Information Security in the Digital Age: The Case of Developing Countries

Iguehi Joy Ikenwe
Ambrose Alli University
Nigeria
ikenweiguehi@yahoo.com

Osahon Magnus Igbinovia
University of Ibadan
Nigeria
infor.migbinovia@gmail.com

Ademakhe Ann Elogie
Ambrose Alli University
Nigeria
elogieanne@yahoo.com

ABSTRACT: Information security is an important issue and a growing concern that affects all sectors in this digital age. Lack of information security can lead to confidential information being accessed by unauthorized persons or integrity of information being compromised. In light of these, the present study addresses information security in developing countries. There are six objectives to guide the study. Findings reveal that information security is an important area, worthy of attention. As such, awareness should be enhanced among all stakeholders in information management. Possible challenges to information security are stated and recommendations proffered.

I. Introduction

This present digital era is characterized by the advent of information technologies to create, collate, manage, manipulate, store, and share information regardless of time and space. In this era, information has been considered as an economic resource or a key factor in modern production (Aina, 2004) and as such, its utilization has become germane to individual and organizational successes. Information is an essential tool for competitive advantage both at the individual, organization, societal, and national level (Abdullahi, Igbinovia, & Solanke, 2015).

The importance of information cannot be overemphasized as it cut across all spheres of human endeavors and professions. However, the difference between the advanced countries and the developing countries lies in their information awareness, access, and use. This is why information is regarded as "power" (Ikenwe & Omigie, 2015).

Uttor (1999) opines that information is the data valuable in the planning, decision making, and evaluation of any program.

There are numerous definitions of information. These vary from one profession to another. Nevertheless there is a common ground for all these definitions, viz, information is a set of structured data which creates (or improve on) some sort of awareness that bridges a gap in the cognitive aspect of the informed (person who receives the information).

It is germane to state here that the authors will not restrict themselves to any particular definition of information as the concept treated in this study is in its universality.

Ii. Statement of Problem

The proliferation of information on the Internet (with emphasis on social media and other related platforms) in this digital age has been highly helpful to mankind, especially in developing countries. However, there is a great need to protect information from abuse, misuse or unauthorized access by securing information from security threat. Necessary policies, protective measures, compliance and enforcement mechanisms, and privacy of information need to be put in place in order to safeguard information in developing countries.

In light of the stated problem, the objective of this study are:

1. To discuss the concept and importance of information security in developing countries in the digital age;
2. To discuss information security awareness (ISA) in developing countries in the digital age;
3. To elucidate on cybercrime in developing countries in the digital age;
4. To discuss cybercrime in the digital age using Nigeria as a case study;
5. To examine the types of cybercrimes in developing countries; and
6. To examine the challenges of information security in developing countries and recommend some solutions.

III. Research Methodology

This study used a literature review approach to collect and analyze existing findings of research with regards to information security in the digital age from the perspective of developing countries. This approach is suitable to provide a summary of literature on the identified problem and the resultant objectives of the study.

IV. Literature Review

Objective One: Concept and importance of information security in developing countries in the digital age

Information security is currently a growing concern that affects all sectors in the developing countries in this digital age, such as government parastatals, financial institutions, businesses, and corporate organizations as well as libraries and other information centers. According to Mellado and Rosado (2012), the “permanent and global nature of security threats and the increasing complexity of IT infrastructures are currently leading organizations throughout the world to revise their approaches towards information security" (p. 1598). They further observed that "Most organizations fully recognize the need to continuously improve their internal security culture by establishing and maintaining proper security governance processes" (p. 1598).

