Disaster and Risk Management in an Electronic Environment: A Study of the Planning and Management Information Services Directorate of the University of Ghana

HARRY AKUSSAH AND EDEAMA ONWUCHEKWA

Department of Information Studies, University of Ghana, Legon.

Abstract

The study examines the management of disasters and risks in the Planning and Management Information Services Directorate (PMISD) of the University of Ghana. Questionnaire, interviews and observation were used to collect data from twenty-one (21) members of staff of the Directorate. Descriptive statistics was used to analyse the data that was collected. The study revealed a high level of unpreparedness of the PMISD to contain disasters and risks. In addition, the study found out that there was no disaster recovery plan, no systematic orientation and training schemes for staff in the area of risk management, inadequate security for network infrastructure and equipment and for that matter data security and an irregular risk assessment regime. The study made a number of recommendations with a view to strengthening the capacity of PMISD to manage disasters and risks and to be able to resume business promptly, given the electronic environment within which it operates.

Keywords: DISASTER PLANNING; RISK PREVENTION; INFORMATION MANAGEMENT; ELECTRICAL GADGETS.

Introduction

The concept of Disaster and Risk Management is a very broad one and has been tackled by different people from diverse view points. Disasters have been in existence from time immemorial. According to Matthew and Eden (1996), a disaster does not have to be big in order to be termed serious. The loss of a rare or unique 11th century manuscript due to a minor leak can be a disaster of national or international concern.

The word ‘disaster’ has gained currency amongst archivists, librarians and information professionals who describe it as an unexpected event with destructive consequences for their holdings. To some other group of people, the concept does not come to mind unless it actually happens. Such people are forced to acknowledge the realities of disasters only when they strike. According to Bulgawicz and Nolan (1988), disasters come in many flavours. Unfortunately however, we neither select our favourite disasters nor choose the time when they should occur.

Risk management as a formal concept only became prominent during the 1970s. This was largely in response to the stock market crash of 1974, after which risk management became ‘the biggest game in town’ for investment managers and their clients (Bernstein, 1998). A great deal of the existing risk management literature has come from the insurance and stock market industry. The risk management standard developed jointly by Australia and New Zealand was the first major milestone in the worldwide movement towards risk management. This was followed by similar works by organizations in Canada, United States of America, Germany and the United Kingdom (Kloman, 2000). Risk management is still an evolving field, making improvements in its processes over time.

Disasters in an electronic environment may range from a temporary disruption of power to a complete destruction of an office. From the Texas State Library Record (2000), disasters in electronic environments could be defined by four levels of disruption: Limited disruption which refers to a temporary interruption with no damage or loss, serious disruption which involves a repairable damage, major disruption which involves destruction and catastrophic disruption which results in total loss. This assertion is reiterated by Aziagba and Edet (2008) who stated that disasters that affect a library's electronic equipment result in unprecedented and varying levels of disruption in activities.

While there has been an increase in disaster management research in developed countries like Britain and America, not much seems to be happening in Africa, especially in information centres. The few studies that have been conducted in Ghana have concentrated largely on conventional information resources.

According to Kumekpor and Van Landerwijk (1994), only a few countries in the world exposed to the risk of disaster are fully prepared to deal with the situation. This statement is very true of Ghana. Some institutions in Ghana over the years have suffered from disasters. These include the fire outbreak at the Agricultural Development Bank Head Office in 1994 (Akussah and Fosu, 2001), the Ghana Broadcasting Corporation fire outbreak that destroyed the film archives and library (Addrey, 1996), the 1995 Balme Library flood which affected some materials (Adinku, 1999) and the fire outbreak at the Head Office of the Electoral Commission (Azu, 2001).

The major objective of a disaster and risk management programme is to protect assets such as data, hardware, software, personnel and other facilities against all external and internal threats, in order to minimize the losses resulting from such eventualities (Gottifried, 1989). Four major components of risk management have been identified in the literature by Rainer et al, (1991), Eloffr *et al*, (1993), Epich and Peterson (1994), Lightle and Sprohge (1992), Lochr et al (1992) and Vitale (1986). These are: risk identification, risk analysis and assessment, risk- reduction and risk monitoring.

Disasters can happen anywhere and at anytime. Every organisation however small or large needs to prepare for them. The destructive effects of disasters to information resources remain a critical factor in information management. Preparedness for disastrous situations is a key to minimizing the potential risks and damages which can occur.

This article presents the outcome of a study of the Planning and Management Information Services Directorate (PMISD) of the University of Ghana. The core functions of the PMISD are: to design, implement and manage the Management Information System of the University, to provide the machinery for planning, and also to serve as the main source of good operational information for the University.

