





Assessing Challenges Facing Implementation of Information Security Critical Success Factors: A Case of National Examination Council, Tanzania

Daniel Maingu Magesa 
National Examination Council, Tanzania

Juma Ally Mshana  
Senior Lecturer, Department of Informatics, Institute of Accountancy Arusha (IAA),
Dar es Salaam Campus, Tanzania

Suggested Citation

Magesa, D.M. & Mshana, J.A. (2023). Assessing Challenges Facing Implementation of Information Security Critical Success Factors: A Case of National Examination Council, Tanzania. *European Journal of Theoretical and Applied Sciences*, 1(5), 883-897.
DOI: [10.59324/ejtas.2023.1\(5\).74](https://doi.org/10.59324/ejtas.2023.1(5).74)

Abstract:

Aim of this study was to assess challenges facing implementation of information security critical success factors. The study employed quantitative research approach and survey research design where case study design was used. A sample of 79 respondents derived from the population sample of 372 were used by using Slovin's formula sampling technique, 86% of respondents questionnaire filled effectively were used. Descriptive data analysis was used to analyze variables based on research questions while, statistical tables and figures were used in data presentation.

Results of this study indicate that, there are challenges in implementation of information security critical success factors such as security training program, security policy, risk assessment, regular system update, system auditing and committed of top management. The study found reasons for challenges of implementation from respondent views as availability of limited resources, weak financial support from top management, lack of understanding of needed technology from information technology professionals; poor security awareness program for top management who may think that information security is the issue of information technology department only and not the whole organization. It is therefore concluded that organization should identify their specific information security critical success factors to enhance useful of organization limited resource, without investing in generalization and give solutions based on risk priority, in order to make organization secure also utilization of information security critical success factors holds significant importance in ensuring security of an organization's data. It is crucial to address and eliminate any challenges that are within the scope of affordability or manageability.

Keywords: *Information Security Government, Information Security Critical Success Factor.*

Introduction

Data security success is a critical issue in organizations recently and make competitive among them. Studies found areas which when are satisfied will assure success in organization

data security, these factors differ organizations wide, hence there is a need of identification of these factors organization wide (Gashgari et al., 2017; Klimoski, 2016). Significant agreement on information security critical success factors assist



the creation of information security culture, which is associated with factors such as training and education, risk analysis and assessment, compliance, ethical conduct, top management support, security policy, information security awareness, information security policies and implementation of security procedure (Alnatheer, 2015; Zammani & Razali, 2016; Arbanas, 2019). Weakness in security practice reveal that there is an increase in threat in many organizations in Tanzania which imply to data vulnerability, apart from organizations measured to protect their data it is due to poor understanding of critical success factors (Gashgari et al., 2017; Anslow & Drechsler, 2019; TCRA, 2019). When organizational information security critical success factors are identified and satisfied they may qualify their data security (Zammani & Razali, 2016). There are numbers of known information security critical success but their effectiveness differ in different studies and different organization as well due to culture, rule, regulations (Alghamdi et al., 2020).

Despite of success in collection of income through system from government there is possibility of attack since new threats are inevitable, vulnerability are discovered while organization aim at increasing profit and reduce security budget (Bada et al., 2016). Much concentrates is given to technical, vast research found that it is not just a technical issues but it is cross cutting issue and address on necessity of identification of information security success factors in totality in order to ensure data safety (Zammani & Razali, 2016)

Organization seek data security but face challenge in identification and implementation of critical areas of concentration, that is information security critical success factors identification which others found that is based on three aspects and these are organization issues that is policy and procedures, process issues such as resource planning, training and awareness, risk management, business continuity management and information system audit but also many studies focus on just internal environment of the organization rather than

technology-focused which need more study (Alghamdi et al., 2020)

Study from Saudi Arabia on identification and implementation of information security critical security factors such as top management active involvement, proper risk management, accountability and compliance, and propose COBIT and ISO/IEC 27014 frameworks which found suitable locally due to local laws and regulations, research need more investigation in the field by using social variables, different organization with different culture to create a best-practice system (Gashgari et al., 2017)

Information security critical success factors assist the creation of information security culture, these factors are; training and education, risk analysis and assessment, compliance, ethical conduct, top management support, security policy, information security awareness and information security policies. Literature not agreed on principle and information security critical success factors that can create security culture and recommend further study to be done qualitatively and in large-scale survey and analysis on challenges of implementation (Alnatheer, 2015; Zammani & Razali, 2016).

According to the study from private Bank in Tehran, information security key factors when implemented properly and practiced frequently results into data security success, expert views identify factors as top management support, awareness, training programs, policy, job responsibilities, and motivation compliance with information security international standards. Similar study conducted in Finland depicted, top management support, security policy, awareness, training and job responsibilities as key factors when properly implemented provide data protection but recommend further study on large sample and different environment (Sadeghi, 2016)

Despite similarities in identified information security key success factors, their effectiveness differ due to sample, political environment but some of them resemble such as information system audit which is the most effective, for the case of similarities further studies is needed to challenges related to modern technology such as

Web of Things, cognitive computing, savvy cars, smart cities and other which bring modern threats (Arbanas, 2019)

Information security success factors guarantee organization data security, but before information security implementation the organization should identify its information security critical success factors in order to focus its limited resources in that area rather than focus on totality. Proper understanding of organization information security success factors, can help organizations to manage on how to focus limited resources on critical areas, therefore saving time and money and creating added value and further enabling operational business when are implemented properly (Tu, 2014; Gashgari et al., 2017; Klimoski, 2016; Arbanas, 2019)

Organizations face challenges in implementation of information security critical success factor due to human behavior such as resistance to change and expose of security risks, lack of top management support in finding project or delay activities as results to outdated security policy to be able to address modern security concerns (Lubua, 2022; Wallin, 2023)

Therefore, the study assesses challenges of information security critical success factors implementation to enhance data security at National Examination Council of Tanzania.

