582440231202086

Abrokwah-Larbi, K., & Awuku-Larbi, Y. (2023). The impact of artificial intelligence in marketing on the performance of business organisations: Evidence from SMEs in an emerging economy. *Journal of Entrepreneurship in Emerging Economies.* https://doi.org/10.1108/jeee-07-2022-0207

Acquah, I. N., Kumi, C. A., Asamoah, D., Agyei-Owusu, B., Agbodza, M., & Agyabeng-Mensah, Y. (2023). Unearthing the relationship between supply chain social capital and firm performance: the role of supply chain responsiveness. *Benchmarking: An International Journal*, *31*(4), 1225–1248. https://doi.org/10.1108/bij-01-2022-0002

Aderibigbe, A. O., Ohenhen, P. E., Nwaobia, N. K., Gidiagba, J. O., & Ani, E. C. (2023). Artificial Intelligence in Developing Countries: Bridging the Gap Between Potential and Implementation. *Computer Science & IT Research Journal, 4*(3), 185–199. https://doi.org/10.51594/csitrj.v4i3.629

Agostini, L., & Filippini, R. (2019). Organisational and managerial challenges in the path toward Industry 4.0. *European Journal of Innovation Management, 22*(3), 406–421. https://doi.org/10.1108/EJIM-02-2018-0030

Ahmadi-Assalemi, G., Al-Khateeb, H., Epiphaniou, G., & Maple, C. (2020). Cyber resilience and incident response in smart cities: A systematic literature review. *Smart Cities, 3*(3), 894–927. https://doi.org/10.3390/smartcities3030046

Ahn, S.-Y., & Kim, S.-H. (2017). What makes firms innovative? The role of social capital in corporate innovation. *Sustainability, 9*(9), 1564. https://doi.org/10.3390/su9091564

Ali-Hassan, H. (2009). Social capital theory. In *Handbook of research on contemporary theoretical models in information systems* (pp. 420–433). IGI Global. https://doi.org/10.4018/978-1-60566-659-4.ch024

Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). Organisational cybersecurity systems and sustainable business performance of small and medium enterprises (SMEs) in Saudi Arabia: The mediating and moderating role of cyber-security resilience and organizational culture. *Sustainability, 16*(5), 1880. https://doi.org/10.3390/su16051880

Antwi, P., Tetteh Kamewor, F., Mohammed, J., Mohammed, J., & Teye, E. (2021). Effect of social capital on SMEs performance: Does innovation matter. *International Journal of Technology and Management Research*, *6*(2), 21–37. https://doi.org/10.47127/ijtmr.v6i2.124

Baabdullah, A. M., Alalwan, A. A., Slade, E. L., Raman, R., & Khatatneh, K. F. (2021). SMEs and artificial intelligence (AI): Antecedents and consequences of AI-based B2B practices. *Industrial Marketing Management, 98*, 255–270. https://doi.org/10.1016/j.indmarman.2021.09.003

Badghish, S., & Soomro, Y. A. (2024). Artificial intelligence adoption by SMEs to achieve sustainable business performance: Application of technology–organization–environment framework. *Sustainability, 16*(5), 1864. https://doi.org/10.3390/su16051864

Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational cyber resilience: Management perspectives. *Journal of Information Systems*, 27. https://doi.org/10.3127/ajis.v27i0.4183

Balijepally, V., Mahapatra, R., & Nerur, S. (2004). Social capital: A theoretical lens for IS research. *AMCIS 2004 Proceedings* (Vol. 187, pp. 1585–1592). http://aisel.aisnet.org/amcis2004/187

Baycan, T., & Öner, Ö. (2023). The dark side of social capital: A contextual perspective. *The Annals of Regional Science, 70*(3), 779–798. https://doi.org/10.1007/s00168-022-01112-2

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

Bernier, Q., & Meinzen-Dick, R. (2014). *Resilience and social capital* (Vol. 4). Intl Food Policy Res Inst. https://core.ac.uk/download/pdf/24066438.pdf

Birthriya, S. K., Ahlawat, P., & Jain, A. K. (2024). A comprehensive survey of social engineering attacks: taxonomy of attacks, prevention, and mitigation strategies. *Journal of Applied Security Research*, 1–49. https://doi.org/10.1080/19361610.2024.2372986

Boateng, H., Visnupriyan, R., Ofori, K. S., & Hinson, R. E. (2020). Examining the link between social capital, knowledge quality, SMEs innovativeness and performance. *Business Information Review, 37*(4), 167–175. https://doi.org/10.1177/0266382120970157

