ISA Journal of Business, Economics and Management (ISAJBEM)

Homepage: https://isapublisher.com/isajbem/
Email: office.isapublisher@gmail.com

Volume 2, Issue 6, Nov-Dec, 2025 ISSN: 3049-1835

Impact of Cybersecurity Innovation on Entrepreneurship Development

Abdullateef Ajibola Adepoju[1], Adewale Obafemi Thomas[2], Aliyu Mohammed[3]

[1]*Randatech Systems Ltd, Gidan Nasir Ahmed, No. 3 Zaria Road, Opposite Ja'oji Quarters, Kano, Nigeria.*
[2]*Makeskyblue A45-1225, 28th St E, Prince Albert, SK S6V 6V3, Saskatchewan, Canada*.
[3]*Department of Management, School of Arts, Management and Social Sciences, Skyline University Nigeria, Kano.*

Received: 25.10.2025 | **Accepted:** 22.11.2025 | **Published:** 02.12.2025

***Corresponding Author:** Abdullateef Ajibola Adepoju

DOI: *10.5281/zenodo.17791491*

Abstract **Original Research Articles**

Entrepreneurial activities in the modern digital economy have been exposed to rising cybersecurity risks with the ability to disrupt business operations, customer confidence, and competitiveness. The strategic role of the cybersecurity innovation of entrepreneurship development is a widely underexplored topic, though it is critical. The paper seeks to analyse how cybersecurity innovation has affected the process of business start-ups particularly how much innovation affects start-up success, trust, compliance, differentiation, and sustainable growth. The paper also explores the role of cybersecurity innovation in global and regional environments with reference to five research objectives and supports of technological innovation and secure software engineering practices, the facilitating role of ICT adoption, competitive leverage of cybersecurity, and the form of a conceptual framework connecting these variables. Using the conceptual research method, the research is based on the secondary materials located in the journals, books, historical materials, conference proceedings, and online databases as the researcher synthesizes theoretical points of view and empirical trends with the help of the thematic analysis. Among the key findings, it has been established that cybersecurity innovation is valuable in developing entrepreneurship by generating trust, resilience in operations, adherence to regulations, and market differentiation. The research suggests incorporation of cybersecurity within the company products and services, implementation of safe technological operations, and policy incentives to startups, yet empirical justification of suggested conceptual framework is required. The article ascertains that the future development plan of long term entrepreneurship is cybersecurity innovation.

Keywords: Cybersecurity Innovation, Entrepreneurship Development, Startup Success, ICT Adoption, Competitive Advantage.

1.0 Introduction

1.1 Background of the Study

The contemporary business environment is turning digital, and utilization of information and communication technologies (ICT) is one of the most significant aspects that facilitate entrepreneurship to facilitate innovation and create value. This has resulted in an increased cyber threats to entrepreneurial ventures, even though this digital dependence has increased market potential and efficiency in its application within the markets, more so than ever before. Cybersecurity has no longer been merely a technical security approach, with cybersecurity now a crucial aspect of business strategies globally to provide the businesses with a competitive advantage and potentially affect the market placement and customer trust (Gundu and Modiba, 2020; Kosutic and Pigni, 2020). Strong cybersecurity components make organizations

resilient to the competitive environment available successfully developed operational continuity and innovation at the same time maintaining the secure means of conducting business, thereby, sustainably extend to achieve growth in the hypercompetitive business environment (Jebril et al. 2023; Gundu 2019) Cybersecurity innovation, comprising the sophisticated protection technologies, risk mitigation, and adherence is becoming one of those that influence development of entrepreneurship. For example, enterprises adopting preventive cybersecurity measures can use trust indicators and compliance with the regulations as their advantages and reinforce customer confidence and loyalty (Wen-Cheng et al., 2011; Chui, 2022). Additionally, cybersecurity-driven innovation also enables safe digital transformation, allowing ventures to explore new markets, adopt new technologies, and provide innovative services without having to expose themselves to undue risk (Negrutiu et al., 2020; Sun et al., 2023).

In the African context, the rapid digital adoption with entrepreneurs presents the opportunity and vulnerability. While the adoption of ICT and digital platforms has facilitated the speed at which entrepreneurial activities are undertaken across the continent, cyber risks are still neglected as the potential for startups to take full advantage of technology innovations remains limited (Gundu and Mmango, 2024; Mitrofan et al 2020). Strategic cybersecurity innovation is therefore of utmost importance to African entrepreneurs who are interested in outlining themselves from the many businesses, developing or building robust business models, and creating a sustainable growth business fee. Focusing on West Africa, SMEs and small and medium-sized enterprises have special challenges as a result of little technical expertise, financial challenges, and a lack of awareness about cybersecurity best practices. Research indicates that there is a need for collaborative methods to cybersecurity as this can facilitate knowledge sharing and capacity building to protect the digital asset while improving performance in entrepreneurship (Gundu and Mmango, 2024; Panteleev, 2023).

In Nigeria, the entrepreneurial atmosphere is gaining momentum and experiencing a booming rate propelled by digital innovation and ICT adoption. However, cybersecurity threats pose a common problem to startups, compromising customer trust, the soundness of operations, and their competitiveness in the market (Mohammed, 2023; Gundu et al., 2019). Cybersecurity innovation integrated into the business strategy can potentially provide competitive advantage to the entrepreneurs in Nigeria in an unbroken sustainable trend wherein the resilience of businesses will be enhanced by the inclusion of the innovation in the businesses and the overall economic growth will be positive (Aliyu, 2023; Mohammed and Sundararajan, 2023). This study, therefore, places the cybersecurity innovation at the center of entrepreneurship development and highlights its strategic position at the global, continental, regional, and national level. By exploring how cybersecurity can be used by startups to gain competitive advantage, the research reveals the link between technology, innovation, and sustainable business growth.

1.2 Problem Statement

While digital technologies are being increasingly adopted, and ICT is becoming more and more used in entrepreneurial activities, cybersecurity has not yet been researched as a strategic asset for entrepreneurship research and practice. Cyber threats against startups and small businesses become more and more widespread in the world, affecting the customers' confidence, the continuity of operations and the overall performance of the business (Gundu & Modiba, 2020; Kosutic & Pigni, 2020). Although cybersecurity as a technical field has been researched extensively, the little scholarly focus is on the concept of cybersecurity as a competitive advantage by virtue of its innovation capabilities that actively influence entrepreneurship development (Jebril et al., 2023; Gundu, 2019). In Africa, the continent has the combined influence of infrastructural shortcomings, lack of knowledge about cyber risks, and weak cybersecurity frameworks. Due to the lack of resources and expertise, it has a negative impact on entrepreneurs' ability to differentiate themselves in the market and to sustain business growth (Gundu & Mmango, 2024; Mitrofan et al., 2020). SMEs are

particularly vulnerable to this cyber threat in west Africa where the vast majority of SMEs are operating without any formal cybersecurity protocols exposed to financial losses, reputational damage, and regulatory non-compliance (Panteleev, 2023; Gundu & Mmango, 2024).