Literature Review

The study on critical success factors as reviewed by Abraham, (2019) identify many critical success factors and the author choose to study the top most effective and these were awareness, top management support and information security policy implementation. Identification of the key success factors principles differ in different organizations due to organization culture and information system practice, some literature agreed in principles and others differ in this study on identification of key information system security factors, some found security risk analysis, ethical conduct policies as key success factors (Alnatheer, 2015)

Review on security-awareness campaigns depict security awareness as among the information system key security factors which stimulate willing to change. Training and continuous feedback is necessary when creating cyber security awareness campaigns (Bada et al., 2016). Establishment of effective information security policy, awareness, training and education, risk analysis, risk assessment, information security compliance, ethical conduct policies, organization culture were identified as keys information system security success factors even though threats are inevitable, as long as new vulnerability are discovered every now and then (Alnatheer, 2015; Klimoski, 2016)

Cyber Security Awareness Campaigns recommend security awareness as the information system security factors, and aims to identify key factors regarding security, they found human as most cited factor and suggest the change of people's behavior through security awareness campaigns as this results correlate with others (Bada et al., 2016; Havlí, 2019). Critical success factors identified based on three aspects, these are organization issues that is policy and procedures, process issues such as resource planning, training and awareness, risk management, business continuity management and information system audit and these were found in seven domains which consists of 27 critical success factors that must be considered during developing effective information security governance framework through systematic literature review and literature analysis (Alghamdi et al., 2020)

Tu et al, (2014) proposed the theoretical model to investigate factors contribute to success in organization information security and propose six critical success factors such as business alignment, organization support, competences, awareness of security risk and control and information security control these factors were identical with other but have a few new factors which were not identified. According to Gashgari et al., (2017) who develop the framework which include information security key factors in government while compared with other successful frameworks in previous research and test his framework which reveal

positive effect at government organization in Saudi Arabia, based on major concertation areas; strategic alignment, performance measurement, value delivery, risk management and resource management

Other information security key factors such as top management support, information security policy, training and education, assessment and risk analysis, information security compliance, ethical conduct policies and organization culture where found as identical to the previous research through literature analysis (Alnatheer, 2015). Surveys of organizations through systematic empirical, find factors recognizable as a performance of ISMS certification indicators to enhance the overall security level (Kong et al., 2016). It is recommended to organization to follow international security standards as key success factor in information system to ensure robust security standards otherwise system compromise is inevitable (Muhati, 2018)

Few studies have examined the effective factors in successful implementation of information security systems but lacked a coherent framework of effective factors; some did not examine the priorities and specific relationship between factors. Some adopted a quantitative approach in addition to identifying and implementation of factors and identify the relative priorities. Other studies found key performance indicators and recommend identified factors to be kept up to date in further studies. Motivation and awareness are among the widely highlighted factors. Training, positive attitude, security stability; clear understanding of security requirements, participation in information security are well supported variables in implementation of information security systems (Kazemi et al., 2012; Waly et al., 2012; Kazemi et al., 2018)

According to study focused on finding success factors for self-implementation from qualitative standpoint, implementer commitment, management commitment and implementer competency were found and the finding were beneficial in providing guidance towards the self-implementation and maneuver of ISMS at the Plan Phase in government sector (Maarop et

al., 2015). Research found that clear information security policy and support the training programs for workers will eliminate the obstacles that limit the development of management information systems in the River Nile State, recommendation and support of the scientific research in this area to reach the best results. Our results coincide with the literature on skills and competencies needed for successful cybersecurity professionals and reinforced the idea that communication skills are critical and this is a key factor (Wang, 2014; Mishra, 2019)

Based on our review more research into information security key success factors is needed due to security challenges associated with new technologies that bring along new threats. Identification of the factors within the organization will ultimately enable the organization to use its limited resources effectively through investing on security factors which matters most (Arbanas, 2019). There are factors that can be extremely helpful such as security awareness; security education, training and continuous feedback and more recommendation on more cyber security awareness campaigns around the world, especially in North America and Asia, to examine the extent to which they have implemented the factors mentioned above and their levels of campaign success (Bada et al., 2016)

The theoretical model is developed through literature review and has never been tested. The model's reliability and validity need support from empirical studies. Little empirical study has been done on information security management from organizational level and its operation need validation for further studies. Hence, stronger theory base is needed to further support this research model (Tu, 2014). The findings of the present study indicate that among the factors influencing successful implementation of information security are existence of regular and appropriate processes that lead operator's specific responsibility, accountability and possibility of monitoring performance regularly, and recommend decision-makers make trade rules for importing the hardware needed for providing information security in businesses and

future studies on evaluation of impact variables identified in this study on the performance indicators of the success of information security project (Sadeghi, 2016)

Surveys of organizations that required ISMS certification recognize that there is a need of consideration of information security factors through experiment and recommend future research in ISMS certified company in accordance with the satisfaction and effectiveness through systematic empirical approach (Kong et al., 2016). According to Mrakovic (2018) it is discovered that cyber attack may have bring harmful impact on people, marine environment and properties, through his structured survey questionnaire he discovered that there is insufficient level of awareness in and knowledge in cyber security, Research studied the risk of cyber security in submarine. Lastly, using the quantitative risk assessment method, the authors propose the best practices for maritime cyber security in the form of implementation of mandatory training course (Kundy & Lyimo, 2019).

To ensure effective resources management in information systems organization should identified and implements its critical information key success factors in order to concentrate with, according to studies there are effective information security governance recommended framework such as COBIT and ISO/IEC 27014, there is a need of reviewed of proposed framework application to another organization to confirm its suitability when subjected to another law and regulations (Gashgari et al., 2017). The current existing literature analyses have not clearly identified factors that have significant influence on information security which can fit for all organizations, many researches reveal weakness of organization security measures and increase in number of information security threat, among other factors human error contribution in cyber-attacks mostly. Most of studies in critical success factors have been done theoretically and not subjected to empirical for verification (Tu, 2014; Sadeghi, 2016).

