Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.7, No.3, 2016

Information Systems and Its' Abuse by Employees of Nigeria Bank

Nwokike O[1] Ajaegbu C[2]
1.Information Resource Management Department, Babcock University
2.Computer Science Department, Babcock University

Abstract
Information and Communication Technology (ICT) plays a vital role in every sector of life. Studies have shown that ICT usage in many sectors has been solely abused. This study investigates the abuse of information system in Nigerian Banks. Employees' perception of abuse of information systems was sought using copies of a structured questionnaire. Findings show that unauthorized access of information or programs via a computer had the highest pick as abuse of information system, followed by unauthorized copying or altering of data or programs, then theft of telecommunications or computer equipment, and so on. In conclusion, it was observed that Unethical practices through the abuse of information system result in lesser productivity, decimation of corporate assets, non-compliance with privacy regulations, legal liabilities, network bandwidth and resources exposure. Thus, deploying comprehensive preventive procedures can help organisations guard against abuse of its information systems.
Keywords: Abuse, Information systems, Nigerian banks and Ethics.

1. Introduction

Information and Communication Technologies (ICT) makes the world a global village. Expansion of information systems brought by the continuous use of ICT necessitated its growing trend in every aspect of human endeavours. Information system is the information and communication technology that an organisation uses and also the way in which people interact with this technology in support of business processes (Kroenke, 2008). According to Reix (2002), an information system plays a key role in organizations as its design has an impact on the design of the organization, individual roles and management process. Information systems through the use of Computers and networks are taking over enterprises, as they break into business processes to the point where these systems are critical to the success of the organization.

Gawde, (2015) notes that use of information systems has become a standard for businesses to perform daily functions efficiently and effectively. Increasing use of Desktop PCs, Laptops, network connectivity including Internet, email at homes or workplaces requires individuals or employees with skills. Skilled employees and networked information systems are becoming the most valuable assets for such organizations to function efficiently. Trust is placed in these employees to ensure that personal data are handled appropriately in organisation. Presently, ethical issues are been raised on widespread use of information systems in organisations which include establishing accountability for the use of information systems, setting standards to safeguard information system quality, protect the safety of individuals and society, preserving values and institutions considered essential to the quality of life in an information society.

More often dubious employees or individuals abuse information system for personal benefits. Increasing incidents of information system abuse poses threats to organisations. This situation should facilitate organisations in taking effective preventive procedures that could assist to curb abuse or enforce appropriate usage policies to minimize losses and increase productivity. The growth in physical infrastructure as well as rising importance of information systems to an organization, has informed the need to safeguard the information system, not only from computer-generated attacks, but from the physical attacks that can be perpetrated against them.

Abuse of Information Systems by employees poses serious challenges to organizations including loss of productivity, loss of revenue, legal liabilities and other workplace issues. Abuse of information and communications technology (ICT) includes theft of hardware and software, unauthorized access to computer systems and inappropriate use of equipment (Hutchings and Jorna, 2015). Computer fraud takes the form of alteration of the programmes or application packages, or intruding into the computer system through remote sensors. Storage drives can also be tampered with so as to gain access to unauthorized domains or credit accounts for which the funds were not intended. Abuse may also include cash thefts and stuffing of counterfeit currency notes into ATM machines by or with connivance bank employees (Ayozie, 2013).

Although there is a sizeable body of knowledge detailing the abuse of information Systems (Reix, 2002; Smith &Jorna 2011; Olumonye, 2013), and others detailing unethical practices reflected in various forms and levels in the commercial banks (Donli, 2004, Ayozie, 2013, Business Day, 2004). However, little is known about the views of Nigerian bank employees on the abuse of information systems, thus the need for adequate knowledge of the various forms of abuse of information system and the level of abuse of information system in

Nigerian banks.

2. Literature Review

It is no longer news that Information and Communication Technologies are used to facilitate unlawful acts in organisations (Choo, Smith &McCusker 2007). More often in organisations, the trusts bestowed on employee have been abused and data have been inappropriately accessed or otherwise used by insiders for illegitimate purposes. Such abuse may provide financial gain, especially where information systems are manipulated by persons both within and external to organisations to commit fraud (Hutchings and Jorna, 2015). Adeyemo (2012) defines fraud as illegal acts characterized by deceit, concealment or violation of trust.

