Kabale University Interdisciplinary Research Journal (KURJ)

An investigation into information security managerial practices in selected public sector organizations

***Benjamin K. Ahimbisibwe, Peter Nabende and Florence Musiimenta**

Kabale University, Uganda

**Corresponding Author*
bahimbisibwe@kab.ac.ug

KURJ
ISSN 2790-1394

pp. 32 - 40
Vol 2. Issue 1.
May 2023

ABSTRACT

The study aims to examine information security managerial practices in organisations. It was guided by three specific objectives: identification of information security practices critical to information assets management; establishment of implementation processes involved in the execution of structured information security governance; and evaluation of policies that influence information security best practices. In line with these objectives, security was acknowledged as a requisite element in protecting organizational information assets. The study covered two public sector organisations specifically, Uganda Wildlife Authority and National Forestry Authority. Focus was made on information security practices critical to managing information like human security, information classification, procedures for information labelling, compliance, standards, command and control techniques. These security practices were selected based on their importance in the protection of confidentiality, integrity and availability of information assets. Descriptive research design was adopted to describe the phenomenon under study. Being an in-depth inquiry, qualitative approach was used, survey questionnaires representing zero and one scores were designed to collect data. The respondents were purposively selected based on their knowledge in the subject area, cost-effectiveness and delivery of timely results. These respondents included information technology officers, administrative secretaries, data clerks and security guards. Findings from the field were analyzed and presented in meaningful tables. The research findings demonstrate that evaluation of users' actions was hierarchical in nature; based on associations with tasks performed; information security practices are not aligned to guidelines set by National Information Technology Authority; there was need to establish appropriate measures to handle new information security risk in organizations. Based on these findings, recommendations that reflect the importance of examining information security managerial practices in organizations were made.

Keywords: Information security, Information security guidelines, Public sector organizations, Security practices, Security management

Introduction

The increasing importance and value of information as an organization asset makes its security a priority to management at all levels (Eroğlu and Çakmak, 2020). As a strategic resource, information need to be protected throughout the lifecycle. Thus, organisations that have successfully implemented information security practices at all managerial levels have stood a high chance of achieving the confidentiality, integrity

and availability of this resource. However, little research has been carried out to investigate managerial practices and their impact on information security in organisations (Kettinger, Ryoo and Marchand, 2021). To address this gap, our study set out to investigation into information security managerial practices (ISMPs) in selected public sector organizations in Uganda. Information like any strategic organizational resource is liable to threats from insiders or outsiders depending on the circumstances or the weaknesses of the system. Interestingly, most organizations especially in developing countries tend not to give more financial support to services like information security that has not direct financial gains or tangible benefits (Everett, 2016). As a result, Everett (2016) noted that during planning, each time, a debate arises on whether to pay or not to pay for information security management services among stakeholders. This scenario creates biased budgetary allocations often reflected in the entries on balance sheets that display financial inclination due to less attention given by the decision-makers to information security as an item. With advancements in information technology, organizations have recognized information security as a valuable component in planning and management (Chang and Ho, 2006). This inclusion of security has indicated a positive step towards addressing the challenges associated with protection of information assets from threats, unauthorized access and users, and malicious codes. These concerns require implementation of information security managerial structures that would streamline practices for protecting information assets. This situation is not unique to the selected organizations, but a challenge to many organizations world over (Wani and Jabin, 2018).

In this study, the researchers investigated information security management practices in two public sector organizations in Uganda: specifically, Uganda Wildlife Authority (UWA) and National Forest Authority (NFA). Both UWA and NFA still employ traditional command and control style of information security management practices which are largely human, outdated and not aligned to the modern time challenges. Such traditional security management practices have exposed information to risks and increased potential for leakages that subsequently lead to damage or loss of vital information assets (Ometov, Molua, Komarov and Nurmi, 2022). This situation has also made it unmanageable to align the security standards and guidelines set by the National Information Technology Authority-Uganda (NITA-U) into specific operational practices. Undeniably, the described state requires a series of continuous research work to improve on the available security controls that match new threats, risks and institute appropriate checks – hence the instant study.

