Information Security Awareness and Effective Use of Electronic Records Systems among Administrative Staff of Private Universities in Ibadan, Oyo State, Nigeria

Oluwatosin A. Ologbosere[1], Veronica Abiola Ayo-Ogunlusi[2]

[1]Department of Information Management, Lead City University, Ibadan

[2]Department of Business Administration, Bamidele Olumilua University of Education, Science and Technology, Ikere Ekiti

DOI: https://dx.doi.org/10.47772/IJRISS.2025.914MG00151

Received: 02 September 2025; Accepted: 08 September 2025; Published: 07 October 2025

ABSTRACT

The study examined the Information Security Awareness on Effective Use of Electronic Records Systems among Administrative Staff of Private Universities in Ibadan, Oyo State, Nigeria. A descriptive survey research design was adopted. The population of the study consists of 685 administrative staff of Lead City University, with a sample size of 248 as determined using the Krejcie and Morgan sampling technique. The research instrument is a structured questionnaire adapted from existing studies. The data collected was analyzed using descriptive and inferential statistics. This result suggests that user information compliance has a higher relative effect on the use of electronic records systems compared to behavioural intentions for administrative staff in private universities in Ibadan, Oyo State, Nigeria. The study concluded that Information security awareness (user information compliance and behavioural intentions) is used by the administrative staff of private universities in Ibadan. Oyo State, Nigeria, significantly influenced the electronic records systems among the administrative staff of private universities in Ibadan. Oyo State, Nigeria. Management should take a more proactive approach to enhancing information security awareness among administrative staff by protecting sensitive information and streamlining record management processes.

Keywords: Information Security Awareness, Electronic Records Systems, Administrative Staff.

INTRODUCTION

Records are essential for the smooth operation of any organization; they carry information and knowledge in various formats and serve as the backbone of ongoing services, without precise and up to date records, any institution would not work effectively. Record-keeping is essential for both individuals and organizations because human memory is fallible, documenting major events, actions, and decisions ensures orderly records for students and staff, supports normal operations, and preserves the memory and history of nations (Ashmarina, 2021). Records refer to information that has been created, taken and retained as evidence by the organization or individuals, in line with their legal requirements or the conducting of business. Records are composed of all recorded information regardless of form or medium which is created, received and acquired as well as maintained by any institution or individual in the execution of his or her legal mandate or in the conduct of its or his business (Herath, 2021,;Abubakari, 2023). Conclusively, record-keeping is the deliberate creation, capture, preservation, and management of information that evidence actions, decisions, and events by individuals or organizations, that supports accountability, legal compliance, operational continuity, and preserves memory and history.

Records keeping involves all activities that have to deal with the creation, maintenance, retrieval, maintenance, and destruction of all data pertaining to all activities performed in an academic institution including personnel, equipment, and other data as is related to the academic growth. However, simply having records, be they statutory or non statutory, is not sufficient, at least not as a management tool: how records are kept, how they are managed, and how they are used must be regarded as a key to management effectiveness. The importance of

record keeping is that it allows the management or educators to make valuable decisions and come up with appropriate policies. An educational approach that does not give importance to sound records management would end up with financial challenges (Adisa, 2024). What have happened or taken place in the past are recorded and used by administrators to plan and manage the current programmes or activities.

This student life cycle and the relationship between the student and his/her alma mater may never end since even after a student has completed studies and has left the school, he/she can run back to the school again to request some relevant academic documents, in the quest to continue his education or in securing a job (Ojo, 2024). When certificates or honours granted to the students become controversial; one of the most likely ways to probably eliminate all the confusion and discredit or establish the truth and authenticity of these documents is to resort to the archives of the academic records of the school, and produce the original documents before rather large groups of men, to confirm them by the testimony of the witnesses whose signature was on them. Records are an essential tool in providing that an educational institution is well governed in a very effective and efficient manner and is also accountable to its own staff members, students and the community that it serves. A sound records management system has the capacity to make sure that an institution complies with its record-keeping requirements since it makes sure that it documents or rather captures and preserves the evidence necessary to prove its activities and existence. Recorded and confirmed records of the decisions made, activities performed and the consequences of such actions; they are able to support the formation of policy, and the decision-making within management. They also safeguard the interest of the school, rights of the students and assist the running of the affairs of the school and the delivering of the services and in consistent and equitable ways.

