Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.4, No.9, 2014

Application of Information Technology System in Office Risk Management in Contemporary Organizations in Rivers State

BESTMAN ANTHONIA ENEFAA (M.Ed)
Department of Information Technology and Office Management, Faculty of Management Sciences, Rivers State University of Science and Technology

Abstract
This study investigated the application of information technology systems in office risk management in organizations in Rivers State. The population of the study comprised 10 insurance companies in Port Harcourt City Local Government Area of Rivers State made up of 350 members of staff. These insurance companies are UNIC, Zenith, Royal Exchange, NEM, Leadway, Guaranty Trust, Equity Life, Cornerstone, Consolidated Hallmark and NAICOM. The sample consists of 161 members of staff selected from the 10 insurance companies in Port Harcourt City L.G.A of Rivers State. The sample was selected through simple random sampling and constituted 46% of the total population of 350. A self-structured questionnaire titled: Office Risk Management Assessment Questionnaire (ORMAQ) was the only instrument used in this study for data collection. The reliability test of the instrument yielded a reliability index of 0.85. Out of the 161 self-administered copies of questionnaire, 150 of them were properly filled, retrieved and used for the study. Mean ($\overline{X}$) was used as a method for analyzing the four research questions. The results revealed that the insurance companies in Rivers States apply the majority of the lectronic data processing, storage and transmission systems in managing their office risks, but they have not gone completely digital in terms of managing the same risks using digital security systems. The study recommended as follows: insurance companies in Rivers State should completely embrace digital technologies for effective management of office risks, integrate digital risk management into their operational policies and review these policies annually, acquire more infrastructures which encourage the use of information technology systems (ITs) in managing office risks, prioritize ITs-based office risk management through robust budgetary allocation and implementation and government should create enabling environment through the provision of infrastructural facilities and legislative backings for effective office risk management.
Keywords: Information Technology, System, office Risk management and contemporary organizations

1. Introduction

Risk is ubiquitous. It is at home, in market place, business transactions, transportation points (road, air and water) and a lot of places, but particularly in our offices. Offices are units or places or points where authorized personnel of an organization carry out routine and formal functions or duties for the actualization of goals and objectives set by an organization. Risk, on the other hand, means the combination of the probability that an undesired event will occur which can prevent an organization for achieving its goals, missions, or the consequences or impact of the risks or doing its business functions. Wikipedia.com defined risk as the potential of losing something of value, weighed against the potential to gain something of value. It is also defined as it as the intentional interaction with uncertainty. Risk is defined by Hansson (2012) as the probability or threat of quantifiable damage, injury, liability, loss or any other negative occurrence that is called is caused by external or internal vulnerabilities and that may be avoided through pre-emptive action. Management means getting things or tasks done by the use of human beings. By the combined effect of the three words 'office', 'risk' and 'management', office risk management, therefore, means the process of identifying risk, assessing risk and taking steps to reduce risks to an acceptable level in the offices of an organization. Hubbard (2009) defined office risk management as the identification, assessment and prioritization of risks in an organization or its units followed by coordinated and economical application of resources to minimize, monitor and control the probability and/or impact of unfortunate events. According to International Organization for Standardization (ISO) (2009), in an ideal office risk management, a prioritization process is followed whereby the risks with the greatest loss (or impact) and the great probability (70%) of occurring are handled first, and risks with lower probability (20%) of occurrence and lower loss are handled in descending order. In practice, the process of assessing the overall risks can be difficult and balancing resources used to mitigate between risks with a high probability of occurrence but lower loss and a risk with high loss but lower probability of occurrence can often be mishandled (ISO, 2009).Intangible office risk management identifies a new type of a risk that has a 100 percent probability of occurring but it is ignored by organizations due to a lack of identification ability. For example, when deficient knowledge is applied to a situation, a knowledge risk materializes. Relationship risk appears when ineffective collaboration occurs. Process- engagement risk may be an issue when ineffective operational procedures are applied. These risks directly reduce the productivity of knowledge workers, decrease cost-effectiveness, profitability, service, quality, reputation, brand value and earnings. Intangible office risk

management allows risk management to create immediate value from the identification and reduction of risks that reduce productivity (ISO, 2009). As Martin (2013) succinctly put it, every organization has a mission. In this digital era, contemporary organizations use automated information technology (IT) system to process information for better support of their missions, office risk management plays a crucial role in protecting an organization's information assets and assets other than information assets(Martins,2013).