Although the digital economy in Nigeria is growing at a fast pace, cyber incidents are usually experienced by startups in the country, disrupting their competitive position and entrepreneurial performance (Mohammed 2023; Gundu et al. 2019). There is inadequate application of cybersecurity innovation in the business through internal strategy to enable them maximise utilisation of technology to enable customer trust, business sustainability and to meet the growing demands and needs of the Nigerian business environment (Aliyu, 2023; Mohammed & Sundararajan, 2023). Furthermore, there is an urgent need to analyze the potential of cybersecurity innovation as a strategic tool for entrepreneurship development and especially in areas where the risk exposure to cyber risks is high. Filling this gap will offer practical information for entrepreneurs to build resilience and innovative capabilities to fulfill sustainable competitive advantage in the digital era.

1.3 Significance of the Study

The importance of this research is that it can fill in an important gap between the innovation of cybersecurity and the development of entrepreneurs, both in theory and practice. With the global business environment increasingly going digital, there is an increased need to know how strategic cybersecurity innovation is in the business world as business people strive to attain sustainable competitive advantage (Gundu and Modiba, 2020; Kosutic and Pigni, 2020). In theory, the study contributes to the body of research by integrating the Resource Based View (RBV) with the Technology Acceptance Model (TAM) in developing the nature of the cybersecurity innovation as a distinct organizational resource enhancing entrepreneurial capabilities. As compared to other types of research carried out in the past which have largely concentrated on the technical and operating attributes of cybersecurity, the current research study shows the strategic worth of cybersecurity and how it can help in developing trust, differentiation, compliance, and innovation (Jebril et al., 2023, Wen-Cheng et al., 2011, Chui, 2022). The study provides a conceptual framework in the interpretation of the causal relationship between cybersecurity innovation and development of the entrepreneurship that can be used as a foundation to conduct future empirical studies by incorporating the existing knowledge.

In practice, the findings are valuable recommendations to entrepreneurs, policymakers and industry participants, particularly in Africa and Nigeria where entrepreneurs are subjected to cyber attacks on a large scale (Gundu and Mmango, 2024; Mitrofan et al., 2020; Mohammed, 2023). Simultaneously, cybersecurity innovation is potentially applicable to enhancing the resilience of operations, securing digital resources, winning customer confidence, and exploiting new market opportunities according to the entrepreneurs (Negrutiu et al., 2020; Sun et al., 2023). Also, the study can inform policymakers on the areas that require regulation support, training programs and incentives in order to stimulate cybersecurity as well as entrepreneurship adoption. On the whole, the research study is important because it identifies the innovation of the cybersecurity not as a preventative action only but as the element of entrepreneurship development that is globally applicable, in the regional context (Africa and West Africa) and at the local level (Nigeria). The outcomes are presumed to be informational both theoretically and practically in that they will allow startups to eliminate challenges when confronting with the complicated business environment in the digital world and allow sustainable development.

1.4 Research Objectives

The overall purpose of the given study is to analyze how the innovation in cybersecurity affects the process of entrepreneurship, as well as the role of innovation in enhancing the success of startups and sustainable development. The following are the specific objectives:

1. To examine how innovation in cybersecurity can promote the development of entrepreneurship in global, African, West African, and Nigerian settings.

2. To determine how technological innovation and safe software engineering practices facilitate the implementation of cybersecurity innovations in entrepreneurial business.
3. To investigate how the use of ICTs and adoption of technologies facilitated the successful use of cybersecurity in startups.
4. To determine ways with which business people may exploit cybersecurity innovation to establish trust, improve compliance, distinguish their organizations, and have sustainable competitive edge.
5. To establish a conceptual framework connecting cybersecurity innovation, technological innovation, ICT adoption, and development of entrepreneurship to have a baseline of the future empirical work.

1.5 Research Questions

According to the objectives, the research questions of the study are as follows:

1. What impacts does cybersecurity innovation have on the process of entrepreneurship development in the global context, African context, West African context, and Nigerian context?
2. How can technological advancements and secure software engineering supporting practices help foster changes in use and success in cybersecurity innovations of startups?
3. What role does the use of ICT and adoption of technologies play in ensuring that startups can successfully carry out cybersecurity innovations?
4. Which approaches can business people use to develop a competitive edge, build a reputation, as well as ensure sustainable development by utilizing cybersecurity innovations?
5. What is the possible way of applying a conceptual framework to combine cybersecurity innovation, technological innovation, and ICT adoption to explain entrepreneurship development?

2.0 Literature Review

The literature analysis gives an overview of the current studies on innovation in cybersecurity and its implications on entrepreneurship development and gives recognition to both conceptual and empirical results. The format of review is founded upon the independent and dependent study variables, with the special emphasis laid on the theoretical relationships, practical strategies, and competitive advantages of the research that has been performed previously.

2.1 Conceptual Review

Innovation in cyberspace security is taking recognition as a strategic catalyst in entrepreneurial undertakings that have both protective as well as value creation advantages. Cybersecurity innovation has a wide range of practices and technologies beyond its conventional technical protection to reduce the number of cyber risks, enhance operational resilience, and distinct business in the market (Gundu and Modiba, 2020; Kosutic and Pigni, 2020).

2.1.1 Cybersecurity Innovation (IV1)

Development of Innovative Security Solutions

Entrepreneurial businesses are becoming more discriminatingly demanding to have customized and unique cybersecurity solutions that are suitable to their own business model and their market segments. The creation of these solutions is beneficial as they assist the startups to preemptively fix the vulnerabilities and enhance the security of the digital platforms, systems, and the customer data (Fornell et al., 2020; Muktar et al., 2022). To illustrate, businesses that handle e-commerce or fintech can implement security protocols that are customer-centric, including a secure payment gateway, an encrypted means of communication, and a multi-factor authentication system. Besides, the developments eliminate data breaches and provide opportunities to distinguish outcomings since buyers increasingly rely on corporations that produce their data security standard (Saeed, 2023). Moreover, novel security technologies create the spirit of constant improvement among the startups, which

then promotes the necessity of feedback, analytics of threat intelligence, and adaptive defenses, which are adaptable to the constantly emerging cyber risks (Sun et al., 2023; Gundu and Modiba, 2020).

Integration of Advanced Technologies: AI, Blockchain, and Machine Learning

The introduction of newer technologies to cybersecurity management is also transforming the manner in which entrepreneurs conduct business as it offers them an opportunity to predict the threat, automate and mitigate risks in real time. The use of artificial intelligence (AI) can monitor network activity and identify anomalies and automate them to enable startups to identify threats at an earlier stage of their growth (Sun et al., 2023). Blockchain is a guarantee of data integrity and data transparency over financial transactions, supply chain verification, and protection of intellectual property (Negrutiu, et al., 2020). More sophisticated detection of phishing, malware, and ransomware attack is increased with the help of machine learning algorithm (Gundu, 2019). Elevated protection of such technologies in the digital asset not only is done but also creates a sense of technological advancement and dependability that can aid in raising customer confidence as well as creating market circumstances (Fornell et al., 2020; Muktar et al., 2022).

