International Journal of Library and Information Science Studies

Vol.5, No.4, pp.48-54, October 2019

Published by **ECRTD- UK**

Print ISSN: 2059-9056, Online ISSN: 2059-9064

USE OF ELECTRONIC INFORMATION SECURITY SYSTEMS IN DOUBLE DAY HOTEL AND COMPLIMENTARY SUITES, OWERRI, IMO STATE

Lovet Ovigue Esievo, PhD, CLN
Senior Librarian, President Kennedy Library, Institute Of Administration, Ahmadu Bello University, Zaria

Dr Magnus Chukwuduziem Unegbu
Senior Librarian, The College Library, Alvan Ikoku Federal College Of Education Owerri Imo State

Dr Jonathan Chima Ogugua
Senior Librarian, The University Library, Federal University Of Technology, Owerri Imo State

Edward C. Amadi
Librarian 1, The University Library, Micheal Okpara University Of Agriculture, Umudike, Abia State

ABSTRACT: *The general purpose of this study is use of electronic information security systems in Double Day Hotel and Complimentary Suites, Owerri, Imo State. The survey design research was used for the study using self constructed and validated questionnaire as an instrument for data collection. The study adopted census method which was used to investigate 44 staff of Double Day Hotel and Complimentary Suites, Owerri, Imo State. Findings showed that staff of Double Day Hotel and Complimentary Suites, Owerri, Imo State have various reasons for the use of electronic information security systems such as effective information service delivery, data/information and system protection and information authenticity/confidentiality. The study recommends that there should be continuous evaluation, review and refinement in the creation of reliable and sustainable security audit traits within electronic information systems and security strategy.*

KEY WORDS: use, electronic information, security, systems

INTRODUCTION

Information system is that set of aspects of a general system (natural phenomenon, physical or logical constructs) identified as information producing. Schulthesis and Sumner (1995) in affirmation say that an information system is the subsystem of the general business system of an organization which provides information on day to day activities in the cases of authorities and directives and for effective decision making.

According to Gattiker (2004) information security is the practice of defending information from unauthorized access, recording, disclosure, disruption, modification, use, perusal, inspection or destruction. Pankja (2006) defines electronic information security as the protection resulting from all the measures designed to deny access to unauthorized persons valuable that might be derived from the possession and usage of electronic sources. Jackson (2002) refers to electronic information security as controlling the access to electronic information so that only those with the legitimate key or authority are allowed to access the information. The author comments that naming institutions and organizations hold relevant information relating to financial, legal, logistics and other areas in electronic format; therefore there is the need for securing these valuable data or information and their systems.

Uhegbu (2007) posits that electronic information security system (EISS) came into play following the introduction of electronic information systems such as computer and telecommunication systems. Electronic information security systems came as means to safeguard effectively harnesses information, highly priced in the new information world (information explosion) against unauthorized access and system vandalism by men with computer and internet competence. Scarf one and Peter (2007) reveal that some examples of EISS are hardware and software applications, security and intrusion detection software, identity authentication, backup procedures, firewalls, alarms, video monitors, and cameras and other digital surveillance devices. Unagha (2011) identifies other modern types as data manipulation modules, statistical techniques and other sophisticated data analysis equipment usually managed by information system analysts.

According to UNESCO (1979), electronic information systems can be discussed under two premises, namely specific premise and general premise. Specific premise is characterized by a system of information involving separate but coordinated sequences of actions leading to an effective information flow and utilization. General premise refers to all information bearing on the activities of an organization directed to some particular ends required by an organization to function and attain her goals. Laudon and Laudon (2006) also observe that electronic information systems can be understood from two perspectives such as technological and business perspectives. Technological, information system can technically defined, while from the business point of view an information system contains information about an organization and her surrounding environment.

Easton (2011) is of the view that with electronic information systems or documentation, it is still very difficult to assure authenticity, integrity, and reliability as information can disassembled, rearranged, reassembled without anyone noticing the differences. The author asserts that the ease with which electronic records can be created, altered, accused, duplicated and stored jeopardizes their value as records or information. So, electronic information security systems (EISS) in any organization will go a long way to ensure the integrity of data or information materials. Imeremba (2007) affirms that electronic information systems approach utilizes all

communication based computer and technology facilities and procedures for provision and delivery of information for planning and decision-making. The author asserts that proper information security measures are essential for effective information flow system as they reduce the susceptibility of any organization to encroachment from outside intruders.

Therefore, every organization or institution requires strong and reliable electronic information security systems to protect her information against attacks (crackers or hackers). In the light of the above background, this study intends to investigate the use of electronic information security systems in Double day hotel and Complimentary suites Owerri Imo State.