Information System abuse involves performing a behavior that is viewed by the organization as a misuse of Information and System resources (Magklaras & Furnell 2002). Preventing the abuse of ICT is fast becoming an important area of concern as employees are often placed in a position of trust, which provides them with electronic access to personal information and records in instances where there are checks on an employee's access (Smith &Jorna 2011). When the abuse of ICT results in data breaches, there can be further negative impacts arising from the loss and consequent misuse of individuals' personal information. The abuse of ICT could be damaging to organisations. There are significant implications of abuse of ICT, particularly owing to the amount of data that an organization holds responsible for individuals. Abuse of ICT may also drain government resources and have a harmful impact on the administration of agencies, upsetting available funds for service and program delivery (Lindley, Jorna& Smith 2012).

Contemporary use of Information systems raises new ethical questions for individual firms and the societies they serve. Ethical issues in the use of information systems at the moment raise immense concern given increase in use of the Internet and electronic commerce. Internet and digital technologies make it easier to assemble, integrate, and distribute information, unleashing new concerns about the appropriate use of customer information, the protection of personal privacy, and the protection of intellectual property. Unlike other technologies such as steam engines, electricity, the telephone, and the radio, information systems can be used to achieve societal progress. On the other hand, it can also be used to commit crimes.

Knowledge of legal and ethical issues on the use of information systems and service delivery can be acquired through education. Ochalla (2009) opined that since information ethics threads through all human activities that generate, process, store, disseminate and use information and knowledge, everyone working in the information and knowledge industry, including consumers of knowledge products and services should undergo information ethics education. Shachaf (2005) raised interest in the implementation of codes of ethics in order to determine the extent the codes are known in each country and the influence of the codes on the practitioners. Babalola (2013) made recommendations for policy implementation while discussing the effects of some ethical issues like digital divide, privacy infringement and cybercrime on adoption of electronic governance in the country.

Ethical issues in the use of information systems

Ajaegbu and Uwom (2014) opined that ethics is a vital issue that should be integrated in all fields of study. It could be seen as a principle of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviors. These principles and values regulate behaviour with respect to what is right or wrong; supporting a legal and ethical workplace and providing a clear guiding philosophy especially when making decisions (Pollack and Hartzel, 2006, Shachaf, 2005). Ethics is a branch of philosophy that is concerned with moral principles of behavior or conduct of individuals in society. Ethics defines and provides ideas that sustain action that is good and right in terms of obligation, fairness and benefits to society (Wengert 2001; Markkula Centre for Applied Ethics, 2010). Ethics is a concern of humans who have freedom of choice. Ethics is about individual choice when faced with alternative courses of action. Ethical choices are decisions made by individuals who are responsible for the consequences of their actions.

Such unethical practices has heightened ethical concerns, taxed existing social arrangements and made some laws obsolete. As it appears information technologies and systems also create new opportunities for illegal behavior and mischief. Halawi and Karkoulian, (2006) point out that Computer storage and networking capabilities are creating new situations, new responsibilities and consequences which existing laws or rules of conduct may not be appropriate and are disrupting the operable norms and values. Hence, there is a need for ethical and intellectual resources with which to understand and confront these changes (Osif, 2005).

Values are often embedded in the numerous concepts of information and professional ethics. Knowledge of these values with a commitment to doing right and upholding professionalism form the foundation to quality service delivery. This helps in identifying some of the principles and obligations that cause workplace problems and dilemmas. When employees work within an ethical framework, they exhibit an understanding of general laws pertinent to work role and particularly information service delivery.

Ethical issues in the use of information systems have been examined from many perspectives including selection or choice of material, access, quality of information, equality of treatment, right, accuracy and

censorship, copyright and data protection, intellectual freedom, reference services, protecting users' rights, information retrieval and dissemination, computer application, use and misuse of information, charging fees and profit making, conflict of interest, confidentiality, personal ethics and professional codes of ethics, concealment of information, misinforming clients, divulging private information; disseminating false information (Mason, 2001; Hauptman, 2000, Milton, 2008; Kaddu, 2010 and Smith 2010)**.** Ethical issues raised by research on the use of information systems include

- establishing accountability for the consequences of use of information systems,
- setting standards to safeguard system quality,
- protecting the safety of the individual and society,
- Preserving values and institutions considered indispensable to the quality of life in an information society.

