Information & Computer Security

Assessing IT disaster recovery plans: the case of publicly listed firms on Abu Dhabi/UAE security exchange

Osama El-Temtamy Munir Majdalawieh Lela Pumphrey

Article information:

To cite this document:
Osama El-Temtamy Munir Majdalawieh Lela Pumphrey , (2016),"Assessing IT disaster recovery plans: the case of publicly listed firms on Abu Dhabi/UAE security exchange", Information & Computer Security, Vol. 24 Iss 5 pp. -
Permanent link to this document:
http://dx.doi.org/10.1108/ICS-04-2016-0030

Downloaded on: 07 November 2016, At: 20:50 (PT)
References: this document contains references to 0 other documents.
To copy this document: permissions@emeraldinsight.com
The fulltext of this document has been downloaded 16 times since 2016*

ASSESSING IT DISASTER RECOVERY PLANS: The Case of Publicly Listed Firms on Abu Dhabi/UAE Security Exchange

Abstract

Purpose – This paper attempts to assess IT disaster recovery plans in publicly listed companies on Abu Dhabi securities exchange in the UAE. We assessed among other things DRP preparedness, documentation, employees' preparedness and awareness and the most significant physical and logical risks that poses the most threads to drive the development of the DRB, etc.

Design/methodology/approach – We surveyed publicly listed companies on the Abu Dhabi Securities Exchange (ADX) using a questionnaire adapted from past research papers as well as from audit programs published by the Information Systems Audit and Control Association (ISACA). The surveys were completed through interviews with middle and senior management familiar with their firm's IT practices.

Findings – The majority of the respondents reported having a DRP and significant number of the respondents reported that their top management were extremely committed to their DRP. Employees were generally aware of their role and the existence of the DRP. The greatest risk/threat to their organization's IT system was logical risk followed closely by power & network connectivity loss as the second highest physical risk. The most highly ranked consequence of an IT disaster was loss of confidence in the organization.

Research limitations/implications – Because this paper only examined publicly listed companies on ADX, the research results may lack generality. Therefore, further research is needed in this area to determine the extent of the deployment of the DRP in the region.

Practical implications – Results of this paper could be used for IT DRP planning bench-marking purposes.

Originality/value – This paper adds value to research by investigating the current IT DRP practices by public companies listed on ADX.

Introduction

Over the past couple of decades, information technology (IT) literature has emphasized the fact that a properly managed organization should have a well-developed IT disaster recovery plan (DRP) to enable it to continue its operations in the event of a disruption and to be able to survive a disastrous interruption to its information systems [Marshall & Schrank 2014; Olshansky et al. 2012; Al Badi et al. 2009; Pregmon 2008; Benton, 2007; Doughty, 2002; Lundquist, 2001;]. In addition, legislative and regulatory bodies have begun mandating disaster recovery plans (e.g. In the USA, since 1989, federally chartered institutions are required to have a disaster recovery plan). In the UAE banks are not required to have a disaster recovery plan, but good business practices would mandate such a plan. Modern business entities are extremely dependent on their IT systems, many of which are highly integrated, not only throughout the various functions of their own organizations but also with systems external to the organization. Organizations must incorporate one or more of the industry best practices approaches (ITIL, ITSM, COSO and COBIT) into their business processes to ensure the continuity of the enterprise business functions in the event of a disaster.

In the literature there are a number of terms used to define and discuss planning related to keeping a business operations going forward despite disruption. It is critical that an organization clearly defines what sort of plan it is working on. Business recovery, disaster recovery, emergency management, crisis management, or emergency response are synonyms and are used interchangeably with the term business continuity. Throughout this paper, the term "IT disaster recovery plan" will be used to answer the identified research questions. IT disaster recovery plan is part of the business continuity program and usually it is focused on the company's technologies involved in the critical aspects of the day to day business operations.

The purpose of this research is to examine the state of IT disaster recovery plans of publically listed companies on Abu Dhabi Securities Exchange (ADX) in the United Arab Emirates (UAE). The main goal will be to determine the development, establishment, maintenance, and the preparedness of the disaster recovery plan of these companies.

Literature Review/Prior Research

International

Because IT disaster recovery planning is a component of business continuity management, it is generally accepted that a business entity should have a well-developed IT disaster recovery plan [Gold, 2007]. According to the American Management Association (as cited by Burton 2012), "About 50% of businesses that suffer from a major disaster without a disaster recovery plan in place never reopen for business." In addition to addressing the need for IT DRPs for business-type entities, there have been numerous academic research articles and practitioner publications over the past three decades addressing the issue of IT disaster recovery planning using a variety of non-business type entities such as libraries [Cervone, 2006], museums [Peterson, 2006], academic computing centers [Rohde ,1990], academic institutions [Omar, 2009], healthcare [Schattner, 2005, Hospital & Health Networks, 2009], telecommunications regulatory agencies [Samarajiva, 2005]. The need for DRPs has also been discussed in terms of an organization's desire to meet the needs of its employees [Stoyanovich, 2009] and to meet legal requirements (HIPAA, FEMA, FISMA, NIST, etc.). For example, in the USA the Health Insurance Portability and Accountability Act (HIPAA) requires that covered entities have "a contingency plan in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities and change control procedures." [1997]