Borah, S., Kama, C., Rakshit, S., spsampsps Vajjhala, N. R. (2022). Applications of artificial intelligence in small-and medium-sized enterprises (SMEs). In *Cognitive Informatics and Soft Computing: Proceeding of CISC 2021* (pp. 717–726). Springer Nature Singapore. https://doi.org/10.1007/978-981-16-8763-1_59

Bourdieu, P. (2018). The Forms of Capital. In *The sociology of economic life*. Routledge. https://doi.org/10.4324/9780429494338-6

Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review, 5*(4), 28. https://doi.org/10.22215/timreview/888

Carias, 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

Carias, J. F., Arrizabalaga, S., Labaka, L., & Hernantes, J. (2021). Cyber resilience self-assessment tool (CR-SAT) for SMEs. *IEEE Access, 9*, 80741–80762. https://doi.org/10.1109/access.2021.3085530

Cavelty, M., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: Adding social considerations to technological fixes. *Journal of Risk Research, 26*, 801–814. https://doi.org/10.1080/13669877.2023.2208146

Chao, Y., & Kim, D. (2023). The influence of corporate social capital on innovation performance: A case study of Chinese technological small and medium-sized enterprises. *Asia-Pacific Journal of Convergent Research Interchange, 9*(3), 95–104. https://doi.org/10.47116/apjcri.2023.03.09

Chatterjee, D. (2021). Cybersecurity readiness: A holistic and high-performance approach. SAGE Publications, Inc. https://doi.org/10.4135/9781071837313

Chumnangoon, P., Chiralaksanakul, A., & Chintakananda, A. (2021). How closeness matters: The role of geographical proximity in social capital development and knowledge sharing in SMEs. *Competitiveness Review: An International Business Journal, 33*(2), 280–301. https://doi.org/10.1108/cr-03-2021-0038

Claridge, T. (2018). Dimensions of Social Capital-structural, cognitive, and relational. *Social Capital Research, 1*, 1–4. https://www.socialcapitalresearch.com/wp-content/uploads/2018/01/Dimensions-of-Social-Capital.pdf

Cohen, W. M., & Levinthal, D. A. (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly, 35*(1), 128–152. https://psycnet.apa.org/doi/10.2307/2393553

Cooke, P., & Clifton, N. (2004). Spatial variation in social capital among UK small and medium sized enterprises. *Entrepreneurship and Regional Economic Development: A Spatial Perspective. Edward Elgar, Cheltenham*, 107–137. https://doi.org/10.4337/9781781959602.00012

Cots, E. G. (2011). Stakeholder social capital: A new approach to stakeholder theory. *Business Ethics: A European Review, 20*(4), 328–341. https://doi.org/10.1111/j.1467-8608.2011.01635.x

Darmi, T., Nuryakin, N., & Mujtahid, I. M. (2022). Social capital analysis in Small and Micro Enterprises (SMEs) management during the Covid-19 pandemic. *JKAP, 26*(1), 47. https://doi.org/10.22146/jkap.67459

De Carolis, D. M., & Saparito, P. (2006). Social capital, cognition, and entrepreneurial opportunities: A theoretical framework. *Entrepreneurship Theory and Practice, 30*(1), 41–56. https://doi.org/10.1111/j.1540-6520.2006.00109.x

De Arroyabe, I. F., Arranz, C. F., Arroyabe, M. F., & de Arroyabe, J. C. F. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Computers & Security, 124*, 102954. https://doi.org/10.1016/j.cose.2022.102954

de Medeiros, M. M., & Maçada, A. C. G. (2021). Competitive advantage of data-driven analytical capabilities: The role of big data visualisation and of organisational agility. *Management Decision, 60*(4), 953–975. https://doi.org/10.1108/md-12-2020-1681

Ebuka, A. A., Emmanuel, D., & Idigo, P. (2023). Artificial intelligence as a catalyst for the sustainability of Small and Medium Scale Businesses (SMEs) in Nigeria. *Annals of Management and Organization Research, 5*(1), 1–11. https://doi.org/10.35912/amor.v5i1.1719

Eller, R., Alford, P., Kallmünzer, A., & Peters, M. (2020). Antecedents, consequences, and challenges of small and medium-sized enterprise digitalization. *Journal of Business Research, 112*, 119–127. https://doi.org/10.1016/j.jbusres.2020.03.004

Fanggidae, H. C., Sutrisno, S., Fanggidae, F. O., & Permana, R. M. (2023). Effects of social capital, financial access, innovation, socioeconomic status and market competition on the growth of small and medium enterprises in West Java province. *The ES Accounting and Finance, 1*(02), 104–112. https://doi.org/10.58812/esaf.v1i02.69

