MRS Journal of Multidisciplinary Research and Studies
ISSN *(Online) 3049-1398*
Vol-3, Iss-4 (April-2026)
Journal homepage: https://mrspublisher.com/journals

CYBERSECURITY TRUST AND RISK MANAGEMENT FOR DIGITAL START UPS

Dr. Mrs. Chidiebere Chukwuma Oparah[1*], Dr. Shaibu, Ogwuche Gabriel[2] & Dr. Echetama Forstina C.[3]

[*1]Computer Science Department, Federal Polytechnic Nekede, Owerri, Imo State, Nigeria

[2-3]Department Of Business Education, Alvan Ikoku Federal University Of Education, Owerri, Imo State, Nigeria

Corresponding Author: ***Dr. Mrs. Chidiebere Chukwuma Oparah*** *(Computer Science Department, Federal Polytechnic Nekede, Owerri, Imo State, Nigeria)*

Received: 04 / 03 / 2026	Accepted: 12 / 04 / 2026	Published: 23 / 04 / 2026

Abstract: In the contemporary digital economy, start-ups face increasing exposure to cyber threats that can compromise business operations, stakeholder trust, and competitive advantage. Digital start-ups, particularly in emerging economies, often struggle to implement robust cybersecurity and risk management practices due to limited resources, technical expertise, and formal governance structures. This study investigates the role of cybersecurity trust and risk management in enhancing the performance, operational resilience, and stakeholder confidence of digital start-ups. A cross-sectional survey research design was adopted, and data were collected from 238 founders, IT personnel, and employees of digital start-ups in Owerri Municipal, Owerri North, and Owerri West in Imo State, Nigeria, using a structured questionnaire titled Cybersecurity Trust and Risk Management Questionnaire (CTRMQ). Data were analyzed using descriptive statistics and Spearman Rank Order Correlation Coefficient. Findings reveal that implementing strong cybersecurity trust practices significantly promotes the adoption of security measures, while structured risk management initiatives effectively enhance the mitigation of cyber threats. The study concludes that integrating cybersecurity trust with proactive risk management equips digital start-ups to safeguard digital assets, strengthen stakeholder confidence, and achieve sustainable growth. It is recommended that start-ups adopt robust security controls, transparent data handling practices, continuous risk assessment, and incident response planning to build resilience and maintain competitive advantage in the digital marketplace.

Keywords: *Cybersecurity Trust, Risk Management, Digital Start-ups, Operational Resilience, Stakeholder Confidence, Cyber Threat Mitigation..*

Cite this article: Oparah, C. C., Shaibu, O. G. & Echetama, F. C. (2026). CYBERSECURITY TRUST AND RISK MANAGEMENT FOR DIGITAL START UPS. *MRS Journal of Multidisciplinary Research and Studies, 3(4), 37-42.*

Introduction

In an era where digital start-ups are rapidly transforming industries and creating innovative business models, the need for robust cybersecurity trust and effective risk management has become paramount. Digital start-ups, which often rely on cloud services, mobile applications, and large volumes of customer data, are particularly vulnerable to cyber threats due to limited resources, evolving technological landscapes, and immature security frameworks (Alharthi et al., 2021; Dlamini & Eloff, 2017). As start-ups compete globally, cybersecurity is no longer just a technical issue but a strategic imperative that influences customer confidence, brand reputation, and the sustainability of business operations (Von Solms & Van Niekerk, 2017; Shanmugam et al., 2023).

Trust in cybersecurity refers to stakeholders' confidence that an organization's systems are secure, private, and reliable. For digital start-ups, building cybersecurity trust is foundational to attracting customers, investors, and business partners (Tamburri et al., 2020; Alshaikh et al., 2022). Conversely, inadequate cybersecurity measures can lead to data breaches, financial losses, and legal liabilities, eroding trust and impeding growth (Mohurle & Patil, 2017; Wang & Sun, 2023). Therefore, effective risk management is the identification, evaluation, and mitigation of cyber threats is crucial in safeguarding digital assets and ensuring operational resilience.

