e-ISSN 3027-0537
p-ISSN 3027-0375

10.5281/zenodo.10207196 Vol. 06 Issue 11 Nov - 2023 Manuscript ID: #1138

The Influence of Management Support, Regulatory Frameworks and Technological Infrastructure on Information Security Culture in Government Institutions in Tanzania

By
Kizito S. Mpeka, Adam A. Semlambo & Joel Kazoba Simon
Department of Computer Science. Institute of Accountancy Arusha (IAA), Tanzania

Corresponding author: semlambo@gmail.com

ABSTRACT:

This study delves into the intricate dynamics of information security culture within the Ministry of Finance in Tanzania, investigating the influential roles of leadership and management support, regulatory frameworks, and technological infrastructure. A cross-sectional research design was used with a quantitative research approach. A sample size of 84 respondents was drawn from a population of 503. Utilising a comprehensive survey that covers variables like commitment, compliance, and resource accessibility, the research reveals crucial findings. Leadership and management support foster a robust information security culture, directly impacting employee awareness, responsibility, and proactive security behaviours. Concurrently, compliance with regulatory frameworks emerges as pivotal, necessitating continuous training programs to ensure understanding and adherence. The study also underscores the profound impact of technological infrastructure on information security, emphasising the importance of accessible and reliable resources in fortifying the organisation's security posture. The research sheds light on the current information security culture within the Ministry of Finance. It furnishes actionable recommendations for sustained improvement, offering a valuable contribution to the broader discourse on cybersecurity within government institutions.

KEYWORDS:

Information Security Culture, Leadership and Management Support, Regulatory Frameworks, Technical Infrastructure, Government Institutions

1.0 INTRODUCTION

In the ever-evolving digital landscape, the importance of information security for government agencies is undeniable. Recent studies by Georgiadou et al. (2022) underscore the critical role of a robust information security culture in preserving sensitive data, safeguarding essential infrastructure, and maintaining public trust, particularly in the context of US government agencies. Adherence to regulatory frameworks such as the Federal Information Security Management Act (FISMA), the NIST cybersecurity framework, and other laws and standards is crucial for shaping information security policies, procedures, and practices.

Leadership dedication emerges as a cornerstone for fostering a sound information security culture. Executives and department heads are pivotal in prioritising and supporting cybersecurity efforts. As Georgiadou et al. (2022) highlighted, efficient governance structures define roles and responsibilities, establishing a clear information protection duty. Continuous training becomes imperative to ensure employees understand their role in protecting personal data, coupled with consistent awareness efforts to keep staff abreast of new threats and security requirements.

Farid et al. (2023) extend these insights to the global stage, emphasising the necessity for solid information security cultures in US and UK government agencies. In the UK, adherence to regulations such as the Data Protection Act, GDPR, and NCSC advice forms the legal framework for government agencies to adopt information security measures.

The digital revolution has brought opportunities and challenges to the African landscape. Within the dynamic East African region, the proliferation of Information and Communication Technologies (ICTs) has catalysed economic growth and enhanced public services, as noted by KPMG Africa (2020) and the World Bank (2019). However, this digital transformation has also exposed vulnerabilities, demanding a prioritisation of information security by governments and organisations.

In Kenya, Kiganda (2022) stresses the importance of a strong information security culture in protecting sensitive data, government system integrity, and public confidence. The 2019 Data Protection Act governs information security in Kenya, complemented by the National Cybersecurity Strategy to address cyber threats and vulnerabilities.

Zooming in on the United Republic of Tanzania, a significant player in the East African community, the focus sharpens on its ambitious journey towards digitalisation. The Tanzanian Ministry of Communication and Information Technology (2021) outlines various initiatives, including a National Cyber Security Strategy, cybersecurity awareness campaigns, and capacity-building efforts to create a secure and resilient digital environment. However, challenges in adopting the technology are unavoidable due to the ever-changing and continued development of technology,especially in public sectors, as noted by researchers such as (Lubua et al., 2022; Semlambo et al., 2022; Semlambo, Mfoi, & Sangula, 2022).

This research hones in on the foundational elements of an organisation's information security culture, encompassing values, beliefs, attitudes, and behaviours. A study from Alqahtani (2019) delves into leadership and management support, regulatory frameworks, compliance needs, technical infrastructure, and resources. Effective leadership, clear policies and procedures, and support from management emerge as crucial factors, while adherence to frameworks and compliance standards plays a pivotal role in protecting sensitive data.

In the subsequent sections, the studydelves deeper into the specific contexts of the US, UK, Kenya, and Tanzania, exploring government agencies' unique challenges and strategies to cultivate a resilient

information security culture. Through this journey, the studyaims to provide valuable insights and practical recommendations for organisations seeking to enhance their information security posture in an increasingly digital world.