Information ethics is an important issue (Hilton, 2000). According to Halawi and Karkoulian (2006) information ethics investigates legal and ethical issues arising from the development and application of technologies in the creation, collection, recording, distribution, conservation, copyright and access of information. Mason's theoretical framework deals with the major information technology ethical issues of the information age. It identifies four issues privacy, accuracy, property and accessibility (PAPA). The concept of PAPA as the foundation of information ethics has remained popular for over two decades (Halawi & McCarthy, 2013).

Halawi & McCarthy, (2013) point to a doubt that IT professionals are unprepared to deal effectively with ethical issues in the workplace. An ethical issue arises each time the system user in pursuit of goals engages in behavior(s) that materially affects the ability of another user to pursue goals. Ethical issues in IT differ from general ethical issues as information in electronic form is more readily available. This raises questions in regard to issues such as intellectual property rights, plagiarism, piracy and privacy when there is less personal contact (Halawi& McCarthy, 2013).

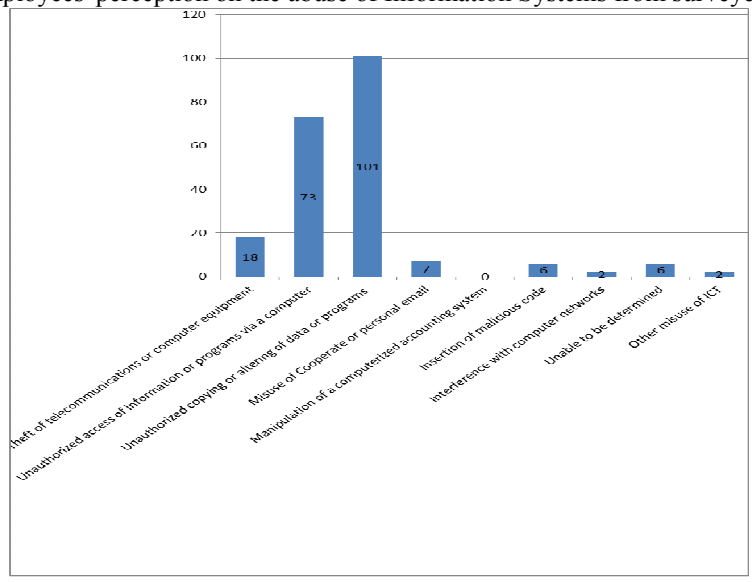
3. Methodology

The study employs a quantitative research design to collect data by means of questionnaire from employees of Banks within Ugbowo, Benin City in relation to the abuse of Information Systems. A random sample of 300 employees was surveyed. A pilot test was carried out to test for the validity and consistency of questionnaire as 10 (ten) copies of the questionnaire were administered to selected employees of banks in Ugbowo, Benin city. The data reliability as measure of the internal consistency of data was determined by means of Cronbach's Alpha coefficient giving 0.70 which is considered reliable (Bryman & Bell, 2007).

4. Data analysis and presentation of results

From the random sample of 300 bank employees' surveyed, only 128 questionnaires was returned valid and used. Data was analysed with percentages and mean. Data is presented in a chart below to enable inference after data have been grouped and classified.

Figure one: Employees' perception on the abuse of Information Systems from surveyed NigerianBanks



Source; *Field survey*, 2015

5. Discussion of findings

Abuse of Information System by bank employees can be seen as performing any behavior that is defined by the organization as an abuse of its information and system resources (Magklaras & Furnell 2002).In the study, the various forms and levels of abuse of information system were grouped or classified as indicated in figure one above.14% of this study's respondents indicate that theft of telecommunications or computer equipment is an abuse of information system. The value of computer equipment is greater than just the replacement cost of the hardware but greatest when such device has been used to store proprietary or customer-related data. Computers and mobile devices may be targeted for this reason (Smith &Jorna 2011).

The findings show that 57% of the respondents indicate that accessing information or programs via a computer without authorization is an abuse of information system.78.91% of the respondents agree that unauthorized copying or altering of information is also an abuse, affirming earlier views (Hutchings and Jorna, 2015). There have been reported cases in the print media, where customers complain against undue access and manipulation of their accounts (Business Day, 2004).Osif, (2005) suggests the need for ethical and intellectual resources with which to understand and confront such abuse. An ethical guide and code is particularly applicable here since employees have access to sensitive information relating to individuals details, business records and even security issues.