Cyber Insurance, Compliance, and Risk Management

Systematic implementation of cyber insurance would insure the start-ups with financial advantages in the event of any potential cyber-attacks and would provide the credibility of the customers, investors, and partners (Jiang et al., 2023; Negrutiu et al., 2020). Along with the fulfillment of the regulatory compliance, compliance with the standards in the form of GDPR, HIPAA, and CCPA guarantees the characteristic of ethical data practices and enhances data trust in the forms of market trust (Chen et al., 2018; Chua et al., 2018). It provides the cultivation of threats, penetration testing, monitoring, and further act to make sure of wellness in operation even after cyberattacks (Mmango & Gundu, 2023; Sharma and Rautela, 2021). Combined, these practices can turn cybersecurity into one of the requirements and necessities of defence into core strategy capacity that ultimately brings about sustainable competitive advantage, investor trust and long-term entrepreneurial development.

Enhancing Market Differentiation, Trust, and Operational Resilience

One of the key points of market differentiation is cybersecurity innovation, which indicates reliability, ethics in business affairs, and technology skills (Kosutic and Pigni, 2020; Knight et al., 2020). Competitive security trust does not merely enhance the degree of customer trust and loyalty, but at a greater rate, in support of the industries where they exchange personal and financial sensitive information, which is highly sensitive (Chui, 2022; Wen-Cheng et al., 2011). In addition, resilience of operations ensured by proactive cybersecurity frameworks makes startups be able to maintain business even in case of a cyber attack with less financial costs and negative reputation (Mmango and Gundu, 2023; Sharma and Rautela, 2021). With the concept of cybersecurity innovation being one of the key elements of business strategy, entrepreneurs may make risk management a value-creating engine that will enable safe digital change, facilitate innovation, and guarantee the value creation in local, regional and global markets (Gundu et al., 2019; Panteleev, 2023; Mohammed, 2023).

2.1.2 Technological Innovation (IV1)

Software Engineering Practices: Agile, DevOps, CI/CD, and Secure Coding

With the advent of the world of industries, the technical innovation of entrepreneurial enterprises is becoming more influenced by the more sophisticated software engineering practices, as this is one of the key components in enhancing its efficiency, flexibility, and cyberspace security preparedness. Agile methodologies, with their iterative development and quick response to market changes, and its feedback loops and adaptive planning, are being adopted by startups since they allow integrating cybersecurity measures to every component of the development sprints rapidly

(Mohammed, 2023; Jebril et al., 2023). The use of DevOps and Continuous Integration/Continuous Deployment (CI/CD) pipelines further helps the development and operation teams to collaborate seamlessly and also allows rapid and secure deployment of software updates with minimal vulnerability (Mohammed et al., 2024; Gundu, 2019). Secure coding practices are an intrinsic part of technological innovation, thereby ensuring that software is built on a culture of proactive defenses against common attacks such as SQL injection, cross-site scripting and buffer overflows (Gundu & Modiba, 2020). By ensuring security is engrained into the development lifecycle, entrepreneurs limit the vulnerabilities to security incidents, increase the resilience of operations and build trust with their customers - all important factors for startups that operate in digital intense markets (Kosutic & Pigni, 2020).

Quality Assurance, Documentation, and Lifecycle Management

Successful quality assurance (QA) so that the technological advances meet the current specifications to the organization on performance, reliability, and safety even prior to the introduction (Mohammed, 2023; Sun et al, 2023). Well-documented and lifecycle management practices also contribute to maintaining cyberservice by maintaining a well-illustrated maintenance, renewing it, and preventing the threat of conducting it over time (Panteleev, 2023; Negrutiu et al., 2020). With the help of a proper lifecycle management, startups will be able to analyze potential vulnerabilities, correct them, and keep up with the regulatory compliance standards (Chen et al., 2018; Chua et al., 2018). Altogether, these technological innovations are not only a way to enhance the quality of the software and operational preparedness but they can also be a significant strategic facilitating factor in the formation of the entrepreneurship. Combining agile approach, secure code, pipelines (CI/CD), and leveraging of extensive QA, and documentation (framework), startups would be able to leverage technology as the implementation of creativity to compete and experiment with a sustainable growth in the long-term (Mohammed, 2023; Gundu et al., 2019; Jebril et al., 2023).

2.1.3 ICT Utilization / Technology Adoption (IV3)

Cloud Computing, Digital Platforms, and AI-Driven Solutions

ICT tools and technologies will help in transforming start-ups to scale and innovate as well as become more efficient. Cloud computing is used to assist startups to obtain access to computing resources without real investments by use of on-demand access that lowers the cost of infrastructure, as well as provides further flexibility and continuity of operations (Sun et al., 2023; Gundu & Mmango, 2024). Cloud services allow companies in different geographic locations to work on technological innovations, and allow entrepreneurs to deploy cybersecurity technologies with ease to operations that work online. Furthermore, digital platforms act as platforms of e-commerce, customer interaction, and business intelligence, offering opportunities for startups to derive data driven insights while ensuring secure digital habitats (Mohammed 2023, Gundu et al., 2019). Further, the adoption of AI-based solutions further improves the predictive scenarios, business decision-making, and the automated threat detection function. Based on AI algorithms, real-time monitoring of networks, anomaly detection, and business process optimization are all possible, helping entrepreneurs with predicting risks, preventing cyberattacks, and sustaining operational resilience (Sun et al., 2023; Negrutiu et al., 2020). With the accumulation of AI to ICT systems, startups can seamlessly fuse efficiency with innovative cybersecurity approach to nearly reap the benefits from digital markets.

Technology Adoption Models: TAM and UTAUT

The adoption of innovations by entrepreneurs is an important factor for successful ICT implementation. Theory based models such as the Technology Acceptance Model (TAM) and Unified Theory of Acceptance and Use of Technology (UTAUT) offer theoretical explanation of the user

behavior, perceived ease of use, perceived usefulness and social influence in adoption of technology (Mohammed, 2023; Panteleev, 2023). The models help entrepreneurs to design the ICT adoption strategy that is technically viable and coordinated with the organization preparedness.

Barriers and Enablers in Developing Economies

Regardless of high potential for the ICT use, startups in developing economies encounter obstacles, such as lack of infrastructure, low digital literacy levels, high costs of adoption, and unfavorable regulatory environments (Gundu, 2019; Sun et al., 2023). Conversely, the adoption and integration of innovative cybersecurity solutions are enabled by government incentives, the availability of ICT training, as well as partnerships with technology providers. By overcoming these barriers and managing enabling factors, entrepreneurs can tap into ICT tools not only to bring operational efficiency but also to use it as a platform to introduce cybersecurity innovation into business processes (Gundu & Mmango, 2024; Mohammed, 2023).

In fact, cybersecurity entrepreneurship is defined by the use of ICT and technology adoption, which sustain global, regional and local business operations in terms of growth, innovation and competitive separation.