Fernandez de Arroyabe, J., Arroyabe, M. F., Fernandez, I., & Arranz, C. F. (2023). Cybersecurity resilience in SMEs. A machine learning approach. *Journal of Computer Information Systems*, 1–17. https://doi.org/10.1080/08874417.2023.2248925

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.2307/3151312

Gautam, D. K., & Gautam, P. K. (2023). Stress and resilience to migrant entrepreneur-managers of small and medium enterprises during COVID-19 pandemic. *Benchmarking: An International Journal, 31*(6), 2129–2150. https://doi.org/10.1108/bij-06-2022-0400

Giguashvili, G. (2024). Opportunities of Using Artificial Intelligence in Small and Medium-Sized Businesses. *Grail of Science, 40*, 63–69. https://doi.org/10.36074/grail-of-science.07.06.2024.006

Gupta, A., & Singh, S. (2023). We're all in this together: Addressing post-pandemic challenges of Indian rural society. *International Journal of Sociology and Social Policy, 44*(1/2), 155–170. https://doi.org/10.1108/ijssp-08-2023-0185

Halim, H. A., Ahmad, N. H., Taghizadeh, S. K., Ramayah, T., & Mohamad, M. N. (2015). promoting innovative performance

through social embeddedness: An analysis on innovative human capital among SMEs. *International Journal of Innovation, Management and Technology, 6*(2), 81–87. https://doi.org/10.7763/ijimt.2015.v6.579

Hayes, A. F. (2022). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. Guilford Publications.

Hibban, M., & Abhishek, D. (2024). Innovation management among the Indian small and medium-sized enterprises focusing on artificial intelligence: Opportunities and the way forward. *Indian Journal of Commerce & Management Studies*, *XV*(2), 10–17. https://doi.org/10.18843/ijcms/v15i2/02

Hsu, B. X., & Chen, Y. M. (2019). Industrial policy, social capital, human capital, and firm-level competitive advantage. *International Entrepreneurship and Management Journal, 15*, 883–903. https://doi.org/10.1007/s11365-019-00584-7

Iftikhar, N., & Nordbjerg, F. E. (2021, October). Adopting artificial intelligence in Danish SMEs: Barriers to become a data driven company, its solutions and benefits. In *IN4PL* (pp. 131–136). https://doi.org/10.5220/0010691800003062

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94–100. https://doi.org/10.1145/1290958.1290968

Jöhnk, J., Weißert, M., & Wyrtki, K. (2020). Ready or not, AI comes—An interview study of organizational AI readiness factors. *Business & Information Systems Engineering, 63*(1), 5–20. https://doi.org/10.1007/s12599-020-00676-7

Johnson, N., Elliott, D., & Drake, P. (2013). Exploring the role of social capital in facilitating supply chain resilience. *Supply Chain Management, 18*, 324–336. https://doi.org/10.1108/SCM-06-2012-0203

Kalra, A., Agnihotri, R., & Briggs, E. (2020). The role of frontline employees' competitive intelligence and intraorganizational social capital in driving customer outcomes. *Journal of Service Research, 24*(2), 269–283. https://doi.org/10.1177/1094670520958070

Kanazawa, S., & Savage, J. (2009). Why nobody seems to know what exactly social capital is. *Journal of Social, Evolutionary, and Cultural Psychology, 3*(2), 118–132. https://doi.org/10.1037/h0099326

Kanini, K. S., & Muathe, S. M. A. (2019). Nexus between social capital and firm performance: A critical literature review and research agenda. *International Journal of Business and Management, 14*(8), 70. https://doi.org/10.5539/ijbm.v14n8p70

Kant, D., & Johannsen, A. (2022). Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs). *Electronic Imaging, 34*(3), 387–388. https://doi.org/10.2352/ei.2022.34.3.mobmu-387

Kareem, H. M., Alsheikh, A. H., Alsheikh, W. H., Dauwed, M., & Meri, A. (2024). The mediating role of accounting information systems in small and medium enterprise strategies and organisational performance in Iraq. *Humanities and Social Sciences Communications*, *11*(1). https://doi.org/10.1057/s41599-024-03273-1

Karuppiah, K., Sankaranarayanan, B., D'Adamo, I., & Ali, S. M. (2023). Evaluation of key factors for industry 4.0 technologies adoption in small and medium enterprises (SMEs): An emerging economy context. *Journal of Asia Business Studies, 17*(2), 347–370. https://doi.org/10.1108/JABS-05-2021-0202