There are a lot of records created by institutions in their nature. Records concerning the academic activity of the students, duties given to the staff, course materials, log books, financial movements, and overall school administration are some of the records that should be created and effectively stored, arranged, and evaluated. Although not all such records will be having values deserving their immediate disposition, some of them will need to be retained over a certain duration or indefinitely. Records management (their appraisal, retention and destruction) therefore is the duty of the administrative personnel of any given institution to ensure that the records are either kept or discarded as may be the case, mainly, in the absence of a policy to guide such an aspect. To be efficient in planning, any document created and/or received by educational institutions during their operation must be arranged in such a way that it is easy to retrieve any time one needs to access it (Prastyaningtyas, 2023).

These discrepancies notwithstanding, proper and updated records are usually agreed as being necessary in organizational development. To enable the organisations to derive maximum value of records, the records ought to be administered, records administration there is therefore much concern about records management at any and all levels of education. Electronic records systems can be called a natural and a feasible solution to the development, maintenance, processing and disposal of records in electronic form and, consequently, the information these records represent. It enables an organisation to manage the quality and quantity of information that it generates electronically; it can manage the information and keep it in a form that effectively supports the organisation and can easily destroy recorded information that it does not need any longer. In this regard, administrative records management has a tactical location of management of educational institutions in its administration. It plays the key role in verification and confirmation in a time of disparity. As an example, it is possible to apply after school several years as an application to further studies, employment or ministerial appointment. This may require one to check whether the applicant attended a school. This verification could demand the year of admission, years of completion as a student, total attendance years, and the continuity assessment of the students to determine whether they were truants or not (Spears, 2010).

A good organisation and a very well-maintained system of administrative records is required when the institution needs to respond to the numerous requests on the personal information of individuals in the institution. The administrative personnel of an institution must maintain proper and current documents of everything as he is answerable to all stakeholders. Lacking a properly operating electronic records system, the decision-making takes place without detailed information (Spears, 2010). In addition, records will be poorly arranged, misplaced, damaged or altered, thus leading to inferior planning and poor scheduling of activities. At the end, the management has a handicapped decision making process and the organizations are in every way incapable of meeting their statuary obligations. Efficiency in education may be considered in an internal and outside point of view. The education system should not only be well-efficient but also very effective. By effectiveness is meant

that the organisation has realised or is approaching to realisation its goals/objectives. Furthermore, organisational efficiency is a ratio of the inputs (resources) and outputs (goods and services provided in the organisation). In laymen terms, an organisation is the more efficient the more output the organisation can generate per unit of input or resource. An effective activity is one that attains its objectives.

It is clear that electronic records can be used in guiding administrative staff who have been deployed in an institution. This is due to the fact that the administrative staff can access the records to outline potential reasons behind certain problems. With such observations being done, the administration staff can take proper actions in correcting the issue. The operations of most organizations depend highly on information systems (Olatubosun, 2021). Therefore, risk management in terms of security threats is becoming more significant as the violation of information security frequently has a severe financial and reputation impact on the organizations, in most cases, academic institutions. Maintaining the security of information has become one of the focal concerns and issues of organizations. Therefore, the field of academia is concerned about the possibilities of minimizing information system security (ISS) threats by means of awareness. Previously, other studies focused on information security covered various technological aspects like use of encryption technology, firewalls or spyware and virus detectors (Nwachukwu, 2020). People and not technology have become one of the most dangerous security threats in most organizations, because just as in the case of computers, people are storing, processing and transferring information.

The activities of many academic institutions that are not exempt, including the private universities in Ibadan, Nigeria, contribute very little to ensure, and protect their human resources, and this exposes the organisation to different processes of risk. This study aims to reflect on the potential aspects of awareness of the information security risk, namely the fact of the user compliance with the information and the intentions to comply with it (Marks, 2023). The informational security awareness of an academic institution is an important part of the general information security of the whole organization. The electronic factors have been recognised as the important elements of the information system security both by the research community and the information system security practitioners. In that regard, information security is a part of individual attitudinal and behavioural patterns of users. These attitudinal and behavioural characteristics however have a dimension that is a socio-cultural and human aspect which must be examined and understood to induce the full commitment and adherence to information security rules by the users. A detailed discussion of findings will be carried out on information security awareness and proper utilization of electronic record systems among administrative employees of the privately owned Universities in Ibadan, Oyo State, Nigeria.