However, information security is the protection of intellectual content or information from unauthorized users. In this vein, Wikipedia defines that information security, "sometimes shortened to InfoSec, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information". A succinct definition of information security as given by the Open University (2014) runs as follows: "Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure". Coertze and Solms (2013) believed that "Information security pertains to the protection of the confidentiality, integrity and availability of information, which is usually managed by a process called 'information security management'" (p. 279). Fakeh, Zulhemay, Shahibi, Ali, .& Zaini (2012) stated that "the growth of computers and multi-processing computer systems has resulted in several additional security mechanisms" (p. 1723). Furthermore, "Most of the information on security issues rely on physical devices. The device is used to guarantee the three main elements of information security. They are confidentiality, integrity and availability" (p. 1723).

There is a tremendous change from the traditional methods of information handling to electronic-based approaches in the digital age. This has helped to meet the demands of the 21st century by rendering effective services, such as digital libraries and electronic resources, to library users. In light of this, Newby (2000) listed some effective information security in libraries:

- Staff assigned to information security tasks
- Training all personnel in information security issues and procedures.
- Specific policies dealing with information privacy, physical security of equipment, and computer security procedures
- Physical security plans
- Data Integrity measures
- Levels of access to data or equipment, and monitoring for different types of access (p. 2)

The financial industry is not immune to information security issues. On the importance of managing information security, Crutchfield (2003) asserted that "information security is critical to delivering the best service you can deliver while reinforcing the perception of trust; obviously trust is of utmost importance in the financial industry".

According to Crutchfield (2003), a well-managed information security program provides competitive advantages, which is the cornerstone to any business ability to generate revenue. Furthermore, without a solid information security program, the financial sector would not have been able to transit competitive advantages to the networked world.

Fakeh, Zulhemay, Shahibi, and Zaini (2012) stated that, the "disruption of information security will kill the main purpose of this sophisticated technology, hinder the smooth operation of an organization, make users feel suspicious and traumatized, and could cause losses to the organizations involved" (p. 1723). Furthermore, Hinde (2003) maintained that carelessness towards privacy could cause an organization to have a big financial loss. In addition, information security helps protect an organization from investigations (court case) and fraud.

Objective Two: Information security awareness (ISA) in developing countries in the digital age

The knowledge and awareness of information security in this digital age in various sectors are essential and should not be overlooked. There exists security threat to information, which should be adequately protected through information security awareness. According to Siponen (2000), information security awareness focuses more on the motivation of the employee in an organization to follow the policy and regulations towards the security of information in the company. An approach taken to raise awareness is having a program, training or seminar in the workplace. In the view of Siponen (2000), information security awareness is “a state where users in an organization are aware -- ideally committed to -- their security mission” (p. 31).

The importance of information security in an organization plays a major role and ISA is as important as the policies and technique used in an organization to secure information. It is obvious that ISA has numerous advantages to an organization. In this vein, Fakeh, Zulhemay, Shahibi, and Zaini (2012) identified four major factors that influence information security awareness as shown in the diagram below:

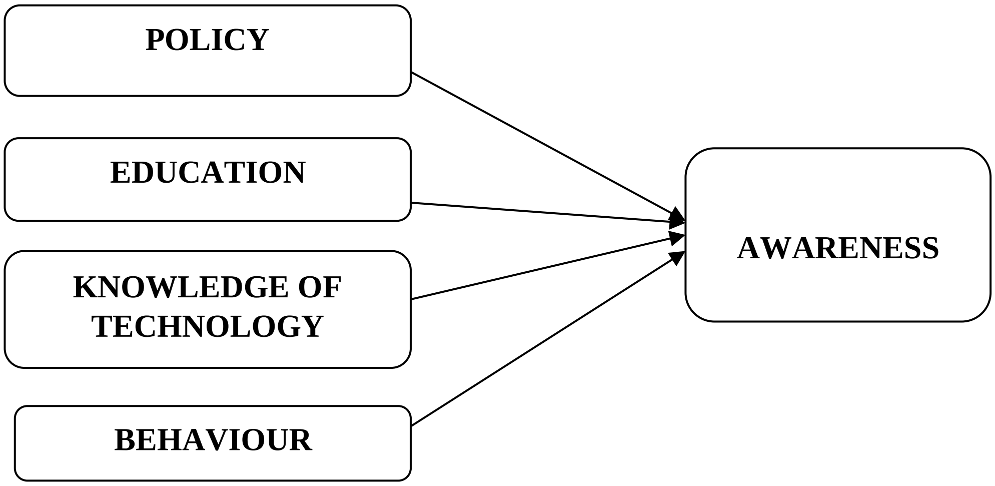

Figure 1. Factors influencing ISA (Fakeh et al., 2012)

