A Critical Assessment of Information Technology Disaster Recovery Strategies in Ghanaian Banks

Paul Danquah, Steve Aryeetey and
Charles Buabeng-Andoh

Abstract

Banks were among the earliest adopters of information technology in the business world. In any business organisation, customer data and other corporate information form a critical and valuable asset of the organisation. Disaster recovery planning protects data against loss. The focus of the research was to investigate the disaster recovery strategies and plans being used by the banking industry in Ghana and the preparedness of the banks' staff for recovery from information technology disaster. Using a combination of quantitative and qualitative research approaches with the simple random sampling technique, the results showed that banks in Ghana are basically ill-prepared for Information technology (IT) disasters, a premise on which a number of recommendations are made to improve the situation. It needs to be emphasized that the results may not be suitable for generalization since only seven out of thirty banks were researched.

Introduction

The banking sector is the backbone of the Ghanaian economy and plays an important financial intermediary role, therefore, its health is very critical to the health of the general economy at large. At the time of the research, the banking sector in Ghana comprises thirty (30) banks and 122 rural banks. Currently, all banks in Ghana are operating as universal banks with almost limitless range of products. The banking sector has seen the arrival of many banks from the sub-region as it is the policy of the Central Bank to encourage international banks with repute to operate in Ghana. The policy is geared toward supporting the development of a well capitalized and robust financial system (PriceWaterhouse Coopers, 2008). The traditional core business of banks in Ghana has been retail and corporate banking.

The Bank of Ghana (BoG) has introduced the Ghana Interbank Payment and Settlement

System enabling common electronic platforms for the payment across financial institutions (Bank of Ghana, 2008). One such platform is the National Switch and Smartcard Payment System dubbed 'Ezwich' and Cheque Codeline Clearing with Cheque Truncation System to replace the existing manual (paper-based) clearing system.

The banks in Ghana are offering a varied range of products and services for customers. These include prestige account, cash passport, executive loan, child account, telephone banking, electronic cards, internet banking, Automated Teller Machines (ATMs) and transaction alert which hitherto were offered by a few banks but is gradually becoming a basic service across the banks. Many products and services are now matter of competitive necessity rather than a competitive advantage (William et al., 2005).

In Ghana, there have been attempts to ensure efficiency and competitiveness in the banking industry. Among these initiatives were the movement to universal banking, the adoption of an open licensing system, and the modernization of the payments system, including establishing a central securities depository and the passage of supportive laws. Universal banking, which involves the removal of restrictions on banking activity, was introduced to allow banks to choose the type of banking services they would like to offer in line with their capital, risk appetite, and business orientation. The purpose of this was to remove the monopoly that was given to commercial banks in the area of retail banking, and create room for diversification of the range of financial services that a bank can provide. In addition, it allowed merchant banks for example to compete for retail deposits. According to the central bank, this process should lead to branch network expansion, increasing banking penetration, and also competition for deposits at the retail level. Indeed, the movement into universal banking also came with a higher capital requirement to ensure that banks are sufficiently capitalized to take on additional risk (Acquah, 2006).

Objectives of the research

The general objective of the research as presented in this article was to investigate the strategies and plans available in the banking industry to recover from Information Technology (IT) disaster and the preparedness of its staff in recovering from IT disaster. To achieve the objectives, the research addressed the following specific issues:

- Evaluate the banks' disaster recovery strategies and plans to determine if there were loopholes to be fixed to provide the needed recovery from any disaster.
- Assess the banks' preparedness to recovery from IT disaster
- Investigate the adequacy of backup systems and plans necessary to restore provisions to ensure the availability of information required to resume processing.

The above listed objectives culminated into the following research questions:

i. What disaster recovery systems and plans are being used by the banking industry?

ii. Are the Disaster Recovery Plans (DRP) being rehearsed, tested, and updated regularly to ensure that they are up to date and effective?

iii. Will the disaster recovery strategies and plans work should a disaster strike?

iv. Are all management and staff aware of the disaster recovery strategies and plan and what is required of them in the event of a disaster?

v. Are the IT staff, functional staff, executive team, and the board of directors on the same wavelength as far as disaster recovery is concerned?

RELEVANT TERMINOLOGIES

Disaster recovery planning protects data against loss. If an organization fails to exercise this due care, it could face civil or criminal lawsuits if a preventable disaster destroys important information (Gregory, 2008). The objectives of the DRP includes protecting an organization from major computer services failure, minimizing the risk to the organization from delays in providing services, guaranteeing the reliability of standby systems through testing and simulation, and minimizing the decision making required by personnel during a disaster (Krutz and Vines, 2007).

Disaster Recovery Planning(DRP): Disaster Recovery (DR) is the process an organization uses to recover access to its software, data, network and hardware that are needed to resume the performance of normal, critical business functions after the event of either a natural disaster or a disaster caused by humans (Krutz, 2007).

Information Technology (IT): Information technology is defined as the use of computer technology such as software and hardware to process and store information. Communication technology is used for transmitting information (**Alavudeen and Venkateshwaran, 2010).**

Service Loss and Data Loss: According to report by Toigo (2002), more than 10 days of computer outage cannot be recovered by most companies. Fifty percent of them go out of business within 5 years if they had outages for that long.