Both UWA and NFA had neither an all-inclusive information security management policy nor embraced a risk analysis training program adequate to current needs. The non-compliance of these organizations to regulate ISMPs guidelines has led to loss of competitive advantage with organisations offering similar services and products in the region (East Africa). This is coupled by non-conformity to set standards which has undermined formal or secure information sharing, processes, inputs and outputs. All these problems and challenges highlighted have threatened these organization's functional units and undermined their operational effectiveness. The study highlights that governing Boards of Directors for the two organizations and management need to adopt suitable guidelines that cover all aspects of information security management practices. Emphasis was put on examining human aspects and the effectiveness of these practices in public sector organizations particularly finding solutions to three research question: a) what are the information security practices critical to information assets management? b) what are the implementation processes involved in the execution of structured information security governance? c) whether information security policies influence best practices in organizations?

Overview of information security.

Information security has gradually become an essential aspect in which information is accepted as an important facet in most organizations (Cherdantseva and Hilton, 2015). This explains the scope of information security as will be used in this paper. In the context of this study, information is defined as facts or data that distinctively identifies organisations' assets used or processed internally from the transactions managed, to derive economic value and if not properly safeguarded could become a liability or loss to the organization (Adesemowo, Von Solms and Botha, 2016). The concept information security on the other hand is defined as the protection of information assets and systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability (Cherdantseva and Hilton, 2015). From these definitions, it stands out clear that standards, best practices and guidelines need to be enforced, mandating the protection of information (Burdon, 2010). Based on this assertion, both information and information security are important elements in the protection of information assets. To achieve this objective, organizations should adopt policies and procedures that spell out how to effectively implement information security practices. These practices ought to point out the general direction, risk management, activities (dos and don'ts) to be performed in order to protect the organization's informational assets. Protection of informational assets require organizations to implement a range of controls based on the identified risks, assessments made and mitigations advocated. Such controls include providing advice to employees, training and awareness programs, outlining punitive measures for non-compliance, and formulation of appropriate policies. Other technical controls as suggested by Al-Safwani, Fazea and Ibrahim (2018) like firewalls, intrusion detection systems, and access control systems may also be implemented and maintained to protect information in organisations.

Need for information security management practices in Uganda

As noted in the previous section, this study was carried out in two selected public sector organizations in Uganda. These were Uganda Wildlife Authority and National Forest Authority.

The two were chosen because they are governed by Laws enacted by Parliament of Uganda with specific provisions that prescribe management of information under their control. Specifically, UWA was selected because one of its objective is to disseminate information, promote public education and awareness of wildlife conservation and management in the country (Government of Uganda, 2019). While NFA was manages vital information on research and practices meant for public consumption on the country's forests reserves and their protection (Government of Uganda, 2003). Based on these statements, the researchers found them suitable case studies with their objectives aligned to the main purpose of this study. From the definitions espoused, the need for ISMPs in Uganda is a fact. Information security is needed to reduce risks to acceptable levels, manage information related risks, improve on business operations and avert threats that would attack the information assets (Ahimbisibwe and Nabende, 2023). Ideally, information security is considered to be an important element in an organization's setting. Fundamentally, organizations need to protect information in order to reduce the risks associated with unauthorized information disclosure (confidentiality), modification (integrity) and destruction (availability). This would be the utmost situation in every organization. Like most organizations in developing countries, the selected public sector organizations in Uganda have tried to implement controls designed to secure information assets. According to the National Information Communication Technology (ICT) policy of Uganda, (2012), these controls include but not limited to:

a. Securing the nation's electronic communication system for individuals (private and public) as part of creating the information society
b. Enhancing confidence and trust among users and the public; and protect data and network integrity.
c. Preventing, detecting and responding to ICT abuse so as to fight against national, regional and international crimes such as pornography, fraud, money laundering, drug trafficking and terrorism.
d. Implementing ICT security awareness programs amongst users and the public
e. Implementing systems that would help in the discovery, avoidance and timely response to threats relating to ICT crimes and misuse.