A policy is a reference for employees and a tool for management to guide their staff. Education is a communication between users and educators, which can influence the knowledge of end users so that they are made more aware. This is how education relates to knowledge of technology and how knowledge can change human behavior (Fakeh et. Al., 2012).

Objective Three: Cybercrime in the digital age in developing countries

“Cyber security is essential given our growing dependence on cyberspace for all aspects of modern society” (Lee, 2013). According to Joe (2013), cyber security encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. “Cybersecurity refers to the technologies and processes designed to protect computers, networks, and data from unauthorized access, vulnerabilities, and attacks delivered via the internet by cyber criminals" (Beal, n.d.).

Objective Four: Cybercrimes in the digital age: a case study of Nigeria

Cybercrimes are crimes that involve the use of computer and network. There is no doubt that cybercrimes have created a terrifying situation in developing countries like Nigeria. Cybercrimes, such as an internet fraud known as "yahoo-yahoo", perpetuated by "yahoo boys", has been of interest and humiliation to Nigeria government. The Nigeria government has made efforts to tackle the cybercrime. According to Goitom (2014), Nigeria's President Goodluck Jonathan "introduced the Cybercrime Bill, 2013 in the National Assembly".

In this digital age, social media powered by the internet create limitless chance for educational, business, social, and commercial activities. However, cybercrime has brought risk to the internet, posing a serious menace to the society as the internet is being used for criminal activities. Cybercrime is a fast growing area of crimes. Many criminals are exploiting the speed and convenience of the internet to commit a diverse range of criminal activities in Nigeria.

According to Hassan, Lass, and Makinde (2012), the causes of cybercrime in Nigeria include,

- Urbanization
- Unemployment
- Inordinate quest for wealth (greed)
- Weak implementation of cybercrime laws
- Inadequately equipped law agencies

Objective Five: Types of cybercrimes in developing countries

According to Wikipedia, "Cybercrime, or computer crime, is crime that involves a computer and a network".

Cybercrimes that are frequently practiced in developing countries include:

E-mail scam: This scam is now prevalent in Nigeria. The targets are individuals anywhere in the world. These scammers solicit for financial assistance, using the names of prominent pastors, persons, institutions, or organizations in the country. They also use GSM to send deceptive text messages in order to lure their victims.

Cyber hacking: This has to do with unauthorized access to online accounts, computers or technologies, such as websites or networks, by manipulating a code to crack. This is a serious invasion of privacy. Hackers break into and deface websites (personal, institutional or organizational) in order to access their sensitive information. At other times, they simulate such websites and use them to defraud others in the guise of the hacked person.

Cyber stalking: Generally, cyber stalkers use the internet, e-mail, and other electronic communication devices to stalk or harass their victims. Cyber stalking is a form of threat or harassment, using communication devices to pursue, harass or threaten their victims.

Computer vandalism: Computer vandalism is the act of removing important information from the computer system by an intruder, denying the owner of the right of access to the information. This may cause financial loss to the victim.

ATM fraud: Automated Teller Machine (ATM) is an electronic cash dispensing machine for people to withdraw cash, purchase airtime, transfer cash, deposit or check account balance inside or outside a bank. There is rise in ATM fraud. Muhammad (2009), as cited by Jegede (2014), postulated that "the level of ATM fraud tend to have overshadowed the improvements which it has brought into the service delivery systems of Nigeria financial institutions".