According to EMC consulting, a Business Continuity Services organisation, only 2% of data loss is caused by disasters. The major cause (45% of cases) is human errors. The rest of the errors are caused by other failures, e.g., software errors.

Disasters primarily affect availability, which affects the ability of the staff to access the data and access working systems, but a disaster can also affect the other two tenets: confidentiality and integrity (Krutz, 2007). Sayana (2005) added that the confidentiality, integrity and availability of information systems must be ensured to protect the business from the risks relating to information technology

Disasters and Other Disruptive Events: These events may require action to recover operational status in order to resume service. Such actions may necessitate restoration of hardware, software or data files. Therefore, a well-defined, risk-based classification system needs to be in place to determine whether a specific disruptive event requires DRP effect (Schmidt, 2006).

Business Impact Analysis: Business impact analysis (BIA) is a critical step in the development of disaster recovery planning (DRP). This involves identifying the various events that could impact the continuity of operations and their financial, human, legal and reputational impacts on the organisation.

Muthukrishnan (2005) added that BCP/ DRP is the act of proactively strategising a method to prevent, if possible, and manage the consequences of a disaster, thus limiting the consequences to the extent that a business can absorb the impact.

Business impact analysis: Risk ranking, classification of operations and critical analysis: Risk is a dynamic phenomenon, constantly fluctuating due to business activities and market changes. Although quantifying risk is an inexact science, the following formula can help track a company's risk exposure as it changes from day to day and week to week. A system's risk ranking involves determining the risk based upon the impact derived from the critical recovery time period and the likelihood that an adverse disruption will occur. Many organizations will use a risk-of-occurrence formula to determine what it deems is a reasonable cost for being prepared. This risk-based analysis process helps prioritize critical systems and develop appropriately scaled recovery strategies. The risk-ranking procedure should be performed in coordination with IS processing and end-user personnel.

A typical risk ranking system may contain the classification found in table 1 below;

Table 1: Classification of risk ranking systems

Classification	Description
Mission Critical	Mission Critical to accomplishing the mission of the organization Can be performed only by computers No alternative manual processing capability exists Must be restored within 24 hour
Critical	Critical in accomplishing the work of the organization Primarily performed by computers Can be performed manually for a limited time period Must be restored starting at 24 hours and within 3days
Essential	Essential in completing the work of the organization Performed by computers Can be performed manually for an extended time period Can be restored as early as 5 days, however it can take longer
Non-Critical	Non-Critical to accomplishing the mission of the organization Can be delayed until damaged site is restored and/or a new computer system is purchased Can be performed manually

Source (SANS Institute 2003)

RECOVERY STRATEGIES

The following paragraphs discuss some IT disaster recovery processes.

Hot Site: Gregory (2008) stated that a hot site is a location that is ready to assume production application processing with little or no preparation. Systems, networks, and applications are all in place and up-to-date, and perhaps live data is already on the site or can be loaded up fairly quickly. Generally speaking, a hot site can assume processing with only a few minutes' or hours' notice.

Hot Swapping: Hot swapping is the replacement of a hard drive, CD-ROM drive, power supply, or other device with a similar

device while the computer system using it remains in operation. The replacement can be due to a device failure or (for storage devices) to substitute other data (Harris 2008).

Remote Journaling: Remote journaling allows one to establish journals and journal receivers on the target system that are associated with specific journals and journal receivers on the source system. Once the remote journal function is activated, the source system continuously replicates journal entries to the target system (Gregg, 2005).

Disk Shadowing: Harris (2008) explained that disk shadowing is a technique used to enhance availability and reliability of secondary storage. It consists of dynamically creating and maintaining a set of two or more identical disk images on different disks coupled as a mirrored disk (two disks) or a shadow set (two or more disks). One or more hosts can be connected to a shadow set, which is considered as a single disk device. When a host directs a write request to the shadow set, the data are written to all disks in the shadow set. A read request is executed by reading from any disk in the set.

Warm Site: Warm sites do not involve a main computer, but are partially configured, usually with network connections and selected peripheral equipment (such as disk drives, tape drives, and controllers). The backup equipment involved in warm site recovery must be turned on periodically to receive backups of data from production servers (Hiles, 2007).

Cold Site: Cold sites are generally just empty processing centres with little or no networking equipment, and few (if any) systems. Communications facilities may or may not be in place.(Gregory 2008)

Table 2 Comparison of hot, warm, and cold sites.

Category	Hot	Warm	Cold
Readiness	Minutes to hours	Hours to days	Days to weeks
Application System	Loaded and ready	Present but not ready	Absent; must be systems purchased and installed
Communications	Ready to go	Capable	Little or none
Application data	Up to date	Not up to date; must be refreshed	Not present; must be loaded
Cost	Very high	Moderate	Low

Source: Gregory (2008)

RESEARCH METHODOLOGY

The research involved a combination of quantitative and qualitative research approaches with the simple random sampling technique used. A simple random sample is a subset of chosen items from a larger set. Each item is chosen randomly and entirely by chance, such that each chosen one has the same probability of being chosen at any stage during the sampling process. A simple random sample is an unbiased surveying technique. This is a

type of sampling technique in which the units to be observed are selected not on any specific basis (Yates et al., 2008; Babbie, 2004).