Wilson Tay, CEO of Management Institute of Malaysia [2009, 2007] quoted data from a variety of sources that found that many companies do not have reasonably complete and actionable DRPs. In 2007 he found that around 60% of companies globally did not have a business continuity plan and strategy in place to mitigate the effect of a disaster. He claimed that companies need to embrace business continuity plans as part of corporate diligence and management should be held accountable if such plans are not prepared. In addition, he stated that such plans are an important factor for any organization's future survival. In 2009 he quoted data from META Group showing that the situation had improved but that only 80% of the Global 2000 organizations had some form of disaster recovery or business continuity plan, and only 60% of those plans were reasonably complete and actionable. He stated that a Gartner Research report had similar findings (85% had established a disaster recovery plan for core technology and infrastructure, but only 15% had a full-fledge business continuity plan). In Malaysia a PwC study found that BCPs were not widely implemented across all sectors of industries, including airlines, multinational oil and gas corporation, telecommunications, and financial services.

The situation was quite similar [Chisholm, 2008] in the USA. Info-Tech Research Group found that almost 60% of North American businesses do not have a disaster recovery plan in place that would resume their information technology services in case of crisis. The seriousness of this problem is supported by research from Faulkner Information Services, which found that 50% of companies that lose their data due to disasters go out of business within 24 months.

Gulf Cooperation Council (GCC) Countries[1]

A survey conducted to measure the awareness of computer security in the Gulf Cooperation Council countries was distributed to public as well as private sector organization. A scoring system was devised and used to associate a grade for each response. The results of this survey indicated a very low level of computer security awareness in the region. Only 56% of the respondents stated that they have a disaster recovery plan. One of the recommendations was that a disaster recovery plan for information system be developed [Al Musa, 2009].

Another research paper specifically targeting the UAE, "Using Quality Models to Evaluate National ID systems: the Case of the UAE," has some significance to the current project [Al-Khouri, 2007]. That paper revealed the significance of using quality frameworks and models that may well contribute to a project's success, since it enables the early detection and addressing of risks and issues of concern at an early state of the project. Two quality standards issued by the International Standards Organization (ISO)—reliability and portability —were applied to the software currently in use in the UAE to create the population register and national ID card (PRIDC software). With regard to reliability, the research showed that the proper processes did not exist to use the software effectively after it was delivered. Reliability is the capability of the software to maintain its level of performance under stated conditions for a stated period of time. Recoverability is a component of reliability. Recoverability of data entered in the PRIDC did not meet the quality standards. Portability is the attribute that bears on the ability of the software to be transferred from one environment to another. The software was designed and coded to operate within a unique environment of databases, operating systems and hardware. Most of

[1] The GCC is composed of six countries: Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and United Arab Emirates.

the hardware used proprietary applications programming interface (API) to interface with the system. This automatically locked the system to use only the specified set of hardware.

Methodology

To determine the current status of IT disaster recovery plans in the publicly listed firms on Abu Dhabi/UAE security exchange~~UAE~~, this research attempted to survey the 65 public companies listed on the Abu Dhabi Securities Exchange (ADX; formerly Abu Dhabi Financial Market) which are divided into nine sectors as shown below in Table 1. The researchers made successful contact with 45 companies which agreed to participate in the survey.

Although 45 companies agreed to participate in the survey, only 23 usable responses were received as shown below in Table 1. This yielded a 51% response rate of the participating companies, but only a 35% response rate of the listed companies. However, response rates in survey research are traditionally low and there does not appear to be a problem with non-response bias so the response rate was considered acceptable.

Insert table 1

The research instrument was a questionnaire adapted from past research papers as well as from audit programs published by the Information Systems Audit and Control Association (ISACA). Before sending the questionnaires to the target audience, we obtained suggestions and comments from the officials of the ISACA-UAE chapter and we pilot-tested the questions of the survey with two academics and two practitioners to make sure they are neutral, straightforward, unbiased and not open to misinterpretation. Based on the feedback we received, we have revised the survey several times to further improve upon the earlier versions of the questionnaire. The targets for the questionnaires were the Information Systems Managers or equivalent positions related to IT. The questionnaires were administered either by direct interview, phone interviews, or by mail. The questionnaires examined key areas of developing and maintaining a good DRP including: top management commitment; key DRP development practices; employee awareness and training; identified risk and threats; and actual implemented controls and testing.

This research attempts to answer the following research questions: *1) what is the overall level of disaster preparedness of businesses in the publicly listed firms on Abu Dhabi/United Arab Emirates security exchange? 2) To what extent does your business have a formal and documented disaster recovery plan in place? 3) What is the level of employees' preparedness and awareness of the existence of the DRB and their role in case of a disaster? 4) The most significant physical and logical risks that poses the most threads to drive the development of the DRB? 5) The extent of the controls in place to mitigate, avoid or transfer risk? And 6) what is the frequency of testing and exercising the DRP?*

The questionnaire is designed to enable us to address the above research questions and it is organized as follows: Introductory (RQ1, Questions 1 – 3); Plan Development (RQ2, Questions 4 – 10); Employee Awareness (RQ3, Questions 11 – 13); Risks and Threats (RQ4, Questions 14 – 16); Controls (RQ5, Questions 17 – 19); and Testing (RQ6, Questions 20 – 26). The questionnaire was initially piloted to identify possible revisions.