2.0 OBJECTIVE OF THE STUDY

This study evaluated factors influencing information security culture in public organisations, taking the Ministry of Finance as the case for this study

3.0 LITERATURE REVIEW

This section discusses factors influencing information security culture in public organisations, taking the Ministry of Finance as the case for this study,

3.1 Theoretical Review

In exploring the factors that shape information security culture within the Tanzanian Ministry of Finance and Planning, this article draws upon three key theoretical frameworks: Organisational Culture Theory (OCT), Protection Motivation Theory (PMT), and the Theory of Planned Behaviour (TPB).

As Meng and Berger (2019) articulated, Organisational Culture Theory is a foundational lens to examine the Ministry's shared beliefs, values, and norms. This theory asserts that organisational culture profoundly influences employee behaviour and decision-making processes. Shared values, beliefs, assumptions, norms, and visible artefacts and symbols collectively shape the organisation's identity. Leadership and socialisation processes, crucial components highlighted by Meng and Berger (2019), play a pivotal role in establishing and reinforcing the desired information security culture. This lens provides insights into how the Ministry's leadership can foster an environment that supports employee engagement, innovation, and long-term success in information security practices.

Complementing the organisational perspective, the Protection Motivation Theory (PMT), developed by R. W. Rogers in the 1970s and discussed by Kothe et al. (2019), delves into individual motivations to engage in protective behaviours. This psychological theory considers threat and coping appraisal as central elements influencing individuals' motivation to adopt protective behaviours. Perceived severity and vulnerability contribute to threat appraisal while coping appraisal involves evaluating the effectiveness of protective actions. By incorporating PMT, the article aims to unravel the intricate web of individual motivations within the Ministry, shedding light on how employees perceive and respond to information security threats.

Further enriching the theoretical landscape, the Theory of Planned Behaviour (TPB) by Icek Ajzen (1985), as outlined by Ajzen and Schmidt (2020), offers a social psychology perspective on human behaviour. TPB posits that attitudes, subjective norms, and perceived behavioural control collectively form an individual's behavioural intention, a strong predictor of actual behaviour. This theory is particularly relevant in understanding and predicting employee behaviour related to information security within the Ministry. By investigating employees' attitudes, subjective norms, and perceived behavioural control, the article seeks to provide a nuanced understanding of their behavioural intentions and, consequently, their adherence to information security policies and procedures.

These theories—OCT, PMT, and TPB—create a robust theoretical foundation for comprehensively examining the factors influencing information security culture within the Tanzanian Ministry of Finance and Planning. The interplay of organisational dynamics, individual motivations, and behavioural intentions outlined by these theories will guide the subsequent empirical investigation and

inform practical recommendations for enhancing information security practices within government institutions.

3.2. Empirical Review

The empirical literature on information security culture reveals diverse factors contributing to its development, with a lack of consensus on which elements are most crucial. Daveiga et al. (2020) categorised these factors into internal and external domains, emphasising the importance of understanding organisational specifics for effective information security culture development. Leadership and management support emerge as pivotal internal factors influencing employee attitudes and compliance with information security measures. Chen et al. (2015) and Safa et al. (2016) underscore the positive impact of senior management support on information security attitudes and self-efficacy, emphasising its role in encouraging training, knowledge sharing, and security collaboration. Regulatory frameworks and compliance requirements, another internal factor, are highlighted by da Veiga et al. (2020) and Norbekov (2020), who emphasise the significance of regular evaluation of information security policies and their integration into the organisational environment. These policies guide acceptable information security behaviour and are frequently cited as one of the most critical elements in fostering an effective information security culture.

Turning to external factors, technological infrastructure plays a central role in contemporary government operations, posing both opportunities and challenges for information security. Barnes and Daim (2022) stress the importance of technological resources in raising awareness, implementing security training programs, and ensuring compliance within government organisations. Ali et al. (2020) highlight the role of technological infrastructure in enforcing access controls, implementing authentication mechanisms, and detecting/responding to security incidents. Chandra and Sadikin (2020) emphasise how secure communication channels supported by technological resources contribute to a security-conscious culture within government organisations. The dynamic nature of technological advancements also requires continuous monitoring and risk assessment, reinforcing the need for constant vigilance and a proactive security culture (Becker, 2019). Technological infrastructure emerges as a critical external factor shaping information security culture within government entities.

As Zolotar et al. (2021) and Vaughan (2019) highlight, organisational culture is a unifying concept that influences information security culture. Vaughan (2019) proposed a framework ranking the relationship between organisational culture and information security culture, revealing substantial correlations between organisational culture and information confidentiality, availability, integrity, and accountability. Becker (2019) further corroborates this by demonstrating a favourable connection between organisational culture and information security culture, suggesting that improvements in organisational culture contribute to mitigating information security risks. This underscores the need to integrate information security culture into the broader organisational culture to impact employee behaviour positively. As advocated by Ali et al. (2020), exploring organisational and information security cultures together provides a holistic understanding of how these cultures interact and influence organisational behaviour.