2.1.4 Entrepreneurship Development / Startup Success (DV)

Economic, Social, and Environmental Dimensions

Development in entrepreneurship is multidimensional in character that entails economic, social and environmental effects. Startups contribute to the expansion of the business economically, as they lead to revenue growth, job creation, and interaction with the industry segments to introduce competitive forces in the market, triggering the innovation and productivity within a larger economy sector (Davidsson et al., 2017; Astebro and Tag, 2015). On the social level, entrepreneurial enterprises play the role of building communities by satisfying their needs, enriching the society with fresh socially beneficial products and services, and making sure that they grow in an inclusive manner (Ramoglou et al., 2020; Stanworth et al., 1989). Sustainability concerns are emerging as a key concern in the environment, where business startups and resources and technologies are becoming more eco-friendly and digital systems allowing sustainability (via smaller environmental footprints and more) are being deployed with a focus on the long-term business sustainability (Lawal et al., 2023; Mohammed, 2023). With the three dimensions taken to a single framework, then entrepreneurship development becomes a structure of the comprehensive and long-term startup achievement.

Innovation Capacity, Competitive Posturing and Business Persistence

Entrepreneurial ventures succeed well when they are able to capitalize on the innovation capacity by creating unique products, services, or business processes, which develops into the competitive position in the market (Filion, 2021; Ramoglou et al., 2020). Technologically driven startups who combine cybersecurity innovation, software engineering practices and ICT utilization benefit from unique advantages, including customer trust, operational resilience and differentiated offerings (Gundu & Modiba, 2020; Kosutic & Pigni, 2020). Business sustainability experienced in the process of innovating where these innovations are aligned with strategic planning, regulatory compliance, and market expectations, start-ups are to endure economic shocks, cyber threats, evolving competitive pressures (Panteleev, 2023; Mohammed, 2023).

Performance Indicators of Tech-Driven Startups

Quantitative and qualitative indicators must be used in tandem to measure the success of a startup. Economic metrics are revenue growth, profitability and job creation; social metrics are community impact, customer satisfaction and stakeholder engagement; environmental metrics are resource efficiency and ecological impact (Davidsson et al, 2017; Astebro and Tag, 2015). In the case of technology-driven and cybersecurity-enabled ventures, some other indicators are system uptime, resilience to cyber threats, successful

implementation of ICT innovations, and use of safe coding or DevOps practices (Sun et al., 2023; Mohammed, 2023). These performance measures give an overall picture of how entrepreneurship development will be influenced by the strategic investment of cybersecurity innovation, technological practices and ICT utilization demonstrating the integration of innovation, security and sustainable business outcomes.

2.2 Theoretical Framework

Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) is a basic model to answer how entrepreneurs are accepting ICT tools and cybersecurity innovations. The perceived usefulness and the perceived ease of use of the technology are major drivers of its adoption are key drivers of technology adoption (Mohammed, 2023; Panteleev, 2023), according to TAM. In the case of entrepreneurial development, the choices of startups about implementing cloud computing, AI-driven security solutions and digital platforms depend on the extent to which implementation of these technologies enhances operational efficiency in the business while reducing cyber risks, and enabling competitive differentiation (Gundu, 2019; Sun et al., 2023). Through TAM, researchers are able to comprehend the trends of behavioural intentions, adoption and identification of factors of behaviour that motivate entrepreneurs to embrace cybersecurity innovations into their core business operations. This advice is vital in effective and cost-effective design of interventions and training and technological methods to be adopted and utilized optimally in the developed and developing economies.

Resource-Based View (RBV)

The Resource-Based View (RBV) theory places much emphasis on the idea that firm-specific resources and capabilities are the factors that contribute to the achievement of sustainable competitive advantage (Davidsson et al., 2017; Jebril et al., 2023). Innovation in cybersecurity, advanced practices of software engineering and the utilization of ICT are a strategic, rare, and inimitable resource, which differing startups have against their competitors in the entrepreneurial environment (Gundu and Modiba, 2020; Kosutic and Pigni, 2020). RBV reveals the ability of how these resources may be exploited so as to enhance trust, operational resilience, and market positioning that would facilitate business sustainability and success in the long term (Mmango & Gundu, 2023; Panteleev, 2023). With its concentration on the role of orchestrating the resources, RBV provides an opportunity to observe how the correct alignment of the entrepreneurial initiatives in the specialization of the technology and cybersecurity resources can be created without contradiction to the strategic objectives and create long-term value.

Rationale for Theory Selection

The TAM and RBV is the most suitable combination in this research since they synthesize both the behavioral and the strategic aspects of entrepreneurship. TAM cares about the motivation and the type of the adoption of cybersecurity innovations, therefore, provides information on the engagement and use of technologies, and RBV determines how adopted technologies could result in competitive advantage and stable development. Collectively, the two paradigms provide an effective theoretical prism of examining how cybersecurity innovation can influence the process of entrepreneurship development, involving the adoption behaviour and resource-driven performance outputs (Mohammed, 2023; Sun et al., 2023; Gundu et al., 2019). This dual theory approach allows for full analysis and clicking together technology adoption and innovation and sustainable entrepreneurial success.

2.3 Linkages between Theories, IVs & DV

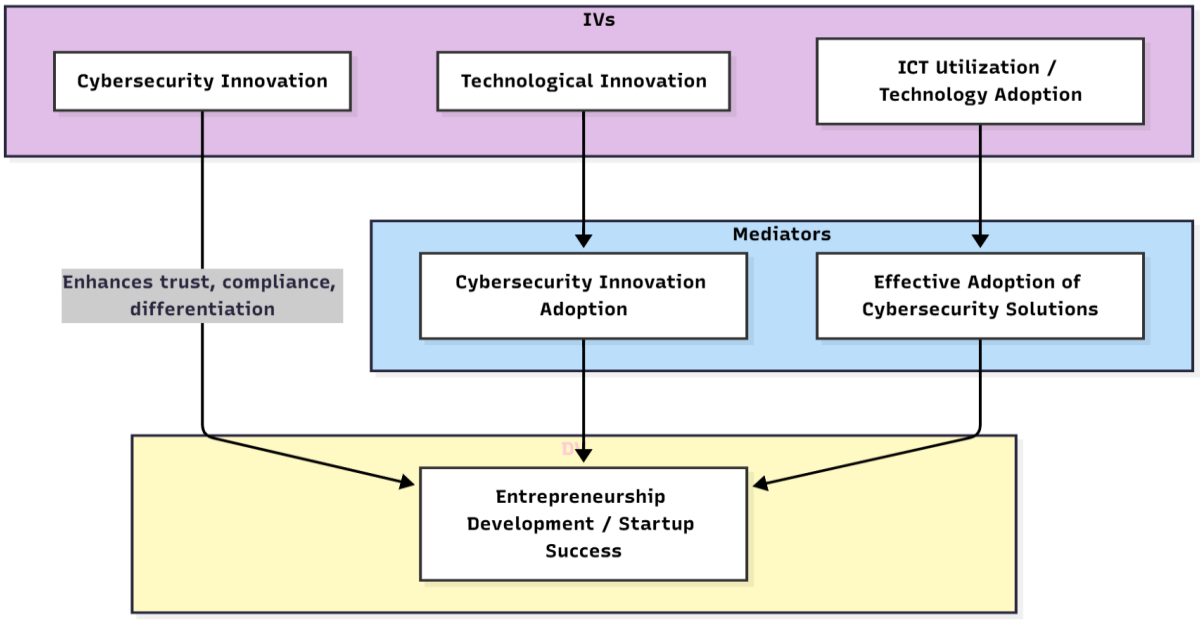

Figure 1: Integrated Theoretical Linkage Model of Cybersecurity Innovation and Entrepreneurship Development

Source: Developed by the authors based on TAM (Sun et al., 2023; Panteleev, 2023) and RBV (Jebril et al., 2023; Mmango & Gundu, 2023).