The purpose of the introductory section is to establish the existence of a Disaster Recovery Plan. If no such plan exists, this section seeks to determine the reason no such plan exists and if such a plan exists, this section seeks to determine the level of commitment to the plan on the part of top management. Getting management commitment "heightens management's awareness of the risk the company faces and the potential damage to continuing operations and the bottom line" [Lawlor, 2003]. For confidentiality issues the authors did not request a copy or review any of the existing DRP to assess their qualities.

The purpose of the Plan Development Section is to capture information about how the DRP was developed, whether or not it is documented, and who has access to the plan. The purpose of the Employee Awareness Section is to capture information about the entity-wide awareness of the DRP. The purpose of the Risks and Threats Section is to capture information about the various risks to the entity information systems. The purpose of the Controls Section is to capture information about the use of various controls identified in the literature as effective in controlling certain risks/threats to the information system of an entity. This section tries to determine which controls are most effective at either preventing a disaster or minimizing the impact of a disaster if the disaster occurs. The last section seeks to determine the how and how often the DRP is tested.

In the following section we will concisely present the main results of the carried out research.

Analysis, Discussion, Results

This section summarizes the results of the questionnaire. Where significant distinctions exist between sectors, the results are presented by sector, otherwise the results are presented in the aggregate. As mentioned before, the questionnaire was designed to address the research questions which was designed based on the basic phases followed in planning a DRP. These phases are: business impact analysis, business recovery strategy development, detailed plan development, plan implementation, and finally plan exercising/testing and maintenance. However, the questions on the questionnaire were not necessarily segregated by phases, but rather were segregated as previously discussed.

RQ1: what is the overall level of disaster preparedness of businesses in the publicly listed firms on Abu Dhabi/United Arab Emirates security exchange~~what is the overall level of disaster preparedness of businesses in the United Arab Emirates~~?

Top management commitment

Top management commitment is an essential component of developing a sound DRP. Top management commitment is the key factor in the success or failure of the development, implementation, and maintenance of the business continuity plans (continuity Central). The following figure~~table~~ summarizes top management commitment to DRP, as perceived by the respondents. Although respondents had an option to indicate that top management was not committed to the development and maintenance of DRP none of the respondents choose that option. –We will analyze this further in the "*Additional Analysis*" section below, after examining the remaining research questions.

Insert Figure 1

It is very clear from the above results that the majority of top management of the companies surveyed are perceived as extremely committed to developing and maintaining a DRP.

Business Impact Analysis:

The first phase in planning a DRP involves conducting a Business Impact Analysis. This analysis requires management to identify all material events that could impact operations and any consequence on their organization. In order to complete this phase successfully, management must analyze and understand their key business processes, technologies that support their key business processes and any support staff required to operate these technologies and processes. The following table summarizes which of these resources were identified and considered in the development of the respondent's DRP.

Insert table 2

The table above indicates that most of the respondents within the seven sectors have actually ranked technologies that support their key business processes above their actual key business processes. While it seems intuitive that key business processes should be ranked first and that the technologies to support those key business processes should be developed after the key business processes have been developed, the results rank technologies first and key business processes second. However, because the respondents were associated with information technology within the surveyed companies, there may have been a bias in their responses.

RQ2: To what extent does your business have a formal and documented disaster recovery plan in place?

Resources utilized in developing DRP:

The companies were also asked about the resources they utilized in developing their DRP. They were also asked to rank these resources based on degree of utilization if more than one resource was used. Table 3 summarizes, by sector, their responses with regard to resources used.

Insert table 3

As expected the majority of the firms used their previous experience in developing their DRP. Previous experience was followed by external consultants, checklists and internet resources. These results indicate that publicly listed companies on Abu Dhabi securities exchange understand the value of their own experience in developing IT strategies and they are more comfortable tailoring existing model plans to their specific situation.

Although most respondents utilized their previous experiences, both banks and real estate companies ranked external consultant as their first primary resource. This is not entirely unexpected. The critical nature of a DRP for the banking industry is emphasized in the fact that such plans are mandatory in many developed economies. External consultants would bring with them a wealth of knowledge accumulated in developing such plans in the banking industry in other countries. The importance of external consultants in developing DRP in the real estate sector is not quite as intuitive. Construction companies on the other hand indicated that model plans were their primary resource utilized. Since the real estate and construction industries are often interrelated, it was expected that they would use the same resources in developing their plans.

DRP Documentation:

Once a detailed DRP has been developed, management should document it. The documentation should be very clear and understandable and usually it should identify key personnel responsible for specific tasks. Moreover, these plans should always be updated to reflect any new changes either in business/IT processes or members of the organization who have key roles to play in a disaster recovery plan.