Khoury, G., El-Far, M. T., Khoury, E. N., & Tovstiga, G. (2020). Internationalisation of developing economy small and medium-sized enterprises: Social capital and learning in Palestinian pharmaceutical firms. *Journal of Small Business and Enterprise Development, 28*(2), 298–316. https://doi.org/10.1108/jsbed-06-2020-0230

Khurana, I., Dutta, D. K., & Ghura, A. S. (2022). SMEs and digital transformation during a crisis: The emergence of resilience as a second-order dynamic capability in an entrepreneurial ecosystem. *Journal of Business Research, 150*, 623–641. https://doi.org/10.1016/j.jbusres.2022.06.048

Kim, N., & Shim, C. (2018). Social capital, knowledge sharing and innovation of small- and medium-sized enterprises in a tourism cluster. *International Journal of Contemporary Hospitality Management, 30*(6), 2417–2437. https://doi.org/10.1108/ijchm-07-2016-0392

Kontinen, T., & Ojala, A. (2012). Social capital in the international operations of family SMEs. *Journal of Small Business and Enterprise Development, 19*(1), 39–55. https://doi.org/10.1108/14626001211196398

Kuckertz, A., Kollmann, T., Krell, P., & Stöckmann, C. (2017). Understanding, differentiating, and measuring opportunity recognition and opportunity exploitation. *International Journal of Entrepreneurial Behaviour & Research, 23*(1), 78–97. https://doi.org/10.1108/IJEBR-12-2015-0290

Lakse, M. C., & Menike, S. (2020). Effect of social capital on firm performance: An empirical study of small enterprises in Sri Lanka. *Journal of Social Science Research, 16*, 108–125. https://doi.org/10.24297/jssr.v16i.8904

Lawa, K. O., & E-Vahdati, S. (2022). The role of entrepreneurial orientation and social capital toward technology innovation among SMEs in Kurdistan. *Global Business Management Review (GBMR)*, *14*(2), 37–55. https://doi.org/10.32890/gbmr2022.14.2.3

Lee, S., Park, J.-G., & Lee, J. (2015). Explaining knowledge sharing with social capital theory in information systems development projects. *Industrial Management & Data Systems, 115*(5), 883–900. https://doi.org/10.1108/imds-01-2015-0017

Lee, R., Tuselmann, H., Jayawarna, D., & Rouse, J. (2019). Effects of structural, relational and cognitive social capital on resource acquisition: A study of entrepreneurs residing in multiply deprived areas. *Entrepreneurship & Regional Development, 31*(5–6), 534–554. https://doi.org/10.1080/08985626.2018.1545873

Lee, G., Kim, S., Lee, I., Brown, S., & Carbajal, Y. A. (2025). Adapting cybersecurity maturity models for resource-constrained settings: A case study of Peru. *The Electronic Journal of Information Systems in Developing Countries, 91*(1), e12350. https://doi.org/10.1002/isd2.12350

Lepak, D. P., Smith, K. G., & Taylor, M. S. (2007). Value creation and value capture: A multi-level perspective. *Academy of Management Review, 32*(1), 180–194.

Lester, M. (2013). Social capital and value creation: A replication of 'The Role of Intrafirm Networks' by Wenpin Tsai and Sumantra Ghoshal. *American Journal of Business and Management, 2*(2), 106–113. https://doi.org/10.11634/216796061706277

Lin, C. P., & Huang, T. Y. (2023). Assessing social capital and knowledge sharing in the high-tech industry: A moderating role of hypercompetition. *Management Decision, 61*(1), 120–143. https://doi.org/10.1108/MD-08-2021-1065

Lin, N. (2017). Building a network theory of social capital. *Social capital*, pp. 3–28. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315129457-1/building-network-theory-social-capital-nanlin

Lineberry, S. (2007). The human element: The weakest link in information security. *Journal of Accountancy, 204*(5), 44.

Ma, H., Zhang, Y. C., Butler, A., Guo, P., & Bozward, D. (2021). Entrepreneurial performance of new-generation rural migrant entrepreneurs in China. *International Journal of Entrepreneurial Behaviour & Research, 28*(2), 412–440. https://doi.org/10.1108/ijebr-07-2020-0456

Marampa, A. M., Garnasih, R. L., & Pariyanti, E. (2023). How to unleash innovative work behaviour of SMEs workers through clan culture? "Testing the mediating role of knowledge sharing." *Industrial and Commercial Training, 56*(1), 1–23. https://doi.org/10.1108/ict-03-2023-0016