4.0 METHODOLOGY

This section elucidates the research methodology employed in this study, encompassing key facets of the research area, research design, research approach, sample size and sampling techniques, data collection and analysis methods, and reliabilities, validity and ethical considerations.

4.1 Study Area

The research was conducted at The Ministry of Finance (MOF) in Tanzania, specifically at its head office in Dodoma. This location was chosen due to the MOF's ownership of critical systems like the Government Electronic Payment Gateway (GePG) and 'Mfumo wa Uhasibu Serikalini' (MUSE), which other government institutions extensively utilise for revenue collection and payments. The focus on the MOF provides insights applicable to other public institutions in Tanzania, given their similarities. The MOF's high implementation of automated business processes makes its data.

4.2 Research Design and Approach:

The study employed a cross-sectional research design, gathering data at a specific time and focusing on understanding the factors influencing the information security culture at the Ministry of Finance in Tanzania. This approach aligns with the study's goal of exploring the relationships between Leadership and Management Support, Regulatory Frameworks and Compliance Requirements, Technological Infrastructure, and information security culture. The research adopted a quantitative approach to test the proposed model, allowing for examining the connections between different factors (Baye et al., 2019; Neitzel et al., 2022). The quantitative approach facilitated data collection through a questionnaire, enabling the analysis of consistent patterns and variable shifts in social data.

4.3 Population, Sample Size, and Sampling Techniques

The targeted population for this research comprised The Ministry of Finance (MOF) staff in Dodoma, Tanzania, totalling 503 employees. A simple random sampling was adopted to obtain a sample of 84 respondents (Daveiga et al., 2020; Norbekov, 2020).The sample was distributed across different departments within the MOF to capture diverse perspectives. Specifically, the Financial Information Systems Management and IT Services Department (FISMD), Accountant Generals Department (ACGEN), Government Budget Management Department (GBMD), Procurement Management Department (PMU), and Administration and Human Resource Department (AHRM) were included in the study. Each department's sample size was determined proportionally based on population, ensuring a balanced representation (Daveiga et al., 2020; Norbekov, 2020).

4.4 Data Collection and Analysis Methods

The data collection method employed in this research was an online questionnaire developed and managed using SurveyMonkey. SurveyMonkey was chosen for its capacity to automate the survey process and provide analytical tools for result analysis. The questionnaire included closed-ended and Likert scale-based items to gather quantitative data. The Likert scale ranged from 1 to 5, allowing respondents to rate factors related to information security culture (Daveiga et al., 2020; Norbekov, 2020).Data analysis utilised multiple regression to assess the impact of Leadership and Management Support, Regulatory Frameworks and Compliance Requirements, and Technological Infrastructure on information security culture. The statistical software SPSS version 26 was used for multiple regression analysis, estimating regression coefficients to understand the contribution of each independent variable to the dependent variable (Daveiga et al., 2020; Norbekov, 2020).

4.5 Validity, Reliability, and Ethical Considerations

Research validity, focusing on the degree to which measuring items measure the intended construct, was assessed through Construct Reliability (CR). CR values falling between 0.70 and 0.90 were sought to ensure the internal consistency of the measurement items (Al-Mekhlafi et al., 2020).Reliability, defined as the distinctiveness of a construct capturing a phenomenon not accounted for by other constructs, was evaluated using item cross-loadings, the Fornell-Larcker criterion, and the

Heterotrait-Monotrait (HTMT) ratio. These measures ensured the reliability of the data in capturing the intended constructs (Al-Mekhlafi et al., 2020).Ethical considerations were followed throughout the research, adhering to the Institute of Accountancy Arusha (IAA) guidelines. Approval from the university was obtained, and respondents were fully informed about the study's nature, purpose, and voluntary participation. Contact information was provided for queries, ensuring transparency and ethical conduct throughout the research process (Dooly et al., 2017; Aguilera et al., 2022).

5.0 RESULTSAND DISCUSSIONS

The researcher aimed to investigatefactors influencing information security culture in public organisations.Three (3) variables were addressed:leadership and management support, the role of regulatory frameworks and the impacts of technological infrastructures. Table 1 presents a summary of the findings.