LITERATURE REVIEW

Theory and Hypotheses Development

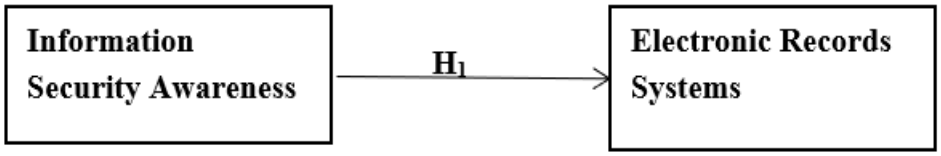
General Deterrence Theory

The General Deterrence Theory (GDT), which has evolved due to the works of Hobbes, Beccaria, and Bentham comes with three distinct aspects including severity, certainty, and celerity (Bond, 2012). GDT is a common approach that is used in the information security literature to examine compliance behaviour. Numerous post hoc developed ISPA models have been derived on the GDT to examine, investigate and evaluate the effects of the perceived sanctions construct on compliance and behavioral intention. The constructs of sanctions are as follows: Sanction certainty is the probability that one walks scot-free, after comminking a prohibited act. Severity of sanction can be referred to as the extent of the severity that is applied in punishments because of violating some of the laws or regulations. Sanction celerity is defined as the rate at which sanction is applied as a result of violation of a set of specific laws or rules. According to this theory, the severity, certainty and swiftness of the sanctions against any illegitimate action enhance potential deterrence against treating a legitimate action. The positive relationship between all factors or some of the sanction factors variable and ISP compliance behaviour has been discovered by numerous studies. To illustrate, at the individual level, perceived severity, though not a certainty, of formal sanctions was negatively related to information security misuse intention. Obtaining a better insight on the concept of deterrence in the context of information security has significant practical implications as well. As a case in point, the ISO/IEC 27002, the information security guidance standard that is most widely adopted, incorporates deterrence theory extensively in its recommendations on policies, guidelines, and

awareness programs that would explicitly define impacts of sanctions applied against errant employees who might be misusing company-owned resources. The following hypothesis, therefore, was formulated;

H_1: Information Security Awareness significantly influences the Use of Electronic Records Systems among administrative staff of Private Universities in Ibadan, Oyo State, Nigeria

Fig.1: Source: Researcher, 2025.



Information Security Awareness and Effective Use of Electronic Records Systems

According to the recent research, human errors are among the most dangerous information assets in organizations (Hofmann, 2020). The security personnel of an information system must be convinced of the necessity to implement information security procedures. One act of abuse may be more expensive as compared with setting up a security mechanism. Education and training are therefore very crucial in enforcing security within a firm. It is critical to make sure that the users are informed about the threats and concerns related to information security and know how to contribute to organizational security policy in the course of their daily activities. This section (a) argues about IS security and surveys current law and procedures, (b) surveys IS security research with particular emphasis on management topics, (c) looks at information security through a Human Computer Interaction (HCI) perspective, and (d) takes a look at existing information security-awareness strategies.

The concept of information security is broad and needs to remain flexible. The literature refers to computer security and information systems security; the two are used interchangeably. Computer security can also be described by domains, functions and/or concepts. The domains of computer security can be divided into physical security, operational security, personnel security, systems security and network security. Concerning the functional areas, it is possible to define risk avoidance, deterrence, prevention, detection, and recovery as a computer security. In computer security, confidentiality, integrity, authentication, access control, non-repudiation, availability and privacy can also be classified as concepts. The issue of risk is closely related to information security of the information. Any event that is prone to an unfavorable effect in the realization of business objectives is considered risky (Huczynski, 2021). According to the international organization of standardization (ISO), risk can be defined as the likelihood of the occurrence of an adverse event in an asset or assets. The proportional impact of the relative severity of the risk is contingent upon the business value of the damage or loss, and upon an estimate of the threat frequency. In general, resources, controlled management, safety and integrity, the implementation of policies and laws, and operational opportunities and economies are the primary reasons why information system security is offered. Security failures can also be costly to any organization. Such losses may be attributed to failure or the cost of fixing it and later on the cost of protecting the systems and preventing repeat failure. Managers and employees further contribute that information systems security come second only to their individual problems of efficiency and effectiveness- of their performance, which is directly and materially related to the result of their performance. The security objectives cannot be met by technical and procedural protection alone since the employees, the management and the external IT users and partners should have an educated attitude towards security to embrace the information system security levels.