Organizations losses a lot of money through cyberattack, South Africa loses \$157 million annually, in 2017 it costed Africa economies \$3.5, countries like Nigeria and Kenya losses estimated to be at \$649 million and \$210 million respectively (Serianu, 2017). TZ-CERT of Jan 2021, reported an increase in cyber security attack from 993,222 to 979,863 within a week and in 2013, financial sector in Tanzania losses almost 1 billion through cybercrime. This poses a huge problem to financial sector and the government at large (Kaimba et al., 2016, World Bank, 2014; TZ-CERT, 2020). There is a problem with identification of information security success key factors and known factors need validation to make a proof with empirical approach since their effectiveness are limited when subjected to another law and regulations (Zammani & Razali, 2016; Bada et al., 2016; Sadeghi, 2016; Kong et al., 2016)

Organizations count their success in collection of income through systems, but there is possibility of attack which may bring down organization operation when cybersecurity investment is not done appropriately. Organization invest in technical aspect, but data security is not just a technical issues but it cut across all organization, and problem is not just investment but is about what make difference between success and failure, hence is necessary to identify the key success factors (Zammani & Razali, 2016; Bada et al., 2016)

Many researches which have been done in identification of information security critical success factor were categorizing its factors in three aspects; these are organization issues, process issues and information system audit. By using literature analyses, study found significant agreement on critical factors that assist the creation of information security culture, these factors are; training and education, risk analysis and assessment, compliance, ethical conduct, top management support, security policy, information security awareness, policies, and organization culture, and suggest confirming of these factors to be done quantitatively through a large-scale survey (Alnatheer, 2015; Zammani & Razali, 2016). Another study found identical results on positive impact on identified key

success through expert views as top management support, awareness, training programs, policy, job responsibilities, and motivation compliance with information security international standards. Finland study found identical results as top management support, information security policy, awareness and training programs and job responsibilities and other three hypotheses have been rejected so large sample space and different environment may show different output (Sadeghi, 2016)

Studies conducted on successful implementation of information security systems lacked a coherent framework of effective factors; some did not examine the priorities and specific relationship between factors. Some adopted a quantitative approach in addition to identifying and implementation of factors and identify the relative priorities. Other studies found key performance indicators and recommend identified factors to be kept up to date in further studies. Motivation and awareness are among the widely highlighted factors in implementation of information security systems. Many proposed models are still not subjected to empirical for verification, hence more grounded hypothesis base is required (Gashgari et al., 2017; Tu, 2014; Klimoski, 2016; Kazemi et al., 2012).

Conceptual framework describes important elements or variables and the postulated relationship among them, in studying the assessment challenges facing implementation of information security critical success factor from participant experience may have concern in enhancement of data security at the National Examination Council of Tanzania.

Methodology

This paper chooses a survey research design as it seems to provide easy way to answer questions and the purposes of the study. The design studied by collecting and analyzing data from a few people as the representative of the entire group public opinion are characterized by using questionnaire and sampling method (Atac & Akleyek, 2019; Avedian, 2014) Quantitative

research approach was used due to the fact that the study needs empirical proof (Johnson & Christensen, 2020; Mertens, 2013). Targeted population was 372 respondents, by using purposive sampling which target respondents who have reliable information concerning the subject matter. Slovin's formula was used because of population behavior (Lono, 2018) and deduce 79 required respondents from the population which was provided with questionnaires

Study questionnaires was adopted from Centre for Internet Security and National Institute of Standards and Technology and customized to meet study requirements Jr et al (2019). Items content validity was done through Lawshe's method of 1975, pre-test was done to check if it will provide the output which will answer the study question appropriately Jr et al (2019) also Cronbach's Alpha was used as it was introduced by Lee J. Cronbach back in 1951 to check questionnaire internal consistency and reliability.

Prior to analysis, the acquired data were processed and confirmed. Before being coded into numerals to make them compatible for analysis, the data were edited, compiled, classified, tabulated, and summarized to detect errors and omissions. SPSS and Microsoft Excel were used for descriptive analysis to analyze variables based on research questions. Descriptive statistics such as frequencies, percentages and cross-tabulations were used in data analysis. Statistical figures were used in data presentation.

Results and Discussions

Based on respondents' views, there is depiction of challenges facing implementation of identified information security critical success factors, specifically information security training. Thus data collected through questionnaires are presented in the figure below.

Information security training implementation

Findings from figure 1 indicate that majority (41%) of the respondents agreed facing

challenge on implementation of information security training (23%) strongly agreed, (7%) of the respondents strongly disagreed and (25%) of the respondents disagreed. The remaining (5%) of the respondents were neutral of facing implementation challenge.

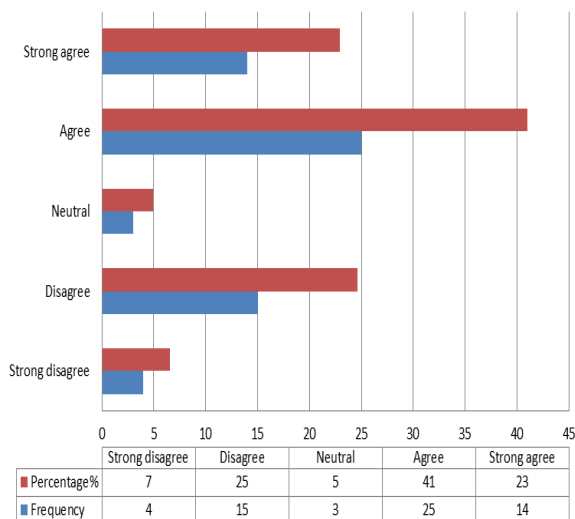


Figure 1. Challenge Facing Information Security Training Implementation

From that point of view it can be argued that, majority of the respondent face challenge the findings collaborate that of Tidwell (2011) who found that challenge and argued organizations to increase employee training and awareness to avoid accidental and careless also Haukilehto (2019) coincide with our study as he found availability of insufficient staff training due to lack of budget and time hence results into organizations cyber security problems and inefficient operation Andra (2019).