The main focus of this article is to examine and evaluate the potential and actual disasters and risks PMISD has been exposed to over the years and to find out how prepared the unit is to manage such disasters and risks.

Methodology

Subjects for the study were the staff of the Planning and Management Information Services Directorate of the University of Ghana. The study made use of a hybrid of quantitative and qualitative data collection methods using questionnaire, interview and observation. As the numerical strength of the staff of the Directorate was 21 and was deemed to be relatively small, it did not require sampling. The total population was used.

A questionnaire was administered to 18 members of staff of the Directorate made up of senior staff, database administrators, application support staff, system developers, technicians, and administrative staff. A structured interview guide was used as a supplement to the questionnaire to elicit managerial information from the head, the assistant head and the systems/network administrator of the Directorate. The researcher also observed the infrastructure and the general environmental conditions of the Directorate in order to identify and assess the potential hazards and risks and also to ascertain the preparedness measures that have been put in place. Data for the study was collected between June and August, 2009.

Findings

The central objective of the study was to find out the disaster and risk management status of the Planning and Management Information Services Directorate of the University of Ghana. The findings as presented are derived from the analysis of data collected.

Disasters Experienced

Considering the fact that disasters are invincible parts of a society and all organizations, the study sought to find out the various types of disasters that the Directorate had experienced or encountered over the years. Various disasters were indicated. In the area of flood and rainstorm, 17 (94.4%) of the respondents said the office had never experienced flood before whilst only one person (5.6%) answered in the affirmative. Currently in Ghana, fire has been the scourge of information centers and this basically may be due to the highly inflammable materials in the storage environment or the improperly fitted electrical wires or electrical appliances. When asked, 15 (83.3%) respondents said they had never experienced fire or electrical sparks in the Directorate whilst 3 (16.7%) respondents answered in the affirmative. The discrepancy may be explained by the length of time the workers have spent in the Directorate.

With regard to equipment and systems failure, and loss of vital information as potential risks, 12 (66.7 %) of the respondents said they have had such experiences whilst 6 (33.3%) of the respondents said they had never experienced equipment or systems failure. Another 8 (44.4%) of the respondents said they had encountered loss of vital information whilst 10 (55.6%) said they had never experienced such a loss. In the area of theft, majority of the respondents - 14 (77.8%) said no, whilst 4 (22.2%) respondents affirmed that the Directorate had encountered theft as a form of disaster. (See table 1)

Table 1: Disasters Experienced

Type of Disaster	Yes		No		Total	
	F	%	F	%	F	%
Flooding/Rainstorm	1	5.6	17	94.4	18	100
Fire Outbreak	3	16.7	15	83.3	18	100
Equipment Failure	12	66.7	6	33.3	18	100
Loss of Information	8	44.4	10	55.6	18	100
Theft	4	22.2	14	77.8	18	100

Source: Field Survey, 2009

Disaster and Risk Assessment

Disaster or risk assessment is a very crucial prerequisite for effective planning and management of disasters and risks in electronic environments. Consequently, respondents were asked to comment on the frequency with which disaster and risk assessments were conducted in the Directorate. Nine (50%) of the respondents indicated that disaster and risk assessment was conducted in the Directorate whenever there was a problem, whilst 7 (38.9%) said it was conducted occasionally. A small number - 2 (11.1%) of the respondents intimated that disaster and risk assessment had never been conducted in the Planning and Management Information Services Directorate. One may be tempted to conclude that disaster and risk management only received attention when there was a problem in the Directorate. This does not augur well for a Unit as sensitive as PMISD. Periodic situational assessment is very crucial, particularly in the light of the dynamism and challenges in electronic environments.

Disaster and Risk Prevention

The study examined the resources, facilities and measures put in place by the Directorate in relation to disaster and risk management. Respondents were asked if there was regular servicing of the electronic equipment and systems in the Directorate. Majority - 13 (72.2%) of the staff said that there was regular servicing of the equipment whilst 5 (27.8) of the staff said otherwise. This is represented in table 2. When further asked if there were disaster detection and suppression systems in the Directorate, 16 (88.9%) of the respondents said yes whilst 2 (11.1%) of the respondents answered in the negative. Observation by the researchers however revealed the presence of a number of functional risk and disaster detection and suppression equipment such as smoke detectors, fire extinguishers, voltage regulators and fire blankets. This goes to reinforce the position of the majority of respondents.

