International Journal of Management Technology
Vol.11, No 3, pp.17-41, 2024
Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Artificial Intelligence and Business Security among SMEs in Abuja Metropolis

[1] Chimezie Seth IZUGBOEKWE, [2] Sonia Sim JOSHUA, [3]Nasamu GAMBO (PhD), [4]Sijibomi Victor OLUBODUN, [5] Blessing Onyemowo AMEH
[1,2,3,4,5]Nile University of Nigeria, Abuja, Nigeria

doi: https://doi.org/10.37745/ijmt.2013/vol11n31741 Published July 16, 2024

Citation: Izugboekwe C.S., Joshua S.S., Gambo N., Olubodun S.V., and Ameh B.O. (2024) Artificial Intelligence and Business Security Among Smes in Abuja Metropolis, *International Journal of Management Technology*, Vol.11, No 3, pp.17-41

Abstract: *This study investigates the impact of Artificial Intelligence (AI) on business security among Small and Medium Enterprises (SMEs) in Abuja, Federal Capital Territory (FCT), Nigeria. The primary objectives are to assess the influence of AI security protocols, employee AI training, customer data privacy measures, and automated threat detection on enhancing business security. Anchored in the Socio-Technical Systems (STS) Theory, which emphasizes the interplay between social and technical elements within organizations, this research explores how these AI-driven measures collectively contribute to securing SMEs. Utilizing a cross-sectional survey design, data was collected from a representative sample of 379 employees within the Information and Communication sector, derived from an estimated population of 24,832 employees according to SMEDAN (2021). Multiple regression analysis revealed that AI security protocols, customer data privacy measures, and automated threat detection significantly enhance business security, while employee AI training showed no substantial impact. These findings underscore the necessity for integrating advanced technological measures with robust social frameworks to optimize business security. The study's results align with STS Theory, highlighting the importance of a balanced approach that incorporates both technical and social components for effective security management in SMEs.*

Keywords: artificial intelligence, business security, SMEs, AI security protocols, employee AI training, customer data privacy, automated threat detection, cybersecurity

INTRODUCTION

Artificial intelligence (AI) has become a cornerstone of modern business strategy, revolutionizing various aspects of operations, including security. For small and medium-sized enterprises (SMEs) in Abuja Federal Capital Territory (FCT), AI adoption is essential for enhancing business security amid escalating cyber threats. SMEs, which play a critical role in Nigeria's economy, often struggle with limited resources and expertise, making AI-driven security solutions not just beneficial but necessary (Okonkwo & Nwosu, 2023). Global research underscores the significant role of AI in bolstering business security. Key AI applications such as AI security protocols, employee AI training, customer data privacy measures, and automated threat detection systems have demonstrated effectiveness in strengthening security frameworks. Firms that integrate these AI solutions are better positioned to protect sensitive data, mitigate risks, and respond swiftly to security incidents, thereby ensuring operational continuity and maintaining customer trust (World Economic Forum, 2021).

For SMEs, the integration of AI technologies presents both opportunities and challenges. These businesses often operate under financial constraints and limited technical expertise, which complicates the effective implementation of AI solutions. In the context of Abuja FCT, where SMEs are rapidly expanding and facing intense competition, understanding the specific impacts of AI on business security is crucial.

The research focuses on four critical AI dimensions: AI security protocols, employee AI training, customer data privacy measures, and automated threat detection. These dimensions collectively contribute to a robust security framework. AI security protocols utilize advanced algorithms and machine learning to detect and prevent cyber threats in real time. Employee AI training equips staff with the skills necessary to effectively use AI tools to manage security risks. Customer data privacy measures leverage AI to safeguard sensitive information through encryption and access controls, enhancing trust and regulatory compliance. Automated threat detection employs AI to rapidly identify and address security breaches, minimizing potential damage and downtime (Okechukwu & Afolabi, 2022).

Despite the recognized benefits of AI for business security, there is a significant gap in the literature specifically addressing the Nigerian SME context, particularly in Abuja FCT. Global studies often overlook the unique challenges faced by Nigerian SMEs, which impedes the development of optimized AI strategies tailored to local conditions. For example, research by Eze and Chukwu (2023) highlights that Nigerian SMEs face unique cybersecurity challenges due to limited access to advanced technologies and expertise. Similarly, Akinbinu and Adedeji (2024) point out that while AI technologies are beneficial, their implementation is often hampered by financial and infrastructural constraints specific to Nigerian SMEs.

Furthermore, empirical evidence suggests that the effective adoption of AI in Nigerian SMEs is hindered by a lack of targeted training and development programs. A study by Okechukwu and Afolabi (2022) found that many SMEs in Nigeria lack the necessary skills to leverage AI technologies fully, resulting in suboptimal security practices. This gap underscores the need for tailored AI training programs that address the specific needs of Nigerian SMEs.

Moreover, the regulatory landscape in Nigeria presents additional challenges. As Okonkwo and Nwosu (2023) argue, compliance with international data protection standards is particularly challenging for Nigerian SMEs, which often lack the resources to implement comprehensive data privacy measures. This situation is exacerbated by the rapid pace of technological change, which outstrips the ability of many SMEs to keep up with new security protocols and technologies.

Addressing this research gap is critical for several reasons. Firstly, it enables the creation of tailored AI solutions that cater to the specific needs and constraints of SMEs in Abuja FCT, thereby improving their security capabilities. Secondly, it provides valuable insights for policymakers and business leaders aiming to promote the adoption of AI technologies in ways that support sustainable business practices and economic growth. Finally, region-specific research offers a deeper understanding of how local market conditions, regulatory environments, and technological readiness interact to influence the effectiveness of AI-driven security measures.
This study aims to achieve the following objectives:

i. To determine the impact of AI security protocols on business security among SMEs in Abuja FCT.
ii. To evaluate the impact of employee AI training on business security among SMEs in Abuja FCT.
iii. To assess the impact customer data privacy measures on business security among SMEs in Abuja FCT.
iv. To investigate the impact of automated threat detection on business security among SMEs in Abuja FCT.

In alignment with the study's objectives, the following null hypotheses are proposed:
H_{01}: AI security protocols have no significant impact on business security among SMEs in Abuja FCT.
H_{02}: Employee AI training have no significant impact on business security among SMEs in Abuja FCT.
H_{03}: Effective customer data privacy measures have no significant impact on business security among SMEs in Abuja FCT.
H_{04}: The use of automated threat detection systems have no significant impact on business security among SMEs in Abuja FCT.
This paper is organized into five distinct sections: Introduction, Literature Review, Methodology, Results and Findings and Conclusion

LITERATURE REVIEW

Conceptual Review

Business Security

Business security remains paramount for the stability and resilience of organizations, particularly within the dynamic landscape of Small and Medium Enterprises (SMEs) in Abuja FCT. It encompasses a multifaceted approach to safeguarding assets, operations, and stakeholders from diverse threats, including cyberattacks, theft, and operational disruptions (Sharma & Sharma, 2023). For SMEs operating in Abuja FCT's competitive business environment, robust business security is essential for maintaining trust with customers, sustaining competitiveness, and ensuring long-term viability (Ahmed et al., 2022). Effective business security measures not only protect physical and digital assets but also contribute to regulatory compliance, customer retention, and overall business continuity (Kumar & Pandey, 2023). As the dependent variable in this study, business security serves as a comprehensive metric reflecting the effectiveness of implemented security measures and their impact on organizational resilience and sustainability.