William (2009) identified five strategic steps for office risk management. These include the establishment of the context, identification of the risks, analysis of the risk, the treatment of the risk and monitoring and review of the risk. To establish the context of the risk means that office risk management needs to occur within the organizational setting and the search for the probability of occurrence of risks should be established and confined within those areas they occur in an organization. The context defines the basic parameters within which risks must be managed and provides guidance for decisions within more detailed risk management studies. To identify the risks means finding out all the potential risks to the organization, its record and record keeping systems, their possible causes and consequences. To analyse the risk means looking critically at risks in terms of their probability and effect, while to treat the risk suggests giving the risk the right approach of solutions or treatment they deserve. To monitor and review the risk implies checking or watching the implementation process of the risk treatment plans, and afterwards, assess whether or not the risks sought to tackle have been mitigated or eliminated (William, 2009). As noted by Vijayan (2005), it is in these five strategic steps of office risk management that information technology systems are required with a view to giving an organization sufficient and solid ground for managing risks and the potential consequences. Information technology systems are electronic or digital devices or systems which can receive, stores, process, transmit and disseminate information and communicate the same information. Dainth (2009) defined Information Technology System (ITS) as the application of computers and telecommunications related equipment or devices to store, retrieve, transmit and manipulate data, often in the context of a business or other enterprises. He further stressed that the term 'ITs' is commonly used in a synonym for computer networks, but they also encompasses other distribution technologies such as television and telephone (mobile phone).

Hibbert and Lopez (2011) defined Information Technology Systems as any devices capable of receiving, storing, managing or transmitting data including but not limited digital enablers such as mainframes, servers, personal computers, notebook computers, IPADs, pagers, ,distributed processing systems, network attached and controlled medical and laboratory digitally powered equipment, telephones, fax machines, printers and service bureaus (departments).

Furthermore, Leavith and Whisler (2008) believed that information technology systems involve using the electronic or digital data processing, storage, transmission, and security systems for information-related purposes or activities. Dorfman (2007), Chandler and Munday (2012) strongly believed and therefore stressed that information technology systems are a sine-qua-non, in this digital age, for modern organizations which can apply them in their various functions or activities, including in risk management related cases.

One of the ways office risk management can be conducted digitally is by the application of the electronic data processing systems. According to Anthony (2000), electronic data processing systems (EDPs) refer to the use of automated methods to process data. Illingworth (2007) defined EDPs as a combination of machines and people, that for a set of inputs produces a defined set of outputs. Therefore, EDPs are applied in interpreting data, facts, information relating to office risks. Consequently, information or data collected to analyse or detect the probability or possibility of disasters such as earthquakes, bushfire, flood, malfunctioning heating and air-conditioned systems, poor wiring, viruses, theft, espionage, terrorism, nuclear or chemical spill can be subject to computer application (Bourque and Clark, 2002). Other EDPs that can be applied in office risk management include digital security doors, card readers, detectors, biometric machines, robots, digital forensic systems, scanner, printers, projectors, digital monitoring system, digital cameras, among others.

Managing Office risks can be carried out through the application of electronic data storage systems (EDSs). Microsoft Computing Dictionary cited by Proctor (2011) defined EDSS as a technology consisting of computer components and recording media used to retain digital data. Anti-viruses are usually stored in computers to prevent virus of any kind from damaging information assets kept in the computers (Goda, 2012). Again, EDSS devices such as DVD, USB flash drive, compact disc, optical disk, flash drive can be very useful for mitigating to possibility information or data loss, especially in a case of computer equipment failure or damage (Olofson, 2009). Other include hard disk, magnetic tapes, paper tapes, punched cards, zip drive, memory cards, digital chips, etc (Olofson, 2009).