Mariyana, A. L. D., Annaufal, A. I., & Roostika, R. (2024). The Impact of artificial intelligence on small and medium enterprises in Yogyakarta. In *Digital technology and changing roles in managerial and financial accounting: Theoretical knowledge and practical application* (pp. 347–354). Emerald Publishing Limited. https://doi.org/10.1108/S1479-351220240000036031

Martín-Rojas, R., Garrido-Moreno, A., & García-Morales, V. J. (2023). Social media use, corporate entrepreneurship and organisational resilience: A recipe for SMEs success in a post-Covid scenario. *Technological Forecasting and Social Change, 190*, 122421. https://doi.org/10.1016/j.techfore.2023.122421

Maurer, I., & Ebers, M. (2006). Dynamics of social capital and their performance implications: Lessons from biotechnology start-ups. *Administrative Science Quarterly, 51*(2), 262–292. https://doi.org/10.2189/asqu.51.2.262

Maurer, I., Bartsch, V., & Ebers, M. (2011). The value of intra-organizational social capital: How it fosters knowledge transfer, innovation performance, and growth. *Organisation Studies, 32*(2), 157–185. https://doi.org/10.1177/0170840610394301

Melo, I., Junior, P., Queiroz, G., Yushimito, W., & Pereira, J. (2023). Do we consider sustainability when we measure Small and Medium Enterprises' (SMEs') performance passing through digital transformation? *Sustainability.* https://doi.org/10.3390/su15064917

Mitsa, V., & Lyakh, I. (2023). Application of digital entrepreneurship platforms in small and medium-sized businesses. *Actual Problems of Economics.* https://doi.org/10.32752/1993-6788-2022-1-262-6-11.

Mudalige, D. M. (2022). The role of dynamic capabilities, digital capabilities and social capital on resilience and recovery of SMEs during Covid-19 in Sri Lanka. *Wayamba Journal of Management, 13*(2), 197. https://doi.org/10.4038/wjm.v13i2.7573

Muniady, R. A., Mamun, A. Al, Mohamad, Mohd. R., Permarupan, P. Y., & Zainol, N. R. B. (2015). The effect of cognitive and relational social capital on structural social capital and micro-enterprise performance. *Sage Open*, *5*(4). https://doi.org/10.1177/2158244015611187

Munusamy, T., & Khodadi, T. (2023). building cyber resilience: Key factors for enhancing organizational cyber security. *Journal of Informatics and Web Engineering, 2*(2), 59–71. https://doi.org/10.33093/jiwe.2023.2.2.5

Nahapiet, J., & Ghoshal, S. (1998). Social capital, intellectual capital, and the organisational advantage. *Academy of Management Review, 23*(2), 242–266. https://doi.org/10.2307/259373

Narooz, R., & Child, J. (2017). Networking responses to different levels of institutional void: A comparison of internationalising SMEs in Egypt and the UK. *International Business Review, 26*, 683–696. https://doi.org/10.1016/J.IBUSREV.2016.12.008

Ngoc, T. M., & Vy, H. D. B. (2022). Social capital and SMEs resilience in the context of Covid-19. *Journal Of Science - Economics and Business Administration*, *13*(1). https://doi.org/10.46223/hcmcoujs.econ.en.13.1.2324.2023

Novandari, W., Gunawan, D. S., Bawono, I. R., Naufalin, R., Maryani, S., Jajang, J., & Sulasih, S. (2023). Social media adoption and SMEs business performance: Examining entrepreneurship orientation and government support policies in Central Java. *The Winners, 24*(1), 57–67. https://doi.org/10.21512/tw.v24i1.9262

Octasylva, A. R. P., Yuliati, L. N., Hartoyo, H., & Soehadi, A. W. (2023). Entrepreneur orientation and social capital as a key to developing dynamic capability: A conceptual framework. *Indonesian Journal of Business and Entrepreneurship.* https://doi.org/10.17358/ijbe.9.2.186

Oldemeyer, L., Jede, A., & Teuteberg, F. (2024). Investigation of artificial intelligence in SMEs: A systematic review of the state of the art and the main implementation challenges. *Management Review Quarterly.* https://doi.org/10.1007/s11301-024-00405-4

Orekhova, S., & Zarutskaya, V. (2022). Assessment of social capital in the work with suppliers: A case of a tourist organization. In *Advances in social science, education and humanities research.* Atlantis Press. https://doi.org/10.2991/assehr.k.220106.022

Ortigueira-Sánchez, L. C., Stein, W. C., Risco-Martínez, S. L., & Ricalde, M. F. (2020). The impact of absorptive capacity on innovation in Peru. *Journal of Technology Management & Innovation, 15*(4), 19–29. https://doi.org/10.4067/s0718-27242020000400019