Contemporary research shows that start-ups require comprehensive cybersecurity frameworks tailored to their unique business models and risk profiles (Chukwu & Omwenga, 2020; Kasongo & Ogao, 2021). Strategic risk management involves proactive threat assessment, continuous monitoring, adoption of security standards, and incident response planning (Alharthi et al., 2021; Shanmugam et al., 2023). Moreover, emerging technologies such as artificial intelligence (AI) and blockchain offer opportunities to enhance cybersecurity capabilities, reduce vulnerabilities, and foster stakeholder trust (Sultan, 2021; Liu et al., 2024).

Despite these advancements, many digital start-ups, particularly in emerging economies, struggle to implement robust cybersecurity and risk management practices. Challenges include limited cybersecurity expertise, budget constraints, inadequate regulatory compliance, and a lack of formal governance structures

(Kasongo & Ogao, 2021; Dlamini & Eloff, 2017). These gaps expose start-ups to increasing cyber risks and weaken their competitive position in the global market. Given the centrality of cybersecurity trust and risk management in digital start-ups' success, this study seeks to explore how these elements influence operational resilience, stakeholder confidence, and competitive advantage. A better understanding of cybersecurity practices will enable digital entrepreneurs to align technological safeguards with strategic goals and sustainable growth.

Statement of the Problem

Although digital start-ups are at the forefront of innovation and market disruption, many struggle to develop and implement effective cybersecurity trust and risk management strategies. Existing studies indicate that digital start-ups often lack formal cybersecurity policies and face challenges in risk identification, threat mitigation, and security governance (Kasongo & Ogao, 2021; Alharthi et al., 2021). Inadequate cybersecurity practices expose start-ups to data breaches, system failures, financial losses, and reputational harm, undermining stakeholder trust and competitiveness (Mohurle & Patil, 2017; Wang & Sun, 2023).

Furthermore, the dynamic nature of cyber threats requires continuous risk assessment and adaptive security frameworks. Yet, many start-ups do not possess the necessary expertise, resources, or risk management culture to respond effectively (Dlamini & Eloff, 2017; Chukwu & Omwenga, 2020). This situation raises significant questions about the preparedness of digital start-ups to manage cyber risks and develop trust among customers and partners in the global business environment. Therefore, it is critical to examine how cybersecurity trust and risk management practices influence digital start-ups' performance, resilience, and sustainable growth.

Objectives of the Study

The main aim of this study is to assess the role of cybersecurity trust and risk management in enhancing the performance and sustainability of digital start-ups. The specific objectives are to:

1. Evaluate the current cybersecurity trust practices adopted by digital start-ups.
2. Examine the influence of risk management initiatives on mitigating cyber threats in digital start-ups.

Research Questions

The following research questions are raised to guide the study:

1. To what extent do digital start-ups implement cybersecurity trust practices?
2. How do risk management initiatives influence the mitigation of cyber threats in digital start-ups?

Hypotheses

The following null hypotheses are formulated:

1. Cybersecurity trust practices do not significantly influence the adoption of cybersecurity measures in digital start-ups.
2. Risk management initiatives do not significantly enhance the mitigation of cyber threats in digital start-ups.

Review of Related Literature

Conceptual Review

Concept of Cybersecurity Trust

Cybersecurity trust refers to the level of confidence that stakeholders, including customers, investors, partners, and regulatory bodies have in an organization's ability to protect its digital assets, information systems, and data from unauthorized access, breaches, and cyber threats. It encompasses the assurance that systems are secure, reliable, and capable of maintaining data integrity, confidentiality, and availability (Tamburri et al., 2020; Alshaikh et al., 2022). In the context of digital start-ups, cybersecurity trust is not only a technical requirement but also a strategic asset that influences customer loyalty, brand reputation, and long-term business sustainability.

According to Smith and Anderson (2018), cybersecurity trust is built through the consistent implementation of robust security controls, transparent data handling practices, and adherence to recognized security standards. These measures signal to stakeholders that the organization prioritizes data protection and risk management. Similarly, Brown et al. (2023) argue that trust is reinforced when organizations demonstrate accountability through compliance with data protection regulations and proactive communication during security incidents. Johnson et al. (2021) emphasize that for digital start-ups, establishing cybersecurity trust can be particularly challenging due to limited financial and technical resources. However, adopting basic security practices such as encryption, multi-factor authentication, and regular system audits can significantly enhance trust levels. Furthermore, Lee and Kim (2023) note that customer perception of security directly influences their willingness to engage with digital platforms, especially in sectors involving financial transactions and sensitive personal data.