More so, office risk can be properly managed through the application of Digital Data Transmission Systems (DDTS). DDTS is the physical transfer of data (a digital but stream) to a point-to-point or point-to-multipoint communication channel (Clark, 2003). Examples of such channels are copper wires, optical fibres, wireless communication channels. DDTS are represented as an electromagnetic signal, such as electrical voltage, radio waves, microwave or infrared signal (Smith, 2003). DDTS can be effectively applied in the office risk

management with the aid of the Local Area Network LANs. LANs usually connects the equipment in the offices. LANs need to be interconnected using telephone lines (providing by the common carriers), cable and satellite communications (Sergio and Ezio, 2008). The major aim of applying DDTS in office risk management is to exchange information effectively between offices or organizations. The information exchange is data, voice and video (Simon, 2013). DDTS designated points or devices are the internet, e-mails, faxes, phone text,, voice mails, satellite, telephone, mobile phones, etc (Proakis, 2000).

Apart from the aforementioned, another way the office risk management can be executed is by applying digital security system (DSS). Lebo (2000) defined digital security systems as the technologies or devices for the protection of an organization or its information assets from intrusion by outsider-users electronically. In this light, Olofson (2009) categorized the DSS applied in office risk management into two, namely computer security and digital security for organization. While the former is all about electronic encryption of the vital information assets of an organization against the intrusion of outsider users, the latter anchors on applying electronic security in protecting an organization, its assets and people from unlawful and disastrous intrusion. Beginning with computer security Illingworth (2007) stressed that, for office risk management to be holistic, organizations should protect their information assets electronically. This can be guaranteed through escrow (meaning data decryption keys hold in trust by a third party to be turned over to the user only upon fulfillment of specific authentication conditions); file-level encryption (meaning a technique where individual files or directories are encrypted by the computer file system itself; encryption is the process of converting data into a cipher or data in order to prevent unauthorized access); intrusion Detection System (IDS) (meaning a device that monitors and analyzes network traffic and can be used to capture data being transmitted on a network). On the other hand, security for organization, its assets and people can be achieved by applying DDS devices such as fire alarm system, closed-circuit television (CCTU), surveillance cameras, wireless cameras, and intruder alarms. These are applied to mitigate or eliminate the possibility of theft, robbery and fire related risks in and around an organization (Illingworth, 2007; Olofson, 2009; Bird, 2002).

2. The Problem

Failure to effectively manage risks has, no doubt, either exposed many organizations in developing world (in Nigeria and Rivers State in particular) to a potential danger of nearly collapse or eminent winding-up. The collapse of some of these organizations has indeed compounded the problem of rising unemployment in our society as many have been laid off as the result. Again, the services so rendered by the collapsed organizations have become unavailable and even expensive to be purchased abroad. These organizations which unfortunately collapsed might have not wished to do so, except that they care not to advertise their minds to their lack of or neglect for risk management, especially through a new reliable approach provided by information technology systems (Olufemi, 2008). It is in light of the foregoing that this study sought to investigate the application of information technology systems in office risk management in organizations in Rivers State.

In a specific term, this study sought to accomplish the following objectives, which are to:

1. examine the electronic data processing systems that are applied in office risk management in insurance companies in Rivers State
2. determine the electronic data storage systems that are applied in office risk management in insurance companies in Rivers State
3. ascertain the digital data transmission systems that are applied in office risk management
4. find out the digital security system that are applied in office risk management in insurance companies in Rivers State

2.1 Research Questions

To achieve these objectives, the study addressed the following questions:

1. What electronic data processing systems are applied in office risk management in insurance companies in Rivers State?
2. What electronic data storage systems are applied in office risk management in insurance companies in Rivers State?
3. What digital data transmission systems are applied in office risk management in insurance companies in Rivers State?
4. What digital security systems are applied in office risk management in insurance company in Rivers State?

3. Methodology

This study was a descriptive survey design. The population of the study comprised 10 insurance companies in Port Harcourt City Local Government Area of Rivers State made up of 350 members of staff. These insurance

companies are UNIC, Zenith, Royal Exchange, NEM, Leadway, Guaranty Trust, Equity Life, Cornerstone, Consolidated Hallmark and NAICOM. The sample consists of 161 members of staff selected from the 10 insurance companies in Port Harcourt City L.G.A of Rivers State.