The survey asked participants about their DRP documentation practices. About 74% of all respondents have documented their DRP. Most companies within the banking, insurance and construction industries had documented their DRP. Again, the critical nature of such plans in the banking industry would, it seems, drive the decision to have such plans well documented. Insurance companies, it would seem, are somewhat related to the banking industry and having a well-documented DRP would be mission critical. The other industries surveyed—consumer, industrial, real estate and energy—lagged behind, thus lowering the overall documentation rate. Of those who had documented recovery plans, 58% used both onsite and offsite locations to store copies of their plans. The rest only used onsite locations. All the banks and 80% of the insurance companies used onsite and offsite storage facilities. Again, this result was not unexpected, relative to banking, because of the importance of such plans to banking. Because the insurance sector is somewhat similar to the banking industry, the documentation of their plan was not unexpected. When asked if their organization maintained strict version controls over their documented plans to ensure that appropriate employees have the latest updated copy, only 58% said yes. Again, all the banks and 80% of the insurance companies had strict version controls over their documented plans. Of all the companies that had documented DRP, 60% kept a log of employees who had current copies. Finally, 38% of the companies indicated that they update their plans every year, 17% every two years and 13% every six months. In addition, 16% indicated that they update their plans only whenever any new systems are implemented or major infrastructure changes take place. It appears that updating plans is not a high priority item with many companies.

> *RQ3: What is the level of employees' preparedness and awareness of the existence of the DRB and their role in case of a disaster?*

Employee preparedness and awareness:
In addition to developing a good DRP, management must ensure that entity's employees are aware of the existence of such a plan and any role they might have in such a plan. Tables 4 & 5 summarize the responses regarding employee awareness of the existence of a DRP and their role in such a plan.

Insert table 4

Since a DRP is considered important to the continued existence of an organization in the event of a disaster, it should be expected that all or almost all of the employees of an organization would be aware of the existence of such a plan. Although most organizations with such a plan believe that more than 50% of their employees are aware of such a plan, one would expect 100% of the employees to be aware of the existence of such a plan.

Having a DRP is important but, if such a plan exists, having employees aware of their role in such a plan is even more important. It was expected that most employees would be aware of their role in a DRP. To make all employees aware of the existence of a DRP and their role in such a plan, companies usually educate and train their employees by holding workshops and training sessions.

Insert table 5

The surveys asked participants if their organizations conducted any workshops to educate their employees about their disaster recovery plan's procedures and clearly specified their employees' roles and responsibilities in case a disaster occurs. About 46% indicated that their entities conducted DRP training sessions. It is assumed that those most directly involved in the plan are the ones most aware of their role—for example security personnel are probably aware of their role in the event of a physical threat to the facilities of the organization and IT personnel are probably aware of their role in the event of a either a physical or logical threat to the security of the IT system and the information contained within that system. However, it is expected that other personnel within the organization would be aware of the roles of these personnel in the BRP.

> *RQ4: The most significant physical and logical risks that poses the most threads to drive the development of the DRB?*

Risk and Threats:
As mentioned before, management should first identify what risks and threats their company faces to assist in developing a more relevant recovery plan. Table 6 summarizes what ~~the~~ the surveyed companies believed posed the biggest threats to their organization's information

systems. These potential threats were divided into two categories—physical risk and logical risk.

Insert table 6

Based on the above results it appears that the respondents believe that their IT system(s) are more threatened by power and network connectivity loss within the Physical Risk category and system crashes within the Logical Risk category. Fire and, surprisingly (our surveyed companies are in the desert), flooding, were the second and third physical threats respectively. Within the Logical Risk category hacking and virus attacks were ranked second and third threats respectively. Trojan horse attacks, deliberate damage and sabotage posed the least risk according to our respondents.

Respondents were also asked to rank the greatest negative consequence they contemplated resulting from the above risks and threats. Table 7 shows the results.

Insert table 7

It appears that business disruption was the greatest negative consequence feared by most of our respondents followed by financial loss and reputation damage. These results appear to capture the natural sequence of events faced by any organization if their IT systems fail. Companies within the real estate sector were the only ones who ranked financial loss as their primary feared negative consequence of threats listed in table 6. While the ultimate risk faced by most companies is a financial loss, such a loss would be the direct result of business disruption so it appears that most companies fully understand that financial loss is tied directly to being able to provide the goods and/or services for which the company was established.

RQ5: The extent of the controls in place to mitigate, avoid or transfer risk?

Controls and Recovery Strategies:

Once the main risks and threats have been identified management should formulate and implement controls to mitigate, avoid, transfer or reduce these risks. In addition, an effective DRP must identify the best recovery strategy available to management if a disaster or a disruption occurs. Since there are a variety of controls to choose from, management usually chooses those controls that are more effective in their industry. Table 8 lists all controls and recovery strategies used by respondents, by sector.

All companies reported the use of controls to protect themselves. Since most banks, insurance, and consumer companies in the UAE do business over the internet the responses indicated that most of these companies relied heavily on the following controls or control-related processes: internet and network access controls such as vulnerability scanning and penetration testing to identify weakness in their internet links and internal networks; introduced intrusion detection systems to monitor networks for attacks , introduced firewalls and proxy servers to protect web and internal servers; and utilized robust password policies to prevent access to their systems. In addition, banks also utilized fully mirrored systems and physical sites including mirrored internet service providers to insure uninterrupted online banking services.

Most companies also tested their back-up media regularly to ensure that their systems could be recovered to a known, stable state. They also utilized back-up power systems to enable their organizations to continue operations, or to carry out controlled shutdown, if the main power fails. These controls are a natural response to the two top risks reported by our respondents in Table 8, which are power and network connectivity loss and system crashes.

