ANALYSIS OF CRITICAL SUCCESS FACTORS FOR INFORMATION SECURITY MANAGEMENT PERFORMANCE

[1]Okediran O. O. and [1*]Oguntoye J. P.

[1]Department of Computer Engineering, Faculty of Engineering and Technology, Ladoke Akintola University of Technology, Ogbomoso, Oyo state
**Corresponding Author: jpoguntoye@lautech.edu.ng*

ABSTRACT

The ever-increasing reliance on information systems for a competitive edge has thrust information security to the forefront of organizational priorities. This strategic concern arises from the widespread adoption of information systems across organizations, underscoring the imperative of safeguarding information in the face of complex systems and rapid technological advancements. This study focuses on the critical success factors analysis of information security management performance. The study investigates the relationships between information security controls, top management support, security awareness and training, and the performance of information security management. A theoretical model was proposed and tested empirically using survey data obtained from 119 IT personnel in high-tech firms across the Lagos metropolis. The results indicate significant positive relationships between information security management performance and the following factors: information security controls ($r = 0.699^{**}$, $P < 0.01$), top management support ($r = 0.751^{**}$, $P < 0.01$), and security awareness and training ($r = 0.778^{**}$, $P < 0.01$). Furthermore, the study reveals that information security controls are significantly determined by top management support ($r = 0.901^{**}$, $P < 0.01$), security awareness and training ($r = 0.579^{**}$, $P < 0.01$), and IT competence ($r = 0.451^{**}$, $P < 0.01$). Moreover, the study demonstrates that business alignment has a strong direct effect on an organization's IT competence, with a significant path coefficient ($r = 0.318^{**}$, $P < 0.01$). The findings emphasize the criticality of information security controls, top management support, security awareness and training, and IT competence in achieving effective information security management. Enhancing these factors in organizations improves information security practices and safeguards valuable assets.

Keywords: *Business Alignment, Information Security, Information Security Management, Top Management Support, Security Awareness and Training.*

INTRODUCTION

Organizations across all sizes are increasingly adopting information systems to gain a competitive edge. The benefits of information systems have been widely recognized, elevating the importance of information to the forefront of organizational priorities (Ostrom *et al.,* 2015). However, rapid technological advancement and the complexity of information systems have increased the reliance on these systems, making information security a crucial strategic issue in organizational management (Ershadi *et al.,* 2020).

Information security management is a systematic process aimed at effectively addressing information security threats and risks within an organization (Kitsios *et al.,* 2022). Information plays a significant role in supporting business operations and achieving a competitive advantage (Posthumus and von Solms, 2004). However, it is susceptible to various threats, both internal and external, such as hackers, viruses, data loss, and more (Alhassan and Adjei-Quaye, 2017; Oguntoye *et al.,* 2019). These security risks can lead to significant losses in terms of finance, legal issues, and reputation (Culnan *et al.,* 2008). Given the criticality of information security, there is a growing focus on implementing effective information security management practices by practitioners and academics (Trim and Lee, 2019). The advancements in information and communication technologies, including the internet and media, have further emphasized the importance of information security in the information age (Mehdi *et al.,* 2012). Organizations need to establish robust information security measures to safeguard their assets and ensure the achievement of their goals (Herath *et al.,* 2022).

To achieve effective information security management, it is essential to identify and address the factors that significantly influence its success (Whitman and Mattord, 2021, Agboola *et al.,* 2022). These factors encompass aspects such as procedural and technical security measures, organizational commitment, and the integration of information security objectives with business objectives (Singh *et al.* 2014). The primary objective of information security management is to ensure that imposed security requirements are adequate to protect data and resources, and to identify and address any deviations in security (Marshall *et al.,* 1995). The complexity of implementing an information security management system necessitates the identification of key success factors that can guide organizations in its successful implementation (AlGhamdi *et al.,* 2020). Information security management aims to protect the confidentiality, integrity, and availability of information while mitigating risks and threats (Chang *et al.,* 2011; Oguntoye *et al.,* 2023). It involves a systematic process of applying physical, technical, and operational security controls to protect information assets and achieve organizational goals (Zammani *et al.,* 2021). Effective information security management can significantly reduce security threats and enable trustworthy information sharing within organizations (Zaini *et al.,* 2020).

