IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4466

Disaster Recovery Planning by Health Maintenance Organizations: The Role of Business Impact Analysis and Testing

Kakoli Bandyopadhyay
Lamar University, Dept of IS and Analysis, Beaumont, TX 77710, Tel: 409/80-8627; Fax: 409/880-8235; bandyopaku@hal.lamar.edu

ABSTRACT

With increasing dependence on information technology, Health Maintenance Organizations (HMOs) need Disaster Recovery Planning to protect their information systems environment. This paper investigates the impact of Business Impact Analysis and testing on successful implementation of Disaster Recovery Plans (DRPs) by HMOs. A survey reveals that HMOs that conduct Business Impact Analysis are more likely to test DRPs and HMOs that actually test DRPs are more likely to implement them.

INTRODUCTION

The integration of clinical (e.g., electronic medical records) and administrative (e.g., billing) systems has resulted in Health Maintenance Organizations (HMOs) being heavily dependent on Health Management Information Systems (HMIS). Consequently, it has become necessary to ensure the continuous availability of HMIS for the effective functioning of HMOs. The uninterrupted operation of HMIS can be accomplished by implementing a working Disaster Recovery Plan (DRP). A DRP ensures the return of businesses to normal operating conditions when disrupted by disasters.

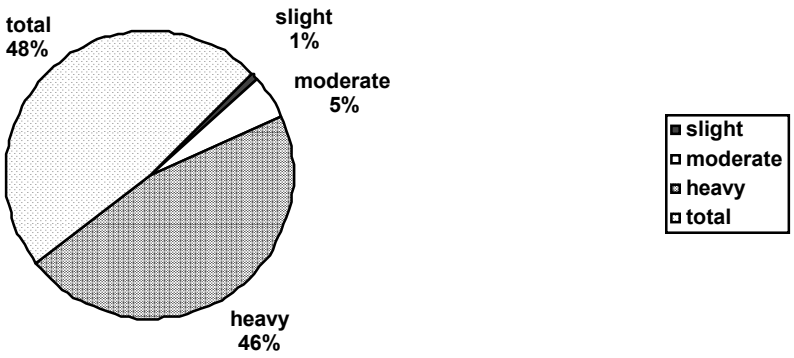
The literature has identified the conducting of a Business Impact Analysis (BIA) and testing as two important elements of the Disaster Recovery Planning process [Keehn, 1993; Terry, 1995]. The purpose of this paper is to report an empirical test to determine the impact of BIA and testing on successful implementation of DRPs by HMOs. In the process, a discussion on the reliance of HMOs on HMIS, the significance of DRP, the importance of BIA and testing is presented first. Next, research hypotheses to study the dependence of DRP implementation on BIA and DRP testing are developed and tested. Finally, the managerial implications of the findings are discussed.

HMOS' RELIANCE ON HMIS

HMOs depend on HMIS in various areas such as electronic medical records, case management system, drug inventory system, drug ordering system, provider's pre-authorization, imaging system, member claims, benefits employer groups, payroll, laboratory, appointment scheduling, diagnostic calling, membership, eligibility verification, call center, and claims history. In a survey of 121 HMOs (survey described in detail later in the article) conducted by the author as part of a bigger study, the participants were asked to indicate the degree of dependence of their HMOs on HMIS by selecting from four options: total, heavy, moderate, and slight. "Totally" dependent HMOs were those that could not survive and would go out of business in the event of complete loss of support from HMIS. When the degree of dependence is "heavy", the HMOs might survive a disaster but with severe difficulty. "Moderately" dependent HMOs could survive but at a lower level of performance. When the dependence was "slight", there would be little, if any, adverse impact due to the unavailability of HMIS. The dependence on HMIS as reported by the respondent HMOs is shown in Table 1. The percentage of HMOs at each level of dependence is illustrated in Figure 1.

Figure 1 indicates that up to 94 percent of HMOs (those with "total" or "heavy" dependence) would either go out of business or would run with severe difficulty in the event of a complete loss of support from HMIS.

Figure 1. Dependence of HMOs on HMIS



DISASTER RECOVERY PLANNING BY HMOS

Several leading researchers have defined Disaster Recovery

Table 1. HMIS Dependence Levels

Dependence	Number of HMOs
Slight	1
Moderate	6
Heavy	56
Total	58
Sum	121

Planning. Andrews [1990] defined Disaster Recovery Planning as "the process of developing and maintaining an effective written plan of how organizations will continue to operate in the event of interruptions of business functions." He further stated that an effective plan should contain the following key elements:

1) a contact list of key personnel with specific assignments during the emergency.
2) a step-by-step guide of what processes and actions must take place in each phase of recovery.
3) specification of minimum equipment requirements.
4) vendor contact information.
5) provision for adequate continuity of telecommunication facilities.
6) minimum alternate site facilities beyond computer requirements.
7) procedures to bring backup files to current status.
8) a methodology for periodically testing the various portions of the plan.