Data and Methods

Descriptive design research methodology was adopted using qualitative approach with survey questionnaires representing Zero (0) and one (1) scores to collect data from selected respondents. Our questionnaire was designed in simple English to cater for the different categories of targeted respondents. The respondents were selected purposively based on knowledge possessed on the subject area, cost-effectiveness and timely delivery of results. Questionnaires were personally administered and where possible explanation was made to respondents to help them understand the motive of our study. These respondents included information technology officers, administrative secretaries, data entrants and security guards drawn for the two organizations. Data from the field was cleaned by eliminating incompletely filled and inconsistent questionnaires before it was coded using SPSS. Data was then analyzed and tabulated in meaningful form (Kothari and Gaurav, 2014). Document analysis was also used to supplement the approach used in data collection and analysis. The researcher relied on latter technique because of its convenience since a number of respondents were hesitant to share information on targeted security practices. Based on answers to the research questions, information security practices critical to information assets was identified, structured information security implementation processes were established, and security policies that influence best practices were evaluated. During analysis phase, the themes were formulated according to the research questions and data analysis was done accordingly. Throughout the data analysis and discussion process, various authors were acknowledged, and possible human biases addressed. Details are expressed in the results and discussion sections that follow.

Results

Under this section, data is tabulated according to the themes aligned to the research questions of the study and shown in tables 1 - 3.

Identification of information security practices.

Table 1: Information security practices critical to information assets at UWA and NFA.

Observations	**Scores n = 6**			
Information security practices	UWA	NFA	N/A	Total
Information security classification	0	1	0	1
Defined procedures for information labeling	0	1	0	1
Compliance with security policies and standards	0	0	2	2
Command and control technique	1	1	0	2
Total	1	3	2	6
Percentage	16.7	50.0	34.3	100%

Source: Researcher, 2020

Table 1 shows that NFA recorded a fair majority of scores (50.0%) with regard to practices critical to information security assets. The elements considered included information security practices, security classification, defined procedures for information labeling, compliance with security policies and standards, and command and control technique. Comparatively, the N/A applicable variable scored 34.3%; UWA obtained 16.7%; and NFA registered 50.0%. This finding was important because it indicated information security inadequacy as recognized and attributed to reliance of the two organizations on the traditional command and control techniques.

Establishment of information security processes.

Table 2: Establishment of implementation processes affecting structured information security governance.

Observations	Scores n = 8			
Processes	UWA	NFA	N/A	Total
3rd party access risks and security controls	1	1	0	2
Types of accesses and reasons	1	1	0	2
Document detailing security requirements and control	0	0	1	1
Meeting information security requirements	0	0	1	1
Conventional information security processes maintained	0	0	1	1
Right of information security audit	0	0	1	1
Total	2	2	4	8
Percentage	25.0	25.0	50.0	100%

Source: Researcher, 2020

According to Table 2, the N/A variable scored 50.0% of the total observations. This indicates that UWA and NFA focused on 3rd party access and security control, and types of access and reasons though disregarded adherence to other variables. This is observed where both organizations uniformly recorded zero scores on documentation of security requirements and controls, meeting information security requirements, maintaining conventional information security processes, and right to information security audit.

Management of information Security policies

The scores presented in table 3 were determined through systematic observation of information security data from selected appropriate documents.

Table 3: Evaluation of information security policies that influence best practices.

Observations	Scores n = 8			
Policies	UWA	NFA	N/A	Total
Register of important assets system	0	0	1	1
Defined ownership	0	0	2	2
Information security technocrats forum	1	1	0	2
Authorization of new information processing facilities	0	0	1	1
Information security specialists employed	1	1	0	2
Maintaining appropriate contacts	1	1	0	2
Action in the event of information security incident	0	0	1	1
Frequency of information security policy checks	0	0	1	1
Total	3	3	6	12
Percentage	25.0	25.0	50.0	100%

Source: Researcher, 2020

Table 3 shows that the N/A variable recorded a fair majority score at 50.0% as compared to 25.0% equal score by UWA and NFA respectively. This explains why UWA and NFA were performing poorly in equal proportions on information security management policies. The outstanding documents were: register of important assets system, defined ownership, authorization of information processing facilities, action in the event of information security incident, and frequency of information security policy checks as variables where both organizations recorded zero scores. Both UWA and NFA scored one in documents like information security technocrats forum, information security specialists employed and maintaining appropriate contacts. In effect, UWA and NFA were not bothered to follow NITA-U information security guidelines. This implies that both organizations were missing out on the benefits aimed at aligning promotion of practices central to information security standards and guidelines.

Discussion.

The study was carried out in two public sector organisations with the view of investigating information security managerial practices in these organisations. This section focused on providing answers to the research questions set as follows:

Identification of information security practices.

