Management of Information Security in Public Universities in Nigeria

Thecla Amogechukwu Eze, Chinelo Chinwe-Ekene Aroh
Enugu State University of Science and Technology, Nigeria
University of Hull, UK

Abstract

Information security aims at protecting information assets of an organization from any unauthorized access, disclosure, interference or destruction. It is a well-known fact that educational institutions store immense amounts of information, which they rely on for effective and hitch-free running of their operations. This information can arguably be classified as one of the most important assets and life blood of any organization. Astute managers increasingly recognize that information security is a critical means of securing these assets. This paper seeks to explore the importance and propriety of information security management in public or state-owned tertiary institutions.

1. Introduction

Information has been defined as data with meaning, relevance and purpose [11]. Immense value is attached to these data in any organization, especially as it pertains to institutions of higher learning. Educational institutions store large amounts of sensitive data ranging from contact information, academic records, financial information, health records and national identity records of both staff and students, making them vulnerable to targeted unauthorised interference and compromise.

This paper interrogates the need for information security management in public institutions of higher learning with a view to establishing the propriety for proper and institutionalised information security management framework that will enhance the protection of data assets and prevent unauthorised access of such assets of public owned tertiary institutions.

This paper shall be divided into four parts. Part 1 contains the introduction to this paper and also sets out the structure for the paper. Part 2 will look at the meaning of the key concepts of data assets and information security management as it relates to educational institutions, especially in tertiary institutions in the West African Nation of Nigeria.
In part three, the paper shall be interrogating the challenges impeding information security management in the identified organizations with a view to establishing the necessity and or need to protect, secure and manage data assets for the enhancement of the objectives for which the institutions have been set up. It will interrogate specifically, the lack of national legislation that would guide the processes, practice and procedure of information security management as well as the parallel phenomenon of development duality, which hampers effectiveness information security.

It will then conclude by analysing the relationship between all the components of control and emphasizing that a Nigerian governance framework tailored to the peculiar needs of the nation is important for establishing the policies and executing the controls of information security.

2. Data and Information Asset

Generally, data is a valuable resource relied upon to aid the efficiency of an organization when accurate, relevant and specific. It has been described as asset collected by businesses to aid and improve their decision-making and to help to attain their organizational goals [2]. Policy Enforcement for Big Bata Security. In 2017, 2nd International Conference on Anti-Cyber Crimes (ICACC) (p. 70-74).

Equally, data has been defined as facts and statistics that can be quantified, measured, counted and stored while information is data that has been categorized, counted and thus given meaning, relevance, or purpose [6]. In order words, information results from processing raw facts known as data, which are then stored for use. It could be argued that once data is processed and termed information, it may be likened to a value-added commodity whose original value has been enhanced, which is susceptible to threats and vulnerabilities. In the National Institute of Standards and Technology special publication document revised in 2017, information was aptly captured as facts or ideas, which can be represented (encoded) as various forms of data; and knowledge in any medium or form that can be communicated between system entities [12].

Since this resource aids organizations to attain their goals, it is at the core of the success or failure of any organization and needs to be stored and managed with utmost care. As mentioned earlier, information as a resource for organizational operation and growth can arguably be suggested to be one of the most valuable assets any organization requires for growth.

2.1. Information Security

Any valuable asset owned by a person or entity needs to be properly kept away from danger of being damaged, stolen or compromised in any form whatsoever. In order words, it needs to be secure. To

be secure, information assets need to be protected from the risk of loss, damage, unwanted modification or other hazards [3], which may affect the value of the asset. Information security focuses on ensuring there is no unauthorized traffic flowing across the network.

Information security as defined in NIST SP 800-12r1 is the protection of information and information systems from unauthorized access, use, disclosure, disruption modification or destruction in order to ensure confidentiality, integrity and availability. Confidentiality, integrity and availability are the three tenets of information security; every action or information security risk or control measures implemented is from the perspective of one or more of these three tenets [5].