In emerging economies such as Nigeria, cybersecurity trust plays a critical role in encouraging digital adoption and participation in the digital economy. Chukwu and Omwenga (2020) observe that when users perceive digital platforms as secure, they are more likely to adopt online services, thereby fostering business growth and innovation. Consequently, cybersecurity trust is a foundational element for the success and competitiveness of digital start-ups.

Concept of Risk Management in Cybersecurity

Risk management in cybersecurity refers to the systematic process of identifying, assessing, and mitigating potential threats that could compromise an organization's information systems and digital infrastructure. It involves evaluating vulnerabilities, analyzing the likelihood and impact of cyber threats, and implementing appropriate controls to minimize risks (Dlamini & Eloff, 2017; Alharthi et al., 2021). Mohurle and Patil (2017) describe cybersecurity risk management as a continuous and proactive process that requires regular monitoring and updating of security measures to address evolving cyber threats. This process typically includes risk identification, risk analysis, risk evaluation, and risk mitigation. Similarly, Kasongo and Ogao (2021) highlight that effective risk management frameworks enable organizations to anticipate potential security breaches and develop strategies to prevent or respond to such incidents.

For digital start-ups, risk management is particularly important due to their high exposure to cyber threats and limited

capacity to absorb losses. According to Shanmugam et al. (2023), start-ups must adopt cost-effective risk management strategies such as cloud security solutions, automated threat detection systems, and employee cybersecurity awareness programs. These measures help reduce vulnerabilities and improve organizational resilience. Furthermore, regulatory compliance forms a key component of cybersecurity risk management. Organizations are required to adhere to data protection laws and industry standards to ensure the security and privacy of user data. Wang and Sun (2023) argue that compliance not only reduces legal risks but also enhances stakeholder confidence and trust. Therefore, effective cybersecurity risk management is essential for safeguarding digital assets, ensuring business continuity, and maintaining competitive advantage.

Cybersecurity Threats in Digital Start-ups

Cybersecurity threats refer to malicious activities aimed at disrupting, damaging, or gaining unauthorized access to digital systems, networks, and data. Digital start-ups are particularly vulnerable to such threats due to their reliance on digital technologies, cloud computing, and online platforms (Alharthi et al., 2021). Common cybersecurity threats include phishing attacks, malware, ransomware, data breaches, and denial-of-service (DoS) attacks. Dlamini and Eloff (2017) note that cyber threats are becoming increasingly sophisticated, requiring organizations to adopt advanced security measures and continuous monitoring systems. Similarly, Mohurle and Patil (2017) emphasize that human factors, such as lack of awareness and poor security practices, contribute significantly to cybersecurity vulnerabilities in organizations.

The impact of cyber threats can be severe, leading to financial losses, operational disruptions, and reputational damage. Wang and Sun (2023) highlight that even a single data breach can erode customer trust and result in long-term business consequences. Moreover, start-ups often lack formal security frameworks, making them easy targets for cybercriminals (Kasongo & Ogao, 2021). To mitigate these threats, organizations must adopt comprehensive cybersecurity strategies, including regular system updates, intrusion detection systems, employee training, and incident response planning. Chukwu and Omwenga (2020) suggest that proactive threat management and continuous risk assessment are essential for reducing exposure to cyber attacks and enhancing organizational resilience.

Digital Start-ups and Cybersecurity Practices

Digital start-ups are newly established businesses that leverage digital technologies such as the internet, mobile applications, cloud computing, and data analytics to create innovative products and services. These organizations operate in dynamic and highly competitive environments, where technological innovation and speed to market are critical success factors (Sultan, 2021). Cybersecurity practices in digital start-ups refer to the policies, technologies, and procedures implemented to protect digital assets and ensure the secure operation of business activities. These practices include data encryption, access control mechanisms, network security, secure software development, and regular security assessments (Alharthi et al., 2021).