Data Collection Methods: Questionnaires and interviews were used as the means of gathering primary data. Interviews were used to answer the questions of what strategies are available in the Ghanaian banking industry while questionnaires were used to answer the question of the preparedness of its staff in recovery from IT disaster.

Data Quality Issues

Validity: Validity, according to Robson (2002) is concerned with whether the findings of a research are really about what they appear to be about. Validity is also defined as the extent to which data collection method or methods accurately measure what they intended to measure (Saunders and Thornhill, 2003, cited by Baraghani, 2007).

Reliability: Robson (2002) refers to reliability as the consistency or stability of a measure; for example, if it were to be repeated, would the same result be obtained? In this study, there is an attempt to minimize bias and ambiguity to obtain valid and reliable data. Interview questions and questionnaires are discussed with colleagues, additionally, the final questionnaire is tested on five respondents to ensure its validity and reliability before launching it to the whole sample. It must be noted that these initial five responses were also used in analyzing the data.

RESULTS AND ANALYSIS

Quantitative analysis

The analysis covered 7 banks with 55 responses representing about 73% response rate. The distribution of staff responses from the banks are as follows.

Table 3: Distribution of respondent banks staff

	Number	Percent
Apex Bank Ghana Ltd.	5	9.1
Ecobank Ghana Limited	6	10.9
Prudential Bank Ghana Ltd	11	20.0
Bank of Ghana	8	14.5
Ghana Commercial Bank Ltd	7	12.7
Agricultural Development Bank	10	18.2
National Investment Bank	8	14.5
Total	**55**	**100.0**

Source: Field Work 2012

From Table 3, the highest response came from Prudential Bank Limited (PBL), followed by Agricultural Development Bank (ADB) and National Investment Bank (NIB). Also work experience of staff at their current place of work shows that slightly over 50% have worked with the banks for less than 5 years (Figure 4). The last 30% of staff had worked in their banks for over 7 years with the longest serving staff having worked for 28 years. Due to the high variance in data, the use of the central tendency median showed that the average length of service in the current organisation was four years while the mode was two years. While two (2) years is enough for bank staff to be well acquainted with the operations of the bank and its polices, it is also enough time for banks staff to have a possible experience with data loss during their course of their work.

Losses with respect to some of the products or platforms listed above deal with software (34.5%), data (58.2%), network (52.7%), and hardware 30(%).

State of Disaster Recovery in Banks

The next few sections present survey responses on issues that reflect mostly the first two objectives of the research. They describe how well banks are prepared to recover from IT disaster. Table 4, however, focuses on staff responses to questions on information and security protocol breaches – in answer to the first objective of the study.

Table 4: Information and Security Protocol Breaches

	Bank 1	Bank 2	Bank 3	Bank 4	Bank 5	Bank 6	Bank 7	All Banks
Action to take when Visitors bypass Security Protocols								
Prompt visitors of security protocols	4(80%)	1(12.5%)	1(10%)	4(57.1%)	4(36.4%)	-	4(50%)	1(32.7%)
Report to Help Desk/ IT	1(20%)	2(25%)	2(20%)	1(14.3)	3(27.3%)	-	-	9(16.4%)
Alert Information Security Officer	-	1(12.5%)	-	-	2(18.2%)	2(33.3%)	2(25%)	7(12.7%)
Alert Risk Management Team	-	-	-	-	-	-	-	1(1.8%)
Report to Management	-	-	3(30%)	2(28.6%)	-	-	-	5(9.1%)
Block IP address and port of remote system	-	1(12.5%)	-	-	-	-	-	1(1.8%)
Put password on hard drive	-	1(12.5%)	-	-	-	-	-	1(1.8%)
No idea what to do	-	2(25%)	4(40%)	-	1(9.1%)	4(66.7%)	2(25%)	13(23.6%)
Action when there is substantial loss of data								
Inform Help Desk/IT department/system administrator	5(100%)	4(50%)	4(40%)	5(71.4%)	6(54.5%)	-	3(37.5%)	27(49.1%)
Report to Internal Control/Security Information department		-	1(10%)	-	1(9.1%)	1(16.7%)	1(12.5%)	4(7.3%)
Fall back on backup		3(37.5%)	2(20%)	1(14.3%)	1(9.1%)	-	1(12.5%)	8(14.5%)
Run data recovery test		-	-		3(27.3%)	-		3(5.5%)
Report to HOD/Supervisor		-	-	1(14.3%)	-	-	1(12.5%)	2(3.6%)
Confer with colleagues		-	1(10%)	-	-	-	(12.5%)	2(3.6%)
Place a password on computer		1(12.5%)	-		-	-	-	1(1.8%)
Do nothing			2(20%)		-	5(83.3%)	1(12.5%)	8(14.5%)

Source: Field work, 2012

From Table 4, almost a quarter of the respondents in the banks did not know exactly how to deal with visitors who bypass security protocols. Predominantly, staff submitted that they will prompt the visitors of security protocols. A relatively larger proportion of staff (dominated by Bank 1 and Bank 4) intimated such action. Bank 1 and Bank 4 did not have any staff showing ignorance as to what to do. All the banks showed low security consciousness except for Bank 6, where a third of the staff mentioned that they would alert the information security officer in case of such breaches.