6. Conclusion

Most often, the abuse of an organization's information system is caused by the employee, as recorded cases of information security compromises are the result of actions by an insider. The abuse of Information Systems by employees has unswerving business cost. These include are lesser productivity, decimation of corporate assets, non-compliance with privacy regulations, harass from legal liabilities, exposing network bandwidth and resources. Therefore, the use of wide-ranging preventive procedures can help organisations to defend against abuse of its information systems.

References

Ajaegbu, C., & Uwom, O.O., (2014) Ethical Roles in Computer Networks. *International Journal of Ethics*, Nova Science Publishers, 10(4).

Adeyemo, K. A. (2012) Frauds in Nigerian Banks, Nature, Deep Seated Causes, Aftermaths and Probable Remedies, Mediterranean Journal of Social Sciences, 3.

Ayozie, D. O. (2012) Ethical Consideration of Integrated Marketing Communication in Nigeria. Chartered Institute of Banking Journal: The Nigerian Bankers. Victoria Island, Lagos.

Ayozie D.O (2013) The Current Ethical Challenges in the Nigerian Commercial Banking Sector. Global Journal of Management and Business Research, 13(10)1

Bryman, A., & Bell, E., (2007) Business Research Methods. New York: Oxford University Press

Business Day Newspaper (2004) Banking Survey: Nigeria and the Challenge of Ethical Banking. Business Day, Monday 16th February, 2004, Lagos, Nigeria.

Donli, J. C. (2004) Causes of Bank Distress and Resolution Options. Bullion Publication of the Central Bank of Nigeria, Abiodun Kinson Enterprises, Lagos, Nigeria.

Foltz, C. B. 2000. The impact of Deterrent Countermeasures upon individual intent to commit Misuse: A Behavioral Approach. Unpublished Doctoral Dissertation, University of Arkansas, Fayetteville.

French C. S. (2006), Computer Science, 8th Edition, New York, Dp Publications, Limited

Gawde,V.(2015).Information Systems Misuse - Threats & Countermeasures. vgawde@riyadbank.com

Halawi, l &Karkoulian, (2006). "Ethical Attitudes of Business Information Systems Students: An Empirical Investigation*": Issues in Information Systems: The Changing Role of IS Education*, *VII* (1), 175-178

Halawi, L. & McCarthy, R. V, (2013).Evaluation of Ethical Issues in the Knowledge Age: An Exploratory Study. Issues in Information Systems; 14(1), 106-112.

Healy, M. & Iles, J. (2002).The establishment and enforcement of codes.*Journal of Business Ethics*, *39*(1/2), 117-124.

Hilton, T. (2000). Information Systems Ethics: A Practitioners Survey, *Journal of Business Ethics, 28*, 279-284.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y. & Wei, K. (2003).An integrative study of information systems security effectiveness. International Journal of Information Management 23(2) 139–154.

Kroenke, D M. (2008).Experiencing MIS. Prentice-Hall, Upper Saddle River, NJ

Lee, S. M., Lee, S. G. &Yoo, S. (2004). An Integrative Model of Computer Abuse based on social control and general deterrence theories. Information Management 41(6) 707–718.

Lim, V. K. (2002). The IT way of Loafing on the Job: Cyberloafing, Neutralizing, and Organizational Justice. *Journal of Organizational Behavior, 23*, 675-694.

McCarthy, R., Halawi, L. & Aronson, J (2005). "Information Technology Ethics: A Research Framework." *Issues in Information Systems: The 21st Century Challenges to Information Technology*, *VI* (2), 64-69.

Peslak, A. R. (2006). PAPA Revisited: A Current Empirical Study of the Mason Framework. *The Journal of Computer Information Systems, 46*(3), 117- 123.

Reix R. 2002, Systèmesd'informationet management des organisations, Editions Vuibert, 4ème édition.

Rezaee, Z., Elmore, R. C. &Szendi, J. Z. (2001). Ethical behavior in higher education institutions: The role of the code of conduct. *Journal of Business Ethics*, *30* (2), 171-183.

Siegfried, R. M. (2004). Students attitudes on software piracy and related issues of computer ethics. *Ethics and Information Technology*. *6*, 215-222.

Wiant, T. L. 2003. Policy and its impact on medical record security. Unpublished doctoral dissertation, University of Kentucky, Lexington