It is interesting to note that due to the critical role IT plays in the Banks and Financial Services industry the survey indicated that about 71% utilized recovery strategies that include hot sites; 86% Test back-up media regularly; 86% Set up both physical and logical controls; 86% Introduce intrusion detection systems, firewalls and proxy servers; and 100% Educate staff in good security management.

Insert table 8
Insert tables 8a-f

RQ6: What is the frequency of testing and exercising the DRP?

Exercising/Testing:
Finally, the questionnaire asked respondents about their DRP testing practices. Only 38% of the surveyed companied indicated that they tested their plans every year followed by 17% who indicated that they tested it every six months. However, 8% indicated that they never tested their DRP. The survey sought to determine how many of the companies indicated in their recovery plan how many times their plans should be tested. Only 35% of all respondents indicate that their plans specified the frequency of testing. In addition, only 20% have retained an independent consultant to work with their testing team to insure integrity and objectivity in the testing process. When asked if their plans specify how to report the test results and any corrective actions if any, 47% indicated yes. In addition, 40% indicated that their top management get a copy of their test results. This, however, should not stop management from partially testing the plan.

The only objective method of assessing a DRP is to exercise/test it and see if the business can recover if a disaster occurs. In practice, there are three options to choose from: Paper Test, which basically entails a paper walkthrough of the plan; Preparedness Test, which is a localized version of a full test; and finally a Full Operational Test, which is one step away from an actual disaster. About 31% of the respondents indicated that they use the paper test method followed by 22% that use a full operational test and 19% who use a preparedness test method.

Additional analysis
Active participation by top management during exercising/testing the DRP is a very high indicator of the top management commitment (continuity Central). This creates awareness on the importance of the DRP objectives and how the employees are responding to such

activities. The periodic and the type of exercising/testing of the DRP (Q20) are another indicator of the commitment of top management. Moreover, updating the DRP in a regular basis is a very good indicator of the top management commitment. The aim of this section is to examine the correlation between the top management commitment and these variables.

By examining the correlation between the top management commitment to the organization's DRP (Q3) and the frequency of the plan update (Q10), the Pearson correlation coefficient was (r = .4), which suggests a modern correlation between the top management commitment and updating the DRP in a regular basis (every six months to every two years).

By examining the correlation between the top management commitment to the organization's DRP (Q3) and the proportion of the employee's knowledge that the organization has a DRP (Q11), the Pearson correlation coefficient was (r = .85), which suggests a strong correlation between the top management commitment and the employee knowledge of the organization DRP.

By examining the correlation between the top management commitment to the organization's DRP (Q3) and the education of the employees and staff about the plan's procedures and clearly specify their roles and responsibilities in case a disaster occurs (Q12), the Pearson correlation coefficient was (r = .612), which suggests a strong correlation between the top management commitment and the employee and staff understanding their roles and responsibilities in case a disaster occurs (by conducting workshops).

By examining the correlation between the top management commitment to the organization's DRP (Q3) and the periodic exercising/testing of the DRP (Q20), the Pearson correlation coefficient was (r = .168), which suggests a small correlation between the top management commitment and the periodic of exercising/testing of the DRP (at least once each two years).

Thus, based on the above analysis, one can conclude that top management of publicly listed companies on ADX are well committed to the development, implementation and maintenance of the DRP in their organizations.

Conclusions and Recommendations

This research indicates that top management of a majority of publicly listed companies on ADX are committed to having a disaster recovery plan and that most companies have such a plan to some degree. Following best practices, most companies document their plans. However, and very importantly, the existence of the plan and the role of individual employees in the DRP do not seem to be well known.

The majority of publicly listed companies on ADX should provide more training for employees to provide information about the existence and nature of the business recovery plan and to insure that all employees are aware of their role in such a plan.

While most companies ranked intentional damage to their system as very low, there is some questions as to the validity of this assumption. For example, in 2007 the UAE, and most other GCC countries, suffered significant loss of communication (internet and telephone) access. The damage was caused by the severing of an underwater communications cables located in the Mediterranean near Egypt. At that time there was some question as to the cause of the damage. It was determined to have been caused accidentally by an anchor from a large ship. However, there remained the possibility that such damage was intentional. Because the UAE remains a stable business environment, there is always the possibility that companies will become too complacent in guarding against intentional damage to their IT systems or to their access to the worldwide web. UAE companies for which electronic commerce is important should ensure that their DRP provides sufficient alternative access to information normally accessed through the worldwide web.

Also, in 2008 many UAE bank customers suffered significant financial losses due to ATM/credit card fraud. While the source of the fraud was determined to have been by individuals located in Eastern Europe, there remains the possibility that similar attacks could be made, not just to banking customers but to any business that make significant use of electronic commerce. This survey indicates that most companies in the UAE do not rank this type of threat as high. Such complacency could leave UAE companies very vulnerable. Insuring that companies engaged in electronic commerce are adequately protected against this type of fraud should be an important part of the DRP.

It was furthermore noted that only 22% of the companies on ADX use a full operational test. A sound DRP should be a proactive document and fully tested on a regular basis to ensure the plan is working as designed and incorporating any new changes in the information technology function. Moreover, testing the plan in a regular basis will identify the weaknesses of a DRP and ultimately should lead to improvement in the plan.