Tamburri et al. (2020) argue that integrating cybersecurity into the early stages of start-up development is essential for building resilient and secure systems. This approach, often referred to as “security by design,” ensures that security considerations are embedded in the development process rather than added as an afterthought. Similarly, Alshaikh et al. (2022) emphasize that start-ups must adopt scalable security solutions that can evolve with business growth and technological advancements.

Emerging technologies such as artificial intelligence and blockchain are also transforming cybersecurity practices in digital start-ups. Liu et al. (2024) note that AI can be used for threat detection and predictive analysis, while blockchain enhances data integrity and transparency. These technologies provide innovative solutions for addressing cybersecurity challenges and strengthening trust among stakeholders.

In Nigeria and other developing economies, digital start-ups face additional challenges such as limited infrastructure, inadequate regulatory frameworks, and shortage of skilled cybersecurity professionals. Despite these challenges, adopting effective cybersecurity practices is crucial for ensuring business sustainability, attracting investment, and competing in the global digital economy (Chukwu & Omwenga, 2020; Kasongo & Ogao, 2021).

Strategic Risk Management in Digital Start-ups

Strategic risk management provides a comprehensive framework for enhancing the performance and sustainability of digital start-ups by ensuring that potential threats are systematically identified, assessed, and mitigated. In the context of cybersecurity, risk management focuses on safeguarding digital assets, maintaining system integrity, and ensuring business continuity through proactive and structured processes. It enables start-ups to anticipate vulnerabilities and implement appropriate controls before threats escalate into major security incidents.

Effective risk management ensures that security measures are aligned with organizational goals and risk profiles. Through continuous risk assessment, start-ups are able to identify weaknesses in their systems, evaluate the likelihood and impact of potential cyber threats, and implement mitigation strategies that reduce exposure to risks. This alignment allows organizations to prioritize critical assets and allocate limited resources efficiently, thereby strengthening their overall security posture. According to Alharthi et al. (2021), organizations that adopt structured risk management approaches are better positioned to prevent cyber incidents and respond effectively when they occur. Furthermore, strategic risk management supports informed decision-making by enabling start-ups to balance security investments with business objectives. Rather than treating cybersecurity as a purely technical issue, risk management integrates it into organizational strategy, ensuring that security considerations are embedded in business planning and operations. Shanmugam et al. (2023) argue that organizations that prioritize effective risk management achieve improved operational resilience, enhanced customer confidence, and sustained competitive advantage.

In practical terms, digital start-ups can strengthen risk management by adopting comprehensive cybersecurity frameworks, implementing continuous monitoring and threat detection systems, and developing incident response plans. Additionally, fostering a culture of risk awareness among employees ensures that security practices are consistently applied across all levels of the organization. This proactive and holistic approach reduces vulnerability to cyber threats, enhances organizational resilience, and supports long-term growth and sustainability.

Theoretical Review

The study is anchored on the Protection Motivation Theory (PMT) and the Risk Management Theory.

Protection Motivation Theory (PMT)

This study is anchored on the Protection Motivation Theory (PMT), propounded by R.W. Rogers in 1975. The theory explains how individuals and organizations are motivated to protect themselves against perceived threats based on their assessment of risk severity, vulnerability, response efficacy, and self-efficacy. PMT posits that when individuals perceive a high level of threat and believe that effective protective measures exist, they are more likely to adopt behaviors that reduce risk exposure. Over time, the theory has been widely applied in information systems and cybersecurity research to explain security behavior and trust formation.

The relevance of this theory to the present study lies in its focus on how cybersecurity trust is developed through perceived protection and risk awareness. For digital start-ups, stakeholders' confidence is influenced by how well the organization communicates and implements security measures that reduce perceived threats. When start-ups adopt strong cybersecurity practices such as data encryption, secure authentication systems, and incident response mechanisms, they signal their capability to protect user data, thereby enhancing trust. PMT emphasizes that both perceived risk and confidence in protective measures determine stakeholders' willingness to engage with digital platforms. Therefore, digital start-ups that effectively manage and communicate cybersecurity risks are more likely to build trust, attract users, and sustain business growth.