Information system auditing

Findings in figure 2 indicate that (36%) of the respondent which is majority strongly agreed facing challenges on implementation of information system auditing, (28%) agreed and (11%) of the respondents strongly disagreed. (15%) of the respondents disagreed and (10%) which is the minority of the respondents were neutral.

As majority of respondent face challenge this study collaborate that of Ceausu et al (2018) who found that challenge in information system auditing due to incompetency in audit personnel and recommend training in order to attain efficient information system audit also Zaslavskiy et al (2018) found, effectiveness of the security measures must include internal audits and recommend best audit option through combine the audit on process with the checklist not to skip specific security issues

Zaslavskiy et al (2018) and Zammani et al (2019) findings coincide with this study on challenges facing implementation information system audit since third party audit feedback take much time and recommend to be done regularly so that identified security problem may be fixed timely and recommend team to possess the necessary auditing skills and applying appropriate auditing techniques.

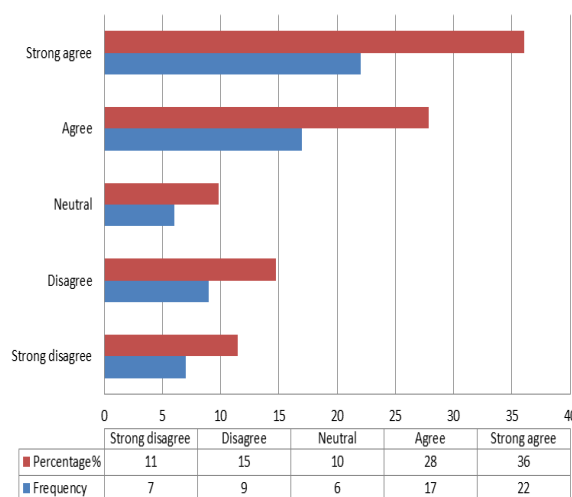


Figure 2. Challenges Facing Information System Auditing Implementation

Implementation of information security policy

Findings in figure 3 indicate that there is a challenge in implementation of information security policy as majority of respondents (43%) agreed with that, (30%) strongly agreed, (13%)

were neutral, (8%) of the respondents strongly disagreed and minority (7%) of the respondents.

The findings from this study collaborate that of Kabanda et al (2018) who found that there is no personal security commitment agreement which make employees, third parties and stakeholders to be committed to follow information security policy, also collaborate that of Alotaibi & Almagwashi (2018) and Tawalbeh et al (2020) who found lack of BYOD security policy to manage and control its use which is needed to maintain security policy for their devices.

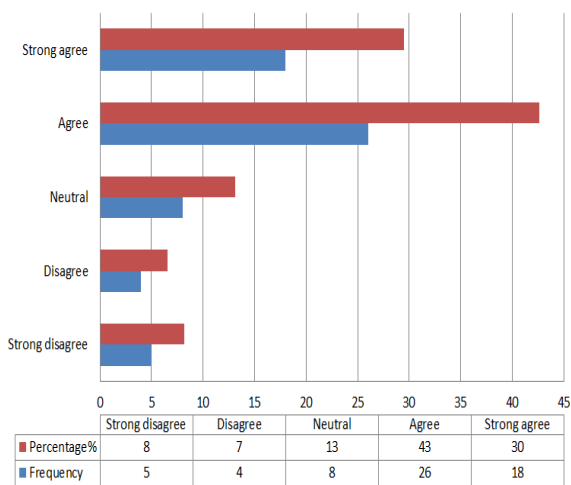


Figure 3. Challenge Facing Implementation of Information Security Policy

Information system risk assessment

Findings in figure 4 above indicate that (16%) of the respondents strongly agreed facing challenge in implementation of information security critical success factors, (41%) of the respondents agreed and (8%) of the respondents strongly disagreed. Also (28%) of the respondents disagreed and (7%) of the respondents were neutral that information system risk assessment was challenges in implementation of information security critical success factors.

From that point of view, it can be argued that, majority of the respondent (41%) agreed that they face challenges in implementation of information system risk assessment as

information security critical success factors in sustainability of information systems security needs. The findings from this study collaborate that of Pham (2019) who found challenge on lack of people with better security skills and risk awareness who comply with the standard, hence violate security policies also risk assessment is a challenging task, tedious and repetitive, and argue organization may seek to build better infrastructure and efficient software which can reduce task complexity and motivate task performance.

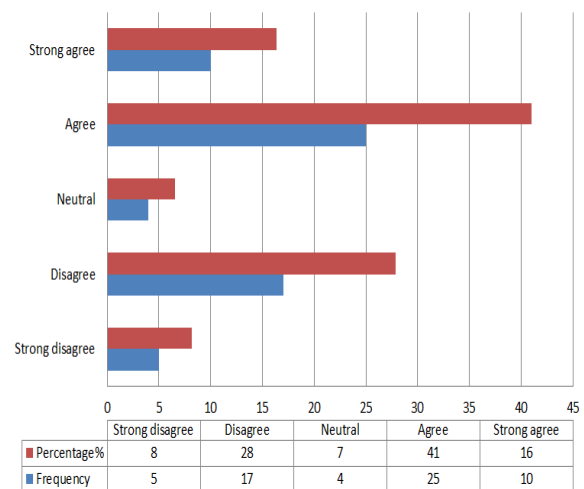


Figure 4. Challenge Facing Information System Risk Assessment

Mura (2019) and Sauerwein et al (2018) findings collate with the study on lack of education so recommend education to participant in order to reduce uncertainties and resource investment to reduce time and software solution to analyze more complex cyber threat intelligence task and also some small organization do not perform security risk assessment and insist all enterprises need to adopt risk management in order to assess and treat risks accordingly and obtain the success of information security management.