The distribution of responses on actions to be taken by staff when there is substantial loss of data showed that the first point of call for most people is the Help or IT Department or the system administrator. This view was shared largely by Bank 1 and Bank 4. About 37.5 percent of the respondents in Bank 2 would fall back on backup while about a quarter of the respondents in Bank 5 would want to run data recovery tests on such substantial loss of data. There is a significant number of staff members in Bank 6 who reportedly would do nothing about such situations. In a nutshell, the respondent banks' staff seemed inclined to consult their IT personnel in case of substantial losses of data though response from Bank 6 is largely at variance.

Banks' Preparedness for IT Disaster

The banks preparedness is determined by two key things. There are systems backup and facilities available and personnel who are competent enough to decipher malfunction and act appropriately to salvage data and restore data when needed. To this end, staff knowledge on the availability of policy on information security, familiarity with organisation's data recovery processes, 'first aid' actions to take in event of identifying huge data losses, and apparently identifying legitimate system disruptions that could cause data integrity to be compromised are examples. These elements are captured in Table 4 on the seven banks. Table 5 examines staff training and emergency actions in data recovery.

Table 5: Knowledge and familiarity with information security, data recovery process and identification of system disruptions.

	Bank 1	Bank 2	Bank 3	Bank 4	Bank 5	Bank 6	Bank 7	All Banks
Has knowledge of policy on information security	5(100%)	5(62.5%)	7(70%)	4(57.1%)	10(90.9%)	6(100%)	7(87.5%)	44 (80%)
Documented policy	*4(80%)*	*3(60%)*	*5(71.4%)*	*3(75%)*	*8(80%)*	*6(100%)*	*7(100%)*	*36(81.8%)*
Not documented	-	*1(20%)*	-	-	*1(9.1%)*	-	-	*2(4.5%)*
Not too sure	*1(20%)*	*1(20%)*	*2(28.6%)*	*1(25%)*	*1(9.1%)*	-	-	*6(13.6%)*
Has no knowledge of policy on information security	-	3(37.5%)	3(30%)	3(42.9%)	1(9.1%)	-	1(12.5%)	11(20%)
Familiar with DRP	3(60%)	4(50%)	4(40%)	-	5(45.5%)	4(66.7%)	4(50%)	24(46.2%)
Not familiar with DRP	2(40%)	4(50%)	6(60%)	7(100%)	6(54.5%)	2(33.3%)	4(50%)	28(53.8%)
Staff knows what to do in event of huge information loss	2(40%)	4(50%)	3(30%)	2(28.6%)	5(45.5%)	1(16.7%)	6(75%)	23(41.8%)
Staff does not know what to do in event of huge information loss	3(60%)	4(50%)	7(70%)	5(71.4%)	6(54.5%)	5(83.3%)	2(25%)	32(58.2%)
When do you know that your computer is effective (hardware, software and network) ?								
Upon login	1(20%)	-	-	-	-	-	1(12.5%)	2(3.6%)
Not functioning as expected	1(20%)	2(25%)	-	1(14.3%)	2(18.2%)	1(16.7%)	1(12.5%)	8(14.5%)
Software prompts user of data changes	1(20%)	1(12.5%)	-	1(14.3%)	1(9.1%)	-	-	3(5.5%)
Computer gives pop-ups	-	1(12.5%)	-	-	2(18.2%)	-	1(12.5%)	3(5.5%)
When PC cannot be used at all	-	-	-	-	2(18.2%)	-	2(25%)	4(7.3%)
When duration of downtime exceeds a number of hours	-	-	-	1(14.3%)	-	-	-	1(1.8%)
Loss of data	-	-	1(10%)	-	-	-	-	1(1.8%)
Slowed system	-	1(12.5%)	1(10%)	-	2(18.2%)	-	-	3(5.5%)
When access is not granted	-	1(12.5%)	1(10%)	2(28.6%)	-	-	-	5(9.1%)
Output is inaccurate data	-	-	-	-	-	-	-	1(1.8%)
Report from system	-	-	1(10%)	-	-	-	-	1(1.8%)
Have no idea at all	2(40%)	-	6(60%)	2(28.6%)	3(27.4%)	5(83.3%)	3(37.5%)	23(41.8%)

Source: Field Work 2013

Table 5 revealed that 80% of the reported being aware of the policy on information security in their banks. About 30% or more of the respondents in Bank 2, Bank 3 and Bank 4 reported not being aware of such provisions in their banks. Of those who reported knowing about such a policy, about 82% reported that the policy is documented while most of the remaining staff were unsure.