Oussi, R., & Chtourou, W. (2020). Social capital dimensions and employee creativity: Does cognitive style matter? *Competitiveness Review: An International Business Journal, 30*(1), 4–21. https://doi.org/10.1108/cr-11-2019-0124

Ozanne, L. K., Chowdhury, M., Prayag, G., & Mollenkopf, D. A. (2022). SMEs navigating COVID-19: The influence of social capital and dynamic capabilities on organisational resilience. *Industrial Marketing Management, 104*, 116–135. https://doi.org/10.1016/j.indmarman.2022.04.009

Paul, S., Daga, V., Gupta, T., & S, A. (2023). A study on the impact of artificial intelligence in small and medium enterprises. *International Journal for Multidisciplinary Research.* https://doi.org/10.36948/ijfmr.2023.v05i06.11145

Pérez-Luño, A., Medina, C. C., Lavado, A. C., & Rodríguez, G. C. (2011). How social capital and knowledge affect innovation. *Journal of Business Research, 64*(12), 1369–1376. https://doi.org/10.1016/j.jbusres.2011.01.014

Philbin, S., Viswanathan, R., & Telukdarie, A. (2022). Understanding how digital transformation can enable SMEs to achieve sustainable development: A systematic literature review. *Small Business International Review.* https://doi.org/10.26784/sbir.v6i1.473

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioural research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Polyviou, M., Croxton, K., & Knemeyer, A. (2019). Resilience of medium-sized firms to supply chain disruptions: The role of internal social capital. *International Journal of Operations & Production Management.* https://doi.org/10.1108/IJOPM-09-2017-0530

Prabandari, S. P., & Yulianti, I. (2023). Does social capital affect SME's performance? *International Journal of Social Service and Research, 3*(11), 2783–2793. https://doi.org/10.46799/ijssr.v3i11.579

Prieto-Pastor, I., Martín-Pérez, V., & Martín-Cruz, N. (2018). Social capital, knowledge integration and learning in project-based organizations: A CEO-based study. *Journal of Knowledge Management, 22*(8), 1803–1825. https://doi.org/10.1108/jkm-05-2017-0210

Punt, E., Monstadt, J., Frank, S., & Witte, P. (2023). Navigating cyber resilience in seaports: Challenges of preparing for cyber-attacks at the Port of Rotterdam. *Digital Policy, Regulation and Governance, 25*(4), 420–438. https://doi.org/10.1108/dprg-12-2022-0150

Ramdani, B., Raja, S., & Kayumova, M. (2021). Digital innovation in SMEs: A systematic review, synthesis and research agenda. *Information Technology for Development, 28*, 56–80. https://doi.org/10.1080/02681102.2021.1893148

Rasaputhra, S., Peiris, V., Magallagoda, R., Panditasekara, C., Wisenthige, K., & Jayasuriya, N. (2024). Do technological,

environmental and entrepreneurial factors affect social commerce adoption? *Journal of Small Business and Enterprise Development, 31*(4), 764–785. https://doi.org/10.1108/jsbed-09-2023-0420

Rupeika-Apoga, R., & Petrovska, K. (2022). Barriers to sustainable digital transformation in micro-, small-, and medium-sized enterprises. *Sustainability*. https://doi.org/10.3390/su142013558

Ruseva, T. B., Farmer, J. R., & Chancellor, C. (2016). Networking for conservation: social capital and perceptions of organisational success among land trust boards. *Ecology and Society*, *21*(2). https://doi.org/10.5751/es-08618-210250

Saz-Gil, I., Bretos, I., & Díaz-Foncea, M. (2021). Cooperatives and social capital: A narrative literature review and directions for future research. *Sustainability, 13*(2), 534. https://doi.org/10.3390/su13020534

Schönberger, M. (2023). Artificial intelligence for small and medium-sized enterprises: Identifying key applications and challenges. *Journal of Business Management, 21*, 89–112. https://doi.org/10.32025/jbm23004

Seo, R. (2020). Entrepreneurial collaboration for R&D alliance performance: A role of social capital configuration. *International Journal of Entrepreneurial Behaviour & Research, 26*(6), 1357–1378. https://doi.org/10.1108/IJEBR-01-2020-0023

Shan, T., & Tian, X. (2022). The effects of social capital on entrepreneurial resilience of SME from China: A moderated mediation model of entrepreneurial passion and Confucian traditional golden-mean thinking. *Frontiers in Psychology, 13*, 961824. https://doi.org/10.3389/fpsyg.2022.961824