Research Questions

The following research questions were posed to guide the study.

i. What are the reasons for the use of electronic information security systems in Double Day Hotels and Complimentary Suites, Owerri Imo State?
ii. What are the challenges of using the electronic information security systems in Double Day Hotel and Complimentary Suites, Owerri Imo State?

LITERATURE REVIEW

Spencer (2002) writes that one of the greatest worries of co-operate organizations in the new information world is how to safeguard their highly priced and esteemed information against unauthorized access and system vandalism by young men with computer and internet competence. The author further argues that too much of security by employers can hamper job performances of employees which may lead to reduced revenue or result to the organization. Less security on the other hand can make an organization susceptible to encroachment from outside intruders. Every organization therefore requires strong security to protect her information from attackers (hackers and crackers). Uhegbu (2007:163) observes that every enterprise is now involved in risk management as a panacea to the rampaging internet vandals to organizations business. Risk management consists of the identification of risks or threats, the implementation of security measures and monitoring of the measures for effectiveness. Establishing what the potential threats are and what parts of the system the vulnerable is the first step in the process. This process is called risk assessment. Risk assessment is the evaluating information technology assets, their importance to the organization and their susceptibility to threats and also to measure the risk exposure of those assets. The united nation study (1986) defines security as a national condition so that countries can develop and progress safely. Different scenarios also give rise to the context in which security is maintained, with respect to classified matters, the condition that prevents unauthorized persons from having access to official information that is safely guarded in the interest of national security. Security as a condition is the degree of resistance to, or protection from harm. It applies to any vulnerable and valuable assets, such as person, community, organization or institution.

In Guralink (2013) definition, information security is the protection of data and information against unauthorized access. Programmes and data can be secured by issuing identification numbers and passwords to authorized users of a computer or an information system. Therefore electronic information security is the protection resulting from all measures designed to deny access to unauthorized persons of valuable information which might be derived from the possession and study of electromagnetic radiation. Examples of electronic information security products include alarms, firewalls, encryption, back-ups, intrusion detector hardware and software procedures and other various kinds. Electronic information security came into play following the introduction of electronic information system, such as telecommunication and computer systems; and the electronic information contained or transferred in them and the possible threats affecting the electronic transfer of data or information using electronic systems. Various types of threats may exist that could, is they occur result to losing information or assets and the exposure or removal of either temporary or permanent damage information or used for unauthorized purposes. To forestall cyber unauthorized access or loss of information, institutions or organization must engage in a number of risk management activities. Generally, security consists of a combination of measures such as back-up procedure, security policy, risk management and disaster recovery plans. There is also the use of access controls such as firewalls and alarms, encryption, security soft ware's, documentation and system auditing (Allen, 2001).

METHODOLOGY

The descriptive survey research design was used for this study using questionnaire as an instrument for data collection. The questionnaire was titled "Use of Electronic Information Security Systems in Double Day Hotel and Complimentary Suites, Owerri, Imo State '' (**UEISSQ**). The population of the study is 44 respondents (Forty Four). This comprised all the staff of Double Day Hotel and Complimentary Suites, Owerri, Imo State. No sample size was drawn from the population. This is because the population of the study is small and accessible. The census method was used to ensure that opinions of all the staff of Double Day Hotel and Complimentary Suites, Owerri, Imo State were captured for the study.

Analysis

A total of forty four (44) copies of the questionnaire were distributed to the hotel staff at Double Day Hotel and Complimentary Suites, Owerri, Imo State. Out of these 39 (39) were duly completed and return for analysis giving a response rate of (88.6%).

Research Question 1: What are the Reasons for the Use of Electronic Information Security Systems in the Hotels?

Table 1: Reasons for the Utilization of Electronic Information Security Systems in Hotels

N=39

	Option	**Frequency**	**%**
a	Effective information Service delivery	36	92.3
b	Data/information and system protection	32	82.1
c	Information authenticity/confidentiality	34	87.2
d	Effective customer service delivery	31	79.5
e	Proper accessibility and utilization	29	74.4

Evidence from Table 1 showed that the number of responses is more than the number of respondents because some respondents ticked more than one choice of options provided from the table. 36 (92.3%) of the respondents stated effective information service delivery as their reasons for the use of electronic information security systems as 32 (82.1%) of the respondents stated data/information and system protection as their reasons for the use of electronic information security systems. 34 (87.2%) of the respondents stated information authenticity/confidentiality as their reasons for the use of electronic information security systems while 31 (79.5%) of the respondents stated effective customer service delivery as their reasons for the use of electronic information security systems. For 29 (74.4%) of the respondents stated proper accessibility and utilization as their reasons for the use of electronic information security systems.

Research Question 2: What are the Challenges Facing the Use of Electronic Information Security Systems in the Hotels?