Moreover, business security extends beyond protection to encompass proactive risk management and strategic planning. SMEs in Abuja FCT face evolving security challenges, requiring adaptive and holistic security approaches (Srivastava & Choudhary, 2023). By investing in robust security protocols, employee training, and technology solutions, SMEs can mitigate potential risks, enhance operational efficiency, and foster a secure environment for conducting business (Singh & Singh, 2023). The effectiveness of business security measures directly correlates with organizational performance, customer trust, and competitive advantage, underscoring its significance as a critical determinant of SME success in Abuja FCT's business landscape.

Artificial Intelligence (AI) in Business Security

Artificial Intelligence (AI) technologies play a pivotal role in revolutionizing business security for SMEs in Abuja FCT, serving as independent variables in this study. AI-driven solutions offer advanced capabilities for threat detection, anomaly identification, and predictive analysis, empowering organizations to proactively mitigate security risks and respond swiftly to emerging threats (Wang & Zhou, 2023). The integration of AI in business security introduces a paradigm shift from reactive to proactive security measures, enabling SMEs to anticipate and address potential vulnerabilities before they escalate into security breaches (Li & Liu, 2023). By leveraging machine learning algorithms, behavioral analytics, and automated response mechanisms, SMEs can enhance their security posture, detect emerging threats, and fortify their resilience against evolving security challenges (Zhao et al., 2022).

Furthermore, AI's transformative impact on business security extends beyond traditional security paradigms to encompass diverse dimensions, including AI security protocols, employee AI training, customer data privacy measures, and automated threat detection (Chen & Li, 2023). AI security protocols entail systematic procedures and practices aimed at protecting digital assets and infrastructure using AI technologies, while employee AI training focuses on educating and upskilling staff members to utilize AI tools effectively for security purposes (Wu & Chen, 2023). Moreover, customer data privacy measures and automated threat detection leverage AI capabilities to safeguard sensitive information and detect security threats in real-time, respectively (Zhang & Wang, 2022). By harnessing the power of AI in business security, SMEs in Abuja FCT can enhance their resilience, adaptability, and competitiveness in an increasingly complex and interconnected business environment.

Theoretical Framework

The theoretical framework anchoring this study on "Artificial Intelligence and Business Security among SMEs in Abuja FCT" is the Socio-Technical Systems Theory (STS). Originally developed by Eric Trist and Ken Bamforth, STS theory emphasizes the interrelatedness of social and technical aspects within an organization (Trist & Bamforth, 1951). This theory posits that the optimal performance of an organization can be achieved when the social and technical systems are designed to mutually support each other. The social system encompasses the people and their roles, relationships, and culture within the organization, while the technical system includes the tools, technologies, and processes employed to achieve organizational goals.

In the context of this study, the Socio-Technical Systems Theory provides a robust framework for understanding how AI-driven measures can enhance business security among SMEs in Abuja FCT. By examining the interplay between technical innovations, such as AI security protocols and automated threat detection, and the social components, such as employee training and customer data privacy measures, this study aims to explore how these elements collectively contribute to enhancing business security.

STS theory suggests that the integration of advanced technical systems, such as AI security protocols, must be complemented by appropriate social adaptations to maximize their effectiveness. AI security protocols, including machine learning algorithms and automated monitoring systems, can significantly enhance the ability of SMEs to detect and mitigate security threats (Zhang, Chen, & Wang, 2022). However, the successful implementation of these protocols requires a supportive organizational culture, clear communication channels, and proper alignment with the business processes of the SMEs.

Employee training is a critical component of the social system in the STS framework. Providing comprehensive AI training to employees enhances their technical skills and understanding of AI technologies, enabling them to effectively utilize and manage AI-driven security measures. This training not only increases the employees' proficiency but also fosters a security-conscious organizational culture. As employees become more adept at using AI tools and understanding their significance, the overall security posture of the organization improves (Nzongola & Kambale, 2021).

Customer data privacy measures are another essential aspect of the socio-technical interplay. Implementing robust AI-driven data encryption and access controls can protect sensitive customer information and ensure compliance with data protection regulations (Gupta et al., 2023). These technical measures must be supported by a strong organizational commitment to data privacy, which involves educating employees about data protection practices and cultivating a culture of trust and transparency with customers. When SMEs prioritize both technical and social aspects of data privacy, they can significantly enhance their business security.

Automated threat detection systems represent a sophisticated technical advancement that can proactively identify and neutralize security threats in real-time. According to STS theory, the effectiveness of these systems is contingent upon their integration with the organization's social framework. This includes ensuring that employees are well-trained to respond to automated alerts and that there are clear protocols for managing detected threats (Song, & Choi, 2021). By harmonizing automated threat detection with human oversight and response mechanisms, SMEs can achieve a more resilient and comprehensive security strategy.

The Socio-Technical Systems Theory serves as a guiding framework for this study, providing a holistic perspective on the impact of AI-related measures on business security among SMEs in Abuja FCT. By emphasizing the interdependence of social and technical systems, this theory underscores the importance of a balanced approach that integrates advanced AI technologies with supportive social structures. This study aims to explore how AI security protocols, employee AI training, customer data privacy measures, and automated threat detection collectively enhance business security, ultimately contributing to the resilience and competitiveness of SMEs in Abuja FCT.

Empirical Review

Ahmad and Jasimuddin, (2018) research in the banking sector of Malaysia provides pertinent insights into the effectiveness of frequent and high-quality training programs. Their findings show that such training enhances job satisfaction and organizational commitment, leading to higher retention rates. While this study was conducted in Malaysia, the principles of continuous professional development are likely applicable to SMEs in Abuja FCT, Nigeria. Similarly, a study by Oluwatobi, Olabisi, and Adesoye (2019) conducted in Lagos, Nigeria, found that frequent and high-quality training programs significantly enhanced employee job satisfaction and organizational commitment across various industries, including manufacturing and services. These findings underscore the universal relevance of training initiatives in fostering employee retention and organizational performance.

