INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) AND CHALLENGES OF ORGANISATIONAL SECURITY

A.N Alozie

The use of Information Technology in business has had major impacts on society, and this raises ethical issues in the areas of crime, privacy, individuality, employment, health and working condition. As remarked by O'Brian and Marakas (2008). Information Technology has had beneficial results as well as detrimental effects on society and people. For example, computerization of manufacturing process has the beneficial result of improving working conditions and producing products of higher quality at less cost, but at the same time has adverse effect of eliminating people's jobs. The overall effect of computerization has raised some ethical responsibilities.

There is no question that the use of Information Technology in business presents major security challenges, poses serious ethical questions and affects society in significant ways.
To properly situate this paper, it is necessary to have a picture of the word "Information Technology, (IT").

Halsey (2009) asserts that information is incomplete without communication. It is this combination that has given rise to information and communication technology, commonly called ICT. It generally refers to cybernetics which is an inter-disciplinary science dealing with communication and control systems in living organisms, machines and organizations.

IT has been variously defined in many contexts. Some of these definitions include that IT is the application of computers and telecommunication equipment to store, retrieve, transmit and manipulate data often in the context of a business or other enterprise. The term is commonly used as a synonym for computers and computer networks, but it also comprises of other information distribution technologies such as television and telephones. Several industries are associated with information technology, such as computer hardware, software, electronics, internet, telecom equipment, e-commerce and computer services. Also Henry (2006) States that Information Technology encompassed all matters concerned with the use and furtherance of computer science and technology as well as the design, development, installation and implementation of information systems and applications.

In a business context, the Information Telecommunication Association of America has defined IT as "the study, design, development, application, implementation, support or management of computer-based information systems". In an academic context, the Association for computing machinery defines IT as "undergraduates' degree programs that prepare students to meet the computer technology needs of business, government, healthcare and other kinds of organizations (Moore, 2009).

What is Information System?

A system is an array of components that work together to achieve a common goal or multiple goals, by accepting input, processing it and producing output in an organized manner. (Effy, 2009). In the same way, Information Systems consists of all the components that work together to process data and produce information. Almost all business information systems consist of many subsystems with sub-goals, all contributing to the organization's main goal. Information System therefore

consists of people hardware, software, data and networks.

Information System Security

Information System Security is one of the most pressing challenges confronting all kinds of present day organizations. Although many companies have discovered how critical information is to the success of their business or organizations, very few have managed to be effective in maintaining their information security, avoiding unauthorized access, that is hacking, which include; preventing intrusions, stopping secret information disclosure and industrial espionage.

Mellado and Rosado (2012) remarked that security is currently a widespread and growing concern that affects all areas of society, business, domestic, financial, government and so on. Information society is increasingly dependent on a wide range of software systems whose mission is critical, such as air traffic control systems, financial systems or public health systems. Information has become a critical asset of all organizations owing to their rapid adoption of ICT (Information and Communication Technology) in the entirety of their business activities, which has arisen from the need of careful management of the company's information. Mellado and Rosado (2012) further remarked that information is asset which is currently as important as capital or work. This reality is even more pressing in new generation companies in which information is part of their core business.

The current tendency towards using information systems which are increasingly bigger and are distributed throughout the entire internet has led to the emergence of many new threats of security. (Opdahi and Sindre 2008). This signifies that present day information systems are vulnerable to a host of threats and cyber-attacks by cyber-terrorists, hackers etc; such as virus which are propagated through the internet, social engineering attacks (phishing etc) or the inappropriate use of the nets assets by companies' employees (Choo, and Smith et al 2007).

Information Systems Security Challenges

Enterprise Security is a classical term that reflects the efforts made by organizations to avoid business risks, thus permitting a company to surpass any threat that may jeopardize its survival. Further, the traditional concept of Security needs to be expanded in order to include the aforementioned information assets whose combination is known as Information Systems Security.

Diego (2007) observed that ICT is gradually and yet increasingly changing the landscape, in this context. ICT is not only a tool but also a medium over which education, social, political and economic transformations occur resulting into development of both physical or material as well as human resources. This can, therefore, most aptly apply to information security system as protection of economic activities.

Security and Information are two closely related terms which is shown by the fact that any company's information is as good as the security mechanisms that are implemented over it. Unreliable information resulting from wrong security policies generates uncertainty and mistrust and has a negative impact on every business area. Otherwise secure Information Systems are a sign of certainty which contribute towards generating value both within and outside the company.

Malledo and Rosado have defined Information Systems Security as a function whose mission is to establish security policies and their associated procedures and control elements over their information assets with the goal of guaranteeing their authenticity, confidentiality, availability and integrity.

Ensuring these four characteristics is the core function of Information System Security.