Objective Six: Examine the challenges of information security in developing countries and recommended solutions

Some challenges of information security in developing countries are personnel, cost, and infrastructure. Also, lack of awareness on basic confidential information, leading to poor handling of documents, identity cards, ATM use, and social devices, is a challenge to information security. Awe (2013) identified the following as Africa's information security challenges:

1. **Lack of understanding of what information security means is a major societal challenge**. Most people online are unaware of the threats and the significance of the threats. It's strange but people still fall victim to recharge card and the "Bill Gates is giving away all his money" scams.
2. **Lack of interest in education and training**. Lack of understanding is compounded by lack of interest in security education. Security is a serious issue but there is very little demand for security education…. The low demand for security education is also a reflection of the low level of security awareness in the environment.
3. **Direction of governments is unclear**. Although several African governments have developed security and ICT policies, implementation is a major challenge. "Paper policies"? There is a need for clearer policy direction. And how realistic are such policies? How much has been invested in terms of time, education, personnel, etc.?
4. **Low confidence exhibited in Africa's e-business structures**. The poor attention paid to Information security has affected the growth of e-business in Africa.
5. **Law Enforcement/Security/Intelligence Agencies Gap**. Information security is about crime. However, a major challenge is that of empowering law enforcement in the digital era. The ICT infrastructure of law enforcement requires massive improvement…. Information security requires not just ICT knowledge but ICT enabled intelligence.

V. Summary of Findings

The findings from the literature reviewed to address the objectives of the study are as follows:

1. Information is a key to individual, organizational, and national success. As such, securing or protecting it from hackers is important to maintain its economic value.
2. Information security awareness is fundamental in the fight against information threat and cybercrimes.

3. Cybercrimes are committed when there is a breach or compromise in information security.
4. Nigeria has experienced the menace of cybercrimes in the past decades, which might be as a result of either urbanization, unemployment, undue quest for wealth, weak implementation of cybercrime laws or inadequately equipped law agencies.
5. Cybercrimes in Nigeria are of various types to include but not limited to email scam, cyber hacking, cyber stalking, computer vandalism, ATM fraud, and cyber terrorism.
6. The challenges of information security in Nigeria centers around adequate manpower or personnel, cost, and infrastructure required to ensure information systems are well secured.

VI. Conclusion

The importance of information, and by extension information systems, is key in all sectors of the economy and at all levels of human endeavor. Information is relevant to organizational success, individual achievement, effective managerial decisions, and national development. It is, therefore, pertinent that information security should be given utmost attention by all stakeholders involved in its handling and management so as to effect or protect its economic and social gains.

References

Aina, L. O. (2004). *Library and information science text for Africa*. Ibadan, Nigeria: Third World Information Services.

Abdullahi, A. O.; Igbinovia, M. O.; & Solanke, O. E. (2015). Assessment of information needs and seeking behaviour of undergraduates in university of Ilorin, Ilorin, Nigeria. *Information and Knowledge Management, 5*(4), 1-16.

Awe, J. (2013). *Africa's information security challenges*. Retrieved from http://nigeriacomputers.com/tech-news/africas-information-security-challenges/

Beal, V. (n.d.). *Cybersecurity*. Retrieved from http://www.webopedia.com/TERM/C/cybersecurity.html

Coertze, J.; & Solms, R. V. (2013). A model for information security governance in developing countries. In K. Jonas, I. A. Rai, & M. Tchuente (Eds.), *AFRICOMM 2012, LNICST 119* (pp. 279-288). Retrieved from https://www.researchgate.net/publication/258431950_A_Model_for_Information_Security_Governance_in_Developing_Countries

Crutchfield, E. E. (2003). The importance of managing information security from a CEO perspective. Retrieved from http://www.secureworks.com/resources/newsletter/2003-07/

Fakeh, S. K. W.; Zulhemay, M. N.; Shahibi, M. S.; Ali, .J.; & Zaini, M. K. (2012). Information security awareness amongst academic librarians. *Journal of Applied Sciences Research, 8*(3), 1723-1735. Retrieved from http://www.aensiweb.com/old/jasr/jasr/2012/1723-1735.pdf