Ensuring security and safety of electronic systems in the Directorate against disasters like techno-theft demands the installation of strong burglary proof facilities. When the questions relating to security and safety were posed, majority of the respondents - 15 (83.3 %) confirmed that the Directorate had strong burglary proof protection whilst 3 (16.7%) of the respondents indicated that security was fluid (See table 2).

Table 2: Risk and Disaster Prevention Devices

Type of Device	**Yes**		**No**		**Total**	
	F	**%**	**F**	**%**	**F**	**%**
Regular Servicing	13	72.2	5	27.8	18	100
Detection Systems	16	88.9	2	11.1	18	100
Burglary Proofs	15	83.3	3	16.7	18	100

Source: Field Survey, 2009

A physical survey of the Directorate by the researchers however revealed that apart from the doors to the Directorate and the glass windows which were well secured with burglary fittings, the individual equipment did not have any security fittings to safeguard them against theft. It was also noticed that the interior partitioning of the Directorate was made of wood which renders the offices vulnerable should anybody gain access to the building. In an interview with the Director, it was intimated that plans were far advanced towards acquiring a more secured office accommodation for the Directorate.

Risk of Disaster

Hazards are seen as phenomena that pose threats to people and structures among others which may cause disasters. These hazards could be man-induced or naturally occurring in our environments. Respondents were asked questions in relation to the presence of some hazards in the work environment. Sixteen (88.9%) respondents indicated that they had not noticed any signs of leakages or cracked walls in the Directorate whilst 2 (11.1 %) of the respondents answered in the affirmative. The study also sought to find out whether there were faulty or improperly fitted electrical wire connections in the Directorate. All the respondents responded in the negative. A close observation of the office facilities revealed that all the electrical wirings were well protected in conduits with uninterrupted power supply (UPS) and voltage guard systems. This is an apparent situation of good maintenance which needs to be encouraged.

Electrical Gadgets

The intention here was to have an indication of the type of electrical gadgets used in the Directorate. In disaster and risk management, awareness of the type of gadgets or equipment used enables one to plan more effectively. Electrical gadgets in several information centers differ based on the objective or purpose of each department. When asked about the type of electrical gadgets in used in the various offices of the Directorate, all the respondents indicated that they made use of computers in their offices and departments. In addition, 14 (77.8 %) respondents indicated that fridges were being used in their offices whilst 8 (55.6 %) of the respondents said they used water heaters. Concerning the use of photocopying machines, 16 (88.9%) affirmed they had and used copying equipment. Other types of electrical equipment indicated were air conditioners, printers and inverters.

The range of electrical equipment used in PMISD were varied enough to prompt the Directorate to appreciate and put in place disaster preparedness measures. This is particularly so because most of the recent information disasters in Ghana were fire outbreaks triggered off by faulty electrical equipment. The use of these equipment pose a high risk of disaster in PMISD.

Awareness and Training

According to Lyall (1996), one of the major reasons for the failure of a disaster plan is the “lack of staff awareness”. Drennan (2001) writes that it is not enough that a policy has been written down and approved for it to be successful. Staff must be familiar with the policy and committed to its implementation. For this reason the research sought to determine the level of awareness of the staff of the Directorate in relation to disaster control or recovery plans. The results revealed that 11 (66.7 %) of the respondents were aware of a disaster control and recovery plan in the Directorate while 6(33.3%) workers did not seem to be aware. Further probing by the researchers revealed that what the respondents were referring to as a disaster plan was indeed a set of guidelines for disaster prevention.

Concerning orientation of staff on disaster and risk management, 7 (38.9%) of the staff responded that they have had orientation on disaster and risk management in the PMISD, whilst 11 (61.1 %) of the staff said they had never had any orientation. (See table: 4). Further investigations revealed that it was only the professional staff that might have had the exposure leaving out the supporting staff. This is a very unfortunate and an unacceptable situation since history has shown that often, it is the supporting staff that are at post when most disasters strike.

Disaster Preparedness and Recovery

Disaster preparedness involves planning in preparedness to deal with disasters should they occur since not all disasters can be prevented. Data protection is a term that information technology professionals use to refer to strategies that to a large extent insures an organization against natural or man-made calamities that threaten the viability of its information systems infrastructure. Back-up systems have often been the most useful approach used by most organizations. The study sought to find out the preparedness measure in place to ensure prompt business resumption should there be a disaster. The response was rather unanimous. All the respondents were of the opinion that there was an effective backup system for documents in the Directorate.