The study found out that NFA adheres to the generally required statutory detail and performance but not to the guidelines set by NITA-U, while UWA was found to be stuck in the culture of command and control approach of doing business. This observation is important because the variables under examination focused on analyzing information security practices, information security classification, defined procedures for labelling information, compliance with best practices, command and control. Practices were understood to take concrete and observable actions underpinned by required skills, organized knowledge and experience of participants either as individuals or groups assigned to do specific works at operational, tactical or strategic levels (DuBrin, 2022). From the findings, NFA had fair performance with regard to observable actions compared to UWA which largely neglected NITA-U guidelines. Therefore, although both organizations missed out on information security management best practices enshrined in ISO/IEC/2700:2013 (Zaini and Masrek, 2013), NFA exhibited some commendable levels of focused practices than UWA. However, since information security standards were potentially interlinked and interrelated, together both organizations could not adequately ensure business continuity in case incidents occurred.

Establishment of information security processes.

From the findings indicated in table 2, four variables showed both organizations recorded zero scores, a proof that there was missing information security gaps. This study found out that failure by the two organizations to comply with NITA-U regulations created adverse effects on protection of business operations. The remaining two variables 3rd party access risks and security controls, and types of accesses and reasons scored one indicating conformity to NITA-U regulations. These results indicate need to create and coordinate enacted laws, harmonize relevant policies, strategies and programs to govern information security concerns (Government of Uganda, 2014). The researchers found low levels of protection offered to targeted information assets. In both organizations, generally there was poor conceptualization of information security management practices in that staff were still relying on elementary methods of processing information. Evidence showed lack of detailed documents on requirements and control, maintenance of conventional

information security processes and information security audit rights to regulate information security governance in the selected public organizations. This posed a range of possible threats varying from leakage of information to unauthorized persons, potential damage of critical infrastructure and malicious attacks inflicted by either insiders or outsiders. Failure to adhere to conventional processes and audit procedures meant that these organizations use outdated measures to support the implementation of security goals in modern times. However, there is a need to adjust such processes and procedures to match modern time challenges pertaining to information security management in organizations, an approach which allows development of required information security management practices including risk identification, assessment and mitigation. This attitude concurs with the organizations' management process at strategic levels designed to review business operations as a good technique to attract top management's attention in order to address challenges pertaining to information security management.

Management of information Security policies.

In this section, we explain the influence of organizational information security management policies on businesses at UWA and NFA. The scores presented in table 3 were determined through systematic observation of information security data from selected appropriate documents. It was observed that both organizations recorded equal scores (one) in information security technocrats forum, employed information security specialists and maintaining appropriate contacts. The result shows the pre-ICT revolution, workplace design where state management followed a blueprint approach was a tendency that persistently made the two organizations to remain stuck in a traditional inefficient culture of protecting information. Basing on the same reason, top management still assumed the ceremonial importance of being over and above others even in areas where they had no skill, a situation that exhibited professional negligence. Consequently, this led to observance of professional negligence that resulted into failure to adopt NITA-U regulations and implementation of the guidelines thereof. Thus, the observed inefficient implementation of best practices partly explains the bureaucratic way of how respective actors attempt to implement information security policies without regard to advances in the ICT arena. This is exemplified by the UWA (2002) clean desk policy which states thus:

> A clean desk policy shall be followed in order to ensure confidentiality, efficiency and security of office files and equipment. No official documents of UWA may be communicated to any member of the public without the sanction of the Executive Director and no member of staff permitted to take copies of official correspondences unless such correspondence is expressly addressed to him/her.

The above statement confirms nonalignment of UWA provisions with NITA-U guidelines that demand organizations to establish avenues to collect data, process, store or share it through internet with other organizations or users provided they are authorized. Such is the safest way organizations could share information assets given the advancements in ICT without compromising its confidentiality, integrity and availability.

Limitations

Given the sensitivity of the study, some respondents were hesitant to share information on security practices. This was evidenced among information technology specialists and users who were not willing to share data about information security management practices under their control for fear of being reprimanded or losing their jobs. Other approaches like document analysis were employed to fill the gap. Associated to

this, the process was challenging as it involved first enlightening respondents about the motive of our study before answering questions hence allowing certain degree of errors in data collected. However, this did not substantially affect the quality (accuracy) of data collected and the purpose of our study.