In today's rapidly evolving digital landscape, high-tech firms are increasingly recognizing the paramount importance of information security management in safeguarding their valuable assets and maintaining a competitive edge (Allioui and Mourdi, 2023). To ensure the effectiveness of information security practices, it is crucial for these firms to identify and understand the critical success factors that significantly influence their information security management performance (Zammani *et al.,* 2021). This study aims to analyse the critical success factors for information security management performance in high-tech firms. The problem at hand revolves around the need to identify and comprehend the key factors that contribute to the success of information security management in high-tech firms. As the digital ecosystem becomes more complex and the threat landscape expands, high-tech firms face various challenges in ensuring the confidentiality, integrity, and availability of their sensitive information (Ogundepo *et al.,* 2022; Li *et al.,* 2023). Failure to adequately address these challenges can result in severe consequences, including data breaches, reputational damage, financial losses, and regulatory non-compliance. Therefore, it is imperative to investigate the critical success factors that play a pivotal role in enhancing the performance of information security management in high-tech firms. In particular, this research endeavor seeks to provide insights into the following questions: (1) Which critical factors are indispensable for ensuring the effectiveness of Information Security Management? (2) In what ways do these factors significantly contribute to the success of Information Security Management?

LITERATURE REVIEW

Information Security Management

Information security is a crucial aspect of organizational management, encompassing the protection of confidential, integral, and available information. It involves implementing physical, technical, and operational security controls to mitigate threats and risks (Okediran, 2019). Information security management encompasses the systematic processes and measures implemented to effectively address information security threats and risks within an organization. It involves the application of physical, technical, and operational security controls to protect information assets and achieve business objectives (Zammani *et al.,* 2021). Key factors contributing to the success of information security management include business alignment, organizational commitment, integration with business objectives, and the identification of essential controls (Ershadi *et al.,* 2020). Additionally, the establishment of procedural and technical security measures, coupled with organizational awareness and IT competence, plays a crucial role in ensuring the confidentiality, integrity, and availability of information (Kitsios *et al.,* 2022;).

Critical Success Factors

Critical Success Factors (CSFs) play a crucial role in the effective implementation and management of Information Security Management (ISM) within organizations (Singh *et al.,* 2014). CSFs are pivotal elements that significantly influence the effectiveness of an organization's approach to securing its information assets (Kitsios et al., 2022). These factors are essential for ensuring robust information security practices and mitigating risks to valuable information. Effective information security management is achieved by addressing critical factors such as business alignment, Top Management Support, information security control, IT competence, and organizational awareness (Ershadi et al., 2020; Alhassan and Adjei-Quaye, 2017).

Business Alignment: Business Alignment is a critical CSF that ensures the integration of information security objectives with the overall strategic goals and objectives of the organization (Singh *et al.,* 2014). By aligning information security initiatives with the organization's mission and business processes, resources can be allocated effectively, executive support can be garnered, and information security can be prioritized within the organization (Kitsios *et al.,* 2022).

Top Management Support: Top management support is a critical success factor in Information Security Management (ISM). It entails the commitment of senior executives and key stakeholders, providing necessary financial resources, enforcing policies, and fostering a security-conscious culture. It ensures effective implementation and maintenance of information security measures (Tu *et al.,* 2018).

Information Security Control: Information Security Control is a critical CSF that encompasses the implementation of policies, procedures, and technical safeguards to protect information assets (Singh *et al.,* 2014). This includes access controls, encryption, firewalls, intrusion detection systems, and incident response mechanisms. Effective information security controls help mitigate risks and prevent unauthorized access, alteration, and disclosure of sensitive information (Posthumus and von Solms, 2004).

IT Competence: IT Competence is a crucial CSF that focuses on the knowledge, skills, and capabilities of the organization's IT staff in managing information security (Singh *et al.,* 2014). IT professionals need expertise in implementing security technologies, conducting risk assessments, managing security incidents, and ensuring compliance with applicable regulations. Their competence is essential for the successful implementation and maintenance of information security systems (Alhassan and Adjei-Quaye, 2017).