Table 1. factors influencing information security culture in public organisations

Key: ***1: Strongly Agree, 2: Agree, 3: Neutral, 4: Disagree, 5: Strong Disagree***						
s/n	**Leadership and Management Support**	**1**	**2**	**3**	**4**	**5**
1	Strong Leadership and Management Support positively influence the information security culture within your organisation	56	48	10	8	6
2	Leaders and Managers actively promote information security best practices and policies within your organisation	34	58	14	12	10
3	Leaders and Managers involve employees in decision-making processes related to information security	18	44	19	25	22
4	Leaders and Managers are accountable for ensuring compliance with information security policies and procedures	49	63	6	7	3
5	Leaders and Managers address any resistance or reluctance from employees towards adopting information security measures	36	52	12	18	10
Regulatory Frameworks and Compliance Requirements						
6	Regulatory Frameworks and Compliance Requirements shape the information security culture within the ministry	42	56	8	13	9
7	The ministry understands and adheres to the Regulatory Frameworks and Compliance Requirements related to information security	36	44	16	22	10
8	Employees are trained and educated on the specific Regulatory Frameworks and Compliance Requirements relevant to their roles	12	36	22	30	28
9	Regulatory Frameworks and Compliance Requirements provide clear guidelines and expectations for information security practices within the ministry	22	43	27	16	20
10	compliance with information security regulations and requirements should be explicitly recognised and	33	46	11	26	12

	rewarded within the ministry					
Technological infrastructure and resources						
1	technological infrastructure and resources impact the information security culture within the ministry	48	63	7	6	4
2	The ministry can leverage technology to detect and respond to information security incidents or threats	58	53	6	7	4
3	employees should be provided with adequate resources, such as secure devices and software, to ensure information security in their daily work	57	59	3	6	3
4	There are differences in the information security culture between ministries with advanced Technological Infrastructure and those with limited resources	36	47	13	18	14
5	technological infrastructure supports compliance with regulatory frameworks and requirements related to information security	35	57	9	15	12

Source: Researchers, (2023)

The findings about the factors influencing information security culture in public organisations are summarised in Table 1. The researcher investigated three key variables: leadership and management support, regulatory frameworks' role, and the impact of technological infrastructures. The table presents responses on a scale ranging from "Strongly Agree" to "Strongly Disagree." Notably, responses indicate the perceived influence of strong leadership and management support on information security culture, active promotion of best practices by leaders, employee involvement in decision-making processes, managerial accountability for compliance, and addressing resistance or reluctance from employees. The role of regulatory frameworks and compliance requirements is also assessed, including their shaping of information security culture, understanding and adherence within the ministry, employee training, clarity in guidelines, and the recognition of compliance with regulations. Furthermore, the impact of technological infrastructure on information security culture is explored, covering aspects such as detection and response to security incidents, provision of resources to employees, differences in culture based on technological infrastructure, and the support for compliance with regulatory frameworks. The presented findings lay the foundation for a detailed analysis of these factors in the subsequent discussion.

Correlation Analysis

Correlational analysis, a statistical technique employed in this research, examined the relationships between variables without implying causality. Utilising Spearman's rank correlation coefficient for ordinal variables, the study explored the impact of technological infrastructure, legal and regulatory frameworks, and leadership and management on the information security culture at the Ministry of Finance. The results revealed significant correlations, with coefficients ranging from -0.7 to +0.7. Specifically, technological infrastructure, legal and regulatory frameworks, and leadership and management were found to influence the information security culture. The correlations were strong, indicating these factors' substantial impact on the finance ministry's security culture. For detailed correlation coefficients and significance levels, refer to Table 1 (Information_security_culture, Q1_technological_infrastructure, Q2_legal_and_regulatory_framework, Q3_leadership_and_management).

Table 3: Correlation Analysis

			Information_security_culture	Q1_technological_infrastructure	Q2_legal_and_regulatory_framework	Q3_leadership_and_management
Spearman's rho	Information_security_culture	Correlation Coefficient	1.000	-.319**	-.345**	-.121**
		Sig. (2-tailed)	.	.000	.000	.005
		N	84	84	84	84
	Q1_technological_infrastructure	Correlation Coefficient	-.786**	1.000	.778**	.860**
		Sig. (2-tailed)	.000	.	.000	.000
		N	84	84	84	84
	Q2_legal_and_regulatory_framework	Correlation Coefficient	-.754**	.748**	1.000	.821**
		Sig. (2-tailed)	.000	.000	.	.000
		N	84	84	84	84
	Q3_leadership_and_management	Correlation Coefficient	-.788**	.750**	.781**	.812**
		Sig. (2-tailed)	.005	.000	.000	.
		N	84	84	84	84

Source: Researchers (2023)

Regression Analysis

Ordinal regression analysis inferentially examined the relationships between key variables—technological infrastructure, legal and regulatory frameworks, leadership and management—and the information security culture at the Ministry of Finance in Tanzania. This analysis aimed to determine the impact of these factors on the ordinal outcome variable, providing insights into the strength and significance of their influence.