Sheng, M. L., & Hartmann, N. N. (2019). Impact of subsidiaries' cross-border knowledge tacitness shared and social capital on MNCs' explorative and exploitative innovation capability. *Journal of International Management, 25*(4), 100705. https://doi.org/10.1016/j.jik.2022.100187

Sombolayuk, W., & Yusuf, R. M. (2019). Innovation strategy for creating successful small and medium businesses. In *Proceedings of the 3rd International Conference on Accounting, Management and Economics 2018 (ICAME 2018)*. Atlantis Press. https://doi.org/10.2991/icame-18.2019.53

Soudi, M. S., & Bauters, M. (2024). AI guidelines and ethical readiness inside SMEs: A review and recommendations. *Digital Society, 3*(1), 3. https://doi.org/10.1007/s44206-024-00087-1

Størseth, F. (2017). Cyber-conformity and safety: The groupthink dilemma. *International Journal of Decision Sciences, Risk and Management, 7*(4), 316–331. https://doi.org/10.1504/IJDSRM.2017.093832

Sugandini, D., Irhas Effendi, M., & Istanto, Y. (2020). The resistance of SMEs in adopting social media: TOE model. In *Covid-19 – Reshaping Marketing and Communications* (pp. 44–53). Proud Pen. https://doi.org/10.51432/978-1-8381524-7-5_5

Sulistyo, H., & Ayuni, S. (2019). Competitive advantages of SMEs: The roles of innovation capability, entrepreneurial orientation, and social capital. *Contaduría y Administración, 65*(1), 156. https://doi.org/10.22201/fca.24488410e.2020.1983

Sutrisno, S., Fachrunnisa, O., & Widodo, W. (2022). The effectiveness of directing optional activities as capital for small and medium enterprises based on digitalisation in the crisis. *International Journal of Professional Business Review*. https://doi.org/10.26668/businessreview/2022.v7i2.468

Taib, R., Yu, K., Berkovsky, S., Wiggins, M., spsampsps Bayl-Smith, P. (2019). Social engineering and organisational dependencies in phishing attacks. In *IFIP conference on human-computer interaction* (pp. 564–584). Springer International Publishing. https://doi.org/10.1007/978-3-030-29381-9_35

Torkkeli, L., Kuivalainen, O., Saarenketo, S., & Puumalainen, K. (2019). Institutional environment and network competence in successful SME internationalisation. *International*

Marketing Review, 36(1), 31–55. https://doi.org/10.1108/IMR-03-2017-0057

Tsai, W., & Ghoshal, S. (1998). Social capital and value creation: The role of intrafirm networks. *Academy of Management Journal, 41*(4), 464–476. https://doi.org/10.2307/257085

Tuma, K., & Van Der Lee, R. (2022, May). The role of diversity in cybersecurity risk analysis: An experimental plan. In *Proceedings of the Third Workshop on Gender Equality, Diversity, and Inclusion in Software Engineering* (pp. 12–18). https://doi.org/10.48550/arXiv.2208.01895

Uddin, M. R., Molla, A. H., Ahmed, M. F., & Chowdhury, T. R. (2023). Advancing cyber resilience: Bridging the divide between cyber security and cyber defence. *International Journal for Multidisciplinary Research*, *5*(6). https://doi.org/10.36948/ijfmr.2023.v05i06.10726

Ul zia, N., Burita, L., & Yang, Y. (2023). Inter-organisational social capital of firms in developing economies and industry 4.0 readiness: the role of innovative capability and absorptive capacity. *Review of Managerial Science*, *17*(2), 661–682. https://doi.org/10.1007/s11846-022-00539-3

van Kranenburg, R., Bohara, R., Yahalom, R., & Ross, M. (2023). Cyber Resilience, Societal Situational Awareness for SME. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 458–463). IEEE. https://doi.org/10.1109/CSR57506.2023.10225011

Varma, A. J., Taleb, N., Said, R. A., Ghazal, T. M., Ahmad, M., Alzoubi, H. M., spsampsps Alshurideh, M. (2023). A roadmap for smes to adopt an AI based cyber threat intelligence. In *The effect of information technology on business and marketing intelligence systems* (pp. 1903–1926). Springer International Publishing. https://doi.org/10.1007/978-3-031-12382-5_105

Wang, J., Lu, Y., Fan, S., Hu, P., & Wang, B. (2021). How to survive in the age of artificial intelligence? Exploring the intelligent transformations of SMEs in central China. *International Journal of Emerging Markets*. https://doi.org/10.1108/ijoem-06-2021-0985

Wasko, M. M., & Faraj, S. (2005). Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. *MIS Quarterly*, 35–57. https://doi.org/10.2307/25148667