In contrast to the above, only 46.2% of the total respondents reported being familiar with the Disaster Recovery Plan (DRP) in the banks studied. Bank 5 was the only bank with as much as two-thirds of the respondents reportedly being familiar with their banks' DRP. Similarly, only 41.8% of the respondents reported knowing what to do in the case of a disaster. Many of the respondents from Bank 7 (75%) claimed to know what to do during information loss.

Asked when the respondents know that their computers, software, or network is defective, the respondents gave varied answers. While about 41.8% of all the respondent banks' staff indicated that they had no idea, the most subscribed response was "when the computer was not functioning as expected (14.5%), This is followed by denial of access (9.1%). Other responses were: identification of malfunctioning computer or software during login; software prompt, computer pop-ups of errors or defective operation, when the computer cannot be used at all, when the duration of down time exceeds a certain number of (unspecified) hours, loss of data, slowed computer system, inaccurate data output and system reports such as that from the server.

Further, quantitative data available on the subject matter include survey responses on staff training in disaster management, emergency steps to take, contacts to make, and staff evaluation of the integrity of data compromised. These are important points to consider given that the staff in the banks (apart from IT personnel) are the frequent users of data. Knowledge about disaster management would help them take the right precautions to ensure that breaches are corrected or professional help is sought in time.

Table 6: Staff involvement in disaster management: Training and identifying breaches in data integrity

Factor	Bank 1	Bank 2	Bank 3	Bank 4	Bank 5	Bank 6	Bank 7	All Banks
Staff trained in disaster Management (DM)	1(20%)	4(50%)	1(10%)	-	2(18.2%)	3(50%)	-	11(20%)
Staff not trained in DM	4(80%)	4(50%)	9(90%)	7(100%)	9(81.8%)	3(50%)	8(100%)	44(80%)
Knows an emergency contact to call in case of a disaster	5(100%)	7(87.5%)	6(60%)	4(57.1%)	5(45.5%)	6(100%)	2(25%)	35(63.6%)
Do not know an emergency contact	-	1(12.5%)	4(40%)	3(42.9%)	6(54.5%)	-	6(75%)	19(34.5%)
How do you know if the integrity of data has been compromised?								
Denied access to data	1(20%)	2(25%)	-	-	1(9.1%)	-	-	4(7.3%)
Last date of data modified/ change in data credentials	-	-	-	-	1(9.1%)	-	-	1(1.8%)
When info is partially displayed	-	1(12.5%)	-	-	1(9.1%)	-	2(25%)	4(7.3%)
Data entry errors, software bugs, virus	-		1(10%)	-	3(27.3%)	-	1(12.5%)	3(5.5%)
Access by unauthorised persons	-	2(25%)	1(10%)	-	-	-	1(12.5%)	4(7.3%)
Saved data is different from working file	-	1(12.5%)	-	-	1(9.1%)	-	1(12.5%)	3(5.5%)
System is not operational	-	-	-	-	-	-	-	2(3.6%)
Does not know	4 (80%)	2(25%)	8(80%)	7(100%)	4(36.4%)	6(100%)	3(37.5%)	34(61.8%)

Source: Field work, 2012

From Table 6, it can be observed that 80% of the respondents have not been trained in disaster management in the banks. Bank 4 and Bank 7 have none of the staff trained in any disaster management programme. Only Bank 2 and Bank 6 had half of the responding staff trained in disaster management. In terms of provisions by the banks to receive notices on emergency situations or signals of potentially worrying situation, the responses from the staff showed that the banks had not done much. Only 63.6% of the respondents reported that they knew an official emergency contact to call in case of a disaster. Nonetheless, Bank 1 and Bank 6 had all of their respondents in the know of such emergency numbers. Bank 2 reported a significant proportion of its staff having knowledge about the contact numbers to call in cases of an emergency. Bank 7 exhibited a lack of preparedness in this instance as only a quarter of its respondents knew who to call in case of a disaster.

Generally, too many of the respondents' staff (61.8%) reported they that they it would not know when the integrity of the data they are working on or with has been compromised. Respondents from Bank 4 and Bank 6 exhibited zero knowledge, Bank 2 and Bank 7 reported being quite conscious of data integrity issues. Many of the respondents from the banks mentioned that when information on their monitors is partially displayed or unauthorized persons have gained access to their data or when there are variations in data between saved file and working file, there is compromise in data integrity. Denial of access to data is another indicator mentioned by staff from some of the banks. Results in the relevant portion of Table 6 show that there were quite huge variations in responses on what will constitute compromise in the integrity of data.

Qualitative Findings

The qualitative findings are responses from the semi-structured interviews bordering on nature of disaster management strategies, preparedness of banks to recover from IT disasters and backup and to restore provisions that have been made by the bank. The ensuing presents a summary of qualitative findings with thematic analysis.

The objectives of the data recovery strategies of the bank varied but bordered around data protection and recovery. Samples of answers given by the various banks include: to recover resources wherever disaster strikes; to protect data loss; to be able to continue with the bank's operations; to continue with business operations in an unlikely case of a disaster; to prevent disruption to service or recover critical systems as early as possible in case of disruption; and to get data back up in time of disaster.