Security Awareness and Training: Security awareness and training are essential critical success factors in Information Security Management (ISM). They focus on increasing employees' understanding and consciousness of information security risks, policies, and best practices (Zammani and Razali, 2016). This involves educating employees about their responsibilities, conducting security training programs, and promoting a security-conscious culture. Improved organizational awareness reduces human errors, enhances compliance, and strengthens the overall information security posture (Singh *et al.,* 2014).

Organizations can establish a robust foundation for effective Information Security Management by leveraging these critical success factors. This ensures the protection of their valuable information assets and helps mitigate risks associated with information security breaches.

RESEARCH MODEL AND HYPOTHESIS DEVELOPMENT

The research model investigates how the CSFs contribute to the success of a high-tech organizations ISM from a strategic value alignment perspective. This ISM success model has six constructs: business alignment, top management support, IT competence, security awareness and training, information security controls, and ISM performance. The research framework is depicted in Figure 1:

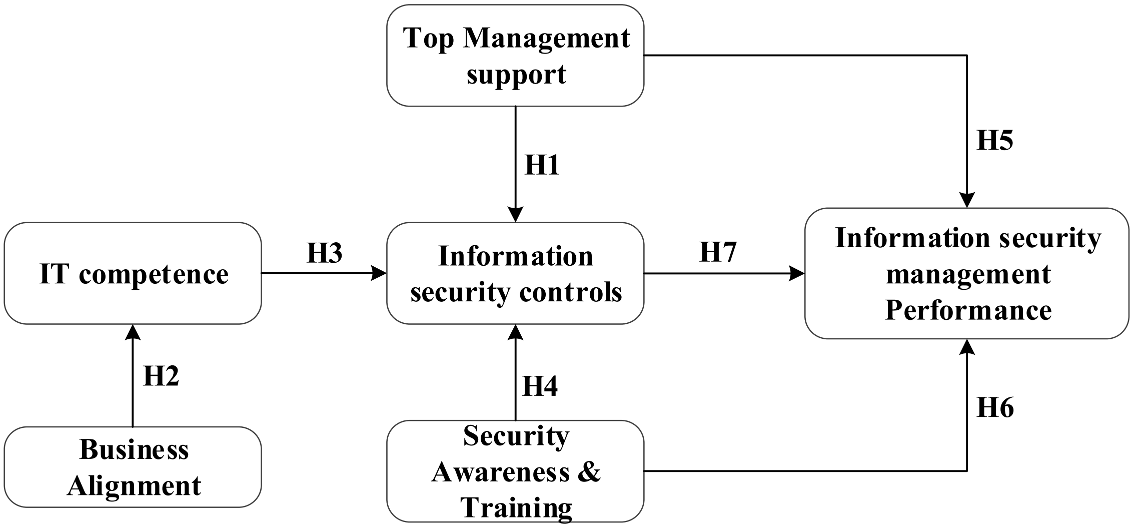
Top Management support
H1
H5
IT competence
H3
Information security controls
H7
Information security management Performance
H2
H4
H6
Business Alignment
Security Awareness & Training

Figure 1: The research framework

The research framework aims to explore the relationships between various factors and their impact on Information Security Management (ISM) performance. Establishing and implementing security controls is crucial for safeguarding information security. It involves security policies and countermeasures, which require resources and expertise. Top management commitment ensures resource availability, while a formal security structure facilitates policy enforcement, reducing security risks (Knapp *et al.,* 2006). This suggests that:

H1: Top management support has a positive influence on the development of information security controls.

Technical competence is vital in an effective information security strategy. It encompasses IT resources and operations, forming the technical foundation of ISM. Strategic alignment between information security objectives and business strategies facilitates acquiring and deploying IT resources that align with the organization's long-term vision (Chang *et al.,* 2011). This implies that:

H2: Business alignment positively affects an organization's IT competence.

Competent IT staff and robust technical resources form the foundation for effective information security controls development, impacting the organization's ability to deploy and manage IT-based security measures (Chang *et al*., 2011). This suggests that:

H3: IT competences positively influence the development of information security controls.