Fox, E.; & ElSherbiny, N. (2011). Security and digital libraries. In K. H. Huang (Ed.), Digital libraries: Methods and applications (pp. 151-160). Rijeka, Croatia: InTech Europe. Retrieve from http://www.intechopen.com/books/digital-libraries-methods-and-applications/security-and-digital-libraries

Goitom, H. (2014). *Nigeria: Cybercrime Bill Proposed*. Retrieved from https://www.loc.gov/law/foreign-news/article/nigeria-cybercrime-bill-proposed/

Hassan, A. B.; Lass, F. D.; & Makinde, J. (2012). Cybercrime in Nigeria: Causes, effects, and the way out. *ARPN Journal of Science and technology*, *2*(7). Retrieved from: http://www.ejournalofscience.org/archive/vol2no7/vol2no7_11.pdf

Hinde, S. (2003). Careless about privacy. *Computers and Security, 22*(4), 284-288.

Hu, Q.; Xu, Z.; Dinex, T.; & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, *54*(6), 54-60. http://dx.doi.org/10.1145/1953122.1953142

Ikenwe, I. J.; & Omigie, C. A. (2015). Obstacles to information access and use in developing countries in the 21st century. *Ekpoma Journal of Social Sciences*, *5*(2).

Jegede, G. A. (2014). Effects of automated teller machine on the performance of Nigerian banks. *American Journal of Applied Mathematics & Statistics*, *2*(1), 40-46. Retrieved from: http://pubs.sciepub.com/ajams/2/1/7/

Lee, R. B. (2013). Improving cyber security. In D. F. Hsu and D. Marinucci (Eds.), *Advances in cyber security: Technology, operations, and experiences* (pp. 37-59). New York: Fordham University Press.

Mellado, D.; & Rosado, D. G. (2012). An overview of current information systems security challenges and innovations. *Journal of Universal Computer Science, 18*(12), 1598-1607. Retrieve from http://www.jucs.org/jucs_18_12/an_overview_of_current/jucs_18_12_1598_1607_editorial.pdf

Muhammad, A. K. (2009). An empirical study of automated teller machine service quality and customer satisfaction in Pakistani banks. *European Journal of Social Sciences, 13*(3), 333-344.

Newby, G. B. (2000). *Information security for libraries*. Retrieved from http://petascale.org/papers/library-security.pdf

Open University. (2014). *An introduction to information security*. Retrieved from http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/introduction-information-security/content-section-1

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41. http://dx.doi.org/10.1108/09685220010371394

Uttor, J. (1999).*The role of law libraries in a democratic culture*. A paper presented at The 1999 NLA National Conference and AGM.Aug.15th-20th.

Wikipedia. (n.d.). Cybercrime. Retrieved from https://en.wikipedia.org/wiki/Cybercrime

Wikipedia. (n.d.). Information security. Retrieved from https://en.wikipedia.org/wiki/Information_security

Authors:
Iguehi Joy Ikenwe, Department of Library and Information Science, Ambrose Alli University, Ekpoma, Nigeria. Email: ikenweiguehi@yahoo.com

Osahon Magnus Igbinovia, Department of Library, Archival and Information Studies, University of Ibadan, Nigeria. Email: infor.migbinovia@gmail.com

Ademakhe Ann Elogie, Department of Library and Information Science, Ambrose Alli University, Ekpoma, Nigeria. Email: elogieanne@yahoo.com

Submitted to CLIEJ on July 9, 2016.

Ikenwe; Iguehi Joy; Igbinovia, Osahon Magnus; & Elogie, Ademakhe Ann. (2016). Information security in the digital age: The case of developing countries. *Chinese Librarianship: an International Electronic Journal*, *42*, 16-24. URL: http://www.iclc.us/cliej/cl42IIE.pdf