All but one bank had a disaster recovery plan that has been documented into a policy. Nonetheless, the banks without a formal document followed protocols that showed that there are either conventional or declared procedures of doing things. These procedures might have been documented but not put together as a single policy document. The bank however is in the process of adopting a single comprehensive policy

Many of the IT managers could not identify the main structures of their bank disaster recovery plan and could not also describe their emergency mode of operations. The few banks that did, mentioned the following factors: resources, personnel, procedures of disaster recovery, evacuation procedures, and offsite facility. While this looked satisfactory, only one bank intimated these structures -

apparently the organisation with the documented policy. Other banks mentioned combinations of the components mentioned above to constitute their structures.

Only two banks stated their emergency mode operations and they were varied. One constituted staff using approved routes to go to safety, initiating measures to protect or restore data and restoring critical systems. The other involved users connecting to the data recovery site to continue working.

Responses on what constitutes an emergency in the disaster recovery plan received similar responses. The responses came down to activities that can destroy or hamper the organisation's smooth operations. This involves failure of critical IT systems and data loss. One organisation added loss of lives.

All the respondent banks, except one, had a backup policy. The backup policy had to do with replication of data for which some of the banks had real time replication of data. Though one of the banks did not have a policy in place, it actually used oracle application in its database systems. The difference lay only in documentation. Nonetheless, the organisations had different restoration sites: three banking organisations had a 'warm' restoration site, while two had 'mirror' restoration site and another two had 'cold' restoration sites. These were located at different distances from the head offices of the banks. For example, those with 'cold' restoration sites were located between 100 and 250 miles while those with a mirror site were located between 10 – 20 miles away. 'Warm' restoration points were located between a mile and 20 miles away.

While other banks had outsourced their data recovery activity to a specialized company, they made efforts to use genuine software. About 75% of the respondent banks have all software with certificates while the rest have most of their software being genuine.

Recovery policies varied among the banks. While some put data first, others put human life first. It only suffices that disasters that involve human life would warrant that people involved are saved first before an attempt is made to salvage data of any kind. Nonetheless, the prioritizing list commonly involved salvaging the data first, followed by operating systems and then other hard copy files or assets. One bank's policy was to save everything at the same time.

In terms of risk analysis, a couple of banks do not engage analysis into potential threats in the bank. Many of the banks that reported doing it do so only on quarterly basis. Another one did it biannually. One of the banks reported doing it daily, which did not seem very realistic for a comprehensive risk analysis. This last organisation used only observed system warnings as a data source for its risk analysis. Some of the banks reported using a combination of complaint forms, observed system warnings, third party information (from such sources as meteorologists and operations) and system disruptions from other players in the banking industry. Incidents from the past also inspired results of risk analysis for some banks. To this end, the banks made it a policy for the employees to tender daily and weekly reports on the IT systems they use.

With regards to data recovery, three organisations have never had their data recovery plan tested or rehearsed. Others had it tested annually, some biannually, and others quarterly.

Per their reported plans or conventions, all the banks have at least manual systems for proceeding with business in case their IT systems fail. Almost all of the banks reported having designated points where people in the building could converge during an evacuation process. The DRPs of five out the seven banks studied provide for disaster training for all the employees.

Further, while many failed to explain how the process operates, they claimed that they had an administrative structure and authority chain that supports a disaster recovery plan in terms of pronouncing information security breaches, giving passes, sanctioning activities, and following recovery processes. Only one bank mentioned how the Chief Information Security Officer handles such issues.

Questions on the type of information models used by the banks and detailed procedures employed received very poor responses. Alerts to staff of the banks are reportedly done through an electronic mailing system or use of sirens, though the latter seem more effective. Auditing of recovery processes is reportedly done annually by one of the two banks that engaged in it. The other reportedly makes sure that the auditors are present during recovery processes. This might not be feasible under certain circumstances, such as salvaging equipments from a fire outbreak or some other natural disasters.

Risk mitigation involved an annual re-examination of DRPs and consideration for changes in technology for four out of the seven banks. Two of the respondent banks never conducted any reviews while the other bank reportedly does it biannually.

In other activities that involve risk mitigation, the banks reportedly use generator sets, UPS, and power arrestors to mitigate power failure related disasters while they made use of AVR systems to mitigate power surges.

While a couple of banks did not have clear cut policies or practices on the following causes of disaster, the rest of the banks engaged regular servicing of air conditioners, and use of heat sensors to forestall utility failure related disasters. Smoke detectors and fire suppressors were used by banks to mitigate smoke or fire related disasters.

Equipment or hardware failures are reportedly prevented through regular servicing. Flooding and water damages are avoided by some of the banks by locating their IT and data systems in a room that had no pipes running through the walls.

All the respondent banks did not really have any mechanism to mitigate explosions and its associated disasters. The same can be said of storm damages except that one bank intimated that there were systems well located above the ground to control such events.

System/application/software failures were avoided through the use of backups and in some cases systems would have to be reconstructed in the event of failure. Softwares are also duplicated.