A quantification of the existence of the following would provide a clear picture of the status of information systems security within an organization; the support and commitment of the senior management, policies and procedures in place, a clear set up within an organization, awareness and security training, monitoring and compliance mechanisms and incident response and handling. The Threats to information security are Deliberate Software Attacks, Technical Software Failure or Errors, Act of Human Error or Failure, Deliberate Act of Espionage or Trespass, Deliberate Act of Sabotage or Vandalism, Technical Hardware Failure or Errors, Deliberate Act of Theft, Forces of Nature, Compromises to Intellectual Property, Technological Obsolescence and Deliberate Act of Information Extortion. The safeguards that accompany information security are: Use of

Passwords, Media Backup, Virus Protection Software, Employee Education, Audit Procedures, Consistent Security Policy, Firewall, Violation Reporting, Auto Account Logoff, Monitor Computer Usage, Publish Formal Standards, Control of Workstations, Network IDS, Host Intrusion Detection and Ethics Training (Kruger, 2021).

Another significant factor that can be in the minds of consumers who want to use e-banking facilities is privacy and security (Magklaras, 2020). Think of it in the situation whereby the service providers of e-banking provide a secure e-banking platform in which customers conduct their financial transactions and are guaranteed of privacy of their personal data being transferred over the platform. Here, consumers will have an easier time trusting the e-banking provider and they will turn loyal to the provider. The second aspect of EBSQ would be the web site design. Under the e-banking environment, quick processing and page loading, frequent updating and brevity on the e-banking portal and how it is presented, all instills confidence in the customer that the e-banking organization is trustworthy. This way, the customers will be more loyal to them. Customer service and support is the following EBSQ dimension. The e-customer care component (e.g. demonstrating empathetic attitude of the customer care team, simple accessibility of their services e.g. 24/7 access, commitment of the provider to answer customer queries etc.) all work in the direction of developing the customer trust in the e-banking providers in the e bank scenario. Because of this, customers will build long-term relationships with them (Siponen, 2020).

When it comes to e-commerce, the attitude of the consumers to products and other services is dependent on whether they are engaged in the e-services or not (Thomson, 1998). Enjoyment/involvement/involvement with products/services refers to understanding of products or services or a sense of personal relevance to a product or a service based on individual interests, needs and values of the consumers?48. The literature has shown that online service providers can enhance consumer confidence in their service by providing good services to consumers; this is however different among high and low involved consumers. To be precise, the service quality has a stronger impact on the level of trust in the case of high-involved but not low-involved consumers. Due to the high-involved and low-involved consumers, the level of consumer cognitive effort in processing the presented cues in the environment varies. The degree of consumer involvement moderates the effect of environmental cues and the sequential interaction between the quality of e-banking services and consumer trust, in this paper the authors are proposing that consumer involvement in e-banking can mediate the intensity of the mediated effects that initial trust in e-banking produces on the relationship between EBSQ dimensions and consumer loyalty. Online purchasers who are highly involved are supposed to have superior search analysis and their online buying process is more thoughtful and calculated when compared to low involved online purchasers.