The sample was selected through simple random sampling and constituted 46% of the total population of 350.

A self-structured questionnaire titled: Office Risk Management Assessment Questionnaire (ORMAQ) was the only instrument used in this study for data collection. The reliability test of the instrument yielded a reliability index of 0.85. Out of the 161 self-administered copies of questionnaire, 150 of them were properly filled, retrieved and used for the study. Mean ($\overline{X}$) was used as a method for analyzing the four research questions. The criterion mean for measuring each item of questionnaire is 2.50.Hence, any calculated mean value above 2.50 indicates the acceptance of item while any below 2.50 shows the rejection of the item measured.

4. Results

Research Question 1

What electronic data processing systems are applied in office risk management in insurance companies in Rivers State?

Table 1: Responses on Electronic Data Processing Systems applied in Office Risk management

S/No	Items	Mean ($\overline{X}$)	Remark
1.	Computers to process data or facts gathered	2.97	Accept
2.	Digital Security doors to process data or information of people before gaining entrance	2.99	Accept
3.	Scanners to process information needed to be scanned	3.02	Accept
4.	Printers to process data or information needed to be printed	3.39	Accept
5.	Digital forensic machines to process finger print related information	1.54	Reject
6.	Card-readers to process information or data related card transactions	3.35	Accept
7.	Digital cameras to process monitoring related information	2.89	Accept

Table 1 reveals that the items whose calculated mean values fell above the criterion mean of 2.50 were accepted by the respondents as those electronic data processing systems they apply in office risk management. However, the item whose mean value fell below 2.50 indicates rejection. Thus, this result indicates that computers, digital security doors, scanners, printers, card readers and digital cameras are the electronic data processing systems that the insurance companies in Rivers State applied in their office risk management.

Research Question 2

What electronic data storage systems are applied in office risk management in insurance companies in Rivers State?

Table 2: Responses on Electronic Data Processing Systems applied in Office Risk management

S/No	Items	Mean ($\overline{X}$)	Remark
1.	Magnetic tapes to store data	2.87	Accept
2.	Compact disks to store data	2.20	Reject
3.	USB Flash drives to store data	3.36	Accept
4.	Dissociate Vertical Disks (DVDs) to store data	3.54	Accept
5.	Optical disks to store data	3.21	Accept
6.	Memory cards to store data	3.24	Accept
7.	Hard disks to store data	2.21	Reject
8.	Flash drives to store data	3.13	Accept

Table 2 shows that the items whose weighted mean values fell above the criterion mean of 2.50 were accepted by the respondents as the electronic data storage systems they apply in office risk management in insurance companies in Rivers State. The items that had their calculated mean values below 2.50 were rejected. The result therefore, shows that the following are the electronic data storage systems applied in office risk management in insurance companies in Rivers State.: magnetic tapes, USB flash drives, Dissociated Vertical Disks (DVDs), optical disks, memory cards and flash drives.

Research Question 3

What digital data transmission systems are applied in office risk management in Insurance Companies in Rivers State?

Table 3: Responses on Digital Data Transmission Systems applied in Office Risk management

S/No	Items	Mean ($\overline{X}$)	Remark
1.	The Internet/intranet to transmit information	3.27	Accept
2.	E-mails to transmit information	3.46	Accept
3.	Phone texts to transmit information	3.24	Accept
4.	Satellite aided network to transmit information	3.50	Accept
5.	Voice-mails to transmit information	1.70	Reject
6.	Mobile phones/telephones to transmit information	3.28	Accept

Table 3 reveals that the items whose calculated mean values fell above the criterion mean of 2.50 were accepted by the respondents as the digital data transmission systems they apply in office risk management in insurance companies in Rivers State. The item that had its calculated mean value below 2.50 was rejected. Therefore, the result indicates that the internet/intranet, e-mails, phone texts, satellite-aided network and mobile/telephones are the digital data transmission systems applied in office risk management in insurance companies in Rivers State.

Research Question 4

What digital security systems are applied in office risk management in insurance companies in Rivers State?