In the realm of AI security protocols, Zhang, Chen, and Wang (2022) conducted a study in the technology sector that found the implementation of robust AI-driven security protocols significantly reduced security breaches and enhanced overall business security. Although this study was not conducted in Nigeria, the findings are relevant to SMEs in Abuja FCT, where the adoption of AI technologies for security purposes is becoming increasingly common. This is supported by research from Amadi, Ogwueleka, and Chukwuma (2020) in Ghana, which explored the effectiveness of AI-driven security protocols in mitigating cybersecurity risks in small and medium enterprises. Their study revealed that AI-based security measures significantly reduced the incidence of cyber threats and improved overall business security. These insights are valuable for SMEs in Abuja FCT facing similar cybersecurity challenges.

Regarding employee AI training, research by Lee and Park (2023) in South Korean SMEs revealed that comprehensive AI training programs not only improved employees' understanding of AI technologies but also empowered them to contribute effectively to business security measures. While the study was conducted in South Korea, similar initiatives could be adapted and evaluated within SMEs in Abuja FCT, Nigeria. Additionally, a study by Nzongola and Kambale (2021) in the Democratic Republic of Congo examined the impact of employee AI training on business security in SMEs. The results indicated that comprehensive AI training programs enhanced employees' technical skills and contributed to a security-conscious organizational culture, reducing the vulnerability of SMEs to cyberattacks and other security threats. These findings suggest the potential benefits of AI training initiatives for SMEs across the continent.

Furthermore, research by Njoku, Uzuegbunam, and Ajaegbu (2022) in Nigeria's technology hub, Lagos, investigated the effectiveness of customer data privacy measures in safeguarding sensitive information in e-commerce businesses. The study highlighted the importance of AI-driven encryption and access controls in ensuring compliance with data protection regulations and building customer trust. Although the study was conducted in a different Nigerian city, the findings offer insights relevant to SMEs in Abuja FCT seeking to enhance data privacy and security measures. Similarly, Gupta et al. (2023) examined the effectiveness of privacy-enhancing technologies, including AI-driven encryption and access controls, in safeguarding customer data in e-commerce businesses. Although this study did not specifically focus on Nigeria, similar measures could be adapted and evaluated within SMEs in Abuja FCT to mitigate privacy risks and enhance overall business security.

Automated threat detection systems have been shown to significantly bolster business security in SMEs. For instance, research by Kim, Song, and Choi (2021) demonstrated that AI-powered threat detection systems effectively identify and neutralize security threats in real-time, thereby minimizing the potential impact of cyberattacks on business operations. Implementing such systems could enhance the security posture of SMEs in Abuja FCT, Nigeria, making them more resilient to evolving cyber threats.

While existing empirical studies have contributed valuable insights into the impact of AI-related measures on business security, there remains a notable gap in research specifically examining these dynamics within the context of SMEs in Abuja FCT, Nigeria. Addressing this gap would provide actionable insights to guide the development and implementation of effective AI-driven security strategies tailored to the needs and challenges of SMEs in the region. By drawing from experiences and lessons learned in other parts of Nigeria and across Africa, such research could significantly enhance our understanding of business security dynamics in Abuja FCT.

METHODOLOGY

This study employs a cross-sectional survey design to investigate the impact of various AI-related measures on business security among SMEs in Abuja FCT. This design facilitates the collection of data at a single point in time, providing a snapshot of the relationships between the variables under study. The target population for this study consists of employees from SMEs in Abuja FCT, Nigeria, specifically within the Information and Communication sector. According to data from the Small and Medium Enterprises Development Agency of Nigeria (SMEDAN, 2021), the total number of employees in these SMEs is estimated to be 24,832. These SMEs have implemented key AI-driven measures within their organizations, including AI security protocols, employee AI training, customer data privacy measures, and automated threat detection systems, which are the independent variables under investigation.

To determine the appropriate sample size, the Krejcie and Morgan (1970) table was utilized, resulting in a sample size of approximately 379 respondents. This sampling method ensures that the sample is representative of the population, thereby enhancing the reliability and validity of the study's findings. The selected sample size allows for a comprehensive analysis of the impact of the aforementioned AI measures on business security within the context of SMEs in Abuja FCT. Primary data was collected using a structured questionnaire designed to capture detailed information on AI security protocols, employee AI training, customer data privacy measures, automated threat detection, and overall business security. The questionnaire was divided into five main sections:

i. **AI Security Protocols (AISP):** This section utilized a Likert-scale questionnaire to evaluate the implementation and effectiveness of AI security protocols. Participants were asked to express their level of agreement with statements regarding the robustness, consistency, and impact of these protocols, on a scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). The items for assessing AI security protocols were adapted from Zhang, Chen, and Wang (2022).
ii. **Employee AI Training (EAT):** To assess the quality and frequency of AI training programs, a Likert-scale questionnaire was employed. Participants rated statements regarding the comprehensiveness, relevance, and regularity of AI training sessions on a scale from 1 (Strongly

Disagree) to 5 (Strongly Agree). The items for evaluating employee AI training were adapted from Lee and Park (2023).

iii. **Customer Data Privacy Measures (CDPM):** This section aimed to evaluate the effectiveness of data privacy measures implemented by the SMEs. Participants rated their agreement with statements regarding data encryption, access controls, and compliance with data protection regulations on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree). The questionnaire items were adapted from Gupta et al. (2023).

iv. **Automated Threat Detection (ATD):** This section utilized a Likert-scale questionnaire to assess the implementation and impact of automated threat detection systems. Participants rated statements regarding the effectiveness, efficiency, and timeliness of threat detection systems on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree). The items for assessing automated threat detection were adapted from Kim, Song, and Choi (2021).

v. **Business Security (BS):** To measure overall business security, a Likert-scale questionnaire was used. Participants rated their perception of business security improvements, incident response effectiveness, and overall security posture on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree). The items for evaluating business security were adapted from multiple sources to ensure comprehensive coverage of the construct.

The instruments underwent rigorous validation and reliability testing to ensure the accuracy and consistency of the data collected:

i. **Content Validity:** The instruments were selected from established scales known for their strong content validity, ensuring they accurately captured the core aspects of AI security protocols, employee AI training, customer data privacy measures, automated threat detection, and business security.

ii. **Construct Validity:** Factor analysis was used to validate the constructs, confirming that each set of items measured the intended aspects accurately. The substantial explained variance for AI Security Protocols (82%), Employee AI Training (78%), Customer Data Privacy Measures (81%), Automated Threat Detection (84%), and Business Security (83%) highlighted the distinctiveness of these constructs.

iii. **Criterion Validity:** Strong criterion validity was demonstrated by significant correlations between the constructs, with a correlation coefficient of 0.80 between AI security protocols and overall business security, affirming their relevance to the study.

iv. **Reliability:** The internal consistency of the instruments was evaluated using Cronbach's alpha, yielding values of 0.89 for AI Security Protocols, 0.87 for Employee AI Training, 0.88 for Customer Data Privacy Measures, 0.90 for Automated Threat Detection, and 0.91 for Business Security, indicating strong internal consistency. Test-retest reliability was assessed by administering the questionnaire twice to a subset of participants with a two-week interval, resulting in correlation coefficients of 0.92 for AI Security Protocols, 0.90 for Employee AI Training, 0.91 for Customer Data Privacy Measures, 0.92 for Automated Threat Detection, and 0.93 for Business Security, demonstrating high stability. Inter-rater reliability was confirmed with intra-class correlation coefficients (ICCs) of 0.88 for AI Security Protocols, 0.87 for Employee AI Training, 0.89 for

Print ISSN: ISSN 2055-0847(Print)
Online ISSN: ISSN 2055-0855(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Customer Data Privacy Measures, 0.90 for Automated Threat Detection, and 0.91 for Business Security.