ISM standards necessitate thorough training for employees, ensuring awareness of security threats and policy adherence. Inadequate training impedes security control implementation, emphasizing the significance of fostering an information security culture. This implies that:

H4: Security awareness and training positively impact the development of information security controls.

ISM performance evaluation is a crucial control procedure assessing information security management's effectiveness. Management's role involves implementing safety measures, policies, resource allocation, and demonstrating commitment (Singh *et al.,* 2014). Top management support and organizational structuring enhance security effectiveness, and placing the information security group strategically improves integration and control. Therefore:

H5: Top management support positively influences the performance of ISM.

Security awareness and training ensure employees comprehend information security risks, policies, and procedures. Insufficient knowledge can lead to control failures. Studies reveal that awareness of vulnerability and consequences increases compliance. Deterrence arises from high-risk perception and severe penalties. Enhancing security awareness improves management system effectiveness (Tu *et al.,* 2018). Hence, this implies that:

H6: Security awareness and training positively influences the performance of ISM.

Effective security management relies on well-defined policies governing the use of the information system. Well-designed controls improve performance and efficiency. Identifying, implementing, and maintaining the right security controls is crucial. Measuring progress and complying with standards drive successful information security management (Singh *et al.,* 2014).

. This suggest that:

H7: Effective security controls development positively influences the performance of ISM.

These hypotheses form the basis of the research model, which will be empirically tested to investigate the relationships between these factors and the performance of ISM within organizations.

RESEARCH METHOD

This study employs a quantitative research approach to investigate the relationships between critical success factors (CSFs) and the success of Information Security Management (ISM) in high-tech organizations, focusing on strategic value alignment. The research model consists of six constructs: business alignment, organizational support, IT competences, organizational awareness, information security controls, and information security management (ISM) performance. The study population includes 119 IT personnel from various high-tech firms in the Lagos metropolis. Simple random sampling was employed to select participants. Statistical data were collected through a voluntary field survey. The participants consisted of Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), IT managers, security managers, system administrators, network administrators, IT security analysts, IT risk managers, compliance officers, and IT auditors. All participants actively contributed to decision-making processes concerning their company's information security. Primary data sources were collected through a questionnaire divided into three sections. Section A gathered demographic information, while sections B and C measured critical success factors and information security management performance using a Likert scale. Data analysis involved frequency counts and simple percentages for demographic information. Hypotheses 1 to 7 were tested using Pearson's correlation analysis. Ethical considerations were followed to ensure participant confidentiality and informed consent. The collected data were analyzed using IBM SPSS statistical software.

RESULTS AND DISCUSSIONS

Table 1 summaries demographic characteristics of the respondents. This demographic profile provides insights into the composition of the respondents based on gender, age, work experience, and professional positions.

Table 1: Characteristics of the respondent

	Options	Frequency (N)	Percentage (%)
Gender	Male	62	52.1
	Female	57	47.9
Age	16-25yrs	35	29.4
	26-40yrs	79	66.4
	41 and above	5	4.2
Work Experience	10 years or less	24	20.2
	10-20 years	80	67.2
	20years and above	15	12.6
Position	Information Security Officers	18	15.1
	IT managers	27	22.7
	Security Managers	14	11.8
	System Administrators	13	10.9
	Network Administrators	16	13.4
	IT security analysts	31	26.1

The diversity of the demographic profile provides a foundation for understanding the relationship between critical success factors and information security management performance across different demographic groups. They offer insights into potential variations, considerations, and implications that can be taken into account when analyzing and interpreting the study's results.

Reliability Analysis

To ensure the reliability of the collected data from the questionnaire, this study conducted a reliability analysis to assess the internal consistency among the critical success factors and information security management performance.

Table 2: Reliability Analysis of the CSFs

CSFs	Cronbach's Alpha	Number of Items
Business Alignment	0.719	3
Top Management Support	0.802	3
IT Competence	0.791	3
Security Awareness and Training	0.629	3
Information Security Controls	0.824	3
ISM Performance	0.747	3
All items	0.929	18

Cronbach's Alpha was utilized as the measure to examine the reliability among the critical success factors to evaluate information security management performance. This analysis provides assurance regarding the consistency and dependability of the data used in the study. Table 2 depicts Reliability Analysis of the CSFs.