Information system security management support

Findings in figure 5 indicate that (25%) of the respondents strongly agreed that they face challenge from management during

implementation of information system security as information security critical success factors, (3%) of the respondents agreed and (3%) of the respondents strongly disagreed. Also (46%) of the respondents disagreed and (23%) of the respondents were neutral, respondents were asked whether there were facing challenges in implementation of information system security from top management.

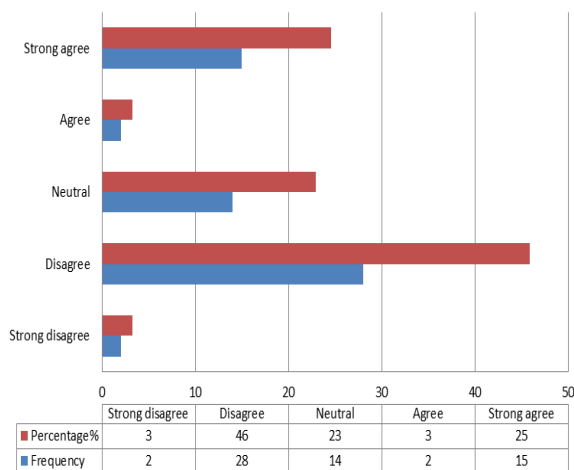


Figure 5. Challenge Facing Management Supports Implementation

From that point of view, it can be argued that, majority of the respondent (46%) disagreed that there are challenges of implementation of information security system from top management as information security critical success factors in sustainability of information systems security needs. The findings from this study collaborate that of Twizeyimana et al (2018) who found many e-government projects failure is due to poor management supports as the key challenge, some institutions want effective information security solution without preparation during working with partners and expect to everything from partner hick is due to lack of awareness about the nature of the problem and solution coverage.

Findings of Somepalli et al (2020) coincide our study as he found some organization consider that information security management is the IT department issue only and not of the whole

organization, hence the process of finding solution become the issue of the department with limited authority and the organization issue with full of management supports, hence recommend management to ensure that everyone now is aware of information system security needs and importance and COBIT was designed for management to bridge the gap, also Ionescu et al (2018).

Information system security awareness

The respondents were asked whether there were challenges in implementation of information system security awareness programs. Findings in figure 6 indicate that (26%) of the respondents strongly agreed that they face challenge in implementation of information system security awareness as information security critical success factors at the Organization, (49%) of the respondents agreed and (8%) of the respondents strongly disagreed. Also (13%) of the respondents disagreed and (3%) of the respondents were neutral about facing challenges in implementation of information system security awareness program information security critical success factors. From that point of view, it can be argued that, majority of the respondent (49%) agreed that there are challenges of implementation of security awareness as an identified information security critical success factors in sustainability of information systems security needs.

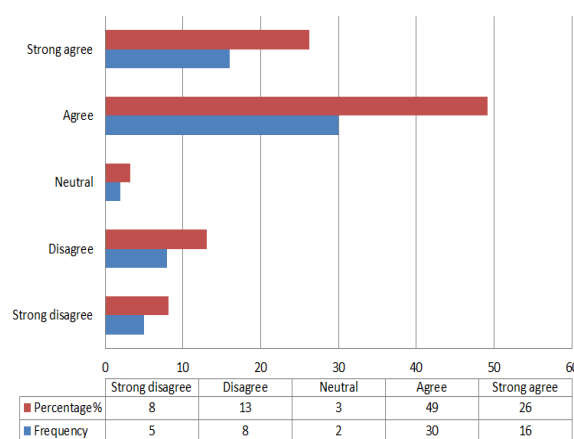


Figure 6. Challenge Facing Information System Security Awareness Implementation

The finding of the study coincide that of Alotaibi & Almagwashi (2018) who found that in order to implement information system security awareness there are cost need to be incurred that is material and technology cost needs money, the study collaborate that of Alghamdi et al (2020) who found cost in changing organization culture, because after awareness program the organization culture should change to become with security change as is found in ISG framework.

Zammani et al (2019) argued that there is no motivation towards awareness of latest security policy, threats and issues that occur in the organization hence cost of awareness programs is to ensure the employees, third parties and stakeholders are aware of IS policy, IS issues and IS threats as well as their responsibilities in protecting the organization's information is needed.

Zaslavskiy et al (2018) found challenge that some stakeholders are not aware of specific threats to the cloud infrastructure, hence there is a need to take measures to detect threats and avoid them before they occur, Also according to Alotaibi et al (2018) there is a challenge in both information security technology and human factor awareness and many organization concentrate mainly on technology awareness and weaken human factor awareness which is considered as the weakest link in line of defense.

Regular system update

The findings presented in Figure 7 highlight respondents' views on the challenges associated with regular system updates as a critical factor in information security implementation. A significant portion, 34%, strongly agreed that such updates posed challenges, while 26% agreed, and 11% strongly disagreed. Additionally, 18% disagreed, and 10% were neutral on this issue.

This suggests that a majority (34%) of respondents acknowledged the difficulties in implementing regular system updates, which aligns with the research of Kabanda et al (2018). Their work found that keeping systems up-to-date, including operating systems and antivirus

software, is challenging and costly, especially in regions with poor security practices. Similarly, Gyunka & Christiana (2015) pointed out that investing resource in maintaining workers' security knowledge can reduce cyber breaches but is often challenging due to budget constraints and a lack of awareness about the importance of information system security.

Furthermore, the study coincides with Waithaka (2016) findings, emphasizing the weak information infrastructure and unpatched systems due to budget limitations and a lack of understanding of information system security's necessity. Sen (2018) also noted the complexity and potential negative impacts of software patches, causing concerns about business continuity.