Human failure and sabotage that could cause risk is controlled through the use of access controls and the efforts of supervisors.

CONCLUSIONS AND RECOMMENDATIONS

Data integrity is receiving increasing attention from all stakeholders in the banking sector because of the sensitive nature of operations in banks. Banks hold people's investment and so

have very high security issues. Literature on disaster in information technology (IT) shows that the causes of data disaster could be natural or systems and human induced. This presents a complex array of mitigation processes and recovery. Given that the banking industry and indeed the financial sector of Ghana are becoming more competitive and complex, it becomes pertinent that the disaster recovery strategies available in the banking industry in Ghana and the preparedness of the banks' staff to recover from disaster is taken very seriously. With the research mirroring the problems stated, the study set out to find out the disaster recovery strategies of the banks, how prepared the banks are to recover from IT disaster , the sufficiency of the system backup, and restore points for data restoration.

The study found that Ghanaian banks are not prepared to recover from disaster early enough. This indicates a higher recovery time objective (RTO) and disaster tolerance. This would undoubtedly culminate in higher costs for the banks in case of disaster. The study also found that banks are basically less prepared for disasters. This is because staff admitted ignorance or lack of familiarity with disaster recovery plans (DRP) and backup policies; poor course of action when visitors bypass security protocols; inability to determine when data integrity has been compromised and the apparent information asymmetry in the banks. The latter point is explained by the fact that though there exist policies as indicated by IT management of the banks, the staff generally admitted having poor knowledge of these provisions. About 35% of the respondents do not know of the emergency contact to call in case of a disaster. The majority of the staff has not had any training in disaster management. It needs to be emphasized that the results may not be suitable for generalization since only seven out of thirty banks took part in the study. It is against these findings that the study made the recommendations that follow.

Recommendations

It is recommended that:

1. The banks should make it a point to have annual or semi-annual reviews of their disaster recovery plans.

2. Human failure or sabotage was curbed through access control, a feature that runs in many banks, but does not prevent sabotage from staff. It is recommended that banks should introduce authorization limits so that beyond certain sections of the bank, security protocols demand scanning the personnel before entry. This can go a long way to check human sabotage at all levels.

3. The banks must develop good information models to ensure that all staff know about the disaster recovery plan and adhere to its dictates and provisions must be strengthened by finding ways of articulation such provisions through simulations or testing or any other means.

4. The staff should be educated or trained on protocols in case of substantial loss in information.

5. The staff should become more proactive in determining malfunctioning of their computer or information systems and take action in time to call for help.

6. The banks should better publicize emergency numbers that staff could call in case of any disaster. They must

also implement strategies and plans to ensure that all staff actually know and understand what to do in cases of disasters.

7. The banks must increase their investments in data backup and recovery systems through the use of warm and cold sites.

8. The banks must construct mirror or hot sites or enter into contracts with other relevant parties to provide these services.

9. The administrative structure and authority chain should be designed to support disaster recovery plan in terms of pronouncing information security breaches, giving passes, sanctioning activities, and following recovery processes. In the least, personnel in management should be mandated to follow a certain due protocol in events of disaster.

REFERENCES

Acquah P.A (2006); Evaluating the banking system in Ghana, Bank of Ghana

Alavudeen, A. and Venkateshwaran, N. (2010), Computer Integrated Manufacturing, PHI Learning, ISBN 978-81-203-3345-1

Asmah, G. Baruwa Y. & Abdulrafiu A. (June 2005) Managing IT security in an Organisation. A look at Administrative and Physical Controls.

Babbie, E. (2004), The Practice of Social Research, (10th Ed.), California: Thomson Wadsworth

Berg, B. L. (2001), Qualitative Research Methods for the Social Sciences, (4th Ed.), USA: Pearson Education Ltd

Brassil R.A (2003) Mobile and onsite recovery services have emerged recently as viable alternatives to the traditional options for recovery, ISACA Journal, Volume 2

Bronner R.F. (1997). Banking Industry and Disaster Recovery Planning, Bank Security & Fraud Prevention, Vol. 4, No. 11, 11/97

Burg,W.D & Singleton T. W (2005), Assessing the Value of IT: Understanding and Measuring the Link Between IT and Strategy. ISACA Journal, Volume 3

Cummings, E., Haag, S., & McCubbrey D. (2005). Management Information Systems for the Information Age. McGraw-Hill Ryerson Higher Education.

Easterby-Smith, M., Thorpe, R. and Jackson, P. R. (2008), Management

Research. London: SAGE

Doughty K.(2002) Business Continuity: A Business Survival Strategy, ISACA Journal, Volume 1

Gregory P. (2008), IT Disaster Recovery Planning For Dummies, Wiley Publishing, Inc.

Harris S. (2008), CISSP All-in-One Exam Guide, Fourth Edition, Wiley Publishing, Inc.