Limitations and Future Research

The major limitation of this research is that it surveyed only the companies listed on ADX and therefore the results cannot be generalized to all companies in the UAE nor can they be generalized to companies in other countries. The data set captured from this study can be used in future cross-country research projects to evaluate DRPs in other security exchange markets in the region.

Another limitation is that no response or non-response bias follow-up research was conducted. The respondents to this survey may well realize the importance of a well-documented DRP and sought to conform their answers to the accepted norm rather than to the reality within their organization. It remains possible that the non-responders failed to respond because their companies do not conform to the accepted norm for DRPs. The authors did not conduct any follow-up research to address what impact response bias or non-response bias might have been present in the current research.

References

Al-Badi, A. H., Ashrafi, R., Al-Majeeni, A. O., Mayhew, P. J. (2009). "IT disaster recovery: Oman and Cyclone Gonu lessons learned", Information Management & Computer Security, Vol. 17 Iss: 2, pp.114 – 126

Al-Khouri, A.M. (2007). Using Quality Models to Evaluate National ID Systems: The Case of the UAE. Proceedings of World Academy of Science, Engineering and Technology 21:1-15.

Al Musa, A.O., M.M.A. Abbadi, et al. (2009). Computer Security Awareness in GCC Countries. Computer Securities Policies and Standards in the Gulf Region: 1-16.

Benton, D. (2007). Disaster Recovery: A Pragmatist's Viewpoint. Data Recovery Journal, Winter: 70-81

Burton, K. (2012). Catastrophic Impact and Loss: The Capstone of Impact Assessment. CRC Press, Taylor & Francis Group, 2013.

Cervone, H.F. (2006). Disaster Recovery and Continuity Planning for Digital Library Systems. 22(3): 173-178.

Chisholm, P. (2008). Disaster Recovery Planning is Business-Critical. The CPA Journal. NY,NY, July 2008, Vol 78, Iss 7, page 11

Continuity Central, "TEN THINGS THAT INDICATE TOP MANAGEMENT SUPPORT FOR BUSINESS CONTINUITY". Retrieved from http://www.continuitycentral.com/feature0430.htm

Doughty, K. (2002). Business Continuity: A Business Survival Strategy. Information Systems Control Journal. Vol. 1.

Federal Emergency Management Agency (2014). Business continuity plan implementation. Retrieved April 06, 2016 from http://www.ready.gov/business/implementation/continuity

Gold, L. (2007). Disaster Recovery Planning: How do you measure up? Accounting Today. New York, Accounting Today, 21:1. HIPAA (1997). U.S. Health and Human Services, www.hhs./hipaa Hospital & Health Networks. Disaster Recovery: Preparing for the Worst on a Regular Basis. March, 2009, Vol. 83, Issue 3 , p 30.

Lundquist, E. (2001). Disaster Plans Ties to Business Success. Eweek (March 5, 2001).

Marshall, M. and Schrank, H. (2014). "Small business disaster recovery: a research framework." Natural Hazards, 10.1007/s11069-013-1025-z, 597-616. Online publication date: 16-January-2014.

Omar, A., D. Alijani, R. Mason (2009). Information Technology Disaster Recovery Plan: A Case Study. Academy of Information and Management Sciences, Volume 13, No. 1.

Peterson, K.M. (2006). Disaster Preparedness and Recovery for Museums: A Business Recovery Model

Rohde, R. and Haskett, J. (1990). Disaster Recovery Planning for Academic Computing Centers. Communications of the ACM, June 1990, Volume 33, Number 6.

Samarajiva, D.R. (Dec 2005). Mobilizing information and communications technologies for effective disaster warning: lessons from the 2004 tsunami, New Media & Society, Vol. 7 Issue 6, p731-747, 17p

Schattner, P. (2005). The GPCG Computer Security Self-Assessment Guideline and Checklist for General Practitioners. General Practice Computing Group. Stoyanovich, M. (2009). Your Disaster Recovery Plan. Benefits & Compensation Digest. Vol. 46, No. 5, May 2009, p. 1,11-15

Tay, W. (2009). Business Continuity: Planning for a disaster vital for business survival. The Edge Malaysia (www.theedgemalaysia.com. 22 June 2009

Tay, W. (2007). Planning for business continuity. *The Edge Malaysia*.

Table 1. Number of Responses

Sector	Listed	Responses
Banks and Financial Services	18	8
Insurance	15	5
Consumer	7	3
Construction	9	2
Industrial	4	2
Real Estate	3	2
Energy	3	1
Health Care	2	0
Telecommunications	4	0
Total	65	23

Table 2: Which resources were identified?

Resources identified	Rank
Key business processes	2
Technologies that support your key business processes	1
Support staff required to operate these technologies and processes	3

Table 3: Which resources were utilized?

Resources used	Used (%)	Banks	Insurance	Consumer	Industrial	Construction	Real Estate
Previous experience	87		●	●	●		
External consultants	54	●					●
Checklists	44						
Internet resources	43						
Workshops between BRP staff and end-user staff	30						
International standards like ISO 17799	22						
Model plans	16					●	

● Indicates primary resource utilized

Table 4: What percent of your employees who know that your organization has a DRP?