The results indicate the reliability of critical success factors (CSFs) measured in terms of Cronbach's Alpha and the number of items. Business Alignment, Top Management Support, IT Competence, Security Awareness and Training, and Information Security Controls show good internal consistency with Cronbach's Alpha ranging from 0.629 to 0.824. The overall Cronbach's Alpha for all items is high at 0.929, demonstrating strong internal consistency for the entire set of 18 items. This suggests that the combined measures maintain a high level of reliability.

Correlation Analysis for Hypothesis Testing

The hypotheses of the proposed theoretical model were tested by examining the research framework. Table 3 depicts the result of correlation analysis.

Table 3: The result of correlation analysis

	ISMP	BA	ITC	SAT	TMS	ISC
ISMP	1					
BA	.701**	1				
ITC	.669**	.318**	1			
SAT	.778**	.247**	.904**	1		
TMS	.751**	.164	.676**	.685**	1	
ISC	.699**	-.003	.451*	.579**	.901**	1

Notes: ****Correlation is significant at the 0.01 level (2-tailed); ISMP,** Information Security Management Performance; **BA**, Business Alignment; **ITC**, IT Competence; **SAT**, Security Awareness and Training; **TMS**, Top Management Support; **ISC**, Information Security Controls.

As hypothesized, Information Security Management Performance was significantly determined by information security controls (r = .699**, N= 119, P < .01), top management support (r = .751**, N= 119, P < .01), and security awareness and training (r = .778**, N= 119, P < .01), providing support for H7, H5, and H6 respectively. The implication is that a 1% change in information security control, top management support, and security awareness and training will correspond to a 69.9%, 75.1%, and 77.8% change in the performance of information security management, respectively. Hence, it could be deduced that information security control, top management support, and security awareness and training positively influences the performance of information security management in the study.

Furthermore, information security control was significantly determined by top management support (r = .901**, N= 119, P < .01), security awareness and training (r = .579**, N= 119, P < .01), and IT competence (r = .451**, N= 119, P < .01). This supported H1, H3, and H4. The implication is that a 1% change in top management support, security awareness and training, and IT competence will correspond to a 90.1%, 57.9%, and 45.1% change in Information security controls, respectively. Hence, it could be deduced that top management support, security awareness and training, and IT competence positively influences the performance of Information security controls in the study. Moreover, business alignment had a strong direct effect on organization's IT competence, as demonstrated by the significant path coefficient (r = .318**, N= 119, P < .01). The implication of this is that a 1% change in Business alignment will result in 31.8% change in organization's IT competence. Hence, it could be deduced that business alignment positively influences organization's IT competence in the study. Table 4 depicts hypothesis testing path. Figure 2 depicts the structural model.

Table 4: Hypothesis Testing

Hypothesis	Path	R	p-values	Supported
H1	TMS > ISC	.901**	.000	YES
H2	BA>ITC	.318**	.000	YES
H3	ITC>ISC	451*	.000	YES
H4	SAT>ISC	.579**	.000	YES
H5	TMS>ISMP	.751**	.001	YES
H6	SAT>ISMP	.778**	.003	YES
H7	ISC>ISMP	.699**	.000	YES