Widyawati, F., Soemaryani, I., & Muizu, W. O. Z. (2023). The effect of social capital and organizational health on competitive advantages of culinary and craft SMEs in Samarinda City. *Sustainability, 15*(10), 7945. https://doi.org/10.3390/su15107945

Wilson, M., & McDonald, S. (2024). One size does not fit all: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses. *Information Security Journal: A Global Perspective*, 1–35. https://doi.org/10.1080/19393555.2024.2357310

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security, 16*(6), 315–331. https://doi.org/10.1080/10658980701788165

Xie, J., Huang, Q., Yan, M., & Liang, Y. (2023). It is tough to detach from gossip: the impact of perceived negative workplace gossip on life satisfaction. *Journal of Business and Psychology*, 1–15. https://doi.org/10.1007/s10869-023-09894-8

Dr. Egena, Ode is a Senior Fellow of the UK Higher Education Academy, a recognition of his sustained record of excellence in teaching, learning support, and leadership in higher education. He is also a Chartered Management and Business Educator (CMBE), awarded by the Chartered Association of Business Schools, demonstrating

his commitment to high standards in business education and professional practice.

Currently, he works at the Centre for Enterprise, Manchester Metropolitan University. He also serves as the Scholarship Lead for the Innovation in Teaching and Learning Excellence Lab (I-TELL) within the Faculty of Business and Law, Manchester Metropolitan University. Prior to joining Manchester Metropolitan University, Dr. Egena Ode was a Research Fellow at the University of Huddersfield, UK where he led a £126,000 project focused on enhancing SME productivity in the West Yorkshire region of the UK. Dr. Ode has taught in the UK, Hong Kong, and Nigeria. Dr. Ode's research interests include co-creation and innovation, SME productivity, organisational resilience, and knowledge management, particularly in resource-constrained environments.

Dr. Ifedapo, Francis, Awolowo is an accomplished scholar and Senior Lecturer in Financial and Management Accountingat Sheffield Business School, Sheffield Hallam University. Dr. Awolowo is recognised as a leading authority in his field. He has an exceptional academic background, holds seven degrees, and has a PhD in forensic accounting. His professional credentials include the Certified Fraud Examiner (CFE) and Certified Public Accountant (CPA) designations, as well as recognition as a Senior Fellow of the Higher Education Academy (SFHEA), Certified Management and Business Educator (CMBE), and Fellow of the Association of International Accountants (FAIA). An interdisciplinary researcher, his areas of expertise span forensic accounting, audit failures, entrepreneurship, leadership, AI, corporate governance, occupational fraud and abuse, and the intersections of race and ethnicity. Dr. Awolowo currently serves as the Principal Investigator and Project Lead of the Accomplished Study Programme in Research Excellence (ASPIRE), an OFS/UKRI-funded initiative aimed at addressing the underrepresentation of Black doctoral students through personalised mentorship. A passionate advocate for inclusion and equity, he actively contributes to the anti-racist university agenda through workshops and thought leadership across the UK higher education sector. With a strong record of quality publications and keynote speaking engagements, Dr. Awolowo continues to influence academic and professional communities, championing a more inclusive and socially responsible future in education and research.

Dr. Rabake, Nana is a lecturer in the Department of Management at the University of Huddersfield's Business School . She joined Huddersfield Business School in January 2021 as a lecturer after previously serving as an associate lecturer from 2017 to 2020 . Dr Nana holds an MSc and a PhD in International Business Management, and her doctoral research focused on how multinational corporations implement corporate community involvement in leastn developed countries. Her research interests include corporate social responsibility (CSR), sustainable entrepreneurship, and the operations of multinational enterprises in developing economies. She has authored and co-authored publications on AI use in business education, CSR in West Africa's mining industry and promoting sustainable entrepreneurship in Africa . One of Dr Nana's papers on sustainable development in West African mining even earned a Best Paper Award at the 2017 British Academy of Management conference .

Dr. Femi, Stephen, Olawoyin is a lecturer and researcher in Business and Management, currently working with Sheffield Hallam University. He has previously lectured at Kwara State University and Igbinedion University, specialising in entrepreneurship, international business management, financial management, marketing, human resource management, and strategic management.

He has a passion for research and loves investigating trending issues in the fields of Management, Business Administration and Entrepreneurship. An active contributor to international scholarly literature, He has published in reputable journals on HR analytics, entrepreneurship, platform work in Sub-Saharan Africa, the digital divide in higher education, and transformational leadership in academia. Femi remains committed to advancing academic knowledge and contributing to the global business through research.