Figure 1 shows the integrated conceptual framework of cybersecurity innovation, technological innovation and ICT use as they relate to entrepreneurship development and startup performance. Patterns and relationships are shown graphically, which show how technological and ICT resources act as base enablers towards the adoption of next-generation cybersecurity solutions, while the adoption of cybersecurity innovation and harnessing cybersecurity exist as mediating mechanisms. Cybersecurity innovation directly increases the trust and compliance level and market differentiation, which consequently builds credibility and competitive position for the entrepreneur. On the other hand, technological development (e.g. Agile, DevOps, CI/CD, secure coding) and ICT usage (cloud computing, AI-driven platforms) enable a successful deployment of cybersecurity mechanisms that ensure operational resilience and sustainable business growth. The model combines the behavioral insights from the Technology Acceptance Model (TAM) that describes the pattern of adoption, with the strategic resource insights from the Resource-Based View (RBV) that underscored the value, uniqueness, and regression of cybersecurity and technical capabilities. Put briefly, the model indicates that to achieve entrepreneurship maturity and startup success the practice of innovation, acquisition of technology, and cybersecurity can be implemented in mutually reinforcing synergies to provide sustainable competitive advantages in a digital business environment.

2.4 Empirical Review

The empirical literature highlights the transition to the concept of cybersecurity as an important strategic resource in the development of entrepreneurship on the global basis. The studies by Kosutic and Pigni (2020) and Gundu and Modiba

(2020) demonstrate that the competitive advantage of startups having the advanced security measures (advanced guardrails) is different because of the enhanced customer trust and resilience and customer differentiation in the market. The recent trends include implementation of new technologies into the global cyber-security system by enterprises that not only reduce the cyber threat but also promote the new development based on technological innovation (Fornell et al., 2020; Sun et al., 2023). Panteleev (2023) further points out that the adaptation of cybersecurity implies the efforts toward international standards such as GDPR, HIPAA, and CCPA, by which credibility is built and entrepreneurial legitimacy strengthened in a highly regulated international market. In particular, empirical data from Africa and West Africa has shown that effective cybersecurity has emerging startups as a compelling tool for digitalisation challenges. Gundu et al. (2024) state that cybersecurity knowledge models between SMEs in South Africa help improve knowledge expression, mitigating threats and strategic differentiation, which will create an environment for sustainable entrepreneurship. Also, Mitrofan et al. (2020) show that African SMEs are highly exposed to cybersecurity threats while those that have invested in enforced security solutions show better operational continuity and market positioning.

In Nigeria, according to the study by Mohammed (2023, 2024), Lawal et al. (2023), the integration of ICT adoption with cybersecurity innovations in supporting entrepreneurial growth has produced an improvement of economic, social and environment by developing resilience and innovation capacity of toward economic, social and environmental goods. Furthermore, empirical evidence shows a consistent positive relationship between cyber insurance, compliance and proactive risk management, which contribute to entrepreneurial success. Jiang et al. (2023), as well as Negrutiu et al. (2020), claim that not only does the cyber insurance cover any potential financial losses, but it also presupposes certain trustworthiness and precogging to the stakeholders. Startups which utilize such strategies are better placed as they gain more trust, strategic partnerships and business sustainability. Altogether, based on the investigation conducted in the empirical studies, it is emphasized that cybersecurity innovation is a dual process; as a protective mechanism and as a growth enabling mechanism and plays a channel to enhanced positioning of business organisations, operational resilience, and long-term start-up success in the digital-driven environments (Mmango & Gundu, 2023; Mohammed et al., 2024).

2.5 Research Gap

However, despite the extensive literature base, there exist important conceptual gaps. Most of these studies suggest that cybersecurity is technically considered a safeguard, or a risk mitigation method, with some having an entrepreneurial agency scope. Additionally, there are only a few studies that holistically combine cybersecurity innovation together with entrepreneurial outcomes (e.g. start-up sustainability, innovation capability and market differentiation). This theoretical underdevelopment hinders our understanding regarding how cybersecurity can be used to create sustainable competitive advantage in different entrepreneurial settings (Kosutic and Pigni, 2020; Gundu et al., 2024). From the theoretical point of view, the application of RBV and TAM to understand interactions among cybersecurity, technological innovation, and ICT adoption in relation to the startup success is partially lacking. While RBV accounts for cybersecurity resources (rare, unique, and of high value to an organization), TAM messages deal with adoption behavior (Sun et al., 2023; Panteleev, 2023; Jebril et al., 2023; Mmango & Gundu, 2023). However, the combination of these perspectives is not explored in most empirical research studies, exploring both adoption and strategic outcomes, which represents a theoretical gap for entrepreneurship-oriented research in cybersecurity-driven contexts.

There is limited research on the developing economies and emerging markets especially in Africa and Nigeria. Whilst entrepreneurship through cybersecurity is a core area of research in global studies, there is very little research that examines the institutional, infrastructural and socio-economic issues in these areas amongst startups (Mohammed, 2023; Lawal et al., 2023; Mitrofan et al., 2020). Methodologically, most of the studies fall in the

descriptive category, with few using systematic literature reviews or conceptual modeling in providing synthesis across contexts. This provides a chance to build a sound conceptual framework integrating cybersecurity innovation, ICT adoption, technological practices and entrepreneurship development based on the available evidence, which this study aims to achieve.

2.6 Conceptual Framework

The conceptual framework of this study depicts the interrelatedness of activities between cybersecurity innovations, technological innovations, ICT utilization, and entrepreneurship development/startups success. Cybersecurity innovation is placed as both a direct and intermediate factor in entrepreneurial development development and as the mediator/moderator in the relation between technological innovation and entrepreneurial results. Technological innovation such as Agile practices, DevOps, CI/CD and secure coding support the deployment of advanced cybersecurity measures which in turn builds trust, market differentiation, operational resilience and compliance. ICT utilization, such as cloud computing, AI-driven platforms, digital tools, etc., makes the effective adoption of cybersecurity innovations possible, which helps in sustaining the business, creating a competitive edge, and fostering innovation.