Data Analysis

The research hypotheses were tested using multiple regression analysis, which allows for the examination of the impact of multiple independent variables on a single dependent variable. The multiple regression model employed was specified as follows:

$BS = \beta 0 + \beta 1AISP + \beta 2EAT + \beta 3CDPM + \beta 4ATD + \epsilon$

Where:

BS = Business Security (Dependent Variable)
AISP = AI Security Protocols (Independent Variable)
EAT = Employee AI Training (Independent Variable)
CDPM = Customer Data Privacy Measures (Independent Variable)
ATD = Automated Threat Detection (Independent Variable)
β0 = Intercept
β1 = Coefficient for AI Security Protocols
β2 = Coefficient for Employee AI Training
β3 = Coefficient for Customer Data Privacy Measures
β4 = Coefficient for Automated Threat Detection
ε = Error Term

This model allows for a comprehensive analysis of how each AI-related measure impacts business security among SMEs in Abuja FCT, providing valuable insights into the effectiveness of these technologies and practices.

Table 1 Descriptive Statistics

	N	Mean	Std. Deviation	Variance	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
BS	637	2.1476	1.40536	1.975	.926	.097	-.539	.193
AISP	637	2.3626	1.48537	2.206	.716	.097	-.972	.193
EAT	637	2.3940	1.49217	2.227	.676	.097	-1.020	.193
CDPM	637	2.1491	1.41468	2.001	.968	.097	-.495	.193
ATD	637	2.3014	1.51311	2.290	.728	.097	-1.024	.193
Valid N (listwise)	637							

SPSS OUTPUT, 2024

The descriptive statistics presented in Table 1 provide a detailed overview of the central tendencies, variability, and distributions of the variables studied. The dependent variable, Business Security (BS), and the independent variables AI Security Protocols (AISP), Employee AI Training (EAT), Customer Data Privacy Measures (CDPM), and Automated Threat Detection (ATD) were analyzed. The mean score for Business Security (BS) is 2.1476, with a standard deviation of 1.40536. This suggests that SMEs in Abuja FCT report moderate levels of business security. The skewness value of 0.926 indicates a positive skew, meaning that more SMEs report lower levels of business security. Additionally, the kurtosis value of -0.539 signifies a slightly platykurtic distribution, indicating a flatter distribution than the normal curve. This implies a diverse range of perceptions regarding business security among SMEs.

AI Security Protocols (AISP) have a mean score of 2.3626 and a standard deviation of 1.48537. The skewness of 0.716 points to a moderate positive skew, suggesting that AI security protocols are not widely implemented or perceived as ineffective by most SMEs. The kurtosis value of -0.972 points to a flatter than normal distribution. This highlights a significant variation in the adoption and effectiveness of AI security protocols among the surveyed SMEs.

For Employee AI Training (EAT), the mean score is 2.3940, with a standard deviation of 1.49217. The skewness value of 0.676 indicates a moderate positive skew, suggesting that AI training is infrequent or inadequate. The kurtosis of -1.020 further confirms a flatter distribution. This indicates that while some SMEs might provide comprehensive AI training, many others do not prioritize it, leading to varying levels of employee preparedness in dealing with AI-related security issues.

Customer Data Privacy Measures (CDPM) have a mean score of 2.1491 and a standard deviation of 1.41468. A skewness of 0.968 indicates a positive skew, suggesting that effective data privacy measures are not commonly implemented. The kurtosis value of -0.495 indicates a near-normal distribution, though slightly flatter. This suggests that while some SMEs have robust data privacy measures, a significant number do not, potentially exposing customer data to security risks. Automated Threat Detection (ATD) has a mean score of 2.3014 and a standard deviation of 1.51311. The skewness of 0.728 indicates a positive skew, suggesting that automated threat detection systems are not widely adopted. The kurtosis value of -1.024 points to a flatter distribution. This highlights a significant variation in the implementation of automated threat detection systems, which are crucial for proactive security management.

The descriptive statistics reveal that SMEs in Abuja FCT generally report low to moderate levels of business security and adoption of AI-related measures. The positively skewed distributions across all variables suggest that many SMEs have not fully implemented robust AI security protocols, comprehensive employee AI training, effective customer data privacy measures, or automated threat detection systems. The moderate mean values indicate significant room for improvement in these areas. For instance, the mean scores around 2.3 for AISP, EAT, and ATD imply that these AI-related measures are either in their early stages of implementation or perceived as ineffective. This is critical as the effectiveness of AI security protocols and training directly impacts the overall security posture of the SMEs.

The standard deviations, ranging from 1.4 to 1.5, reflect considerable variation in the responses, highlighting that while some SMEs might have advanced security measures, others lag significantly behind. This variance could be due to differences in resources, knowledge, or the priority given to AI security measures among different SMEs. These findings underscore the need for increased emphasis on AI-related security measures among SMEs in Abuja FCT.

Given the variability and the skewed nature of the data, multiple regression analysis is appropriate to understand the relationship between the independent variables (AISP, EAT, CDPM, ATD) and the dependent variable (BS). Multiple regression will help determine the extent to which each AI-related measure influences business security and identify which measures are most impactful. The justification for using multiple regression lies in its ability to handle multiple predictors simultaneously, providing a comprehensive analysis of their individual and combined effects on business security. This is essential for developing targeted interventions that can enhance the security posture of SMEs by focusing on the most significant factors identified through the regression analysis.

These descriptive statistics underscore the need for increased emphasis on AI-related security measures among SMEs in Abuja FCT. By improving AI security protocols, enhancing employee training, ensuring robust data privacy measures, and implementing effective automated threat detection systems, SMEs can significantly bolster their business security.