Hiles, A. (2007). The Definitive Handbook of Business Continuity Management (2nd Ed), England: John Wiley & Sons Ltd,

Information Security (ISO 27001) The User Awareness Training Of ISMS ISO/IEC 27001:

Musaji Y. F (2002), Disaster Recovery and Business Continuity Planning: Testing an Organization's Plans, ISACA Journal, Volume 1

Maykut, P. and Morehouse, R. (1994), Beginning Qualitative Research: A Philosophic and Practical Guide, Philadelphia: The Falmer Press Teachers' Library

Muthukrishnan R.(2005),The Auditor's Role in Reviewing Business Continuity Planning, ISACA Journal, Volume 4

Neuman, W. L. (2006), Social Research Methods: Quantitative and Qualitative Approaches, USA: Pearson Education Inc.

Pearson Education, Inc. (2009) Managing Information Technology, (6th Ed.) Publishing as Prentice Hall.

PricewaterHouse Coopers (2009); Banking Survey Report, PricewaterHouse Coopers Gh. Ltd.

Robson, C. (2002), Real World Research: A resource for Social Scientists and Practitioner-Researchers (2nd Ed.), Oxford, UK: Blackwell Publishing.

Ronald L. Krutz and Russell Dean Vines (2007) The CISSP and CAP Prep Guide: Platinum Edition , John Wiley & Sons

Ross S.J (2006), Downtime and Data Loss, ISACA Journal, Volume 6

Ross S.J (2010),Service Availability & Disaster Recovery, ISACA Journal, Volume 6

Saunders, M. K., Lewis, P. and Thornhill, A. (2000), Research Methods for Business Students, New York: Prentice Hall

Saunders, M. K., Lewis, P. and Thornhill, A. (2007), Research Methods for Business Students, (4th Ed.), USA: Pearson Education Ltd.

Sayana A.S (2005) Auditing Business Continuity, . ISACA Journal, Volume 1

Schmidt K. (2006), High Availability and Disaster Recovery Concepts, Design, implementation, Springer, Germany.

Snedaker S., (2007), Business Continuity and Disaster Recovery Planning for IT Professionals, Syngress Publishing, Inc

Stewart J. M., Tittel E., Chapple M (2005), Certified Information Systems Security Professional, Study Guide (3rd Ed.), Wiley Publishing, Inc.,

Sullivan, T. J. (2001), Methods of Social Research, USA: Harcourt College Publishers.

Wallance M. & Webber L. (2004), The Disaster Recovery Hand Book, AMACOM

Wandrei P.L(2007), Maximizing Backup and Recovery of Data and Systems, ISACA Journal, Volume 3

Yates, Daniel S.; David S. Moore, Daren S. Starnes (2008). The Practice of Statistics, 3rd Ed.. Freeman. ISBN 978-0-7167-7309-2

Yin, R. K. (2003), Case Study Research: Design and Methods, (3rd Ed.), Thousand Oaks, CA: SAGE Publications

Zikmund, W. G. (1984), Business Research Methods, New York: CGS College Publishing

Internet Resource:

wikipedia.org, Disaster recovery - Retrieved May 23, 2011, from- http://en.wikipedia.org/wiki/Disaster_recovery.

DisasterRecovery.org, Information about business continuity and disaster recovery plan Retrieved May 23, 2011, from http://disasterrecovery.org/disaster_recovery.html

wikipedia.org, Information security retrieved May 29, 2011, from- http://en.wikipedia.org/wiki/Information_security

List of Banks in Ghana (2011), accessed on 2nd June 2011, from http://www.bog.gov.gh/privatecontent/public/File/BSD/-Licensed%20Banks%20%20Addresses%20Feb%202011.pdf.

Retrieved from http://www.bankersonline.com/articles/sfpv04n11/sfpv04n11a16.html

SANS Institute InfoSec Reading Room , The Disaster Recovery Plan retrieved 8th August 2011 from http://www.sans.org/reading_room/whitepapers/recovery/disaster-recovery-plan_1164.

Reserve Bank of India (2011), Report of the Working Group on Electronic Banking, Chapter 7, Business Continuity Planning retrieved from 12th August 2011 http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111_C7.pdf

National Academy of Sciences (2007), Improving Disaster Management: The Role of IT in Mitigation, Preparedness, Response, and Recovery. retrieved 18th August 2011 from http://www.nap.edu-/catalog/11824.html

ABOUT THE AUTHORS

Paul Danquah is a Lecturer in the Faculty of Engineering, Science and Computing (FESAC) Pentecost University College. He has a background in MSc Information Security from Anglia Ruskin University (UK), BSc. (Hons) in Computing from the University of Greenwich (UK), Graduate Diploma in MIS, MCSE and CCNP professional certificates in Computing.

Stephen Aryeetey is a banker who has been in the banking industry for almost decade. He holds a graduate degree in Information Technology from the Accra Institute of Technology and a BSc. (Hons) in Computer Science and Economics from the University of Ghana, Legon.

Charles Buaben-Andoh is a Lecturer with the Faculty of Engineering, Health and Computing, Pentecost University College. He is currently a PhD candidate at the Accra Institute of Technology, he holds an MSc in Computing, BSc in Physics and Diploma in Education. Currently, he lectures in Digital electronics, Statistics, Operating Systems and Computing Mathematics. . He was a lecturer at Greenwich Community College, United Kingdom.