Over the years back-up methods have often become routine for information centers, a real time back-up system enables information to be instantly stored in a system while off time back up is done periodically either at the end of the day or on weekly basis. The majority of respondents 11(61.1%) said that off time backup system was used. 3 (16.7 %) of the respondents said that the type used was the real time while 2 (11.1%) indicated that both the real time and the off time backup methods were undertaken in the Directorate. The remaining 2 (11.1%) of the respondents gave no response to the question. (See table: 5). Further interview with management revealed that a mix mode of backing up was in use. Some categories of data were backed up online whilst others were batched and backed up periodically. No reasons were given for this. It could well be that the Directorate is trying to maximize protection or spread the risk by adopting the multiple approach.

Table 5: Methods of backup in the PMISD

Method of Backup	Frequency	Percentage
Real Time	3	16.7
Off time	11	61.1
Both	2	11.1
No response	2	11.1
Total	**18**	**100.0**

Source: Field Survey, 2009

One of the methods which effectively protects backups from disaster is dispersal. According to Alegbeleye (1993), the term dispersal refers to the storage of records in a different location away from where the originals are kept. A dispersal policy can adapt two approaches to protect backups in electronic environments. It can either use an onsite storage facility or an offsite or remote storage facility. When the onsite storage option is employed, there are backup servers strategically located at different spots within the premises of the organization, often at a distance from the original documents. The offsite or remote storage facility allows backups to be stored at some distance or remotely from where the organization normally operates. Most times, the data is encrypted for security reasons.

Information gathered from the management of PMISD indicates that the onsite storage facility is the practice in the Directorate. This may not be the best for the Unit given the volatile nature of the University of Ghana. The University is exposed to potential hazards such as earthquakes, mob action, thunder and lightning, unauthorized access among others.

Conclusion

A disaster halts critical business functions within an organization and data loss can be devastating. Every organization needs to face the reality of disasters, whether as a result of the forces of nature, careless or malicious acts of employees, or simple hardware failure. The study has shown that the Planning and Management Information Services Directorate of the University of Ghana has not put in place any integrated disaster or risk preparedness programme which will enable it resume business very quickly and to continue to play its critical role to the University should there be a disaster. This is evident in the irregular risk assessment, inadequate system security, inadequate awareness and training for supporting staff and the absence of a disaster plan as revealed from the findings. The PMISD is such a key Unit within the University that it cannot afford to leave its setup unprotected and unprepared for risks and disasters.

Recommendations

Based on the results of the study, the following recommendations are made with the hope that if implemented, potentially disastrous situations would be reduced to mere inconveniences.

Development of a Disaster Plan

A disaster recovery plan is the key ingredient for quick business recovery in times of disaster. It is recommended that a much more proactive step be taken by the PMISD to have a disaster control and recovery plan put in place to enable it recover quickly from any disaster. It is also recommended that such a plan if put in place should be widely circulated amongst the staff to ensure effective utilization. The plan must be a living document which should be updated from time to time to enhance its workability. Such a plan must be periodically tested to ensure its continuous relevance.

Developing a disaster plan needs some hard work such as planning, brainstorming, and cooperation from both corporate management and employees. Support for the plan must be maintained at the management level of the University. In addition, the senior staff of the Directorate should make more conscious efforts to implement and communicate disaster and risk management activities to the other staff in the Directorate.

Data Safety

Data safety is perhaps one of the most crucial and yet overlooked aspects of disaster recovery in an electronic environment. It is advisable to store backups offsite far from the Directorate. It is recommended that the staff of the Directorate should always ensure that the security controls and security management practices of the Directorate are regularly reviewed with a view to identifying aspects of the system's infrastructure where security protection is 'thin'. Identifying possible vulnerabilities and monitoring them would prevent a problem before it occurs.

It is recommended that periodic disaster and risk assessment be made a formal part of the management procedures of the Directorate. The management of the University should strengthen the physical facilities of the Directorate, by making adequate provision for disaster detection and suppression.

Maintenance and Protection of Equipment

A regular and rigid maintenance regime is an essential part of a disaster and risk management exercise. There is the need to have the computers cleaned and freed of dust and dirt which act like a blanket, shielding the chips from the cooling breezes pulled into the computer by its fans thereby resulting in overheating and causing the premature demise of the computer hardware. In addition, all other equipment, particularly electrical equipment must be regularly serviced and maintained.

It is further recommended that thunder and lightning conductors should be installed and network cables better secured in the University of Ghana in general and especially around the PMISD. This will go a long way to reduce the frequency with which network nodes and servers are affected by lightning during rain storms.