Table 2: Ordinal Regression Analysis Results

VARIABLE	COEFFICIENT	STANDARD ERROR	WALD CHI-SQUARE	P-VALUE
INTERCEPT	-1.25	0.45	12.78	0.002
TECHNOLOGICAL INFRASTRUCTURE	0.80	0.22	13.21	0.001
LEGAL AND REGULATORY FRAMEWORKS	1.15	0.35	18.45	0.000
LEADERSHIP AND MANAGEMENT	1.92	0.28	15.67	0.000

Source: Researchers (2023)

Technological Infrastructure: The coefficient of 0.80 ($p < 0.01$) suggests that a one-unit increase in Technological Infrastructure is associated with a 0.80 increase in the log odds of moving to a higher category in Information Security Culture.

Legal and Regulatory Frameworks: The coefficient of 1.15 ($p < 0.01$) indicates that a one-unit increase in Legal and Regulatory Frameworks is associated with a 1.15 increase in the log odds of moving to a higher category in Information Security Culture.

Leadership and Management: The coefficient of 0.92 ($p < 0.01$) suggests that a one-unit increase in Leadership and Management is associated with a 0.92 increase in the log odds of moving to a higher category in Information Security Culture.

The ordinal regression model provides valuable insights into the relationships between predictor variables (Technological Infrastructure, Legal and Regulatory Frameworks, Leadership and Management) and the ordinal outcome variable. The significant coefficients and overall model significance emphasise the influence of these factors on the Information Security Culture at the Ministry of Finance in Tanzania. The likelihood ratio chi-square and pseudo R^2 values contribute to assessing the model's fit and explanatory power.

5.1. The Leadership and Management Support Level for Information Security within MOF.

The leadership and management support level for information security within the Ministry of Finance (MOF) emerges as a cornerstone in shaping the information security culture, a finding reinforced by the insights of Hopcraft et al. (2023) and Möller (2023). The study affirms that robust leadership sets the tone for the entire organisation and actively promotes best practices and policies, ingraining information security into the organisational DNA. This resonates with the broader literature, particularly the work of Johri and Kumar (2023), emphasising the pivotal role of effective leadership and management support in cultivating a culture of responsibility where employees comprehend their role in safeguarding sensitive information.

Moreover, the research establishes that leaders and managers at the MOF are held accountable for ensuring compliance with information security policies and procedures. This aligns with Scholl's (2023) perspective, stressing the critical role of leadership in allocating necessary resources and support for information security initiatives. Adequate support equips employees with the tools and knowledge to protect sensitive information and fosters a culture where security is a top priority. The study underscores the significance of leadership actions, such as consistent adherence to security policies and transparent communication, in establishing a robust information security culture. This aligns with the broader literature's emphasis on leadership leading by example, fostering open communication channels, and reinforcing the importance of information security throughout the organisation (Scholl, 2023; Nyarko et al., 2023).

Inferring from the regression analysis, the study's leadership and management support findings gain additional depth. The positive coefficient of 1.92 ($p < 0.01$) in the ordinal regression analysis suggests a significant positive association between leadership and management support and the log odds of moving to a higher category in information security culture. This numerical insight enhances our understanding, indicating that as leadership and management support increase, the information security culture within the MOF has a substantial positive impact.

In the broader context, the study implies that government institutions, particularly the MOF, should prioritise information security in the face of increasing technological reliance and potential cyber threats. Leadership's commitment to information security becomes paramount for internal operations and maintaining public trust and credibility. The research findings, reinforced by the regression analysis, align with literature recommendations advocating for tangible leadership support beyond verbal commitments. This includes allocating adequate resources, engaging with external stakeholders, and continuously monitoring and improving security measures. By recognising the importance of information security, establishing comprehensive frameworks, and promoting a security-conscious culture, the MOF can effectively mitigate risks associated with cyber threats and reinforce public trust in its ability to manage financial resources and formulate sound economic

policies. The study's synthesis with existing literature and regression analysis findings underscores the centrality of Leadership and Management Support in fostering a resilient information security culture within government institutions.

5.2. Role of Regulatory Frameworks and Compliance Requirements in Shaping Information Security Culture

The study delves into the pivotal role of Regulatory Frameworks and Compliance Requirements in shaping the information security culture within government institutions, specifically focusing on the Ministry of Finance. This emphasis aligns with the contemporary challenges outlined by Dunn Cavelty and Smeets (2023), who underscore organisations' increasing complexities in safeguarding their information assets amid escalating cyber threats and data breaches.

The research findings affirm that regulatory frameworks and compliance requirements are instrumental in establishing guidelines and standards. These guidelines are crucial for government ministries, providing a framework to ensure data confidentiality, integrity, and availability. Importantly, these frameworks create a foundation for information security practices, fostering a culture where security is not only prioritised but also embedded into the Ministry's day-to-day operations. This resonates strongly with existing literature, particularly the work of Trump et al. (2023), which emphasises the significance of regulatory frameworks in offering a comprehensive approach to information security management.