Table 2 Correlations

		BS	AISP	EAT	CDPM	ATD
BS	Pearson Correlation	1	.787**	.850**	.849**	.842**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	637	637	637	637	637
AISP	Pearson Correlation	.787**	1	.871**	.728**	.687**
	Sig. (2-tailed)	.000		.000	.000	.000
	N	637	637	637	637	637
EAT	Pearson Correlation	.850**	.871**	1	.913**	.863**
	Sig. (2-tailed)	.000	.000		.000	.000
	N	637	637	637	637	637
CDPM	Pearson Correlation	.849**	.728**	.913**	1	.907**
	Sig. (2-tailed)	.000	.000	.000		.000
	N	637	637	637	637	637
ATD	Pearson Correlation	.842**	.687**	.863**	.907**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	637	637	637	637	637

**. Correlation is significant at the 0.01 level (2-tailed).

SPSS OUTPUT, 2024

The correlation matrix in Table 2 provides crucial insights into the relationships between business security (BS) and various independent variables: AI security protocols (AISP), employee AI training (EAT), customer data privacy measures (CDPM), and automated threat detection (ATD). Pearson correlation coefficients, accompanied by significance levels, reveal the strength and direction of these relationships.

The relationship between BS and AISP is notably strong, with a Pearson correlation coefficient of 0.787 and a p-value of 0.000. This indicates a robust positive correlation, meaning that as the implementation of AI security protocols increases, the overall business security among SMEs in Abuja FCT also significantly improves. The statistical significance of this relationship underscores its reliability, suggesting that AI security protocols are a critical component of business security strategies.

Similarly, BS shows an even stronger positive correlation with EAT, with a coefficient of 0.850 and a p-value of 0.000. This strong correlation implies that providing effective AI training to employees greatly enhances business security. Trained employees are better equipped to handle AI systems and respond to security threats, highlighting the importance of human capital development in maintaining robust security measures within SMEs.

The correlation between BS and CDPM is also strong, with a coefficient of 0.849 and a p-value of 0.000. This suggests that effective customer data privacy measures are essential for business security. Protecting customer data not only safeguards sensitive information but also strengthens overall organizational security by building trust and reducing vulnerabilities. This relationship emphasizes the need for stringent data privacy policies and practices within SMEs.

Further, the correlation between BS and ATD is strong, with a coefficient of 0.842 and a p-value of 0.000. This strong positive correlation highlights the critical role of automated threat detection systems in enhancing business security. Automated systems that can identify and respond to threats in real-time significantly bolster an organization's defense against potential security breaches. This finding suggests that SMEs should invest in advanced threat detection technologies to maintain a proactive security posture.

The inter-relationships among the independent variables (AISP, EAT, CDPM, and ATD) are also noteworthy. For instance, AISP and EAT have a Pearson correlation coefficient of 0.871, indicating that firms investing in AI security protocols are also likely to provide comprehensive AI training to their employees. Similarly, the high correlation between EAT and CDPM (0.913) suggests that organizations prioritizing employee training are also likely to implement robust data privacy measures. These strong inter-correlations imply that effective security practices are often implemented in a complementary manner, creating a holistic approach to business security.

The significant positive correlations between business security and the independent variables have profound implications for SMEs in Abuja FCT. The strong relationship between BS and AISP suggests that enhancing AI security protocols is crucial for improving overall business security. SMEs should prioritize the development and implementation of robust AI security frameworks to mitigate risks effectively. This involves adopting best practices in AI security and continuously updating these protocols to address emerging threats.

The robust correlation between BS and EAT highlights the importance of investing in employee training. Comprehensive AI training programs equip employees with the necessary skills to manage AI systems and respond to security incidents. Regular training sessions ensure that employees remain proficient in the latest AI technologies and security practices, thereby enhancing the organization's overall security posture.

The strong positive relationship between BS and CDPM underscores the necessity of protecting customer data. Effective data privacy measures not only comply with regulatory requirements but also build customer trust and safeguard against data breaches. SMEs should ensure that their data privacy policies are stringent and regularly updated to protect sensitive customer information adequately.

The significant correlation between BS and ATD indicates that automated threat detection systems are vital for business security. Investing in advanced threat detection technologies allows organizations to identify and neutralize potential threats proactively, thereby maintaining a secure operating environment.

Table 3 Model Summary[b]

					Change Statistics					
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	F Change	df1	df2	Sig. F Change	Durbin-Watson
1	.897[a]	.804	.803	.62359	.804	649.561	4	632	.000	1.620

a. Predictors: (Constant), ATD , AISP, CDPM, EAT
b. Dependent Variable: BS

SPSS OUTPUT, 2024

The model summary provided in Table 3 presents the results of the multiple regression analysis examining the impact of AI security protocols (AISP), employee AI training (EAT), customer data privacy measures (CDPM), and automated threat detection (ATD) on business security (BS) among SMEs in Abuja FCT.

The R value of 0.897 indicates a very strong correlation between the independent variables (AISP, EAT, CDPM, and ATD) and the dependent variable (BS). This suggests a substantial linear relationship between these variables.

The R^2 value of 0.804 means that approximately 80.4% of the variance in business security can be explained by the four independent variables in the model. This high R^2 value indicates that the model has a good explanatory power.

The Adjusted R^2 value of 0.803 is very close to the R^2 value, confirming that the model remains robust even when adjusted for the number of predictors. This suggests that adding more predictors would not significantly improve the model's explanatory power.

The standard error of the estimate is 0.62359, which measures the average distance that the observed values fall from the regression line. A smaller standard error indicates a more precise estimate of the dependent variable, suggesting that the model's predictions are relatively accurate.

The F change value of 649.561 with a significance level (Sig. F Change) of 0.000 indicates that the model is statistically significant. This means that the independent variables collectively have a significant impact on the dependent variable, business security. The high F-statistic and the corresponding low p-value confirm that the overall regression model is a good fit for the data.

The Durbin-Watson statistic is 1.620, which is within the acceptable range of 1.5 to 2.5, suggesting that there is no significant autocorrelation in the residuals of the model. This indicates that the assumption of independence of errors is met, enhancing the reliability of the regression results.

The findings from the model summary imply that AI security protocols, employee AI training, customer data privacy measures, and automated threat detection collectively play a significant role in enhancing business security among SMEs in Abuja FCT. The high R² value underscores the substantial influence these factors have on business security, suggesting that SMEs should prioritize the implementation and improvement of these AI-related measures to bolster their security posture. The statistical significance of the model indicates that investments in these AI-driven initiatives are likely to yield measurable improvements in business security, thereby reducing vulnerabilities and enhancing the overall resilience of SMEs against security threats. The robustness of the model, as indicated by the adjusted R² and the standard error of the estimate, suggests that the findings are reliable and can inform strategic decision-making for SMEs aiming to enhance their security frameworks through AI-driven solutions.

Table 4 ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1010.366	4	252.592	649.561	.000[b]
	Residual	245.763	632	.389		
	Total	1256.129	636			

a. Dependent Variable: BS
b. Predictors: (Constant), ATD , AISP, CDPM, EAT

SPSS OUTPUT, 2024

The ANOVA table provided offers crucial insights into the multiple regression analysis performed to evaluate the impact of AI security protocols, employee AI training, customer data privacy measures, and automated threat detection on business security among SMEs in Abuja FCT.The regression sum of squares (1010.366) indicates the amount of variance in business security (BS) that is explained by the independent variables: AI Security Protocols (AISP), Employee AI Training (EAT), Customer Data Privacy Measures (CDPM), and Automated Threat Detection (ATD). This high value suggests that these predictors collectively explain a substantial portion of the variability in business security. It signifies the effectiveness of these AI-related factors in accounting for changes in business security levels.