- Authenticity allows trustful operations by guaranteeing that the handler of Information is whoever he/she claims to be.
- Confidentiality is understood in the sense that only authorized users can access the information, thus avoiding this information being spread among users who do not have the proper rights.
- Availability refers to being able to access information whenever necessary, thus guaranteeing that the services offered can be used when needed.
- Integrity is the quality which shows that the information has not been modified by third parties and ensures its correctness and completeness.

Furthermore, O'Brian has mentioned two areas of ethical issues thus: Business Ethics and Technological Ethics.

Business ethics is concerned with the numerous ethical questions that Managers must confront as part of their daily business decision. These include the issues of intellectual property rights, customer and employee privacy, security of company records and workplace safety have been major areas of ethical controversy in Information Technology.

On the other hand, technology ethics deals with the use of any form of technology. One common example of technology ethics involves some of the health risks of using computer workstation for extended periods in high-volume data entry job positions.

Cyber Crimes

Perhaps one of the major challenges of today's Information Technology is the issue of cybercrime. Cybercrime refers to criminal activities that involve the use of computers and the internet; otherwise, known as World Wide Web (www). These crimes cover a very large and diverse range of offenses. According to the Association of Information Technology Professionals (AITP), computer crimes include:

(1) The unauthorized use, access, modification, and destruction of hardware, software data or network resources.

(2) The unauthorized release of Information

(3) The unauthorized copying of software

(4) Denying an end user access to his or her own hardware, software, data or network resources

(5) Using or conspiring to use computer or network resources to illegally obtain information or tangible property.

Azeez and Osunade (2009) also defined computer crime (cybercrime) as "any harmful act committed from or against a computer or network, it differs from most terrestrial crimes in four ways: They

(a) are easy to learn how to commit.

(b) require few resources relative to the potential damages caused.

(c) can be committed in the jurisdiction without being physically present in it.

(d) are not clearly illegal".

The U.S. Department of Justice (DOJ) divides computer crime into three general categories:

1. The crime of obtaining computer hardware peripherals and software illegally.
2. Crimes that actually target a computer network or device directly (computer hacking, virus, worms, Trojan horses) logic bombs, malware, sniffers, bots spyware etc)
3. Crimes committed through the use of computer networks or devices popularly known as cyberspace crimes. Although such crimes does not target the actual computer or the network. It involves fraud and identify theft, phishing and pharming scams, corporate espionage, embezzlement; copyright infringement with software,

music and money piracy; Cyber terrorism, child pornography, trafficking and more.

One gets worried over certain reports on increased cybercrimes in Nigeria. One of such reports published in Issue No.302 of Journal on computing has it that Nigeria ranked third in the world for cyber-crimes, as well as the third most internet fraudulent country in Africa.

This development has called for concerted effort among stakeholders, civil society groups, corporate bodies and government institutions to join forces together to rid the continent of the imminent terrorist attacks through the use of information technology.

"Law enforcement agencies such as Economic and Financial Commission (EFCC), Independent Corrupt Practice and other related offences Commission (ICPC), State Security Service (SSS), the Nigeria Police among others should play prominent roles in the fight against the new trend of social challenge.

"Computer security and cybercrime awareness should be created with a view to sensitizing all users of the internet facility with the emerging indicators of crime and fraud being committed through computer.

"Need now arises to the surviving mega banks, oil multinationals, business conglomerates and communication firms from untold sorrow which the cyber criminals have resolved to inflict on most businesses.

Moore (2009), upholding the standpoint of the internet group's effort stated that the diplomats, international legal practitioners and international institutions have roles to play in ensuring that legal provisions at the international level are provided.

In support of use of ICT in organizational security, Diego (2009), holds the view that security breaches has become so rife and frequent that it required concerted efforts of stakeholders in the industry to bring an end to computer crime in the country.

He further stated that "variants of cybercrime include unauthorised access, theft of proprietary info, denial of service, inside net abuse, financial fraud, misuse of public web application system penetration, laptop theft, and abuse of wireless network, sabotage telecom fraud and web site defacement".

There is need to devise means to stop perpetrators of internet crime. There is need to secure the present global village, mega businesses and the posterity from the protracted evil of cybercrime without delay.

Halsey (2009) agrees with Trucano (2005) on the need to regularly conduct Computer Crime and Security Survey, as it is necessary for ICT practitioners, including security services such as CST and FBI to conduct survey and research with a view to containing cyber-related crimes and computer security breaches.

Solution to the Challenges

Computer security are techniques developed to protect single computers as well as networked computer systems from all the threats that is associated with computer based information system, such as accidental or intentional harm, including destruction of computer hardware and software, physical loss of data, deception of computer users and the deliberate invasion of databases by unauthorized persons. This can be seen as access control and permissions that are designed to monitor, detect and prevent any security threats or unintentional disclosure to unauthorized persons, programs or systems thus ensuring continuous availability, integrity and confidentiality of data/information in the computer system.

This safeguard/protection control can be through hardware, software, physical and procedural means and all these should combine to give appropriate coverage against all the

threats which information systems are vulnerable to.