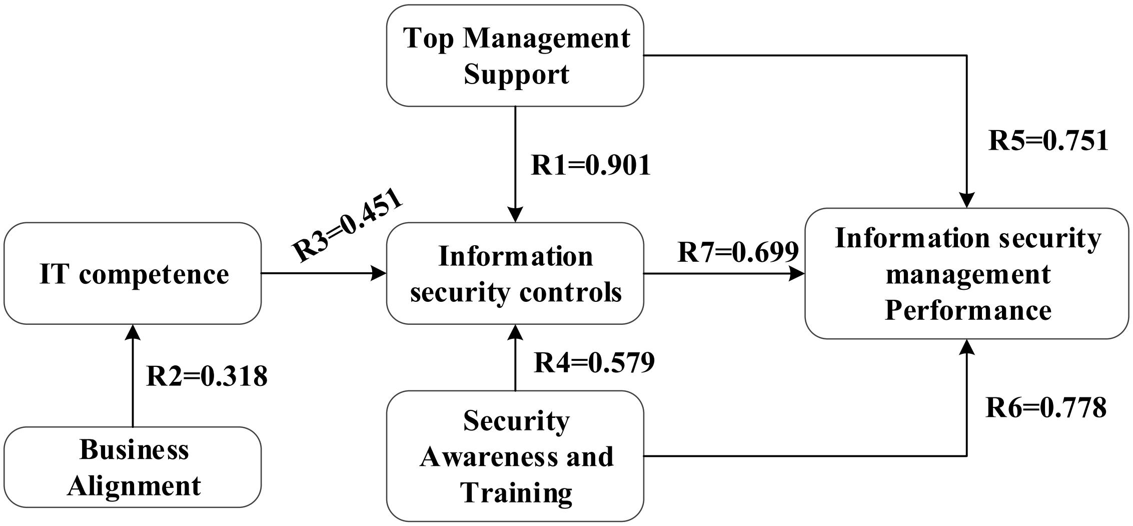

Figure 2: Structural model Result

The data analysis results demonstrate the theoretical model's effectiveness in capturing the primary factors influencing ISM performance. The examination of the proposed research model validated all hypotheses, addressing both research questions. The findings further endorse the adoption of the balanced scorecard framework to assess ISM performance (Bremser and Chung, 2005; Kaplan and Norton, 2004). This suggests the applicability of the balanced scorecard, commonly employed for overall organizational performance measurement, in gauging intangible aspects like ISM (Marr and Schiuma, 2003).

Summary of Findings and Discussion

The results indicate strong support for the hypothesized relationships in the study. The significant influence of information security controls, top management support, and security awareness and training on Information Security Management (ISM) performance underscores their crucial role in enhancing overall security effectiveness. Therefore, these factors should be considered in the development of information security management system. The substantial percentage changes associated with a 1% change in these factors emphasize their substantial impact, offering practical insights for organizations aiming to improve ISM performance.

In terms of theoretical implications, these findings align with established theories such as the Social Exchange Theory and Resource-Based View, which posit the importance of support mechanisms, training, and competence in organizational success (Zhang and Jia, M. 2010; Ramon-Jeronimo *et al.,* 2019). The strong direct effect of business alignment on IT competence reaffirms the strategic role of aligning business objectives with IT functions. Practically, organizations should prioritize investments in information security controls, top management support, and security awareness and training programs to foster robust ISM performance. The substantial impact of these factors on ISM underscores the need for a holistic approach that considers both technical and managerial aspects of information security (Singh and Gupta, 2019).

The findings have significant implications for the management of information and communication technology (ICT) in various domains. The study demonstrates that information security controls, top management support, and security awareness and training significantly influence the performance of information security management (Alzahrani and Seth, 2021). This implies that organizations should prioritize these factors to enhance their information security management practices. Investing in robust information security controls, securing top management support, and providing effective security awareness and training programs can lead to substantial improvements in information security management performance (Hwang *et al.,* 2021).

Furthermore, the study reveals that top management support, security awareness and training, and IT competence significantly impact information security controls. Organizations should ensure strong support from top management, promote a culture of security awareness and training, and develop IT competence to enhance their information security controls (Onumo *et al.,* 2021). These findings highlight the importance of a holistic approach to information security, encompassing technical controls, management support, employee awareness, and technical expertise. Moreover, the results suggest that business alignment positively influences an organization's IT competence. This implies that organizations should align their IT strategies and initiatives with their broader business objectives. A strong alignment between business goals and IT competence enables organizations to effectively leverage technology to support their business operations, enhance efficiencies, and achieve competitive advantage (Luftman *et al.,* 2017).