Table 4: Responses on Digital Data Transmission Systems applied in Office Risk management

S/No	Items	Mean ($\overline{X}$)	Remark
1.	Surveillance cameras to generate security-related information	3.13	Accept
2.	Intruder alarm system to generate alert-related information	2.22	Reject
3.	Closed-Circuit Television (CCTV) to generate monitoring related information	1.31	Reject
4.	Wireless cameras to generate security-related information	3.18	Accept
5.	Fire alarm system to generate alarms	3.56	Accept
6.	File-level-encryption system to encrypt confidential information	3.20	Accept
7.	Intrusion detection system to detect the intrusion of the outsider users into the information assets	1.90	Reject

Table 4 shows that the items that had their weighted mean values above the criterion mean of 2.50 were accepted by the respondents as the digital security systems they apply in office risk management in insurance companies in Rivers State. Hence, this result indicates that the following are the digital security systems applied in office risk management in insurance companies in Rivers State: surveillance cameras, wireless cameras, fire alarm system and file-level-encryption system.

5. Discussions

Judging from result realized from Table 1, there exits a deduction that the insurance companies in Rivers State apply electronic data processing systems for managing risks. Apart from not using closed-circuit television (CCTV) to generate monitoring-related information, the respondents overwhelmingly agreed that they apply some vital electronic data processing systems in managing office-related risks in their companies. Weighted mean values of 2.97, 2.99, 3.02, 3.39, 3.35, and 2.89 which indicate the application of computers, digital security doors, scanners, printers, card readers and digital cameras respectively, in office risk management is a glaring fact that the insurance companies in Rivers State are catching up with the contemporary approaches for managing risks. The reason for relying on the foregoing deduction is that all the weighted mean values fell above the criterion mean of 2.50 which represents a cut-off mark for acceptance of an item. The implication of this result is that office risk management in insurance companies in Rivers State has assumed a high proportion in processing of data electronically for reducing avoidable risks in doing business. This result contradicts with the postulation by Olufemi (2008) that electronic based risk management is still low in most organizations in the developing world.

Similarly, going by the result generating from Table 2, there is a deduction that the insurance companies in Rivers State apply electronic data storage systems for office risk management. Except compact disks and hard disks which the respondents never apply, all other electronic data storage systems such as magnetic tapes, USB flash drives, Dissociated Vertical Disks (DVDs), optical disks, memory cards and flash drives are applied by them for office risk management. The calculated mean values of 2.87, 3.36, 3.54, 3.1, 3.24 and 3.21 respectively for the above items indicate that the insurance companies in the state have really embraced the use of electronic data storage system for managing their office risks. The reason for such deduction being that all the above

calculated mean values fell above the criterion mean of 2.50 which serves as a cut of mark for accepting any item measured. The implication of the result is that the insurance companies in Rivers State are high in their drive to eliminate or mitigate office associated risks through the use of a new approach, electronic data storage systems. This result yet goes contrary to the submission of Olufemi (2008) as highlighted above.

From the result realized from Table 3, it can be deducted that the insurance companies in Rivers State apply digital data transmission systems in managing office risks. With the exception of voice-mails which they never use, the respondents agreed totally that they apply digital data transmission systems such as the internet/intranet, e-mails, phone texts, satellite-aided network, mobile/telephones to transmit information for managing office risks. The weighted mean values of 3.7, 3.46, 3.24, 3.50 and 3.28 respectively for the above items reveal that the insurance companies in Rivers State have made the application of digital data transmission systems for office risk management a tall priority. The reason for this deduction is anchored on the fact that all the above weighted mean values fell above the criterion mean of 2.50. The implication is that office risk management is a task insurance companies in Rivers State do using a contemporary approach, digital data transmission systems. This result equally opposes the view of Sergio and Ezio (2008) that the level of application of information technology systems in managing risks in an organization is still very low in developing countries.
With a critical glace at Table 4, it can be deduced that the insurance companies in Rivers State apply some of but not all the digital security systems for managing risks.