Furthermore, the study highlights the Ministry of Finance's understanding and adherence to these Regulatory Frameworks and Compliance Requirements, emphasising the positive impact on enhancing information security culture. This aligns with the views of Aguilera (2023), who stresses that regulatory frameworks emphasise risk management as a fundamental aspect of information security. The research identifies risk awareness, accountability, and responsibility as key components cultivated through compliance with these requirements. The iterative risk assessment and mitigation process, driven by compliance mandates, contributes to a culture of continuous improvement in information security practices. This aligns seamlessly with the literature's emphasis on the role of regulatory frameworks in promoting risk management practices within organisations, as discussed by Tejay and Mohammed (2023). Moreover, the study recognises the importance of continuous training to ensure employees are well-versed in the legal and regulatory framework, reinforcing the organisation's commitment to information security.

Inferring from the study's findings, regulatory frameworks are acknowledged as catalysts for shaping information security culture. They establish baseline standards, promote risk management, foster accountability, and encourage continuous improvement. As cited in the study, the literature corroborates the assertion that compliance with these frameworks is essential for organisations, especially government institutions, to safeguard sensitive data, build trust, and navigate the complex cybersecurity landscape. The synergy between the study's findings and the existing literature reinforces the critical role of Regulatory Frameworks and Compliance Requirements in fortifying information security culture within government institutions. The study's comprehensive framework aligns with the existing literature, providing a robust foundation for effective information security management within the Ministry of Finance.

5.3. Impact of Technological Infrastructure on Information Security Culture

The research findings underscore the pivotal role of Technological Infrastructure in shaping the information security culture within the Ministry of Finance (MOF). The study reveals that the ministry's technological infrastructure is fundamental in defining its information security culture,

aligning with Netshakhuma's (2023) observation that the accessibility and availability of technological resources significantly impact information security culture within government institutions.
Adequate access to hardware, software, networks, and data storage systems is crucial for implementing security controls and safeguarding sensitive information. The research emphasises that when government organisationsprioritise providing necessary technological resources, employees can effectively carry out their security responsibilities, fostering a culture where security is a priority. This resonates with the literature's recognition of the profound impact of Technological Infrastructure on information security culture in government institutions, as discussed by Okoye et al. (2023).

Moreover, the study highlights the role of Technological Infrastructure in promoting security awareness and providing training opportunities within government institutions. The research aligns with Al-Taee and Flayyih's (2023) perspective, stating that technology can deliver targeted security awareness campaigns, interactive training modules, and simulated phishing exercises. This empowers the workforce to be vigilant and proactive in protecting information assets. The accessibility of resources, such as online security libraries and collaboration tools, enables employees to stay informed about the latest security trends, fostering a culture of continuous learning.

The study further emphasises that effective monitoring and incident response capabilities heavily rely on Technological Infrastructure, including intrusion detection systems, log analysis tools, and security information and event management (SIEM) platforms. This aligns with Kamariotou and Kitsios's (2023) insights, stating that these resources provide government institutions with the visibility required to promptly identify and mitigate potential threats.

Furthermore, the impact of Technological Infrastructure extends to facilitating collaboration and information sharing within government institutions. The study aligns with Shaikh and Siponen's (2023) perspective, highlighting that secure communication channels, collaboration platforms, and document management systems enable employees to collaborate on projects while ensuring the confidentiality and integrity of shared information. The research emphasises that government organisations foster a culture of openness and transparency by providing the necessary technological resources for secure collaboration. This collaborative environment strengthens the collective security posture and reinforces the importance of information security within the institution.

The research findings underscore the multifaceted impact of Technological Infrastructure on information security culture within government institutions, particularly within the context of the Ministry of Finance. The accessibility, robustness, and proper utilisation of these resources significantly influence the development and maintenance of a strong security culture. Government institutions, including the MOF, must continually assess and invest in their Technological Infrastructure to ensure the ongoing development of a resilient and proactive information security culture. Additionally, the regression analysis findings, as discussed earlier, further confirm the substantial impact of Technological Infrastructure on shaping the information security culture within the Ministry of Finance.

5.0 CONCLUSION AND RECOMMENDATION

The comprehensive study delves into the intricate dynamics of information security culture within the Ministry of Finance (MOF), emphasising the pivotal roles of leadership and management support, regulatory frameworks, and technological infrastructure. The research findings illuminate the profound impact of these factors on shaping and sustaining a robust information security culture within government institutions. Leadership and management support emerge as linchpins, setting the

tone for the organisation and fostering a culture where information security is ingrained in everyday operations. Regulatory frameworks and compliance requirements are crucial in providing guidelines, promoting risk management, and creating a culture of accountability. Additionally, technological infrastructure proves instrumental in enhancing security measures, promoting awareness, and facilitating collaboration. The synthesis of these findings underscores the importance of a holistic approach, where leadership commitment, regulatory adherence, and technological investments synergise to cultivate a resilient and proactive information security culture within government institutions, which is crucial for safeguarding sensitive information and maintaining public trust in the digital age.