Hence, organizations should prioritize these factors to strengthen their information security practices and effectively manage ICT in various domains. In mitigating security risks, ensuring regulatory compliance, and safeguarding valuable assets, organizations can maintain the confidentiality, integrity, and availability of their information systems.

CONCLUSION

In conclusion, this study focused on analyzing the critical success factors influencing information security management performance in high-tech firms in Lagos. The findings provide valuable insights into the factors that significantly influence information security management performance and information security controls in this context. The results support the hypothesis that information security management performance is significantly determined by information security controls, top management support, and security awareness and training.

Additionally, information security controls are influenced by top management support, security awareness and training, and IT competence. Moreover, the study demonstrates that business alignment positively affects the IT competence of high-tech firms in Lagos. These findings emphasize the importance of prioritizing information security controls, top management support, security awareness and training, and business alignment to achieve effective information security management in high-tech firms. By focusing on these critical success factors, organizations can enhance their information security practices and ensure the confidentiality, integrity, and availability of their information systems.

To improve information security management performance in high-tech firms in Lagos, it is crucial to focus on several key areas. High-tech firms should invest in tailored and robust information security controls, including advanced security technologies, regular vulnerability assessments, and stringent access controls. Securing sustained top management support is vital, achieved through effective communication about the importance of information security, aligning it with business objectives, and allocating sufficient resources. Prioritizing security awareness and training programs will help establish a security-conscious culture within the organization. High-tech firms should focus on developing and nurturing IT competence through targeted training programs, certifications, and staying up to date with the latest technological advancements. Aligning IT with business objectives requires close collaboration between IT and other units to understand specific technology needs, with regular evaluations ensuring ongoing alignment and adaptability. Implementing these recommendations will strengthen information security management practices, mitigate risks, and protect valuable assets, thereby establishing a secure and resilient IT infrastructure tailored to the high-tech industry in Lagos.

REFERENCES

Agboola, F. F., Malgwi, Y. M., Mahmud, M. A., and Oguntoye, J. P. (2022). Development of a Web-Based Platform for Automating an Inventory Management of a Small And Medium Enterprise. FUDMA Journal of Sciences, 6(5): pp. 57-65.

AlGhamdi, S., Win, K. T., and Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers and Security*, *99*, 102030.

Alhassan, M. M., and Adjei-Quaye, A. (2017). Information security in an organization. *International Journal of Computer (IJC)*, *24*(1), 100-116.

Allioui, H., & Mourdi, Y. (2023). Exploring the full potentials of IoT for better financial growth and stability: A comprehensive survey. *Sensors*, *23*(19), 8015.

Alzahrani, L., & Seth, K. P. (2021). The impact of organizational practices on the information security management performance. *Information*, *12*(10), 398.

Bremser, W. G., & Chung, Q. B. (2005). A framework for performance measurement in the e-business environment. *Electronic Commerce Research and Applications*, *4*(4), 395-412.

Chang, S. E., Chen, S. Y., and Chen, C. Y. (2011). Exploring the relationships between IT capabilities and information security management. *International Journal of Technology Management*, *54*(2/3): 147-166.

Culnan, M. J., Foxman, E. R., and Ray, A. W. (2008). Why IT executives should help employees secure their home computers. *MIS Quarterly Executive*, *7*(1), 6.

Ershadi, M., Jefferies, M., Davis, P., and Mojtahedi, M. (2020). Towards successful establishment of a project portfolio management system: business process management approach. *The Journal of Modern Project Management*, *8*(1): 1-7.

Herath, T. C., Herath, H. S., and Cullum, D. (2022). An Information Security Performance Measurement Tool for Senior Managers: Balanced Scorecard Integration for Security Governance and Control Frameworks. *Information Systems Frontiers*, 1-41.

Hwang, I., Wakefield, R., Kim, S., & Kim, T. (2021). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems*, *61*(4), 345-356.

Kaplan, R. S., & Norton, D. P. (2004). *Strategy maps: Converting intangible assets into tangible outcomes*. Harvard Business Press.

Kitsios, F., Chatzidimitriou, E., and Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability*, *14*(3), 1269.