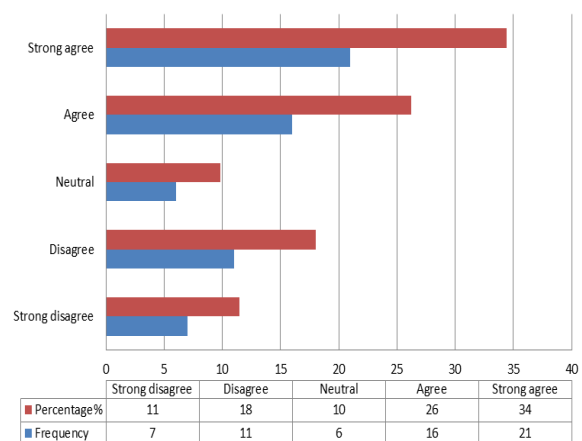


Figure 7. Challenge Facing Regular System Update

Conclusions

The study's findings indicate significant challenges in implementing various aspects of security measures, including security training programs, information security policies, routine risk assessments, regular system updates, information system audits, and receiving support from dedicated top management. These findings are valuable for future research as they contribute to the existing body of knowledge in the field of security implementation.

Recommendations

It is worth to conclude that in order to strengthen information system security at the National Examination Council of Tanzania, challenges faced during implementation of information security critical success factors challenges should be removed, since their effective implementations enable the organization data to be secure.

This study makes the following recommendations; First, Priority should be given to information security training program in order to equip them to be able to handle organization data threat and protect organization data that will improve capability of new knowledge and their effective application in the context of globalization to cope information security threat due to lack of its expertise and provision of regular risk assessment task. Second, Organization should implement information security policy effectively per international security standards to avoid threat due to failure to comply with information security policies. Thirdly, provision of management supports through funding information system security projects, provide proper security hygiene through performing systems regularly update such updating operating system currently released systems patches, anti-virus software and infrastructure systems to reduce organization's cyber security breaches. Fourthly, Organization should enhance motivation towards awareness of latest security threats and policy implementation for in-house, third parties and stakeholders as human factor considered as the weakest link in line of defense, through awareness behavior should change and security culture establishment. The study was limited to the case study; hence similar study including additional organization of the same nature with bigger sample size is required for generalization purposes as well as qualitative study.

References

Abdullov, A. J., Odinayeva, N. F., & Adizov, B. B. (2021). Training Highly Qualified Staff in

Development of Uzbekistan. *Research Innovation In Multidisciplinary Sciences*, 2021, 288–292.

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

<https://doi.org/10.1016/j.cose.2020.102030>

Alnatheer, M. A. (2015). *Information Security Culture Critical Success Factors*. In 12 th International Conference on Information Technology - New Generations, 731–735.

<https://doi.org/10.1109/ITNG.2015.124>

Alotaibi, B., & Almagwash, H. (2018). *A Review of BYOD Security Challenges, Solutions and Policy Best Practices*. 2018 1st International Conference on Computer Applications & Information Security, 1–6.

<https://doi.org/10.1109/CAIS.2018.8441967>

Alotaibi, M. & Alfahid, W. (2019). *Information Security Awareness: A Review of Methods, Challenges and Solutions*. In Internet Technology and Secured Transactions (ICITST-2018). At: University of Cambridge, Churchill College.

<https://doi.org/10.2053/ICITST.WorldCIS.WCST.WCICSS.2018.0016>

Andra, C. (2019). *Applying design system in cybersecurity dashboard development*. Aalto University School of Science.

Anslo, C., & Drechsler, A. (2019). *Information Security in Agile Software Development Projects: A Critical Success factor Perspective*. In European Conference on Information Systems, 1–17.

Arbanas, K. (2019). Key Success Factors of Information Systems Security. *Journal of Information and Organizational Sciences*, 43(2), 131–144. <https://doi.org/10.31341/jios.43.2.1>

Atac, C., & Akleyek, S. (2019). A Survey on Security Threats and Solutions in the Age of IoT. *European Journal of Science and Technology*, 15, 36–42. <https://doi.org/10.31590/ejosat.494066>

Avedian, A. (2014). Survey Design. Retrieved from <https://hnmcp.law.harvard.edu/wp-content/uploads/2012/02/Arevik-Avedian-Survey-Design-PowerPoint.pdf>

- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2016). *Cyber Security Awareness Campaigns : Why do they fail to change behaviour ?* In International Conference on Cyber Security for Sustainable Society. <https://doi.org/10.48550/arXiv.1901.02672>
- Bada, M.B. & Von Solms, A.I. (2019). Reviewing National Cybersecurity Awareness in Africa : An Empirical Study. Academy for Computer Science and Software Engineering. Retrieved from <https://api.repository.cam.ac.uk/server/api/core/bitstreams/5c149709-b619-4f5d-8f9f-14fdb467e45/content>
- Caulkins, B.P. & Bockelman, L.R. (2016). Using a Behavioral Cybersecurity Paradigm. *IEEE Computer Society*.
- Choeje, P., Murray, D., & Fung, C. C. (2016). *Exploring critical success factors for Cybersecurity in Bhutan's Government Organizations*. In Eighth International Conference on Networks & Communications, 49–61. <https://doi.org/10.5121/csit.2016.61505>
- Choi, S., Martins, J. T., & Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. *Journal of Information Science*, 44(6), 752–767. <https://doi.org/10.1177/0165551517748288>
- Cohen, N., Hulvey, R., Mongkolnchaiarunya, J., Novak, A., Robert, W., & Segal, A. (2017). Cybersecurity as an engine for growth. Cybersecurity Initiative, September. Retrieved from <https://www.jstor.org/stable/pdf/resrep10491.1.pdf>
- Crick, T., Davenport, J. H., Irons, A., & Prickett, T. (2019). *A UK Case Study on Cybersecurity Education and Accreditation*. 49th Annual Frontiers in Education Conference (FIE 2019), 1–16. <https://doi.org/10.48550/arXiv.1906.09584>
- Gashgari, G., Walters, R., & Wills, G. (2017). *A Proposed Best-practice Framework for Information Security Governance*. IoTBDS 2017 - 2nd International Conference on Internet of Things, Big Data and Security, 295–301. <https://doi.org/10.5220/0006303102950301>
- Gupta, H., Mondal, S., Ray, S., Giri, B., Majumdar, R., & Mishra, V. P. (2019). Impact of SQL Injection in Database Security. In ReseachGate (Ed.), *Computational Intelligence and Knowledge Economy* (Issue December, pp. 296–299). IEEE. <https://doi.org/10.1109/ICCIKE47802.2019.9004430>
- Gyunka, B. A., & Christiana, A. O. (2015). *Analysis of Human Factors in Cyber Security : A Case Study of Anonymous Attack on Hbgary*. University of Ilorin.
- Haney, J. M., & Lutters, W. G. (2017). *Skills and Characteristics of Successful Cybersecurity Advocates*. *Symposium on Usable Privacy and Security (SOUPS)*. Thirteenth Symposium on Usable Privacy and Security, SOUPS 2017, Santa Clara, CA, USA, July 12-14.
- Hashim, R., & Razali, R. (2019). Contributing Factors for Successful Information Security Management Implementation. *Innovative Technology and Exploring Engineering*, 9(2), 4491–4499. <https://doi.org/10.35940/ijtee.B7214.129219>
- Haukilehto, T. (2019). *Improving Cyber Security awareness*. JAMK University of Applied Science.
- Havli, D. (2019). Human Factors in the Cybersecurity of Autonomous Vehicles. *Trends in Current Research*. 10(May), 1–7. <https://doi.org/10.3389/fpsyg.2019.00995>
- Hayashi, P., Abib, G., & Hoppen, N. (2019). Validity in Qualitative Research: A Processual Approach. *The Qualitative Report*, 24(1), 98–112. <https://doi.org/10.46743/2160-3715/2019.3443>
- Horne, C. A., Maynard, S. B., & Atif, A. (2019). *A Theory on Information Security : A Pilot Study*. Proceedings of the 14th Pre-ICIS Workshop on Information Security and Privacy, Munich, 1–23.
- Ionescu, R. C., & Ilie, Ceausu, I. (2018). *Considerations on the implementation steps for an information security management system*. Proceedings of the 12th International Conference on Business Excellence 2018, 476–485. <https://doi.org/10.2478/picbe-2018-0043>

- Johnson, R. B., & Christensen, L. (2020). Methods of data collection in quantitative, qualitative and mixed reserach. *SAGE Journal Article*, 179–206.
- Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, 28(3), 269–282. <https://doi.org/10.1080/10919392.2018.1484598>
- Kaimba, B., Musuva-Kigen, P., Matafu, R., Masesa, D., Kimani, K., Mwangi, M., Munyendo, B., Mueni, F., & Ndegwa, D. (2016). *Achieving Cyber Security Resilience: Enhancing Visibility and Increasing Awareness*. In Tanzania Cyber Security Report.
- Kavitha, V., & Preetha, S. (2019). Cyber Security issues and Challenges - A Review. *International Journal of Computer Science and Mobile Computing*, 8(11), 1–6.
- Kazemi, M., Khajouei, H., & Nasrabadi, H. (2012). Evaluation of information security management system success factors: Case study of Municipal organization. *African Journal of Business Management*, 6(14), 4982–4989. <https://doi.org/10.5897/AJBM11.2323>
- Klimoski, R. (2016). Critical Success Factors for Cyber Security Leaders: Not Just Technical Competence. *People + Strategy*, 39(1), 14–18.
- Kljucnikov, A., Mura, L. & Sklenar, D. (2019). Information security management in SMEs: factors of success. *Entrepreneurship and Sustainability Issues*, 6(4), 2081–2093. [https://doi.org/10.9770/jesi.2019.6.4\(37\)](https://doi.org/10.9770/jesi.2019.6.4(37))
- Kong, H., Woo, J., Kim, T., & Im, H. (2016). Will the Certification System for Information Security Management Help to Improve Organizations' Information Security Performance? The Case of. *Indian Journal of Science and Technology*, 9(June), 1–12. <https://doi.org/10.17485/ijst/2016/v9i24/96106>
- Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77–81. <https://doi.org/10.1080/1097198X.2019.1603527>
- Kundy, E. V. A. D., & Lyimo, B. J. (2019). Cyber Security Threats in Higher Learning Institutions in Tanzania, A case of University of Arusha and Tumaini University Makumira. *Olva Academy – School of Researchers*, 2(3), 1–38.
- Lono, L. (2018). Microcredit And Its Relationship To The Growth Of Small And Medium Enterprises In Konoin Subcounty, Kenya. *International Journal of Advanced Research*, 6(4), 961–968. <https://doi.org/10.21474/IJAR01/6935>
- Maarop, N., Mustapha, N. M., Yusoff, R., Ibrahim, R., Megat, N., & Zainuddin, M. (2015). Understanding Success Factors of an Information Security Management System Plan Phase. *World Academy of Science, Engineering and Technology, Open Science Index 99, International Journal of Computer and Information Engineering*, 9(3), 884–889.
- Marinagi, C. C., Trivellas, P., Eberhagen, N., & Skourlas, C. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia – Social and Behavioral Sciences*, 147, 424–428. <https://doi.org/10.1016/j.sbspro.2014.07.133>
- Mehregan, M. R., Jamporzam, M., & Hosseinzadeh, M. (2012). An integrated approach of critical success factors (CSFs) and grey relational analysis for ranking KM systems. *Procedia – Social and Behavioral Sciences*, 41, 402–409. <https://doi.org/10.1016/j.sbspro.2012.04.048>
- Mertens, D. M. (2013). Mixed methods. Reviewing Qualitative Research in the Social Sciences, 139–150. <https://doi.org/10.4324/9780203813324-11>
- Mishra, S.P., Cellante, J., & Poullet, D.K. (2019). Student perceptions of skills and competencies needed for Cybersecurity programs and careers. *Issues in Information Systems*, 20(2), 9–17. <https://doi.org/https://doi.org/10.48009/2>
- Muhati, E. (2018). cc
- Muhati, E. (2018). *Factors affecting cyber-security in Kenya – A Case of Small Medium Enterprises*