The respondents agreed that they use surveillance cameras, wireless cameras, fire alarm system and file-level-encryption system, but, on the other hand, declined using intruder alarm system, Closed-Circuit Television (CCTV) and intrusion detection system in office risk management. This shows that these insurance companies have not completely adopted all the technologies required for managing office risks. This deduction is affirmed by the result realized from Table 4.On the Table it is shown that the weighted mean values for the digital security systems (surveillance, cameras, wireless, fire alarm system and file-level-encryption system) which the respondents admitted they use for managing office risks are 3.27, 3.13, 3.18, 3.56 and 3.20 respectively. However, they do not use intruder alarm system, CCTV and intrusion detection system. This is because the weighted mean values of these items fell below the criterion mean of 2.50, a cut of mark for accepting an item. The implication of this result is that the insurance companies in Rivers State will find it difficult to completely manage risks such as theft, robbery, stealing of confidential information assets from the computer, among others. Thus, the use of digital security systems in managing office risks in insurance companies in Rivers is not complete and adequate. The above submission of Sergio and Ezio (2008) is in conformity with the result.

In conclusion, it can be said that the insurance companies in Rivers States apply the majority of the electronic data processing, storage and transmission systems in managing their office risks, but they have not gone completely digital in terms of managing the same risks using digital security systems.

6. Recommendations

Based on the results of this study, the following recommendations were made:

1. Insurance companies in Rivers State should completely embrace digital technologies for effective management of office risks.
2. They should integrate digital risk management into their operational policies and review these policies annually.
3. They should acquire more infrastructures which encourage the use of information technology systems (ITs) in managing office risks.
4. They should prioritize ITs-based office risk management through robust budgetary allocation and implementation.
5. Government should create enabling environment through the provision of infrastructural facilities and legislative backings for effective office risk management.

References

Bird, C. (2002). Digital Era: Security Systems Perspective. Indiana: Boulvand Press.
Chandler, D. & Munday, R. (2012). Information technology. A Dictionary of Media and Communication (first ed.) Oxford: Oxford University Press.
Clark, A.P. (2003). Transmission Principles of Digital Data Transmission.
Crockford, N. (2006). An Introduction to Risk Management (3rd ed.) Cambridge, UK: Woodhead-Faulker.
Daintith, J. (2009). 'IT', A Dictionary of Physics, Oxford University Press.
Dorfman, M.S. 92007). Introduction of Risk Management and Insurance (9th ed.) Englewood Cliffs, New Jersey: Prentice Hall.

Goda, K.K.M. (2012). The History of Storage Systems Proceedings of the IEEE 100: 1433 -1440.
Hannson, S.K. (2012). ICT and Risk Management. New Jersey: Image Publishers.
Hilbert, M. & Lopez, P. (2011). The World's Technological Capacity to Store, Communicate and Compute Information. Science 332 (6025): 60 -65.
Hubbard, D. (2009). The Failure of Risk Management: Why It's Broken and How to Fix it. John Wiley& Sons, p.46.
Illingworth, Valerie (2007). Optimizing and Assessing Information Technology: Improving Business Project Execution. N.J: John Wiley & Sons.
ISO/IEC Guide (2009). Risk Management Vocabulary. International Organization for Standardization.
Leavitt, H.J. & Whisler, T.L. (1958). Management in the 1980s. Harvard Business Review.
Lebo, H. (2000). The UCLA Internet Report: Surveying the Digital Future. World Internet Project, 1.5.
Martin, R. (2013). Information Technology: A risk management Approach. Ohio: George Allen and Irwin.
Mike, C. (2004). IS the Silent PC Future 2.5 inches wide.
Olofson, C. W. (2009). A Platform for Enterprise Data Services.
Olufemi, S. (2008). The Problem with Risk Management in developing world: An IT Perspective. London: IM Press Limited.
Proakis, J. (2000).Digital Communications, McGraw-Hill.
Proctor, K. (2011). Optimizing and Assessing Information technology: Improving Business Project Execution. N.J: John Wiley & Sons.
Sergio, B. & Ezio (2005). Principles of Digital Transmission: With Wireless Applications, Springer.
Simon, H. (2010). Digital Communication. John Wiley & Sons.
Smith, D.R. (2003). Digital Transmission Systems. Kluwer International Publishers.
Vijayan, F. (2005). Introduction to Information Technology. New York: Weldenfield and Nicholson Inc