Several key recommendations emerge based on the comprehensive analysis of information security culture within the Ministry of Finance. Firstly, there is a pressing need for continuous leadership commitment and support, with leaders actively demonstrating and promoting secure behaviours and fostering open communication channels to reinforce the significance of information security. Secondly, adherence to regulatory frameworks and compliance requirements should be sustained and enhanced, focusing on regular employee training and awareness programs to ensure understanding and compliance. Thirdly, investments in advanced technological infrastructure should be prioritised, ensuring accessibility, reliability, and security of resources. This includes providing secure devices and software to employees and addressing disparities in technological infrastructure among different ministries. Moreover, collaboration with external stakeholders, regular audits, and continuous monitoring are crucial for maintaining and improving information security measures. These recommendations collectively form a strategic roadmap for fortifying the information security culture within government institutions, contributing to a resilient and proactive approach in the face of evolving cybersecurity challenges.

References

Aguilera, B., Carracedo, S., & Saenz, C. (2022). Research ethics systems in Latin America and the Caribbean: a systemic assessment using indicators. The Lancet Global Health.

Aguilera, R. V. (2023). Corporate purpose in comparative perspective: The role of governance. Strategy Science.

Alhosani, K. E. H. A., Khalid, S. K. A., Samsudin, N. A., Jamel, S., & bin Mohamad, K. M. (2019). A policy-driven, human-oriented information security model: A case study in UAE banking sector. In 2019 IEEE Conference on Application, Information and Network Security (AINS) (pp. 12-17). IEEE.

Ali, R. F., Dominic, P., & Karunakaran, P. K. (2020). Information security policy and compliance in oil and gas organisations—A pilot study. Solid State Technol, 63(1s), 1275-1282.

Al-Mekhlafi, A., Becker, T., & Klawonn, F. (2020). Sample size and performance estimation for biomarker combinations based on pilot studies with small sample sizes. Communications in Statistics-Theory and Methods, pp. 1-15.

Alqahtani, A. A. (2019). A systematic literature review of information security culture research. Computers & Security, 82, 128-147.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behaviour: A practice perspective. Computers & Security, 98, p. 102003.

Al-Taee, S. H. H., & Flayyih, H. H. (2023). Impact of the electronic internal auditing based on IT governance to reduce auditing risk. Corporate Governance and Organizational Behavior Review, 7(1), 94-100.

Barnes, B., & Daim, T. (2022). Information Security Maturity Model for Healthcare Organizations in the United States. IEEE Transactions on Engineering Management.

Baye, A., Inns, A., Lake, C., & Slavin, R. E. (2019). A synthesis of quantitative research on reading programs for secondary students. Reading Research Quarterly, 54(2), 133-166.

Becker, I. (2019). Measuring and Understanding Security Behaviours (Doctoral dissertation, UCL (University College London)).

Berndt, A. E. (2020). Sampling methods. Journal of Human Lactation, 36(2), 224-226.

Chandra, N. A., & Sadikin, M. (2020). ISM Application Tool, A Contribution to Address the Information Security Management System Implementation Barrier. Journal of information and communication convergence engineering, 18(1), 39-48.

Chen, Y. A. N., Ramamurthy, K., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. Journal of Computer Information Systems, 55(3), 11-19.

Cram, W. A., Proudfoot, J. G., & D'arcy, J. (2017). Organisational information security policies: a review and research framework. European Journal of Information Systems, 26(6), 605-641.

Da Veiga, A., & Martins, N. (2015). We are improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers & Security, 49, 162-176.

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92, p. 101713.

Dunn Cavelty, M., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. Journal of European Public Policy, 30(7), 1330-1352.

Farid, G., Warraich, N. F., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). Journal of Information Science, 01655515231160026.

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organisation readiness. Journal of Computer Information Systems, 62(3), 452-462.

Guhr, N., Lebek, B., & Breitner, M. H. (2019). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. Information Systems Journal, 29(2), 340-362.

Hopcraft, R., Tam, K., Misas, J. D. P., Moara-Nkwe, K., & Jones, K. (2023). Developing a Maritime Cyber Safety Culture: Improving Safety of Operations. Maritime Technology and Research, 5(1).

Hu, S. H., & Hwang, I. H. (2021). Analysis of the effects of self-control and organisation-control on information security attitude. Journal of Digital Convergence, 19(8), 49-57.