McCormac (2020) examined how the students of secondary schools in Oyo and Ondo States, Nigeria, perceived incidences of Internet crimes as associated with school-age children. The study revealed that students are fraudulently cheating their fellow students to Internet crime by students in universities, poly-techniques, colleges of learning. In addition, the male students are more active compared to their female counterparts which should be replicated throughout the globe. Moreover, the socioeconomic status of parents does not affect the participation of students in senior secondary schools in Internet crime since both poor and wealthy households are represented by their students committing the crime. Not only this, the involvement of students in the crime of the internet has not affected the performance of students negatively since, whatever level of the thinking which is used to make money by scamming people using the internet is being used in a positive direction to uplift the academic status of the students. Some argued that in the example of Nigeria, the Internet fraud enterprise is gender-neutral as the role of males and females are equally functional in the fraud (Obikwelu, 2021). The privacy and anonymity the internet offers to the target consumers has excessively increased the degree of fluidity as well as structural complexity of the yahoo-boys operations in Nigeria. Even now they do not need to go out to use internet. Mapped cases of bees, electronic scams, fake sales of properties and cars are being done in a manner that none can be tracked. So has the instance of gender switching a new sense of self, which is decentralized, multiple among yahoo-boys of Nigeria. This is in fact in order to predispose their vices. At a moment of avowal or even at this very moment, someone may declare himself to be a beautiful lady or a big man or a famous person, all depending on what is required by him/her.

Rijal (2023) says that Nigeria and its external counterparts are the best opportunists because they can capitalize on growth and development of global finances and ICT since such foreign geographical expression have become extraneous. Today and tomorrow, it is now possible to plan a crime in one country, perform the crime itself in

another, and move the money gained in a third or even more countries, all of this through a personal computer. It is too broad to list all the economic and financial offences in Nigeria here58. However, it is the newborn economic crimes of phishing, identity theft and credit card fraud, the like-wise related fields of internet fraud and internet piracy, which the current criminal law of Nigeria is to address. They also said that phishing, credit card fraud and identity fraud are not distinct forms of ICT-enabled or internet-related economic offences, but another form of online fraud schemes. During this process, the fraudsters create websites which appear real but in real sense are just fronts that either defraud or acquire information that can be utilized to commit other economic offences. There are no studies that examine the area of organization of internet fraud in the undergraduates.

METHODOLOGY

The inferential research design was applied in conducting this study since it sought to reach a subset of the population that would represent the needs at a given occasion, which was to determine the effect of information security knowledge on the misuse of electronic record systems by administrative staffs at a Private University in Ibadan, Oyo State, Nigeria. Two hundred and forty eight (248) administrative staff of Lead City University, Ibadan were administered the research instrument (questionnaire). Krejcie and Morgan chose the sampling technique to determine the size of a population of six hundred and eighty five (685) administrative staff of Lead City University. They applied the linear regression analyses to establish the inferential statistics of the formulated hypothesis. The data collected as a part of the study were analyzed using Statistical Package of Social Sciences (SPSS) version 29. The hypothesis is tested in the study at the level of 0.05.

Test of Hypothesis

Table 1a-c: Summary of regression analysis for the influence of information security awareness on the use of electronic records systems of administrative staff in private universities in Ibadan, Oyo State, Nigeria.

Model Summary						
Model	R	R Square		Adjusted R Square		Std. Error of the Estimate
1	.669[a]	.448		.441		.32368
a. Predictors: (Constant), information security awareness						
ANOVA						
Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	15.365	2	7.682	73.327	.000[b]
	Residual	18.963	281	.105		
	Total	34.328	283			
a. Dependent Variable: electronic records systems						
b. Predictors: (Constant), information security awareness						
Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	.825	.189		4.364	.000
	User of Information Compliance	.408	.051	.456	8.011	.000
	Behavioural Intentions	.320	.046	.394	6.924	.000
a. Dependent Variable: Electronic Records Systems						

Source: Researcher's Field Survey Results (2025)

The results of the regression analysis to determine the effect of the information security awareness on the use of the electronic records systems by the administrative staff in case of universities located in the city of Ibadan, Oyo State, Nigeria are presented in Table 4.1a-c. Table 1a includes a summary of the model that identifies the location of the model equation in the data. To ascertain the predictive power of the model applied in this study,

the JJ/R2 was used. Based on the results, information security awareness is significantly and positively related to the use of electronic records system of administrative staff at the universities in Ibadan, Oyo state in Nigeria ($R = 0.669$, $p<0.05$).