The residual sum of squares (245.763) represents the variance in business security that is not explained by the independent variables included in the model. This relatively lower value compared to the regression sum of squares indicates that the model has a good fit, as a smaller portion of the variance remains unexplained. This residual variance signifies the amount of variation that might be due to other factors not included in the model or inherent randomness in the data.The total sum of squares (1256.129) is the sum of the regression and residual sums of squares. It represents the total variance in business security observed in the data. This value is critical as it sets the benchmark for understanding how much of the total variance is explained by the model versus what remains unexplained.

The F-statistic (649.561) is a ratio of the mean square regression to the mean square residual. This high F-value indicates that the model provides a significantly better fit to the data compared to a model with no predictors. The F-statistic essentially tests whether the explained variance in the model is significantly greater than the unexplained variance, and in this case, it strongly supports the model's validity.

The p-value associated with the F-statistic is 0.000, which is less than the conventional threshold of 0.05. This indicates that the overall regression model is statistically significant, meaning that the independent variables collectively have a significant impact on business security. The low p-value confirms that the relationships observed in the model are not due to random chance.
The results from the ANOVA table have important implications for SMEs in Abuja FCT. The high F-value and the corresponding low p-value underscore the effectiveness of AI Security Protocols, Employee AI Training, Customer Data Privacy Measures, and Automated Threat Detection in enhancing business security. The statistical significance of the model highlights the critical role these factors play in safeguarding business operations.

Table 5 Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.030	.049		.625	.532
	AISP	.363	.036	.384	10.048	.000
	EAT	-.096	.062	-.101	-1.553	.121
	CDPM	.324	.054	.326	6.012	.000
	ATD	.344	.040	.370	8.651	.000

a. Dependent Variable: BS

SPSS OUTPUT, 2024

The coefficients table provides insight into the individual impact of each predictor on business security. The constant term (B = 0.030, p = 0.532) is not statistically significant, indicating that the baseline level of business security is not different from zero when all predictors are absent.
AI Security Protocols (AISP) have a positive and significant impact on business security (B = 0.363, p < 0.001). This suggests that enhancing AI security protocols directly improves business security, making it a critical focus area for SMEs. Employee AI Training (EAT), however, shows a negative but non-significant effect (B = -0.096, p = 0.121), indicating that current training programs might

not be effectively contributing to business security, or their impact may be mediated by other factors not included in this model.

Customer Data Privacy Measures (CDPM) also show a positive and significant effect on business security (B = 0.324, $p < 0.001$). This highlights the importance of robust data privacy practices in safeguarding business operations. Automated Threat Detection (ATD) is another significant predictor (B = 0.344, $p < 0.001$), demonstrating that automated systems for identifying and mitigating threats are vital for enhancing business security.

The findings from this analysis have several implications for SMEs in Abuja FCT. First, the significant positive impact of AI Security Protocols, Customer Data Privacy Measures, and Automated Threat Detection suggests that these areas should be prioritized for investment and development. Implementing robust AI security protocols and automated threat detection systems can substantially enhance business security, reducing vulnerabilities and protecting against potential threats.

The non-significant impact of Employee AI Training indicates a need for SMEs to re-evaluate their training programs. This might involve developing more targeted and practical training modules that directly address security concerns and enhance employees' capabilities to manage and mitigate risks. By improving the effectiveness of training programs, SMEs can better leverage their human resources to support overall business security.

The study underscores the critical role of advanced AI technologies and data privacy measures in securing business operations among SMEs. By focusing on these key areas, SMEs can enhance their resilience against security threats, ensuring sustainable business growth and customer trust. The findings also suggest the need for continuous assessment and improvement of employee training programs to maximize their contribution to business security.

Hypothesis Testing and Implications

H01: AI security protocols have no significant impact on business security among SMEs in Abuja FCT.

The analysis reveals that AI Security Protocols (AISP) have a positive and significant impact on business security, with a coefficient (B) of 0.363 and a p-value of less than 0.001. This indicates that enhancing AI security protocols directly improves business security among SMEs in Abuja. Given the significant p-value, we reject the null hypothesis (H01) and accept the alternative hypothesis that AI security protocols significantly impact business security. This indicates that for every one-unit increase in the effectiveness or implementation of AI security protocols, business security (BS) increases by 0.363 units.

The significant positive impact of AI security protocols suggests that SMEs should prioritize the development and implementation of robust AI security measures. By doing so, businesses can effectively safeguard their operations against potential cyber threats and vulnerabilities. This investment in AI security can lead to improved protection of business assets, maintaining the integrity of business operations, and fostering a secure business environment. Therefore, SMEs are encouraged to allocate resources towards advanced AI security technologies to enhance their overall security posture.

H02: Employee AI training has no significant impact on business security among SMEs in Abuja FCT.

The coefficient for Employee AI Training (EAT) is -0.096 with a p-value of 0.121. Since the p-value is greater than the significance level of 0.05, we fail to reject the null hypothesis (H02). This result suggests that current employee AI training programs do not have a significant impact on business security among SMEs in Abuja.

The non-significant impact of employee AI training indicates that existing training programs may not be effectively contributing to business security. This calls for a critical evaluation and redesign of the training curriculum to ensure it addresses the specific security needs of SMEs. It is essential to develop more targeted and practical training modules that enhance employees' capabilities in managing and mitigating security risks. By improving the effectiveness of these programs, SMEs can better leverage their human resources to support overall business security.

H03: Effective customer data privacy measures have no significant impact on business security among SMEs in Abuja FCT.

The analysis shows that Customer Data Privacy Measures (CDPM) have a positive and significant impact on business security, with a coefficient (B) of 0.324 and a p-value of less than 0.001. Therefore, we reject the null hypothesis (H03) and accept the alternative hypothesis that effective customer data privacy measures significantly impact business security. This indicates that for every one-unit increase in the effectiveness of data privacy measures, business security (BS) increases by 0.324 units.

The significant positive effect of customer data privacy measures underscores the importance of robust data protection practices. SMEs must prioritize the implementation of stringent data privacy protocols to safeguard customer information, which in turn enhances business security. By ensuring the confidentiality, integrity, and availability of customer data, businesses can build trust with their clients, reduce the risk of data breaches, and comply with regulatory requirements. Consequently, investing in effective data privacy measures is crucial for maintaining a secure and trustworthy business environment.

H04: The use of automated threat detection systems have no significant impact on business security among SMEs in Abuja FCT.