According to Epich and Persson [1994], a DRP is a "written plan of action that enables a company to respond quickly to a disaster." They also noted:

> "probably the most convincing reason for having a business disaster recovery plan is that it simply makes good business sense to have a company protected from a major disaster. Other convincing reasons to have a recovery plan include a potential for greater profits and reduced stress on both management and employees."

A DRP contains a very detailed list of all Information Systems personnel, users, vendors, and company management. The plan also contains a detailed up-to-date list of all hardware, software, and communications lines that make up the information network. All business procedures, forms, records, supplies, and layouts referred to in case of business disruptions are also detailed.

Toigo [1992] defined Disaster Recovery Planning as "a fundamental component of effective resource management, the protection of vital corporate assets." He also stated:

> "the disaster recovery planning project is propelled by a number of considerations, ranging from a common-sense business impetus to safeguard corporate assets from loss or damage to a natural disaster to reduce legal exposure and personal loss."

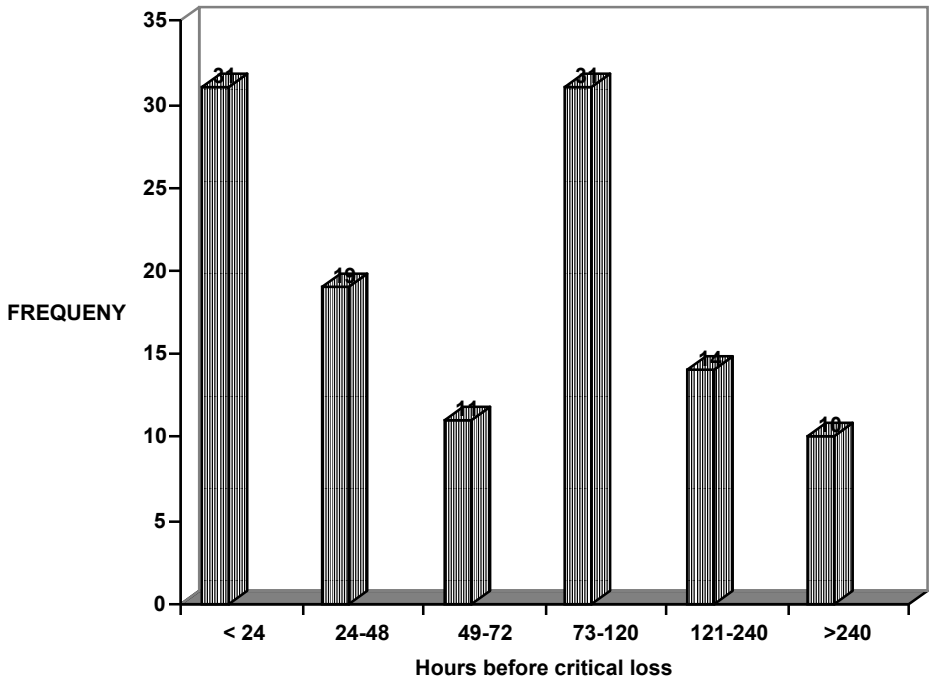
A disaster, in the context of the health care environment, can be defined as the interruption of the operations of HMOs due to the loss or unavailability of HMIS for normal operations. HMIS can suffer disasters caused by both external and internal sources. Natural disasters pose external threats for HMIS assets such as data, hardware, software, personnel, and facilities. Internal threats to assets can come from authorized or unauthorized physical or electronic access and technical failures. As HMOs' dependence on HMIS grows, so does the likelihood of suffering loss of information and the ability to perform necessary operations in the event of a disaster.

Traditionally, the focus of DRP has almost entirely been on recovering critical software applications and data. This comes from an isolated, partial view of the impact of HMIS on HMOs. This narrow approach of searching only the data center for evaluating the impact of unavailability of HMIS can be particularly detrimental in an health care environment, where integration leads to electronic linkages of different health care providers, employers, payers, and patients. As the overall impact of HMIS pervades the organization and its environment, the effect of a disaster will no longer be restricted to a single organization but will be propagated to all other organizations in the network. It is vital that HMOs adopt a holistic view and assess potential threats to HMIS by considering the entire spectrum of the HMIS environment.