Knapp, K. J., Marshall, T. E., Rainer, R. K., and Ford, F. N. (2006). Information security: management's effect on culture and policy. *Information Management and Computer Security*, *14*(1), 24-36.

Li, W., Yigitcanlar, T., Nili, A., & Browne, W. (2023). Tech Giants' Responsible Innovation and Technology Strategy: An International Policy Review. *Smart Cities*, *6*(6), 3454-3492.

Luftman, J., Lyytinen, K., & Zvi, T. B. (2017). Enhancing the measurement of information technology (IT) business alignment and its influence on company performance. *Journal of Information Technology*, *32*, 26-46.

Marr, B., & Schiuma, G. (2003). Business performance measurement–past, present and future. *Management decision*, *41*(8), 680-687.

Marshall, W. L., & Mazzucco, A. (1995). Self-esteem and parental attachments in child molesters. *Sexual Abuse: A Journal of Research and Treatment*, *7*, 279-285.

Mehdi, K., Hamid, K., and Hashem, N. (2012). Evaluation of information security management system success factors: Case study of Municipal organization. *African Journal of Business Management*, *6*(14), 4982-4989.

Ogundepo O. Y., Omeiza I. O. A. and Oguntoye J. P. (2022). Optimized Textural Features for Mass Classification in Digital Mammography Using a Weighted Average Gravitational Search Algorithm. *International Journal of Electrical and Computer Engineering (IJECE)*. 12 (5): pp 1-12.

Oguntoye, J. P., Awodoye, O. O., Oladunjoye, J. A., Faluyi, B. I., Ajagbe, S. A., & Omidiora, E. O. (2023). Predicting COVID-19 From Chest X-Ray Images using Optimized Convolution Neural Network. *LAUTECH Journal of Engineering and Technology*, *17*(2), 28-39.

Oguntoye, J. P., Ola, B. O. and Awodoye, O. O. (2019). Development of an Improved Palm Vein Recognition System Using a Swarm Intelligent Based Support Vector Machine. Proceedings of the 22nd iSTEAMS Multidisciplinary SPRING Conference. Aurora Conference centre, Osogbo, Nigeria. 171-182.

Okediran, O. O. (2019). A security scheme for patient information Privacy in digital medical imaging. *University of Pitesti Scientific Bulletin Series: Electronics and Computer Science*, *19*(2), 13-24.

Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures. *ACM Transactions on Management Information Systems (TMIS)*, *12*(2), 1-29.

Ostrom, A. L., Parasuraman, A., Bowen, D. E., Patrício, L., & Voss, C. A. (2015). Service research priorities in a rapidly changing context. *Journal of service research*, *18*(2), 127-159.

Posthumus, S., and Von Solms, R. (2004). A framework for the governance of information security. *Computers and security*, *23*(8), 638-646.

Ramon-Jeronimo, J. M., Florez-Lopez, R., & Araujo-Pinzon, P. (2019). Resource-based view and SMEs performance exporting through foreign intermediaries: The mediating effect of management controls. *Sustainability*, *11*(12), 3241.

Singh, A. N., & Gupta, M. P. (2019). Information security management practices: case studies from India. *Global Business Review*, *20*(1), 253-271.

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management". *Journal of Enterprise Information Management*, *27*(5), 644-667.

Trim, P. R., and Lee, Y. I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management*, *83*, 224-238.

Tu, C. Z., Yuan, Y., Archer, N., & Connelly, C. E. (2018). Strategic value alignment for information security management: A critical success factor analysis. *Information & Computer Security*, *26*(2), 150-170.

Whitman, M. E., and Mattord, H. J. (2021). *Principles of information security*. Cengage learning.

Zammani, M., & Razali, R. (2016). An empirical study of information security management success factors. *Commitment*, *5*(7).

Zammani, M., Razali, R., and Singh, D. (2021). Organisational Information Security Management Maturity Model. *International Journal of Advanced Computer Science and Applications*, *12*(9): 2-12.

Zhang, Z., & Jia, M. (2010). Using social exchange theory to predict the effects of high-performance human resource practices on Corporate Entrepreneurship: Evidence from China. *Human Resource Management*, *49*(4), 743-765.