Conclusion

The study established that implementation of effective information security practices depends on top management's commitment and established structures at all management levels in organizations. This is possible when:

a. Use' actions are evaluated based on work assigned, tasks accomplished and feedback from line hierarchical managerial levels as opposed to stakeholders only.
b. Information security managerial practices aligned to NITA-U guidelines and enforced accordingly.
c. New information security risks are identified, assessed and appropriate measures established to manage them depending on the circumstances.

Based on the findings, we can conclude that both internal and external attacks are real possible threats to the organizations information assets; and information security is not assured since the risks are associated with multidimensional human activities rather than merely technical concerns. Organizations have been over relying on information technology experts to secure their information assets. However, the organizations need to adjust to more flexible and information-intensive pattern mechanisms that incorporate both human and technical solutions.

Recommendations

This study recommends that organizations should customize and align their information security management guidelines to match NITA-U standards, enforce information security management regulations in compliance with regulations formulated by NITA-U, adopt approaches that would enable them to improve competitiveness and ultimately achieve information security management goals, focus towards production of periodic risk assessment reports as a good practice, persuade top management to allocate adequate resources (financial support), invest in skills development and innovations in information security related infrastructure, improve operations and services in the public sector organizations through use of frontier and disruptive technologies, and regularly review information security management tools to enforce new risks. Future research should focus on developing a framework for implementation of information security managerial practices drawing case studies from both private and public in organizations to produce universally accepted information security guidelines. If the developed framework is tested on site, this could constitute more workable solutions to information security challenges in Uganda.

References

Adesemowo, A.K., Von Solms, R. & Botha, R.A., 2016, 'Safeguarding information as an asset: Do we need a redefinition in the knowledge economy and beyond?' S*outh African Journal of Information Management,* 18(1), a706. http://dx.doi.org/10.4102/sajim.v18i1.706

Ahimbisibwe, B. K., & Nabende, P. (2023). The Institutionalisation of Information Security Management Practices in selected Organisations in Uganda. *International Journal of Advanced Research*, 6(1), 48-63.

Al-Safwani, N., Fazea, Y., & Ibrahim, H. (2018). ISCP: In-depth model for selecting critical security controls. *Computers & Security*, 77, 565-577.

Burdon, M., 2010, 'Contextualizing the tensions and weaknesses of information privacy and data breach notification laws', *Santa Clara Computer & High Technology Law Journal* 27(1), 63–129, viewed 4 June 2014, from http://digitalcommons.law.scu.edu/chtlj/vol27/iss1/3/California

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3), 345-361.

Cherdantseva, Y., & Hilton, J. (2015). Information security and information assurance: discussion about the meaning, scope, and goals. In *Standards and Standardization: Concepts, Methodologies, Tools, and Applications (pp. 1204-1235)*. IGI Global.

DuBrin, A. J. (2022). *Leadership: Research findings, practice, and skills*. Cengage Learning.

Eroğlu, Ş., & Çakmak, T. (2020). Information as an organizational asset: assessment of a public organization's capabilities in Turkey. *Information Development*, 36(1), 58-77.

Everett, C. (2016). Ransomware: to pay or not to pay?. *Computer Fraud & Security*, 2016(4), 8-12.

Government of Uganda. (2003). *The National Forestry and Tree Planting Act, 2003*.

Government of Uganda. (2012). *National information and communications technology policy for Uganda*, Ministry of Information and Communications Technology, Kampala

Government of Uganda. (2014). *National information security policy framework*", National Information Technology Authority-Uganda (NITA-U), Kampala

Government of Uganda. (2019). *The Uganda Wildlife Act, 2019*.

Kettinger, W. J., Ryoo, S. Y., & Marchand, D. A. (2021). We're engaged! Following the path to a successful information management capability. *The Journal of Strategic Information Systems*, 30(3), 101681.

Ometov, A., Molua, O. L., Komarov, M., & Nurmi, J. (2022). A survey of security in cloud, edge, and fog computing. *Sensors*, 22(3), 927.

Uganda Wildlife Authority. (2002). *Human resource manual, human resource unit*. Kampala.

Wani, M. A., & Jabin, S. (2018). Big data: issues, challenges, and techniques in business intelligence. In *Big Data Analytics: Proceedings of CSI 2015* (pp. 613-628). Springer Singapore.

Zaini, M. K., & Masrek, M. N. (2013, December). Conceptualizing the relationships between information security management practices and organizational agility. In *2013 International Conference on Advanced Computer Science Applications and Technologies* (pp. 269-273). IEEE.