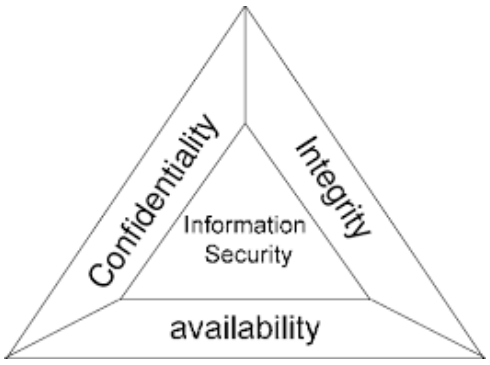

Figure 1. CIA Triad illustrating the tenets of information security (CIA Triad)

In some cases, you will observe that at the centre of the CIA triad is "asset", indicating that every action or control regarding information assets revolves around these tenets. For the avoidance of doubts, ISO/IEC 27000:2017 defines these components as:

a. Confidentiality: Where information is not made available or disclosed to unauthorized individuals, entities or processes;
b. Integrity: The property of accuracy and completeness of assets; and
c. Availability: The property of being accessible and usable upon demand by authorized entity. (ISO/IEC 27000:2017 series)

It presupposes therefore that, a breach in information security occurs where an unauthorized individual, entity or process comes in contact with information asset of an organization; or there is a compromise in the accuracy or completeness of stored information; or when needed by an authorized entity, information is not accessible or usable.

Protection of critical information assets require IT departments to build a strong security posture. Best practices according to include:

- Leverage partnerships with agencies and external entities to improve security controls
- Establish a culture of vigilance and ongoing audit of those controls
- Expand security resilience beyond cybersecurity into the design of processes, the organizational culture, and the executive suite
- Establish and enforce an acceptable-use policy that provides enforceable guidance on what is and is not acceptable in the use of IT assets
- Establish data sharing agreements that structure partner relationships with clear provisions for indemnification, data governance, security expectations, and conditions for remedy or termination
- Encourage a culture of collaboration by setting clear expectations, for collaborative behaviour within departmental routine
- Create incident response plans that clearly identify roles, communication protocols, and expectations for escalation to ensure incident resolution.

3. Challenges impeding Information Security Management in Tertiary Institutions

As established earlier, one of the greatest assets of any organization is information. This is applicable to educational institutions because their information assets contain personal data of both their staff and students, institutional policies and regulations, assessments results of both staff and students and other data that aid the planning and running of their institutions. Accounts for educational institutions are unique in that there are multiple groups of users, each with their own set of needs and challenges. Accordingly, Al-Awadi and Renaud [1] opine that information is an asset, and having specific, relevant and correct information can make a massive difference to an organization's efficiency. In view of these reasons, these assets being of utmost importance need to be securely stored and managed. Managing accounts can be laborious, to make this easier, it can be automated. Information security has been established as a core support for mission of organizations and so, would require a comprehensive and integrated approach that will involve both management and staff of organizations.

Due to the fact that there is a great premium attached to the information asset of these organizations, they are vulnerable to the risk of threats from unauthorized persons and entity. Risk in the context of information security is the outcome the business faces when a threat exploits a vulnerability to successfully attack a target that is being defended [5]. This is where managing information security becomes very important.

Spafford in Okpanem (2013) asserts that the only true security system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards- and even then there are still doubts. Bearing this in mind therefore, it behooves on the institutions to device means of managing information security most appropriately. Threats are continually evolving such as spam mails, identity thefts, phishing, data leakage and many more. The primary role of an information security manager is to identify, manage and mitigate security risks on behalf of the organization [5]. In addition to the manager's technical competences, it is also important that the role is carried out within set principles and regulations in order to be able to understand what is, and how it is, allowable by law to carry out this function. Campbell opines that most information security managers in executing their roles, build a process framework known as information security management system (ISMS) that integrates corporate policy with legislation and compliance requirements, linking in external process, procedures and records [5]. Unfortunately, research carried out show that this is not the case in Nigerian Universities were questionnaires were administered. Further research confirmed that there is as yet no information security legislation in the country. An unsuccessful attempt in 2016 was made to enact the Critical Infrastructure Protection bill. The bill was at best, to be an enactment to protect the technological infrastructure of the government from attack. It is arguable whether this bill, even if passed into law can fill the need for regulating information security practice for both the public and private sector establishments in the country. This is because securing information assets goes beyond physical infrastructure. In fact, due to the risk mitigating factors in information security management which allows for contingency plans, physical threats to assets remain the lowest risks any organization can face. It is the ISMS that specify the requirements any organization must establish, implement, operate, monitor, review, maintain and improve information security. It provides an organization with a comprehensive approach to information security management, which focuses on management of risks [5]. A framework for this is still absent.