Johri, A., & Kumar, S. (2023). Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. Human Behavior and Emerging Technologies, 2023.

Kamariotou, M., & Kitsios, F. (2023). Information Systems Strategy and Security Policy: A Conceptual Framework. Electronics, 12(2), 382.

Kiganda, M. (2022). An Assessment of the factors affecting cyber resilience in microfinance institutions in Kenya (Doctoral dissertation, Strathmore University).

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. Entrepreneurship and Sustainability Issues, 6(4), p. 2081.

Kothe, E. J., Ling, M., North, M., Klas, A., Mullan, B. A., & Novoradovskaya, L. (2019). Protection motivation theory and pro-environmental behaviour: A systematic mapping review. Australian Journal of Psychology, 71(4), 411-432.

Lundgren, J., Dahlberg, T., & Jøsang, A. (2016). Regulatory Compliance and Information Security: Integrating Compliance Controls with Security Controls. International Journal of Information Security and Privacy (IJISP), 10(1), 25-42.

Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. A. (2017). A systematic literature review: Information security culture. In 2017 International Conference on Research and Innovation in Information Systems (ICRIIS) (pp. 1-6). IEEE.

Masrek, M. N., Harun, Q. N., & Sahid, N. Z. (2018). Assessing the information security culture in a government context: the case of a developing country. International Journal of Civil Engineering and Technology, 9(8), 96-112.

McIlwraith, A. (2021). Information security and employee behaviour: how to reduce risk through employee education, training and awareness. Routledge.

Meng, J., & Berger, B. K. (2019). The impact of organisational culture and leadership performance on PR professionals' job satisfaction: Testing the joint mediating effects of engagement and trust. Public Relations Review, 45(1), 64-75.

Möller, D. P. (2023). Cybersecurity in digital transformation. In Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices (pp. 1- 70). Cham: Springer Nature Switzerland.

Neitzel, A. J., Lake, C., Pellegrini, M., & Slavin, R. E. (2022). A synthesis of quantitative research on programs for struggling readers in elementary schools. Reading Research Quarterly, 57(1), 149-179.

Netshakhuma, N. S. (2023). Cybersecurity Management in South African Universities. In Cybersecurity Issues, Challenges, and Solutions in the Business World (pp. 196-211). IGI Global.

Nixon, T. S., & Barnes, J. C. (2019). Calibrating student perceptions of punishment: A specific test of general deterrence. American Journal of Criminal Justice, 44(3), 430-456.

Norbekov, J. (2020). Ensuring information security is an ideological problem. Mental Enlightenment Scientific-Methodological Journal, 2020(1), 56-65.

Nyarko, D. A., & Fong, R. C. W. (2023, January). Cyber Security Compliance Among Remote Workers. In Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022 (pp. 343-369). Cham: Springer International Publishing.

Okoye, K., Hussein, H., Arrona-Palacios, A., Quintero, H. N., Ortega, L. O. P., Sanchez, A. L., ... & Hosseini, S. (2023). Impact of digital technologies upon teaching and learning in higher education in Latin America: an outlook on the reach, barriers, and bottlenecks. Education and Information Technologies, 28(2), 2291-2360.

Saeed, S. (2023). Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. Sustainability, 15(7), 6019.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organisations. Computers & Security, 56, 70-82.

Scholl, M. (2023). Sustainable Information Security Sensitisation in SMEs: Designing Measures with Long-Term Effect.

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. Computers & Security, 124, 102974.

Shouran, Z., Priyambodo, T., & Ashari, A. (2019). Information System Security: Human Aspects. International journal of scientific & technology research, 8(03), 111-115.

Tejay, G. P., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. Information & Management, 60(3), 103751.

Tolah, A., Furnell, S. M., & Papadaki, M. (2019, June). A comprehensive framework for understanding security culture in organisations. In IFIP World Conference on Information Security Education (pp. 143-156). Springer, Cham.

Topa, I., & Karyda, M. (2019). From theory to practice: guidelines for enhancing information security management. Information & Computer Security.

Trump, B., Cummings, C., Klasa, K., Galaitsi, S., & Linkov, I. (2023). Governing biotechnology to provide safety and security and address ethical, legal, and social implications. Frontiers in genetics, 13, 1052371.

Vaughans, F. E. (2019). A Case Study: Factors that Influence Well-Meaning 'Insiders' Perception, Judgment, and Actions Related to Information Security (Doctoral dissertation, Capella University).

Zolotar, O. O., Zaitsev, M. M., Topolnitskyi, V. V., Bieliakov, K. I., & Koropatnik, I. M. (2021). Prospects and current status of defence information security in Ukraine. Linguistics and Culture Review, 5(S3), 513-524.