The coefficient for Automated Threat Detection (ATD) is 0.344 with a p-value of less than 0.001. This result indicates a significant positive impact of automated threat detection systems on business security. Thus, we reject the null hypothesis (H04) and accept the alternative hypothesis that automated threat detection systems significantly impact business security. This indicates that for every one-unit increase in the effectiveness or implementation of automated threat detection systems, business security (BS) increases by 0.344 units.

The significant positive relationship between automated threat detection systems and business security highlights the critical role of these technologies in protecting SMEs. Automated threat detection systems are essential for promptly identifying and mitigating security threats, thereby reducing the potential for damage and loss. SMEs should invest in these systems to enhance their ability to detect and respond to threats in real-time. By doing so, businesses can improve their resilience against cyberattacks and ensure continuous protection of their operations and assets.
The results of the multiple regression analysis provide strong evidence that AI Security Protocols, Customer Data Privacy Measures, and Automated Threat Detection Systems significantly enhance business security among SMEs in Abuja FCT. However, Employee AI Training does not show a significant impact, suggesting a need for improvement in training programs. These findings underscore the importance of investing in advanced security technologies and effective data privacy measures to protect business operations and foster a secure environment for growth and development.

DISCUSSION OF THE FINDINGS

This study explores the impact of various AI-driven measures on business security among SMEs in Abuja FCT. Specifically, it examines the effects of AI security protocols, employee AI training, customer data privacy measures, and automated threat detection systems. The findings underscore the significant roles these factors play in enhancing business security, providing a comprehensive understanding aligned with the Socio-Technical Systems (STS) Theory. This theory emphasizes the interrelatedness of social and technical elements within an organization, highlighting the need for their integration to achieve optimal performance.

The study reveals that AI Security Protocols (AISP) have a significant positive impact on business security, with a coefficient (B) of 0.363 and a p-value of less than 0.001. This suggests that enhancing AI security protocols directly improves business security. This finding aligns with the research conducted by Zhang, Chen, and Wang (2022), which demonstrated that robust AI-driven security protocols significantly reduce security breaches in the technology sector. For SMEs in Abuja FCT, investing in advanced AI security measures, such as machine learning algorithms and automated monitoring systems, can enhance their ability to detect and mitigate security threats. This improvement in security protocols will likely result in a more secure operational environment, fostering customer trust and potentially leading to increased business resilience and growth.

The positive impact of AI security protocols can be understood through the lens of the Socio-Technical Systems (STS) Theory, which posits that integrating advanced technical systems within an organization's social framework enhances overall performance. Implementing sophisticated AI security protocols necessitates a supportive social system where employees are aware and trained to operate these systems effectively. Thus, AI security protocols not only bolster technical defenses but also require and benefit from a cohesive social structure that supports their use and management. Employee AI Training (EAT) shows a negative but non-significant effect on business security, with a coefficient (B) of -0.096 and a p-value of 0.121. This indicates that the current training programs might not be effectively contributing to business security. This finding suggests a need for SMEs to re-evaluate their training programs, ensuring they are more targeted and practical. Research by Lee and Park (2023) in South Korean SMEs found that comprehensive AI training programs significantly improved employees' understanding of AI technologies and their ability to contribute to business security measures. For SMEs in Abuja FCT, developing more effective training modules that directly address security concerns and enhance employees' skills in managing AI tools could lead to better security outcomes. Over time, as training programs become more relevant and robust, their impact on business security is expected to increase.

The STS Theory supports this finding by emphasizing that the social components, such as employee training, must complement the technical systems for optimal organizational performance. Effective training programs can enhance employees' proficiency in using AI tools, thereby integrating the social and technical aspects of the organization. This integration is crucial for maximizing the effectiveness of AI security protocols and other technological measures.

Customer Data Privacy Measures (CDPM) have a significant positive effect on business security, with a coefficient (B) of 0.324 and a p-value of less than 0.001. This highlights the importance of robust data privacy practices in safeguarding business operations. Research by Gupta et al. (2023) supports this finding, showing that privacy-enhancing technologies, including AI-driven encryption and access controls, are effective in protecting customer data. For SMEs in Abuja FCT, implementing strong data privacy measures can significantly reduce the risk of data breaches, enhance regulatory compliance, and build customer trust. These practices are essential for maintaining the integrity and reputation of the business, thereby fostering a secure and trustworthy operational environment.

The STS Theory elucidates that technical measures like data privacy controls must be embedded within the organization's social framework, which includes policies, employee awareness, and customer trust-building practices. By integrating these technical and social elements, SMEs can achieve a more robust and effective approach to data privacy and overall business security.

Automated Threat Detection (ATD) systems also have a significant positive impact on business security, with a coefficient (B) of 0.344 and a p-value of less than 0.001. This indicates that automated systems for identifying and mitigating threats are vital for enhancing business security. Kim, Song, and Choi (2021) found that AI-powered threat detection systems effectively identify and neutralize security threats in real-time, minimizing the potential impact of cyberattacks. For SMEs in Abuja FCT, investing in such technologies will bolster their security posture, making them more resilient to evolving cyber threats. These systems can help detect anomalies and potential threats quickly, reducing the response time and mitigating the impact of security incidents.

According to the STS Theory, the effectiveness of automated threat detection systems is contingent upon their integration with the organization's social framework. This includes ensuring that employees are well-trained to respond to automated alerts and that there are clear protocols for managing detected threats. By harmonizing automated threat detection with human oversight and response mechanisms, SMEs can achieve a more resilient and comprehensive security strategy.
The findings from this study have several implications for SMEs in Abuja FCT. The significant positive impacts of AI Security Protocols, Customer Data Privacy Measures, and Automated Threat Detection suggest that these areas should be prioritized for investment and development. Implementing robust AI security protocols and automated threat detection systems can substantially enhance business security, reducing vulnerabilities and protecting against potential threats.

The non-significant impact of Employee AI Training indicates a need for SMEs to re-evaluate their training programs. This might involve developing more targeted and practical training modules that directly address security concerns and enhance employees' capabilities to manage and mitigate risks. By improving the effectiveness of training programs, SMEs can better leverage their human resources to support overall business security.

The study underscores the critical role of advanced AI technologies and data privacy measures in securing business operations among SMEs. By focusing on these key areas, SMEs can enhance their resilience against security threats, ensuring sustainable business growth and customer trust. The findings also suggest the need for continuous assessment and improvement of employee training programs to maximize their contribution to business security.

This study provides valuable insights into the impact of AI-driven measures on business security among SMEs in Abuja FCT. The significant positive effects of AI Security Protocols, Customer Data Privacy Measures, and Automated Threat Detection highlight the importance of these factors in enhancing business security. While Employee AI Training currently shows a non-significant impact, improvements in training programs can potentially lead to better security outcomes. By integrating advanced AI technologies with supportive social structures, SMEs can create a more secure business environment, protect against cyber threats, and build customer trust, ultimately contributing to sustainable business growth and success.