Alozie, Iheukwumere and Uteh (2013) have outlined some security measures which an organization can adopt. These include:

Data Security:

Survival of every organization depends on the information stored in the information system, hence practical safeguards must be installed to protect and ensure accuracy, availability and integrity of important programs, files and data in the computer based information systems.

Data security is a control aimed at preventing the unauthorized use of data and ensuring that data are not accidentally altered or destroyed. It is access control and permission designed to monitor, detect and prevent any security threats or intentional disclosure to unauthorized persons/programs thus ensuring availability, integrity and confidentiality of information. According to different models of data security, include the following: Encryption, passwords, Firewalls, approved users, diskless workstation, users level security, auditing, account management, share level security, etc.

Personnel Security:

Similarly, the personnel security measures, are some of the measures that can be taken to control access and safeguard computer base information system from the threats that can emanate from the personnel in the organization that make use of the information systems. It has been observed that most computer crimes against an organization are not without insider influence. This may either be by abusing the simplest of procedures or capitalizing on the carelessness of others. No matter how good a security system is, it becomes undependable if the employees cannot be trusted.

The following security measures can be employed to check the personnel of organization and computer based information system: dual control, observation of policy/principle, rotation of duties, etc.

Importance of Security

1. Availability of Information:

Knowing that information can always be accesses, and it is also available to authorized users, programs and systems. That is there should be the assurance that the use of data, programs or other system resources are not denied to authorize users, programs or systems.

2. Integrity: Knowing that information is accurate and up-to-date, and has not been deliberately or unintentionally modified from previously approved version. It answers the question "can the information be changed or corrupted in any way".

3. Confidentiality: Knowing that sensitive information can be accessed only by those authorized to do so. This is the assurance that system resources are protected against disclosure to unauthorized users, program or system.

Conclusion

The Internet and other information technologies can have many and far reaching effects on society, especially, on organizations. We can use information technologies to solve human and social problems through societal solutions such as medical diagnosis, computer assisted instruction, governmental programme planning, environmental quality control, and law enforcement. For example, computers can help diagnose an illness, prescribe necessary treatment, and monitor the progress of hospital patients. Computer-assisted instruction (CAI) and computer-based training (CBT) enable interactive instruction tailored to the need of students. Distance learning is supported by telecommunications networks, video conferencing, e-mail, and other technologies.

Information technologies can be used for crime control through various law enforcement applications. For example, computerized alarm systems allow police to identify and respond quickly to evidence of criminal activity. Computers have been used to monitor the level of pollution in the air and in bodies of water, to detect the sources of pollution, and to issue early warnings when dangerous levels are reached. Computers are also used for the program planning of many government agencies in such areas as urban planning, population density and land use studies, highway planning, and urban transit studies. Computers are being used in job placement systems to help match unemployed persons with available jobs. These and other applications illustrate that information technology can be used to help solve the problems of society.

Obviously, many of the detrimental effects of information technology are caused by individuals or organizations that are not accepting the ethical responsibility for their actions. Like other powerful technologies, information technology possesses the potential for great harm or great good for all humankind. If managers, business professionals, and IS specialists accept their ethical responsibilities, then information technology can help improve living and working conditions for all of society.

References

Alozie A. N., Iheukwumere O. C. and Uteh C. K (2013) ICT, Office Applications (Micro Soft Access) Aba Chiedal Global Prints Ltd.

Azeez N. U. and Osunde O. Z (2009): International Journal of Computer Science and Information Security Vol. 3.1.

ChooK k. and Smith R. G. (2007) Future directions in technology enabled crimes 2007-2009. Research and Public Policy Series Australian Government. Australian Institute of Criminology.

Diego, R. (2007) "New Roads to Development". Buenos Aires: School of Economic Sciences of the University of Buenos Aires.

Effy O. Z. (2009) Management Information Systems (6^{th}ed) Area valley. The Pennsylvania State University.

Halsey, R. (2009) "Information Science" Encarta, Redmond WA: Microsoft Corporation.

Henry W. (2006) Illustrated Dictionary of IT. New Delhi, Lotus Press.

Mellado D. and Rosado, D. C. (2012). An Overview of current Information System Security Challenges and Innovations J. U. C. S vol. 18/issues 12.

Moore, M. (2009) "Distance Education", Encarta, Redmond, WA: Microsoft Corporation.

O'Brain J. A. and Marakas G. M. (2008) Management Information Systems (8^{th}ed) Boston, McGraw Hill.

Opdahi A. L. and Sundre G. (2008) "Experimental Comparison of attack trees and misuse cases for security threat identification" Information and software.

Trucano, Michael (2005) infoDev: The Information for Development Programme. Washington, DC: The International Bank for Reconstruction and Development/The World Bank.

A.N. Alozie
Department of Office Technology and Management.
Abia State Polytechnic,
Aba.