The observed adjusted coefficient of determination (Adj. R2) value of 0.441 indicates that the information security awareness (user information compliance) explains 44.1 percent of the variation in use of electronic record systems by administrative staff members in the sample population of private universities in Ibadan, Oyo State, Nigeria. The remaining 55.9 percent variations in electronic records systems can be explained by changes in other exogenous variables than the examined information security awareness. This fact shows that information security awareness affects 44.1 percent of electronic records systems utilization of administrative staff in the Ibadan private universities in Oyo State, Nigeria. The ANOVA (overall model significance) of the regression analysis (Table 1b) revealed that there is a significant effect of the user information compliance factor on the use of the electronic records systems by administrative personnel in the private universities in Ibadan, Oyo State in Nigeria. This can be attributed to the F-value (73.327) and significant p-value at a 95 percent confidence interval. Consequently, the result revealed that the information security awareness as adopted by the private universities within the state of Ibadan, Oyo, state of Nigeria, had a significant influence on the utilization of the electric-records information systems by the administrative staff within university.

Also, the results in the regression coefficients in Table 1c showed that at 95 level of significance, a one unit change in behavioural intentions will lead to increase in the use of electronic records systems of administrative staff among the employees of the private universities in the city of Ibadan, Oyo State, Nigeria by 0.408 units all other factors remaining constant. When everything else remains the same, a one unit change in behavioural intentions will result in an increase of 0.320 the usage of the e-records systems among the administrative staff of the privately owned universities of Ibadan, Oyo State, Nigeria. This result suggests that compliance of user information presents a more significant comparative influence on the utilization of the electronic records systems than the behavioural intentions that target administrative workers in the privately owned universities in Ibadan, Oyo State, Nigeria. According to this result (Adj. $R2 = 0.441$, $F(2,281) = 73.327$, $p= 0.000$), this research study rejects the null hypothesis one (H01) that there will be no significant effect of information security awareness on the use of electronic record systems among administrative personnel of the private universities in Ibadan metropolis, Oyo State, Nigeria.

DISCUSSION OF FINDINGS

Here is the section to explain the findings about the past research of the study. The research results are elaborated and classified by the formulated hypotheses and by the previously carried out studies.

Linear regression analysis of Hypothesis one indicates that the information security awareness will not have any meaningful impact on the use of electronic records systems among administrative employees of private universities in Ibadan, Oyo State, Nigeria. The results of hypothesis one were analyzed and revealed that information security awareness was a major factor to the use of electronic records systems by the administrative staff in the private universities in Ibadan, Oyo State in Nigeria. The findings of the earlier empirical research supported the hypothesis one. Using the example, McCormac (2020) examined the attitude of secondary school students towards incidents of crimes committed with the assistance of the Internet among school-age children in Oyo State and Ondo State in Nigeria. This study has shown that students are being initiated into Internet crime by their friends in universities, polytechnics and colleges of education.

Moreover, the male students are more involved than the female students everywhere. Moreover, the involvement of the students of senior secondary school in Internet crimes is not related to the social status of their parents as students of high and low status homes are involved in the crime. This is in addition to the fact that students who commit Internet crime do not slow down in regards to academic performance because what they do during scamming the people in the computer is the higher mental level thinking that they apply in scamming people is being put into practice so that they can be prepared to have a better academic level. They argued that in Nigeria, Internet fraud is a practice where both genders actively participate on a functional level with various specific roles identified (Obikwelu, 2021). The sense of anonymity and privacy that the internet presents to the potential users has abnormally increased the fluidity and structural dynamism of the activities of the yahoo-boys in

Nigeria. The internet is now available to them at the comfort of the home. False sale of real estates and vehicles, false sale of vehicles, be-cheated, electronic defrauds are all done without any trace. In Nigeria, the yahoo-boys, as well have brought gender switching a decentred and multiple sense of self. The reason behind this is simply to allow them to get their way in their criminal activities. Any given time, an individual can say that he/she is a beautiful lady or a big man or a celebrity depending on what he/she needs at that particular time.