Percent of employees who know that their organization has a DRP?	(%) Who Know
All or most of them (more than 90%)	22
Significant majority of them (more than 70% but less than 90%)	38
50% know and the other 50% does not	14
Significant minority less than 30%	17
Less than 10% know	9

Table 5: What percent of your employees know their roles in case a disaster occurs?

Percent of employees who know their roles in case a disaster occurs	(%) Who Know
All or most of them (more than 90%)	24
Significant majority of them (more than 70% but less than 90%)	39
50% know and the other 50% does not	3
Significant minority less than 30%	22
Less than 10% know	12

Table 6: Risk and Threats Rank (the lower the rank the higher the risk)

In developing your BRP which risk do you believe poses the most threat to your organization information systems?	Rank
Physical Risks	
Power & Network connectivity loss	1
Fire	2
Flood	3
Accidental damage	4
Theft	5
Deliberate damage	6
Sabotage	7
Logical Risk	
System crash	1
Hacking	2
Virus attacks	3
Denial of service attacks	4
Trojan horses attacks	5

Table 7: Greatest consequence contemplated (the lower the rank the higher the risk)

Please rank the following consequences which you consider posed the greatest threat in relation to the above Logical & Physical risks and your organization's operating environment	Over all Rank	Banks	Insurance	Consumer	Industrial	Construction	Real Estate
Business disruption	1	●	●	●	●	●	
Financial loss	2						●
Reputation damage	3						
Loss of confidence in your system	4						
Loss of confidence in your organization	5						

● Ranked highest within this sector

Table 8: The Top Ten Controls and Recovery Strategies in use by Sector

Which of the following controls and recovery strategies does your organization use and considers as most effective to either preventing a disaster or minimizing its impact?	Banks	Insurance	Consumer	Industrial	Construction	Real estate
	Rank	Rank	Rank	Rank	Rank	Rank
Use of vulnerability scanning and penetration testing to identify weakness in your internet links and internal networks	8		1	6		1
Introduce intrusion detection systems to monitor networks for attacks	2		2	7		2
Introduce firewalls and proxy servers to protect web and internal servers	3	1	3	8	3	3
Set up both physical and logical controls, including a robust password policy, to prevent access to systems	4	2	4	9	1	4
Educate staff in good security management, and segregate duties to frustrate collusion attempts	1		5	10	4	5
Control third party dependencies and weakness, including suppliers remote access rights		6			5	
Use challenge systems, public private key infrastructure authentication and certification to protect systems, and especially those developed over the web	5				2	
Scan and ban email attachments, as appropriate, and monitor the websites that staff visit: make sure they do not expose the organization to legal action or reputations damage		3	6		6	
Ensure there are reliable back-ups procedures	6	4	7	1	7	6
Use offsite storage of media, equipment and documentation		7		2		7
Test back-up media regularly to ensure that systems can be recovered to a known, stable state.	7	8	8		8	8
Keep spares for critical BRP components both onsite and offsite	9				9	9
Ensure that adequate fire detection, prevention and suppression equipment's is installed and working	10	5	9		10	10
Provide back-up power systems to enable the organization to continue operations, or to carry out controlled shutdown if the main power fails		9	10	3		
Use appropriate redundancy systems for certain technology assets for example networks, etc.		10		4		
Keep metrics on system performance and monitor helpdesk logs to identify known or potential problems.				5		

Table 8-a: The Top Ten Controls and Recovery Strategies in use in Banks & Financial Services

Which of the following controls and recovery strategies does your organization use and considers as most effective to either preventing a disaster or minimizing its impact?	Top Ten
Educate staff in good security management, and segregate duties to frustrate collusion attempts	1
Introduce intrusion detection systems to monitor networks for attacks	2
Introduce firewalls and proxy servers to protect web and internal servers	3
Set up both physical and logical controls, including a robust password policy, to prevent access to systems	4
Use challenge systems, public private key infrastructure authentication and certification to protect systems, and especially those developed over the web	5
Ensure there are reliable back-ups procedures	6
Test back-up media regularly to ensure that systems can be recovered to a known, stable state.	7
Use of vulnerability scanning and penetration testing to identify weakness in your internet links and internal networks	8
Keep spares for critical BRP components both onsite and offsite	9
Ensure that adequate fire detection, prevention and suppression equipment's is installed and working	10

Table 8-b: The Top Ten Controls and Recovery Strategies in use in Insurance

Which of the following controls and recovery strategies does your organization use and considers as most effective to either preventing a disaster or minimizing its impact?	Top Ten
Introduce firewalls and proxy servers to protect web and internal servers	1
Set up both physical and logical controls, including a robust password policy, to prevent access to systems	2
Scan and ban email attachments, as appropriate, and monitor the websites that staff visit: make sure they do not expose the organization to legal action or reputations damage	3
Ensure there are reliable back-ups procedures	4
Ensure that adequate fire detection, prevention and suppression equipment's is installed and working	5
Control third party dependencies and weakness, including suppliers remote access rights	6
Use offsite storage of media, equipment and documentation	7
Test back-up media regularly to ensure that systems can be recovered to a known, stable state.	8
Provide back-up power systems to enable the organization to continue operations, or to carry out controlled shutdown if the main power fails	9
Use appropriate redundancy systems for certain technology assets for example networks, etc.	10