Conclusion and Recommendations

This study investigates the impact of AI security protocols, employee AI training, customer data privacy measures, and automated threat detection on business security among SMEs in Abuja FCT. The findings offer significant insights for both academic research and practical application within the fields of cybersecurity and SME management.

The study reveals that AI security protocols, customer data privacy measures, and automated threat detection systems significantly enhance business security among SMEs in Abuja FCT. Specifically, AI security protocols show a substantial positive impact on business security, indicating that robust and well-implemented AI-driven security measures are crucial for mitigating cyber threats. Similarly, customer data privacy measures play a critical role in safeguarding sensitive information, thus enhancing overall business security. Automated threat detection systems are also found to be highly effective, providing real-time monitoring and rapid response to potential security breaches. Conversely, employee AI training, while essential for equipping staff with the necessary skills to manage AI tools, does not show a significant impact on business security. This finding suggests that current training programs may not be sufficiently aligned with security objectives or practical enough to address the immediate needs of the business.

These results underscore the importance of integrating advanced technological measures with appropriate social frameworks to enhance business security. The study aligns with the Socio-Technical Systems (STS) Theory, which posits that the optimal performance of an organization is achieved through the harmonious integration of social and technical elements. Effective AI security protocols, data privacy measures, and automated threat detection systems necessitate a supportive social structure, including well-informed and capable employees.

Recommendations

SMEs should prioritize the development and implementation of robust AI security protocols. These measures will help detect and mitigate potential threats, enhancing the overall security posture of the organization.

There is a need to re-evaluate and improve existing AI training programs. Training should be more targeted and practical, focusing on current security challenges and equipping employees with the skills necessary to effectively manage AI tools in the context of security.

Implementing comprehensive data privacy measures is critical. These measures not only protect sensitive customer information but also build trust and ensure compliance with regulatory requirements.

Investing in advanced automated threat detection technologies is essential. These systems provide real-time monitoring and rapid response to potential threats, significantly enhancing business security.

To effectively reduce turnover rates and improve job satisfaction, SMEs should consider integrating other motivational strategies and organizational factors beyond training and development. This multifaceted approach will help create a more satisfied and stable workforce.

Further Research

Future research should build on these findings by exploring additional factors influencing business security among SMEs in Abuja FCT. Investigating the role of organizational culture and its interaction with AI-driven security measures could provide deeper insights into effective security strategies. Examining employee engagement as a mediating factor between AI training, job satisfaction, and business security could identify key engagement drivers. Additionally, aligning organizational security measures with employees' career aspirations might enhance both job satisfaction and retention.

REFERENCES

Akinbinu, A., & Adedeji, O. (2024). Financial and infrastructural constraints in the adoption of AI technologies by Nigerian SMEs. *Journal of Business Research*, 34(2), 123-138.

Ahmad, R., & Jasimuddin, S. M. (2018). The role of training in enhancing job satisfaction and organizational commitment in the banking sector of Malaysia. *Human Resource Development Quarterly*, 29(4), 449-474.

Ahmed, T., Khan, M., Iqbal, Z., & Malik, M. (2022). Business security and competitive advantage in SMEs. *Journal of Business and Security Studies*, 15(3), 210-225.

Amadi, P., Ogwueleka, F., & Chukwuma, I. (2020). Effectiveness of AI-driven security protocols in mitigating cybersecurity risks in Ghanaian SMEs. *African Journal of Information Systems*, 12(1), 56-72.

Chen, S., & Li, H. (2023). The transformative impact of AI on business security in SMEs. *International Journal of Security Studies*, 18(1), 45-60.

Eze, N., & Chukwu, M. (2023). Cybersecurity challenges faced by Nigerian SMEs. *Cybersecurity Journal of Africa*, 7(2), 67-85.

Gupta, R., Patel, A., & Desai, P. (2023). Effectiveness of privacy-enhancing technologies in e-commerce. *Journal of Information Privacy*, 20(4), 188-204.

Kim, S., Song, H., & Choi, J. (2021). Real-time security threat detection using AI-powered systems. *Cybersecurity & Data Protection Journal*, 14(3), 99-115.

Kumar, V., & Pandey, R. (2023). Regulatory compliance and business security in SMEs. *Journal of Business Compliance*, 11(2), 150-168.

Lee, J., & Park, S. (2023). Comprehensive AI training programs and their impact on SMEs. *Asia-Pacific Journal of Small Business and Entrepreneurship*, 19(1), 78-95.

Li, X., & Liu, Y. (2023). Proactive security measures enabled by AI in SMEs. *Journal of Business Security*, 22(2), 34-50.

Njoku, C., Uzuegbunam, C., & Ajaegbu, A. (2022). Customer data privacy measures in Nigerian e-commerce businesses. *African Journal of Information Security*, 9(2), 45-60.

Nkongola, D., & Kambale, M. (2021). Impact of AI training on business security in Congolese SMEs. *Journal of African Business Studies*, 12(3), 301-318.

Okonkwo, E., & Nwosu, K. (2023). AI adoption and business security challenges in Nigerian SMEs. *Journal of Business and Technology*, 21(1), 55-70.

Okechukwu, A., & Afolabi, B. (2022). Skills gap in the adoption of AI technologies in Nigerian SMEs. *West African Journal of Business and Management*, 18(3), 102-120.

Oluwatobi, E., Olabisi, O., & Adesoye, A. (2019). The impact of frequent training programs on employee retention in Nigerian industries. *Journal of Human Resources and Training*, 27(2), 89-103.

Sharma, R., & Sharma, P. (2023). Multidimensional approaches to business security in SMEs. *Global Journal of Business Security*, 16(2), 76-92.

Singh, A., & Singh, R. (2023). Enhancing operational efficiency through robust security protocols in SMEs. *Journal of Business Efficiency and Security*, 10(1), 133-150.

Srivastava, S., & Choudhary, M. (2023). Adaptive security approaches for SMEs in a dynamic business environment. *Journal of Business Adaptation and Security*, 14(2), 105-120.

Trist, E., & Bamforth, K. (1951). Socio-Technical Systems Theory and organizational performance. *Human Relations*, 4(3), 3-38.

Wang, T., & Zhou, L. (2023). Predictive analysis and AI threat detection in SMEs. *Journal of Predictive Analysis and Security*, 9(2), 90-108.

World Economic Forum. (2021). The role of AI in enhancing business security. *Global Security Report*, 2021, 45-65.

Wu, Q., & Chen, Y. (2023). Employee AI training for enhanced business security. *Journal of AI Training and Security*, 15(4), 201-215.

Zhang, Y., Chen, X., & Wang, T. (2022). Impact of AI security protocols on business security in the technology sector. *Journal of Cybersecurity Research*, 19(3), 78-95.

Zhao, H., Liu, J., & Wong, K. (2022). Automated threat detection and response in SMEs. *Journal of AI and Cybersecurity*, 23(1), 112-130.