Table 2: Responses to Challenges Facing the Use of Electronic Information Security Systems

N=39

	Option	**Frequency**	**%**
a	**Electronic Information Security Systems**	32	92.3
b	Inadequate skill/training	35	89.7
c	High cost of availability and maintenance	37	94.9
d	Inconsiderate attitudes of users	36	92.3
e	Incessant power failure	38	97.4
F	Attackers and intruders	36	92.3
g	Lack of adequate and regular funding	34	87.2

Evidence from Table 2 showed that the number of responses is more than the number of respondents because some respondents ticked more than one choice of options provided from the table. Table 2 identifies some challenges in the utilization of electronic information security systems in the hotels. Challenge such as inadequate skill/training, high cost of availability and maintenance, inconsiderate attitudes of users, incessant power failure, attackers and intruders and lack of adequate and regular funding.

FINDINGS

The reasons for the use of electronic information security systems is supported by Adeyinka (1999), that hotels are characters by accountability, confidentiality, accessibility and availability all summing up in integrity. In this regard, the following options were presented-effective information service delivery; protection of data/information and their systems; information authenticity and confidentiality; effective customer service delivery and proper accessibility and utilization of information and their systems. The respondents agreed with the options presented to them, which implies that they have a cause and need to use electronic information security systems in their services. They know that they need to protect their valued information and their systems from unauthorized access and jeopardy.

The challenges presented as options were generally identified by the respondents. The challenges are: lack of adequate and regular funding, inadequate supply of electronic information security systems; inadequate skill/training in the use of electronic information security systems; high cost of availability and maintenance; inconsiderate attitudes by the users; incessant power failure and intruders and attackers. All these corroborate with Watawala (2005) that lack of awareness and training; lack of legislation and disaster recovery plans; inadequate funding, incessant power failure and so on being serious problems affecting the use of electronic information security systems generally, especially in a developing country of which Nigeria is one.

CONCLUSION AND RECOMMENDATIONS

Based on the findings of this study, the study recommends that there should be continuous evaluation, review and refinement in the creation of reliable and sustainable security audit traits within electronic information systems and security strategy. This is to ensure that security softwares such as anti-virus and other applications acquired are compatible with the available hardware components and other resources. Also to be encouraged is the establishment of generally accepted or acclaimed standard for the use of electronic information security systems in hotel sectors. These will bring confidence in the use of electronic information security systems and promotion of information security will be ensured.

Again, strengthening education, training and orientation on the use, maintenance and management of electronic information security systems should be encouraged among all the staff of these hotels in Owerri, Imo State. Users should be adequately trained in the use of electronic information security systems. They should also have knowledge on the security measures and policies for protecting electronic information, therefore, regular training should be considered for maintenance and use of electronic information security systems available.

REFERENCES

Adeyinka, F (1999). *The impact of information and communication technology (ICT), on employmen in banks*. Ibadan: Nigeria Institute of Social Economic Research (NISER).

Allen, J. H. (2001). *The certificate guide to system and network security practices*. Boston, MA: Addison-Wesley.

Easton, C. (2011). *Computer security fundamentals*. London: Pearson Press.

Gattiker, U. (2004). *The information security dictionary: defining the terms that defines security for e-business, internet, information and wireless technology*: Boston: Khuwer Academic Publishers.

Gurilink, D. B. (2013). *Webster new world dictionary of the American language.* Cleveland: World Publishing Company.

Imeremba, D. U. (2007). *Information technology: products and services in a cyber culture,* Enugu: John Jacob's Classic Publishers.

Jackson, M. E. (2012). Who gets what and how all that is changing. *Journal of American Library*. 2 (4), 15 – 28.

Laudon, K. C. and Laudon, J. P. (2006). *Management information systems: managing the digital form,* 9th ed. New Jersey: Pearson Education Inc.

Pankaj, A. (2006). *Academic dictionary of computer and information technology*. New Delhi: Academic Publishers.

Scarfone, K. and Peter, M. (2007). *Guide to intrusion, detection and prevention system (IDPs).* Computer Security Resource Centre.

Schuthesis, R. and Summer, M. (1995). *Management information system:* the managers' view (3rd ed). Irwin: R & O

Spencer, V. (2002). Risk management: danger of the cyber deep. *Canadian underwriter,* 4 (8), 87 – 94.

Uhegbu, A. N. (2007). *The information users: issues and themes*. Okigwe: Whytem

Unagha, A. O. (2011). *Organization and management of information systems:* Enugu: Ernesco.

UNESCO (1979). *Computerized Management of educational systems: accompanying document.* Paris: operational Programmed Division 21 (8): 58 – 68.

Watawala, E. O. (2005). Potentials for utilization of information and communication technology: integrated post management. *African Journal Library Archival and Information Services* 15 (5), 44 – 79.