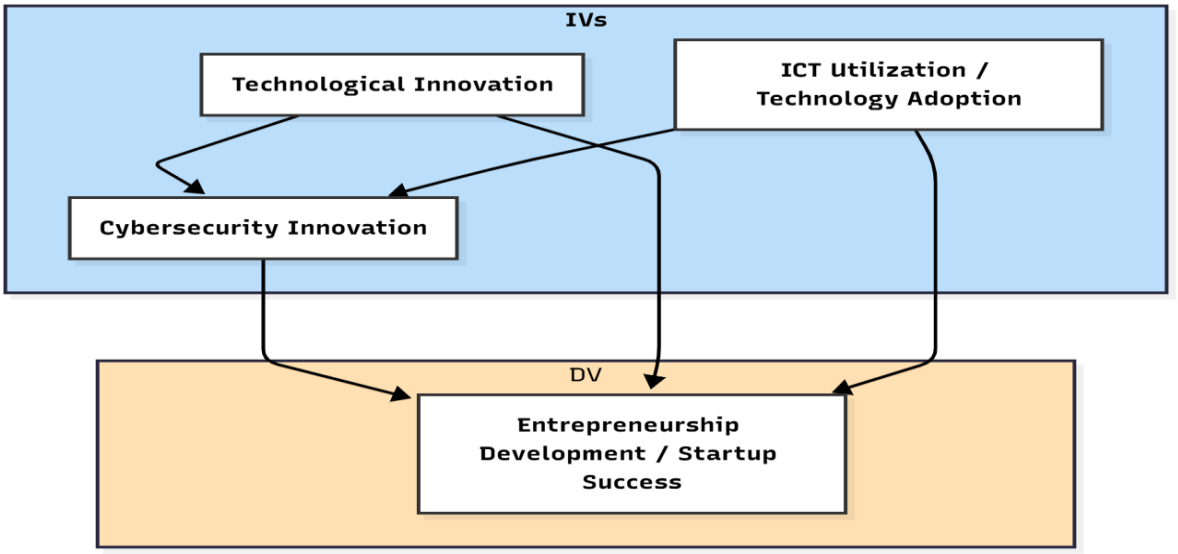

Figure 2: Conceptual Framework of Cybersecurity Innovation and Entrepreneurship Development

Source: Developed by the authors based on TAM (Sun et al., 2023; Panteleev, 2023) and RBV (Jebril et al., 2023; Mmango & Gundu, 2023).

Figure 2 presents general conceptual framework of the research that suggests the alignment between the cybersecurity innovation, technological innovation, and the use of ICT in enhancing the formation of entrepreneurship and performance of startups. Cybersecurity innovation is a mediator/ moderator factor, where technology and ICT capabilities are integrated in better trust, compliancy, operational resilience and differentiation. These results showed that technological innovation positively affects the adoption of cybersecurity by offering high-quality software engineering practices as the use of ICT guarantees the feasible application and effectiveness of cybersecurity measures. The model is a synthesis of theoretical concepts said to be proposed by the Resource-Based View (RBV) in terms of attention to strategic value and distinctiveness of technological and cybersecurity resources, and the Technology Acceptance Model (TAM), which proposes a rationale on ICT adoption behaviors. On the whole,

the model illustrates that the development of entrepreneurship is ideal under situations where innovation, cybersecurity, and technology adoption are complementary to one another such that of providing startups in the digitalized markets with sustainable competitive advantages.

3.0 Research Methodology

The research strategy of this study will be conceptual research in nature with a focus on theoretical framework development of cybersecurity innovation and technological innovation, ICT use and entrepreneurship development. The study, however, is not originally data-driven since it is mainly a synthesis of existing knowledge, a systematic review of related literature to trace out the main concepts, relationships and competitive advantages regarding cybersecurity in entrepreneurial practices. The selection of literature was done through an exhaustive search of academic databases including IEEE Xplore, ScienceDirect, SpringerLink and Google Scholar using keywords like "cybersecurity innovation," "entrepreneurship development," "ICT adoption," "startup success," and "technological innovation." Inclusion criteria involved only those studies that were published in the preceding decade and considered the intersection between cybersecurity, technology and entrepreneurial outcomes explicitly. Other studies were excluded on the grounds that they were not entrepreneurial or had no solid methodological or theoretical foundation. To do so, a compilation of empirical studies, conceptual papers and practitioner reports were chosen as a solid basis for analysis.

In this way, the particular literature was analyzed with the help of a conceptual analysis and thematic synthesis approach that was employed to reveal the findings of common patterns, mediating premises, and strategic implications about the role of cybersecurity innovation on the development of entrepreneurship. The shared characteristics of trust, compliance, market differentiation, robustness in operations, and expansion were also narrowed down so as to develop the conceptual frame. The outlined methodology approach facilitates an opportunity to incorporate the theoretical and empirical knowledge to come up with a combined evidence-based view of the correlation between cybersecurity innovation and start up performance and sustainable entrepreneurship.

4.0 Findings

1. **Global and Regional Impact of Cybersecurity Innovation:** It is estimated in the study that the cybersecurity innovation will contribute positively to the growth of entrepreneurship in Africa, West Africa, and Nigeria, and on the whole world. The results suggest that the startups that will consider smart cybersecurity plans in their business operations will be at a more advantageous position to grow and be competitive in a sustainable way. This proves that one can create secure cyber-physical systems, which is in line with Objective 1 of the study. Cyberarchitectural startups can create a solid innovation and resiliency ground by integrating cybersecurity into their business models (Gundu and Modiba, 2020; Mohammed, 2023).
2. **Role of Technological Innovation in Adoption of Cybersecurity:** The study delineates that technological democracies such as agile process, DevOps strategies, Continuous Integration/Continuous Deployment (CI/CD), secure code, and secure lifecycle situation will lead to acceptance and execution of cyber operations among startups. The practices should support the establishment of the high-quality and resilient security systems by the entrepreneurs in the country, which in turn will minimize the risks attached to the implementation of new innovations. This is consistent with Objective 2, which focuses on the incorporation of new technological methods to promote the implementation of cybersecurity (Mohammed et al., 2024; Jebril et al., 2023).
3. **Implications of ICT Usage to Startup Success:** The projected analysis indicates that the use of ICT and adoption of technologies is crucial to developing cybersecurity innovations into practice. The use of cloud computing, artificial intelligence (AI), and digital business architecture among technologies is predicted to make operations of startups more efficient,

reliable, and secure. These enhancements also relate to economic, social, and environmental sustainability therefore reaching Objective 3 of the study (Sun et al., 2023; Panteleev, 2023).