Table 8-c: The Top Ten Controls and Recovery Strategies in use in Consumer

Which of the following controls and recovery strategies does your organization use and considers as most effective to either preventing a disaster or minimizing its impact?	Top Ten
Use of vulnerability scanning and penetration testing to identify weakness in your internet links and internal networks	1
Introduce intrusion detection systems to monitor networks for attacks	2
Introduce firewalls and proxy servers to protect web and internal servers	3
Set up both physical and logical controls, including a robust password policy, to prevent access to systems	4
Educate staff in good security management, and segregate duties to frustrate collusion attempts	5
Scan and ban email attachments, as appropriate, and monitor the websites that staff visit: make sure they do not expose the organization to legal action or reputations damage	6
Ensure there are reliable back-ups procedures	7
Test back-up media regularly to ensure that systems can be recovered to a known, stable state.	8
Ensure that adequate fire detection, prevention and suppression equipment's is installed and working	9
Provide back-up power systems to enable the organization to continue operations, or to carry out controlled shutdown if the main power fails	10

Table 8-d: The Top Ten Controls and Recovery Strategies in use in Industrial

Which of the following controls and recovery strategies does your organization use and considers as most effective to either preventing a disaster or minimizing its impact?	Top Ten
Ensure there are reliable back-ups procedures	1
Use offsite storage of media, equipment and documentation	2
Provide back-up power systems to enable the organization to continue operations, or to carry out controlled shutdown if the main power fails	3
Use appropriate redundancy systems for certain technology assets for example networks, etc.	4
Keep metrics on system performance and monitor helpdesk logs to identify known or potential problems.	5
Use of vulnerability scanning and penetration testing to identify weakness in your internet links and internal networks	6
Introduce intrusion detection systems to monitor networks for attacks	7
Introduce firewalls and proxy servers to protect web and internal servers	8
Set up both physical and logical controls, including a robust password policy, to prevent access to systems	9
Educate staff in good security management, and segregate duties to frustrate collusion attempts	10

Table 8-e: The Top Ten Controls and Recovery Strategies in use in Construction

Which of the following controls and recovery strategies does your organization use and considers as most effective to either preventing a disaster or minimizing its impact?	Top Ten
Set up both physical and logical controls, including a robust password policy, to prevent access to systems	1
Use challenge systems, public private key infrastructure authentication and certification to protect systems, and especially those developed over the web	2
Introduce firewalls and proxy servers to protect web and internal servers	3
Educate staff in good security management, and segregate duties to frustrate collusion attempts	4
Control third party dependencies and weakness, including suppliers remote access rights	5
Scan and ban email attachments, as appropriate, and monitor the websites that staff visit: make sure they do not expose the organization to legal action or reputations damage	6
Ensure there are reliable back-ups procedures	7
Test back-up media regularly to ensure that systems can be recovered to a known, stable state.	8
Keep spares for critical BRP components both onsite and offsite	9
Ensure that adequate fire detection, prevention and suppression equipment's is installed and working	10

Table 8-f: The Top Ten Controls and Recovery Strategies in use in Real Estate

Which of the following controls and recovery strategies does your organization use and considers as most effective to either preventing a disaster or minimizing its impact?	Top Ten
Use of vulnerability scanning and penetration testing to identify weakness in your internet links and internal networks	1
Introduce intrusion detection systems to monitor networks for attacks	2
Introduce firewalls and proxy servers to protect web and internal servers	3
Set up both physical and logical controls, including a robust password policy, to prevent access to systems	4
Educate staff in good security management, and segregate duties to frustrate collusion attempts	5
Ensure there are reliable back-ups procedures	6
Use offsite storage of media, equipment and documentation	7
Test back-up media regularly to ensure that systems can be recovered to a known, stable state.	8
Keep spares for critical BRP components both onsite and offsite	9
Ensure that adequate fire detection, prevention and suppression equipment's is installed and working	10

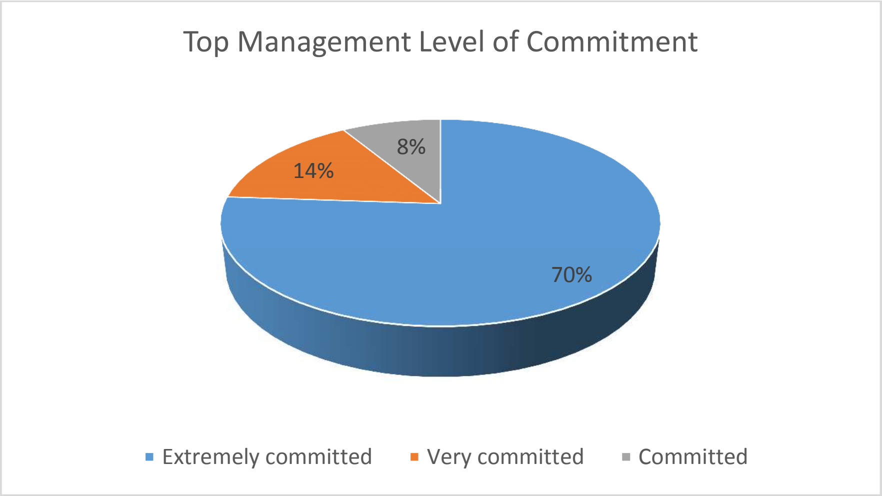

Figure 1: Top management level of commitment