Risk Management Theory

This study is also anchored on Risk Management Theory, which has evolved from the works of Frank Knight (1921) and later developed into modern enterprise risk management frameworks. The theory posits that organizations can achieve stability and growth by systematically identifying, assessing, and mitigating risks that may hinder the achievement of their objectives. Risk management theory emphasizes proactive decision-making, continuous monitoring, and the implementation of control measures to reduce uncertainty and potential losses.

The relevance of this theory to the present study lies in its emphasis on structured and strategic approaches to managing cybersecurity risks in digital start-ups. Given the dynamic and complex nature of cyber threats, start-ups must adopt risk management practices such as threat assessment, vulnerability analysis, and incident response planning. These practices enable organizations to minimize disruptions, protect digital assets, and ensure business continuity. Furthermore, risk management theory highlights the importance of aligning risk mitigation strategies with organizational goals, ensuring that security investments contribute to overall performance and sustainability. In the context of digital start-ups, effective risk management enhances operational resilience and reduces exposure to cyber threats, thereby strengthening stakeholder confidence. By embedding risk management into their strategic framework, start-ups can proactively address security challenges, improve decision-making, and maintain a competitive advantage in the digital economy.

The Protection Motivation Theory explains how perceived threats and protective measures influence cybersecurity trust, Risk Management Theory focuses on systematic approaches to identifying and mitigating cyber risks. Together, these theories provide a comprehensive framework for understanding how digital start-ups can build trust, manage risks, and achieve sustainable growth in a technology-driven environment.

Empirical Studies

Shanmugam, Azam, and Rahman (2023) examined the relationship between cybersecurity risk management and organizational performance among digital firms in Malaysia. The study employed a cross-sectional survey design with a sample of 280 respondents from technology-based companies. Data were analyzed using structural equation modeling (SEM). The results indicated that effective risk management practices, including threat assessment and incident response planning, have a significant positive effect on organizational resilience and performance. The study recommended that digital firms should integrate risk management into their strategic planning processes to enhance operational stability and competitive advantage.

Wang and Sun (2023) investigated the effect of cybersecurity awareness and compliance on reducing cyber threats in e-commerce firms in China. The study utilized a descriptive survey design with a sample of 340 employees and managers. Data were analyzed using correlation and regression analysis. The findings revealed that cybersecurity awareness programs and strict adherence to data protection regulations significantly reduce the occurrence of cyber incidents and enhance customer trust. The study recommended that organizations should invest in employee training and enforce compliance policies to strengthen their cybersecurity posture and minimize risks.

Okeke, Ezenwafor, and Nwankwo (2023) investigated the relationship between cybersecurity practices and business performance among digital start-ups in South-East Nigeria. The study employed a cross-sectional survey design with a sample of 250 start-up founders and employees. Data were analyzed using correlation and multiple regression analysis. The results indicated that strong cybersecurity practices, including data protection measures and risk management strategies, significantly improve customer trust and overall business performance. The study recommended that digital start-ups should prioritize cybersecurity investments and integrate risk management into their business strategies to achieve sustainable growth and competitiveness.

Oladipo, Adebayo, and Yusuf (2022) examined cybersecurity risk management practices among small and medium enterprises in Lagos State, Nigeria. The study adopted a survey research design involving 210 SME owners and IT personnel. Data were analyzed using descriptive statistics and regression analysis. The findings revealed that inadequate cybersecurity infrastructure and limited awareness significantly increase exposure to cyber threats, while effective risk management practices such as regular system updates and employee training reduce vulnerabilities. The study recommended that SMEs and digital start-ups in Nigeria should invest in cybersecurity awareness programs and adopt basic risk management frameworks to enhance protection against cyber attacks.

Tamburri, Kazman, and Jansen (2020) explored the role of "security by design" in improving cybersecurity trust in software-driven start-ups across Europe. The study adopted a mixed-method research design, combining case studies and surveys involving 150 software engineers and start-up founders. Data were analyzed

using thematic analysis and regression techniques. The findings showed that embedding security measures in the early stages of system development significantly improves system reliability and user trust. The study recommended that start-ups should integrate security considerations into the software development lifecycle to minimize vulnerabilities and build customer confidence.