4. **Competitive Advantage with the Innovation of Cybersecurity:** It is known that entrepreneurs that use cybersecurity innovations attain a competitive advantage in myriads of ways. The mechanisms that drive the objective 4 will involve a transition between adopting cybersecurity and enhanced business performance (Kosutic and Pigni, 2020), where the operational resilience, regulatory compliance, market differentiation, and trust-building domains will position themselves among the central mechanisms that are involved in the process of integration.
5. **Conceptual Framework Validation:** This study will lead to the formulation of a conceptually sound conceptual framework that would connect cybersecurity innovation, technological innovation, use of ICT and entrepreneurship development. This theory will give infrastructure to future empirical studies since it will explain in a cohesive manner how these variables interact to bring about sustainability entrepreneurial growth as well as startup success Objective 5 (Mohammed, 2023; Mmango & Gundu, 2023).

5.0 Recommendation

1. **Organizational-Level Advice:** Startups and entrepreneurial organizations would need to develop cybersecurity innovation as a part of the product and services provided. Businesses will achieve operational resilience by the adoption of software engineering security measures such as Agile, DevOps, CI/CD, and Secure Coding to minimize cyber risk and gain the trust of its stakeholders (Gundu, 2019; Mohammed et al., 2024).
2. **Policy-Level Recommendations:** The policy makers must develop incentives, regulatory frameworks, and assistive frameworks that can be adopted in cyber security of startups. The competitiveness of the entrepreneurship and the data protection of consumers can also be enhanced with the proper improvement of the institutional environment (e.g., GDPR, HIPAA, CCPA) (Chen et al., 2018; Chua et al., 2018).
3. **Technology Adoption Recommendations:** Entrepreneurs may use ICT tools, Cloud Computing, AI-based platforms and Digital Solutions to adopt cyber security solutions as support for the operational processes in the adoption area, improve compliance, and market differentiation. As cybersecurity-facilitating competitive advantage is preconditioned by the state of technology, and the training on an uninterrupted order, this will be even a more calming upgrade to cybersecurity (Sun et al., 2023; Panteleev, 2023).
4. **Strategic Cybersecurity Recommendation:** Significant strategies that beginups should implement to establish a credible reaction, promote compliance, differentiate solutions, and resiliency that converts cybersecurity innovation into measurable business accomplishment. Cyber insurance to indicate credibility to the stakeholders with security surveillance bodies that implement a vigilant security monitoring mechanism, proactive threat mitigation, and risk management frameworks (Jiang et al., 2023; Negrutiu et al., 2020).

Future Research and Future Action: It is desirable to push towards an empirical validation of conceptual framework in the form of cross country, cross sector research. Such research would give rise to the theoretical basis of the development of entrepreneurship in relation to cybersecurity innovation and some relevant recommendations that can be made to the producers and decision makers (Mohammed, 2023; Mmango & Gundu, 2023).

REFERENCES

1. Aliyu Mohammed. (2023). *A study on HR strategies for managing talents in global perspective.* IMCSM23, University of Belgrade.

2. Aliyu Mohammed. (2023, May 11). *An agile performance management system for achieving sustainable Industry 4.0.* MSNIM Hybrid Conference.

3. Aliyu Mohammed. (2024). *Investigating reskilling and up-skilling efforts in IT and software development: Case study of Kano State, Nigeria.* International Conference on Paradigm Shift Towards Sustainable Management & Digital Practices.

4. Anisetti, M., Ardagna, C., Cremonini, M., Sessa, J., Costa, L. (2020). *Security Threat Landscape.* Security Threats.

5. Astebro, T.B., Tåg, J. (2015). *Entrepreneurship and Job Creation.* https://papers.ssrn.com/abstract=2576044

6. Chen, X., Wu, D., Chen, L., Teng, J.K.L. (2018). *Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables.* Information & Management. https://doi.org/10.1016/j.im.2018.05.011

7. Chua, H.N., Wong, S.F., Low, Y.C., Chang, Y. (2018). *Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations.* Telematics and Informatics, 35, 1770–1780. https://doi.org/10.1016/j.tele.2018.05.005

8. Chui, K.T. (2022). *Building Digital Trust: Challenges and Strategies in Cybersecurity*. 5.

9. Coyne, K.P. (1986). *Sustainable competitive advantage—What it is, what it isn't.* Business Horizons, 29, 54–61. https://doi.org/10.1016/0007-6813(86)90087-X

10. Craig, J. (2018). *Cybersecurity Research—Essential to a Successful Digital Future.* Engineering, 4, 9–10. https://doi.org/10.1016/j.eng.2018.02.006

11. Davidsson, P., Delmar, F., Wiklund, J. (2017). *Entrepreneurship as Growth: Growth as Entrepreneurship.* In *Strategic Entrepreneurship*, 328–342. John Wiley & Sons. https://doi.org/10.1002/9781405164085.ch15

12. Filion, L.J. (2021). *Defining the entrepreneur*. In *World Encyclopedia of Entrepreneurship*, 72–83. Edward Elgar Publishing.

13. Fornell, C., III, F.V.M., Hult, G.T.M., VanAmburg, D. (2020). *The Reign of the Customer: Customer-Centric Approaches to Improving Satisfaction.* Springer Nature.

14. Gharbaoui, O.E., Boukhari, H.E. (2023). *Navigating the digital landscape: A roadmap to competitive advantage: Theoretical overview.* African Journal of Business and Finance, 1, 63–73.

15. Gundu, T. (2013). *Towards an information security awareness process for engineering SMEs in emerging economies.*

16. Gundu, T. (2019). *Big Data, Big Security, and Privacy Risks.* Journal of Information Warfare, 18, 15–30.

17. Gundu, T., Maronga, M.I., Boucher, D. (2019). *Industry 4.0 Business Perspective: Fostering a Cyber Security Culture in a Culturally Diverse Workplace.* Proceedings of 4th International Conference on the, 85–94.

18. Gundu, T., Mmango, N. (2024). *A Cybersecurity Collaborative Model: Best Practices Sharing Among South African Tourism and Hospitality Businesses.* ICTR, 7, 222–231. https://doi.org/10.34190/ictr.7.1.2159

19. Gundu, T., Modiba, N. (2020). *Building Competitive Advantage from Ubuntu: An African Information Security Awareness Model.* ICISSP, 569–576.

20. Jebril, I., Almaslmani, R., Jarah, B., Mugableh, M., Zaqeeba, N. (2023). *The impact of strategic intelligence and asset management on enhancing competitive advantage: The mediating role of cybersecurity.* Uncertain Supply Chain Management, 11, 1041–1046.

21. Jiang, N.N., Loukas, A., Wang, P., Wu, H. (2023). *Sometimes Less is More: Risk Aversion, Balanced Growth, and the (sub) Optimality of Entrepreneurial Insurance*, 1–21.

22. Klonek, F.E., Isidor, R., Kauffeld, S. (2015). *Different Stages of Entrepreneurship: Lessons from the Transtheoretical Model of Change.* Journal of Change Management, 15, 43–63. https://doi.org/10.1080/14697017.2014.918049

23. Knight, G., Moen, Madsen, T.K. (2020). *Antecedents to differentiation strategy in the*

exporting SME. International Business Review, 29, 101740. https://doi.org/10.1016/j.ibusrev.2020.101740

24. Kosutic, D., Pigni, F. (2020). *Cybersecurity: investing for competitive outcomes.* Journal of Business Strategy, 43, 28–36. https://doi.org/10.1108/JBS-06-2020-0116

25. Kumar, M. A., Mohammed, A., Raj, P., Sundaravadivazhagan, B. (2024). *Entrepreneurial strategies for mitigating risks in smart manufacturing environments.* In *AI solutions for cyber-physical systems*, pp. 165–179. Auerbach Publications.