Another critical factor impeding information security management in organizations, including educational establishments is development duality. This is a phenomenon where systems and security designs are undertaken in parallel rather than in an integrated manner [7]. It is a known fact that for information security to succeed, an all-encompassing multifaceted approach involving all branches of the organization has to be deployed. This is because research has shown that majority of information security failures are due to violations of control by personnel and not due to technical failures. An example is the Equifax incident in 2017 which had about 147 million accounts of personal data hacked.

As far back as 1988, Baskerville [4] argued that development duality can be overcome if security considerations are addressed at the logical design phase of systems development. This cannot be over emphasized since development duality occurs where system developers fail to recognize the security requirements peculiar to a particular system, organization and environment at the onset. Where organizations do not consider the overall security architecture of their information and communication technology to include both infrastructure and security at the onset, it becomes an uphill task to manage or correct such anomalies. It could be argued that development duality can be traceable to improper planning which excludes certain components or personnel at the conception stage of critical systems and security development.

For education managers, in order to improve education within their institutions, heavy reliance is placed on information assets, which they have gathered from the data within their disposal. As has been established, post 1990s, both labour and total factor productivity accelerated in the United States due to the role of Information and communication technology of which information security is an integral component [10]. For acceleration in the education sector to be ignited and sustained, it is imperative that proper measures be put in place to properly secure the information assets of the sector in order to harness the desired growth for educational advancement.

4. Conclusion

Education is very important for development of any society. In fact, it is at the very core of development. It becomes imperative therefore, that any nation that desires sustainable development must embrace all factors which will improve their education by engaging systems and processes. It is quite glaring that one of those processes is proper information security management since reliance on information assets propels the growth of any sector especially the educational sector. As established, information security management system (ISMS) that integrates corporate policy with legislation and compliance requirements is key to information security management. It has become expedient for all concerned to work towards the enactment of a comprehensive national legislation which will regulate the practice and procedure of information security in Nigeria. It could be argued that this regulation will also encompass setting up procedures which will take into account issues like development duality.

5. References

[1] Al-Awadi, M & Renaud, K. (2016). Success factors in information security implementation in organizations. http://www.semanticscholar.org/6aff/eddfdifdiadcf737184ffd887602007afod.pdf

[2] Al-Shomrani, A, Fathy, F, & Jambi, R. (2017). Policy enforcement for big bata security. Paper delivered for International Conference on Anti-Cyber Crimes. (ICACC). 70-74.

[3] Antero, M. C. (2018). Lecture notes, Copenhagen Business School.

[4] Baskerville,R. (1988). Designing information system security. John Wiley & Sons. New York.

[5] Campbell, T. (2016). Practical information security measurement. Appress. Australia.

[6] Chaims, Z. C. (2007). Conceptual approach for defining data, information and knowledge. Journal of the American Society for Information Science and Technology. 58(4), 479-493.

[7] Chobinah, J, Dhillion, G, Grimaila, M. R. & Rees, J. (2007). Management of information security: Challenges and research directions, communication of association for information systems. 20, 958-971.

[8] CIA Triad of information security. ResearchGate.

[9] ISO/IEC 27000:2017 series. http://www.iso.org >isoec27000-information-security.html

[10] Jorgenson, D. W. ((2001). Information technology and the U. S. economy. American Economic Review, 91; 1-32.

[11] SACA. (2006). Information security governance: Guidance for boards of directors and executive Management.

[12] Nieles, M., Dempsey, K., Yan Pillitteri, V., (2017). An Introduction to Information Security. NIST Special Publication 800-12 Revision 1, https://doi.org/10.6028/NIST.SP.800-12r1.