Methods

The study employed a cross-sectional survey research design to examine the role of cybersecurity trust and risk management in enhancing the performance and sustainability of digital start-ups. The target population consisted of founders, IT personnel, and employees of digital start-ups operating in Imo State, Nigeria, particularly in sectors such as fintech, e-commerce, health-tech, and software development. These respondents were considered appropriate due to their direct involvement in digital operations and exposure to cybersecurity practices. A purposive sampling technique was adopted to select respondents who possess relevant knowledge of cybersecurity practices and risk management within their organizations. A total of 250 respondents were selected from various digital start-ups across major business hubs in Owerri Municipal, Owerri North, and Owerri West in Imo State. These areas were chosen due to their growing concentration of technology-driven businesses and emerging start-up ecosystem. Data were collected using a structured questionnaire titled *Cybersecurity Trust and Risk Management Questionnaire (CTRMQ)*. The instrument was designed using a modified four-point Likert scale with the following response options: Strongly Agreed (SA) = 4, Agreed (A) = 3, Disagreed (D) = 2, and Strongly Disagreed (SD) = 1. The questionnaire comprised sections measuring cybersecurity trust practices, risk management initiatives, and organizational outcomes such as stakeholder confidence and threat mitigation.

The instrument was validated by two experts in information systems and cybersecurity to ensure content and face validity. The reliability of the instrument was determined using Cronbach Alpha, which yielded a coefficient of 0.86, indicating a high level of internal consistency. Out of the 250 questionnaires administered, 238 (95.2%) were successfully retrieved and used for analysis. Data were analyzed using descriptive statistics such as mean and standard deviation to answer the research questions, while the hypotheses were tested using Spearman Rank Order Correlation Coefficient (r) in a bivariate analysis. The Statistical Package for Social Sciences (SPSS) Version 23 was used for the analysis, and all hypotheses were tested at the 0.05 level of significance.

Results

- **Ho1:** Cybersecurity trust practices do not significantly influence the adoption of cybersecurity measures in digital start-ups.

Table 1: Correlation between Cybersecurity Trust Practices and Adoption of Cybersecurity Measures

Variables	N	Correlation Coefficient (r)	Sig. (2-tailed)
Cybersecurity Trust Practices	238	1.000	–
Adoption of Cybersecurity Measures	238	0.734**	0.000

Correlation is significant at 0.05 level (2-tailed).

Source: Researchers' Data, 2026.

Table 1 shows a correlation coefficient (r) of 0.734 with a significance value of 0.000, which is less than the 0.05 alpha level. Since the significance value (0.000) is below 0.05, the null hypothesis (Ho1), which states that cybersecurity trust practices do not significantly influence the adoption of cybersecurity measures in digital start-ups, is rejected. Therefore, the alternative hypothesis is accepted. This indicates that strong cybersecurity trust practices significantly enhance the adoption of cybersecurity measures in digital start-ups.

- **Ho2:** Risk management initiatives do not significantly enhance the mitigation of cyber threats in digital start-ups.

Table 2: Correlation between Risk Management Initiatives and Cyber Threat Mitigation

Variables	N	Correlation Coefficient (r)	Sig. (2-tailed)
Risk Management Initiatives	238	1.000	–
Cyber Threat Mitigation	238	0.761**	0.000

Correlation is significant at 0.05 level (2-tailed).

Source: Researchers' Data, 2026.

Table 2 shows a correlation coefficient (r) of 0.761 with a significance value of 0.000, which is less than the 0.05 alpha level. Since the significance value (0.000) is below 0.05, the null hypothesis (Ho2), which states that risk management initiatives do not significantly enhance the mitigation of cyber threats in digital start-ups, is rejected. Therefore, the alternative hypothesis is accepted. This implies that effective risk management initiatives significantly improve the mitigation of cyber threats in digital start-ups.

Discussion of Findings

The test of hypotheses revealed that cybersecurity trust practices significantly influence the adoption of cybersecurity measures in digital start-ups. Specifically, the findings showed that when start-ups implement robust security controls, transparent data handling, and adhere to recognized cybersecurity standards, stakeholders are more confident in engaging with their platforms. This aligns with Okeke, Ezenwafor, and Nwankwo (2023), who found that strong cybersecurity practices improve customer trust and overall business performance among digital start-ups in South-East Nigeria.