26. Lawal, T. O., Abdulsalam, M., Mohammed, A., Sundararajan, S. (2023). *Economic and environmental implications of sustainable agricultural practices in arid regions.* IJMST, 10(3), 3100–3114. https://doi.org/10.15379/ijmst.v10i3.3027

27. Mitrofan, A.-L., Cruceru, E.-V., Barbu, A. (2020). *Determining the Main Causes that Lead to Cybersecurity Risks in SMEs.* Business Excellence and Management, 10, 38–48.

28. Mmango, N., Gundu, T. (2023). *Cyber Resilience in the Entrepreneurial Environment: A Framework for Enhancing Cybersecurity Awareness in SMEs*. ICECET, 1–6. https://doi.org/10.1109/ICECET58911.2023.10389226

29. Mohammed, A. (2023). *Analyzing global impacts and challenges in trade management: A multidisciplinary study*. ECTU, 3.

30. Mohammed, A. (2023). *Navigating the digital marketplace: Strategies for entrepreneurship in electronic commerce.* CAIJ, 10(3/4). https://airccse.com/caij/papers/10423caij06.pdf

31. Mohammed, A. (2023). *Strategic utilization of management information systems for efficient organizational management in the age of big data.* CAIJ, 10(3/4). https://airccse.com/caij/papers/10423caij02.pdf

32. Mohammed, A., Jakada, M. B., Lawal, T. O. (2023). *Examining the impact of managerial attitude on employee performance and organizational outcomes: A conceptual analysis.* IJBRE, 4(1), 1115–9146.

33. Mohammed, A., Shanmugam, S., Subramani, S. K., Pal, S. K. (2024). *Impact of strategic human resource management on mediating the relationship between entrepreneurial ventures and sustainable growth.* Serbian Journal of Management. https://doi.org/10.5937/IMCSM24044M

34. Mohammed, A., Sundararajan, S. (2023). *Analyzing policy challenges in the financial sector: Implications for effective financial management.* In *Digitalization of the banking and financial system*, pp. 32–43. ISBN: 978-93-91772-80-2

35. Mohammed, A., Sundararajan, S. (2023). *Emerging trends of business transformation.* MSNIM Management Review, 1, 36–44.

36. Mohammed, A., Sundararajan, S. (2023). *Exploring the dynamic interplay between startups and entrepreneurship: A conceptual analysis.* In *Digital startup*, pp. 1–7. ISBN: 978-93-93376-66-4

37. Muhammed, A., Sundararajan, S., Lawal, T. (2022). *The effect of training on the performance of SMEs in Kano Metropolis.* Seybold Report, 17(6).

38. Muktar, B.G., Idrissa, Y.L., Orifah, M.O., Nwachukwu, I.M. (2022). *Innovation Centric Extension Services and ICT Benevolence: Implications for Local Innovation Generation and Agripreneurial Promotion for Sustainable Food Systems.* Journal of Agricultural Extension, 27, 26–37.

39. Negrutiu, C., Vasiliu, C., Enache, C. (2020). *Sustainable Entrepreneurship in the Transport and Retail Supply Chain Sector*. Journal of Risk and Financial Management, 13, 267. https://doi.org/10.3390/jrfm13110267

40. Panteleev, D.N. (2023). *Cybersecurity for the Stimulation of Entrepreneurship Development in the Digital Economy Markets.* In Popkova, E.G., Sergi, B.S. (Eds.), Anti-Crisis Approach to the Provision of the Environmental Sustainability of Economy, 263–271. Springer. https://doi.org/10.1007/978-981-99-2198-0_28

41. Ramoglou, S., Gartner, W.B., Tsang, E.W.K. (2020). *"Who is an entrepreneur?" is (still) the*

wrong question. Journal of Business Venturing Insights, 13, e00168. https://doi.org/10.1016/j.jbvi.2020.e00168

42. Saeed, S. (2023). *A Customer-Centric View of E-Commerce Security and Privacy.* Applied Sciences, 13, 1020. https://doi.org/10.3390/app13021020

43. Shanmugam Sundararajan, S., Rajkumar, T., Senthil Kumar, T., Mohammed, A., Prince Martin, V. (2024). *An analytical study on factors influencing individual investors' investment decisions on selecting private commercial banks at Kano City, Nigeria.* European Chemical Bulletin, 12(1), 3706–3717. https://doi.org/10.31838/ecb/2023.12.s1-B.372

44. Sharma, S., Rautela, S. (2021). *Entrepreneurial resilience and self-efficacy during global crisis: study of small businesses in a developing economy.* Journal of Entrepreneurship in Emerging Economies, 14, 1369–1386.

45. Stanworth, J., Stanworth, C., Granger, B., Blyth, S. (1989). *Who Becomes an Entrepreneur?* International Small Business Journal, 8, 11–22. https://doi.org/10.1177/026624268900800101

46. Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., Zhang, J. (2023). *Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives.* IEEE Communications Surveys & Tutorials, 25, 1748–1774. https://doi.org/10.1109/COMST.2023.3273282

47. Sundararajan, S., & Mohammed, A. (2022). *Entrepreneurial opportunities for women.* European Journal of Humanities and Educational Advancements, Special Issue 1, 112–115. 50.

48. Sundararajan, S., & Mohammed, A. (2023). *Evaluation of teachers – History to current era.* Samzodhana – Journal of Management Research, 13(2). http://eecmbajournal.in

49. Sundararajan, S., Mohammed, A., Lawal, T. (2023). *Role of human resource management in the post COVID-19 era: Experiential study.* Bio Gecko, 12(2).

50. Sundararajan, S., Mohammed, A., Senthil Kumar, S. (2023). *A perceptual study on the impact of agile performance management system in IT companies.* Scandinavian Journal of Information Systems, 35(1), 3–38. https://doi.org/10.5281/SJIS.77516

51. Sundararajan, S., Mohammed, M. A., Senthil Kumar, S. (2022). *A perceptual study on impact of agile performance management system in IT companies.* Scandinavian Journal of Information Systems, 34(2), 3–38.

52. Wen-Cheng, W., Chien-Hung, L., Ying-Chien, C. (2011). *Types of Competitive Advantage and Analysis.* IJBM, 6, p100. https://doi.org/10.5539/ijbm.v6n5p100

Zhang, Y., Wang, H., Zhou, X. (2020). *Dare to Be Different? Conformity Versus Differentiation in Corporate Social Activities of Chinese Firms and Market Responses.* AMJ, 63, 717–742. https://doi.org/10.5465/amj.2017.0412