Rijal (2023) says these scammers in Nigeria and other benefiting components elsewhere are the final exploitation of global economic development and transformation of information communication technology, which has rendered the traditional expression of geography irrelevant. A person can now plan a crime in one country and commit the crime in another country and transfer the proceeds of a crime in one country to another country and even to more countries by just using a personal computer. The crimes in Nigeria are so wide in economic and funding aspects that they cannot be listed here58. However, the relatively new phenomena that have to be addressed through the existing criminal legislation in Nigeria are the so-called internet or cyberspace fraud through phishing, identity theft, and credit card fraud, which would be the most similar notions of economic crimes. It was further assumed that the occurrence of phishing, credit card and identify fraud cases are not a unique attribute of ICT-facilitated or internet-enabled economic crimes, but an extra process of internet-based fraudulent arrangements. Under such a method the fraudsters set up sites that appear real but are in fact a deception sites that the scammers use to defraud or obtain information that they can use to commit other economic crimes. Literature has a gap that research on the internet fraud organization among undergraduates.

The subject of information security is broad and a different definition is required. What is said in the literature is that both computer security and information systems security work within the same context. It is possible to model computer security as domains, functions of the concept. The domains of computersecurity can be divided into physical security, operational security, personnel security, systems security and network security. Regarding functional domains, the computer security is a part of risk avoidance, deterrence, prevention, detection and recovery domain. Conceptually speaking: computer security is separated into confidentiality, integrity, authentication, access control, non-repudiation, availability, and privacy. The information system security aspect is also closely associated with the concept of risk. The risk can be defined as something that may affect the goal of the business negatively (Huczynski, 2021). The International Organization of Standardization (ISO) defines risk as the probability that a specific threat will actually take advantage of the vulnerabilities in an asset or assets. The importance of the relative severity risk impacts will then be proportional to both the business value of a loss or damage and the approximate frequency of the threat. Protecting resources, preservation by managers, safety and integrity, policy and law enforcement, and operations benefits and economies are most frequently cited as the motivating factors to provide information system security. Security breaches are extremely expensive to the company. Failure will result in losses, and the money used to recover it and additional expenses to tighten systems to avoid failure will also lead to loss. Moreover, managers and employees rank information systems security concerns as second-order concerns because they are not as important as their own efficiency or effectiveness concerns since those directly and significantly impact what they do. It is not only through technical and procedural protection that security objectives can be achieved, but also through an educated attitude towards security among the employees, the management, external users and partners in the IT sector is also a key aspect in achieving a satisfactory information systems security.

The following elements can be evaluated to give a clear picture of where information systems security is in an organization: commitment and support of the senior management, policies and procedures currently in place, a clear organizational structure, security awareness and education, monitoring and compliance, and incident handling and response. Those information security threats can be intentional software attack, technical software failure or error, intentional acts of human error/failures, intentional acts of espionage/invasion, intentional acts of sabotage/vandalism, technical hardware failure or error, intentional acts of theft, forces of nature, and intellectual property compromise, technological obsolescence and intentional acts of information extortion. Some of the mechanisms of information security include the use of passwords, media backup, virus protection software, employee education, audit procedures, and consistent security policy, firewall, violation reporting, automatically log out of accounts, monitoring the use of computers, formal standards publication, workstation control, network intrusion detection system, host intrusion detection, and ethics training (Kruger, 2021).

SUMMARY OF FINDINGS

This study examined the influence of information security awareness on the effective use of electronic records systems among administrative staff of a private university in Ibadan, Oyo State, Nigeria. From the interpretation of analyses of data collected and findings of the study, the following can be summed up as the main empirical findings of this study:

1. The level of electronic records systems is moderately high among the administrative staff of private universities in Ibadan. Oyo State, Nigeria.
2. The level of information security awareness is moderately high among the administrative staff of private universities in Ibadan. Oyo State, Nigeria.
3. Information security awareness (user information compliance and behavioural intentions) is used by the administrative staff of private universities in Ibadan. Oyo State, Nigeria, significantly influenced the electronic records systems among the administrative staff of private universities in Ibadan. Oyo State, Nigeria.

CONCLUSION

The nature of record management systems in the framework of determining administrative staff success is also important in the academic institutions. The necessity to improve the record management equipment to convert it into full electronic has been beyond imperative as it is the major factor that can lead to enhanced administrative functionalities as greater staff level would be more productive over a long-term scenario and this would maintain the level of success in the academic scenario. On the one hand, information security awareness is significant in the utilization of electronic record system by administrative employees at a privately owned university in Ibadan, Oyo State, Nigeria. It contributes to the capture of all academic information, put into smooth processing and accessibility when necessary in order to fulfil the objectives of the institution.