(Thesis). Strathmore University. Retrieved from <http://suplus.strathmore.edu/handle/11071/6013>

Paresh, R. & Hamalainen, T. (2017). *A Novel Model for Cybersecurity Economics and Analysis*. 17th IEEE International Conference on Computer and Information Technology, 274–279. <https://doi.org/10.1109/CIT.2017.65>

Parrish, A., Impagliazzo, J., Asghar, M. R., & Pereira, T. (2018). *Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-discipline*. Proceedings Of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education, 19. <https://doi.org/10.1145/3293881.3295778>

Pham, H. C. (2019). Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications Information security burnout*, 46, 96–107. <https://doi.org/10.1016/j.jisa.2019.03.012>

Sadeghi, R. A. (2016). Identifying Key Success Factors in the Implementation of Information Security Systems on Service Businesses: A Case Study of the Private Banks of Tehran. *American Journal of Theoretical and Applied Business*, 2(4), 28–37. <https://doi.org/10.11648/j.ajtab.20160204.11>

Sarmah, S. S. (2019). Database Security Threats & Prevention. *International Journal of Computer Trends and Technology*, 67(5), 46–53.

Sauerwein, C., Sillaber, C., & Breu, R. (2018). *Shadow Cyber Threat Intelligence and Its Use in Information Security and Risk Management Processes*. Researchgate.

Sen, R. (2018). Challenges to cybersecurity: Current state of affairs. *Communications of the Association for Information Systems*, 43(1), 22–44. <https://doi.org/10.17705/1CAIS.04302>

Serianu. (2017). Demystifying Africa's Cyber Security Poverty Line. Annual Cybersecurity Report. Retrieved from <https://serianu.com/downloads/AfricaCyberSecurityReport2017.pdf>

Siponen, M., Mahmood, M. A., & Pahlila, S. (2010). Compliance with information security

policies: An Empirical Investigation. *IEEE Computer Society*, 69–70.

Somepalli, S. H., Kishore, S., Tangella, R., & Yalamanchili, S. (2020). Information security management. *Information Security Management. Holistica Journal of Business and Public Administration*, 11(2), 1–16. <https://doi.org/10.2478/hjbpa-2020-0015>

Srinivas, J., Das, A. K., & Kumar, N. (2018). Government Regulations in Cyber Security: Framework, Standards and Recommendations. *Future Generation Computer Systems*. <https://doi.org/10.1016/j.future.2018.09.063>

Suduc, & Ana-Maria Bizoi, M. F. F. G. (2010). Audit for Information Systems Security. *Informatica Economică*, 14(1), 43–48.

Sullivan, D. D. (2018). *Repository The Importance of Transparency and Willingness to Share Personal Information*. University of New Hampshire.

Taherdoost, H. (2016). Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *International Journal of Academic Research in Management (IJARM)*, 5(2), 18–27.

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). *Applied Sciences IOT Privacy and Security: Challenges and Solutions*. Licensee MDPI, Basel, Switzerland.

TCRA. (2020). TZ-CERT Honeypots Weekly Report Period: 06. 6–8. Retrieved from <https://www.tzcert.go.tz/wp-content/uploads/2020/06/Report-08th-June-2020.pdf>

TCRA. (2021). TZ-CERT Honeypots Weekly Report Period: 27. 9–11. Retrieved from <https://www.tzcert.go.tz/wp-content/uploads/2022/11/Report-14th-November-2022.pdf>

Tidwell, C. L. (2011). *Testing the Impact of Training with Simulated Scenarios for Information Security Awareness on Virtual Community of practice Members*. University of Central Florida Orlando, Florida.

Tofan, D. C. (2011). Information Security Standards. *Journal of Mobile, Embedded and Distributed Systems*, III(3), 128–135.

Tu, Z. & Yuan, Y. (2014). *Critical Success Factors Analysis on Effective Information Security Management: A Literature Review*. *AMCIS 2014 Proceedings*, 1–13.

Twizeyimana, J. D., Larsson, H., & Gronlund, A. (2018). E-government in Rwanda: Implementation, Challenges and Reflections. *The Electronic Journal of E-Government*, 16(1), 19–31.

Waithaka, S. (2016). Factors affecting Cyber Security in National Government Ministries in Kenya. Retrieved from http://erepository.uonbi.ac.ke/bitstream/handle/11295/100423/Waithaka_Factors%20Affecting%20Cyber%20Security%20In%20National%20Government%20Ministries%20In%20Kenya.pdf?sequence=1

Wang, P. (2014). The Impact of the Sector Type on the Role of Management Information Systems for the Decision- Making Process: RNS-Sudan as Case Study. *Gecss*, 396–402.

Zammani, M., & Razali, R. (2016). An Empirical Study of Information Security Management Success Factors. *International Journal on Advanced Science Engineering and Information Technology*, 6(6), 904–913.

<https://doi.org/10.18517/ijaseit.6.6.1371>

Zammani, M., Razali, R., & Singh, D. (2019). Factors Contributing to the Success of Information Security Management Implementation. *International Journal of Advanced Computer Science and Applications*, 10(11), 384–391. <https://doi.org/10.14569/IJACSA.2019.0101153>

Zaslavskiy, A. A., & Bolnokin, V E Zaslavskaya, O. Yu. Kravets, O. J. (2018). Features of ensuring Information Security when using Cloud Technologies in Educational Institutions. *International Journal on Information Technologies & Security*, 10, 93–102.