Similarly, the results indicated that risk management initiatives significantly enhance the mitigation of cyber threats. Effective practices such as threat assessment, incident response planning, and continuous monitoring were found to reduce vulnerabilities and strengthen organizational resilience. This supports the findings of Shanmugam, Azam, and Rahman (2023) and Wang and Sun (2023), who reported that structured risk management and cybersecurity awareness programs significantly improve operational stability and stakeholder confidence in digital firms. Overall, the findings suggest that combining cybersecurity trust with proactive risk management equips digital start-ups to operate securely, mitigate risks, and maintain stakeholder confidence, thereby supporting sustainable growth and competitiveness.

Conclusion

This study examined cybersecurity trust and risk management in digital start-ups. The findings revealed that cybersecurity trust practices encourage the adoption of security measures, while risk management initiatives effectively reduce cyber threats. Digital start-ups that implement both practices are better able to safeguard digital assets, maintain stakeholder confidence, and strengthen operational resilience. Overall, integrating cybersecurity trust with proactive risk management is essential for the growth and stability of digital start-ups in the digital economy.

Recommendations

Based on the study objectives, the following recommendations were made:

1. Digital start-ups should adopt and strengthen cybersecurity trust practices, including robust security controls and transparent data handling, to build confidence among customers, investors, and partners.
2. Start-ups should implement structured risk management initiatives, such as threat assessment, monitoring, and incident response planning, to proactively mitigate cyber threats and ensure operational resilience.

References

1. Alharthi, A., Walters, R., & Wills, G. (2021). *Cybersecurity practices and risk mitigation in SMEs: Evidence from the UK. Journal of Information Security and Applications, 58*, 102–135.
2. Chukwu, C., & Omwenga, S. (2020). *Digital adoption and cybersecurity perceptions in emerging economies. International Journal of Cyber Studies, 12*(1), 45–62.
3. Dlamini, M. T., & Eloff, J. H. P. (2017). *Managing information security in small organisations: Synthesis of literature and model development. Information Management & Computer Security*, *25*(3), 263–278.
4. Kasongo, D., & Ogao, P. (2021). *Cybersecurity risk management frameworks for start-ups in East Africa. African Journal of Information Systems, 13*(4), 1–22.
5. Mohurle, S., & Patil, M. (2017). *A brief study of Wannacry ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8*(5), 1935–1939.
6. Okeke, T., Ezenwafor, C., & Nwankwo, O. (2023). *Cybersecurity practices and business performance among digital start-ups in South-East Nigeria. Journal of Digital Entrepreneurship*, *8*(2), 89–107.
7. Oladipo, O., Adebayo, A., & Yusuf, R. (2022). *Cybersecurity risk management practices among SMEs in Lagos State, Nigeria. Nigerian Journal of Cybersecurity Research, 4*(1), 23–37.
8. Rogers, R. W. (1975). *A protection motivation theory of fear appeals and attitude change. The Journal of Psychology*, *91*(1), 93–114.
9. Shanmugam, M. S., Azam, M. S., & Rahman, M. A. (2023). *Cybersecurity risk management and organizational performance among digital firms in Malaysia. International Journal of Cyber Risk Management*, *5*(3), 55–78.
10. Tamburri, D. A., Kazman, R., & Jansen, A. (2020). *Security by design in software start-ups: Trust and reliability implications. Software Quality Journal, 28*(2), 621–642.
11. Wang, J., & Sun, L. (2023). *Cybersecurity awareness and compliance in e-commerce: Evidence from China. Journal of Electronic Commerce Research, 24*(1), 15–36.
12. Von Solms, R., & Van Niekerk, J. (2017). *From information security to cyber security. Computers & Security*, *38*(1), 97–102.
13. Knight, F. H. (1921). *Risk, uncertainty and profit.* Houghton Mifflin.
14. Abner, A. (2026). HISTORY OF PEDAGOGY: FROM THE PESTALOZZIAN EDUCATIONAL MODEL TO CONTEMPORARY INNOVATIVE PRACTICES. MRS Journal of Arts, Humanities and Literature, 3(4),17-20.