RECOMMENDATIONS

Based on the findings in this study, the following recommendations were made:

1. Management should explore every opportunity to achieve a higher level of electronic records systems upgrading, and upgrade record management equipment to the latest level.
2. Management should take a more proactive approach to information security awareness among administrative staff by protecting sensitive information and streamlining record management processes.
3. Management of Private University in Ibadan, Oyo State, Nigeria should explore more opportunities to enhance the training values of their administrative staff.

REFERENCES

1. Ashmarina S. I. & Mantulenko V V. Digital technologies in the new socioeconomic reality. Springer. 2021, 030-83175-2.
2. Bond T., Stephens C., & Piscitello D., "Security Awareness Survey," 2012.
3. Herath T. & Rao H. R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support System, 47(2), 2021, 154–165.
4. Hofmann D. A. & Stetzer A. A cross-level investigation of factors influencing unsafe behaviors and accidents. Personnel Psychology, 49, 2020, 307-339.
5. Huczynski, A. & Buchanan, D. Organizational behavior: An introductory text (4th ed.). Harlow, 2021, UK: Prentice Hall.
6. Kruger, H. A., & Kearney, W. D. A prototype for assessing information security awareness. Computers & Security, 25, 2021, 289-296.
7. Magklaras G. B. & Furnell S. M. A preliminary model of end user sophistication for insider threat prediction in IT systems. Computers & Security, 24, 2020, 371-380.
8. Siponen M. T., "A conceptual foundation for organizational information security awareness," Information Management & Computer Security, vol. 8, 2020, 31-41.

9. Thomson M. E. & Von Solms R., "Information security awareness: educating your users effectively," Information management & computer security, vol. 6, pp. 167–173, 1998.
10. McCormac A., Parsons K. M. & Butavicius M. A. Preventing and profiling malicious insider threats (DSTO Technical Report, DSTO-TR-2012-2697). Canberra, Australia: Defence Science and Technology Organization, 2020.
11. Obikwelu C. N. Resource quality and service delivery in selected universities in South-East Nigeria, 2021.
12. Rijal E. & F. Saranani. The Role of Blockchain Technology in Increasing Economic Transparency and Public Trust. Technology and Society Perspectives (TACIT), 1(2), 2023, 56–67.
13. Abubakari A. R., Inusah M. & Abdulai A A. The Effects of Information Communication Technology on Administrative Efficiency of Tamale Technical University. American Journal of Industrial and Business Management, 13, 2023, 394-417
14. Adisa A. & Bamidele L. Exploring the Influence of Digital Technology on Administrative Service Delivery in Tertiary Institutions: An Empirical Insight from The Federal Polytechnic, Ilaro. International Journal of Research and Innovation in Social Science (IJRISS) 8(11), 2024.
15. Marks A., "Exploring universities' information systems security awareness in a changing higher education environment: A Comparative Case Study Research," PhD, University of Salford, 2023.
16. Nwachukwu V. N. Information and Communication Technologies (ICTs) Education for Effective Human Resource Development in Nigerian Schools, Journal of Curriculum Studies 11(1): 2020, 1110-114
17. Ojo e. e., O. J. Ige & A. Rasaki. Digital technologies: Contemporary tools for reshaping the roles of office managers in selected tertiary institutions, Lagos State, Nigeria. Academic Staff Union of Polytechnic International Conference, Yaba, Lagos, 2024.
18. Olatubosun O. E., O. A. Olusoga & T. O. Olayemi. Impact of ICT on administrative efficiency in Nigerian higher institutions. African Journal of Information Systems, 5(4), 2021, 77- 90
19. Prastyaningtyas E. W., S. Sutrisno, E. D. Soeprajitno, A. M. Ausat & S. Suherlan. Analyzing the Role of Mentors in Entrepreneurship Education: Effective Support and Assistance. Journal on Education, 5(4), 2023, 14571–14577
20. Spears J. L. & Barki H, "User participation in information systems security risk management," MIS Quarterly, 503–522, 2010.