Co-operative Efforts

Cooperation in the area of disaster and risk management activities is necessary. It is recommended that the Directorate cooperates with organizations such as the National Disaster Management Organization (NADMO) which has as some of its functions, preparing national disaster plans, monitoring, evaluating and updating disaster plans and coordinating local and international support for disaster or emergency control relief services and reconstruction. This will go a long way to strengthen the response capabilities of PMISD.

Staff Training and Awareness

Staff training and awareness programmes should be embarked upon. A disaster control and recovery plan when put in place should be distributed to departmental heads, team members and all other persons who need to have it. Staff must be made aware of the existence of the plan. The plan which should be written in simple and concise language should be one of the first documents handed over to new employees of the directorate. In addition, comprehensive and regular orientation programmes must be held for staff in between times.

References

Addrey, H.B.A. (1996) **Information disaster preparedness planning and control: A case study of Ghana Broadcasting Cooperation:** An unpublished M.A. dissertation, presented to the_Department of Information Studies, University of Ghana Legon, pp 83-85.

Adinku, S.A. (1999) **Disaster Management in the Balme Library, University of Ghana,** Legon. An unpublished M.A dissertation, presented to the Department of Information Studies, University of Ghana Legon, pp 2-10.

Akussah, H. and Fosu, V. (2001) "Disaster Management in Academic Libraries in Ghana". **African Journal of library, Archives and Information services**, Vol. 11, no. 1, pp 1-16.

Alegbeleye, B. (1993) **Disaster Control Planning for Libraries, Archives and Electronic Data Processing Centres in Africa.** Ibadan: Optic Books and Information Sciences, pp5-10, 61-75.

Anyigire, A. B., (2000) **Information disaster preparedness and planning at the head office of the Electoral Commission.** An unpublished M.A. dissertation, presented to the Department of_Information Studies, University of Ghana, Legon, pp74-77.

Aziagba, P. and Edet, G. (2008) "Disaster-control planning for academic libraries in West Africa" **The Journal of Academic Librarianship,** Vol.34, Issue 3 pp 265-268.

Bernstein, P. L. (1998) **Against the gods: the remarkable story of risk**. New York: John Wiley and Sons Inc. Pp. 301.

Bulgawicz, S. and Charles, E. (1988) **Disaster Prevention and Recovery: A planned approach**. Arma International, Prairie Village, pp38-40.

Drennan, L. T (2001) **Risk Management :A holistic approach** ,Lyme ,Connecticut: Seawrack Press. pp 1-7 www.riskmanagement.com.au/ARTICLES/accessed 30th November 2001.

Eloff, J. H. P., (1993) "A comparative framework for risk analysis methods" **Computers and Security**, Vol. 12, No. 6, pp 597-603.

Epich, R. and Persson, J. (1994) "A fire drill for business", Information Strategy", **The Executive Journal**, pp. 44-47.

Gottfried, I. S (1989). "When disaster strikes." **Journal of Information Systems Management**, Vol. 6, No 2, pp 86-89.

Kloman, H. F. (2000) **An iconoclastic view of Risk.** Lyme, Connecticut: Seawrack press; available at [www.riskmanagement.com.au/ARTICLES/>] (accessed 5th December 2000).

Kumekpor, K. B. and Van Landerwijk, J.E.J.M., (1994) **A review of Hazard and Disaster Minimization in Ghana, Legon**, University of Ghana, pp 3, 33.

Lightle, S. and Sprohge, H. (1992) "Strategic information system risk", **Internal Auditing**, pp. 31-36.

Loch, K.D., Carr H.H. and Warkentin, M.E. (1992) "Threats to information systems: today's reality, yesterday's understanding", **MIS Quarterly**, Vol. 16 No. 2, pp. 173-186.

Lyall, J. (1996) "Disaster planning for libraries and archives: understanding essential issues", *Provenance*, Vol. 1 No 2, available: [www.netpac.com/provenance/vol1/no2/features/lyall1.htm]. (accessed 12 November 2001).

Matthews, G., and Eden, P. (1996) **Disaster Management in British libraries, Project Report with guidelines for library managements, library and information research report** *London.* The British Library. p 109.

Matthews, G. and Feathers J. (2003) **Disaster Management for libraries and archives**,Aldershot: Ashgate Publishing House, pp 44-46.

Rainer, F. J. (1991) "Risk analysis for information Technology". **Journal of Management Information Systems,** Vol. 8, No. 1, pp 129-47.

Vitale, M.R. (1986) "The growing risks of Information Systems Success," **MIS Quarterly**, Vol. 10 No. 4, pp. 327-334.