BUSINESS IMPACT ANALYSIS

Business Impact Analysis (BIA) is a procedure to study the impact of unavailability of information systems on different functional areas of the business. BIA examines each area of the business to determine: 1) for how long can the organization run when there is a complete loss of HMIS support [Asbrand, 1995]; 2) which functions are critical to the business for its continuous operations [Coleman, 1993]; 3) which functions are most likely to succumb to disasters [Wong, Monaco, and Louise, 1994]; 4) a list of critical business functions in order of priority [Anderson et al., 1994]; 5) the estimated losses to be incurred in each functional area if it stops performing in the event of a disaster [Balas and Brockman, 1985]; 6) the expenditure involved to mitigate the losses from a disaster [Wong, Monaco, and Louise, 1994]; 7) the legal consequences of disasters [Effgen, 1992]; and 8) possible strategies to ensure recovery from disasters [Keehn, 1993]. Each of these items, in the context of the health care environment, is briefly described below:

Figure 2. Hours Before Critical Loss



*HMIS Downtime***.** BIA can indicate the time period beyond which the complete loss of HMIS would become critical for the HMO. Our survey (sampling procedure described later) indicated that for 26.7 percent of HMOs, the complete loss of HMIS support for

even less than 24 hours would become critical for their organizations. If the outage should last for one week, as high as 79.5 percent of the HMOs would be in critical condition. Figure 2 displays the frequency of HMOs and the critical time period beyond which the HMOs would not survive without HMIS support.

Critical Functions. Software packages for BIA such as REXSYS from AT&T Universal Card Services Corporation can determine the processes that are essential for the continuity of the business and have to be restored immediately [Anderson et al., 1994].

Vulnerability to Disasters. BIA ensures business continuity by identifying the functions that are vulnerable to disasters and introducing protective measures to safeguard these vital components.

Priority List. Since all organizations operate under financial constraints, it may not be a practical consideration to protect each and every business function equally. BIA determines a list of functions that *must* be restored after a disaster to ensure return to an agreeable level of operations.

Major Business Losses. BIA can identify the major business losses. Examples of business losses are: duration of business interruptions, lost revenues, customer dissatisfaction and lost customers, loss in market share, employee stress, legal exposure, and higher insurance premiums. Losses in each category can be estimated.

Cost. BIA performs cost-benefit analyses for organizations. If the benefits from deploying protective measures in the form of DRP do not merit the costs incurred, organizations will not be enthusiastic about investing in DRP.

Legal Considerations. BIA evaluates each business function to determine how its disruption would result in legal obligations for the HMOs involved. It also determines whether regulatory requirements mandate developing a DRP to protect the HMIS environment.

Disaster Recovery Strategies. BIA determines the preventive measures that HMOs should deploy to safeguard vital corporate assets such as software, hardware, data, and communication networks. It helps to identify one or more recovery strategies to be adopted by the HMO. The different types of disaster recovery strategies that are currently available include duplicate systems, internal hot sites, cold sites, commercial hot sites, warm sites, reciprocal arrangements, service bureaus, mobile cold sites, and manual processing.

TESTING OF DISASTER RECOVERY PLAN

Testing the DRP, more appropriately referred to as 'exercising the plan' by most disaster recovery planners, is an on-going activity that is essential to ensure its reliability. The DRP should be exercised at least annually. Furthermore, selected area reviews of the plan may be conducted on an as-needed basis, for example, when an HMO functional area undergoes major changes.

Effective functioning of a DRP depends on periodic testing. A DRP, which has not been tested, cannot be trusted. This notion is strengthened by the results of a survey of plans at large IBM mainframe sites which revealed that about half of all DRPs failed when first tested [Brown, 1993]. Testing uncovers possible pitfalls that need to be corrected [Terry, 1995]. Testing reflects any changes in operations, vendors, recovery strategies, procedures, and personnel information from the time it was last updated. Testing also refreshes the minds of all team members about the recovery process. Therefore, it is important to emphasize that the likelihood of the proper implementation of a DRP increases substantially if it is tested.

RESEARCH DESIGN

The Model

The proposed relationship among BIA, testing of a DRP, and DRP implementation is illustrated in Figure 3. The following research questions follow from the model:

1. What is the role of BIA as a precondition to DRP testing and subsequent implementation?
2. What is the role of DRP testing as a precondition to successful DRP implementation?

Research Hypotheses

Several researchers [Keehn, 1993; Coleman, 1993; Wong, Monaco, and Louise, 1994; Asbrand, 1995; Effgen, 1992] have emphasized the importance of conducting BIA as a precursor to Disaster Recovery Planning to make organizations aware of the potential danger that the adverse effects of a disaster can bring. Business Impact Analysis leads to better understanding of critical business functions and losses associated with disruption of various functions which, in turn, makes restoration more effective. By conducting BIA, HMOs become aware of their vulnerability to disasters. Awareness kindles interest in protecting the environment. Interest prompts the evaluation of the benefits of implementing DRP. If the evaluation is favorable, HMOs move toward testing DRPs. Thus, it can be proposed that:

H1: The testing of DRP by HMOs is positively associated with the conducting of BIA.

In most cases, DRPs cannot be perfected initially. Errors can be understood and corrected only by thorough testing (Toigo, 1992). The greater the opportunity to test DRP, the better the chances of improving the development and installation activities to confirm the realization of the desired benefits. Thus, it can be proposed that:

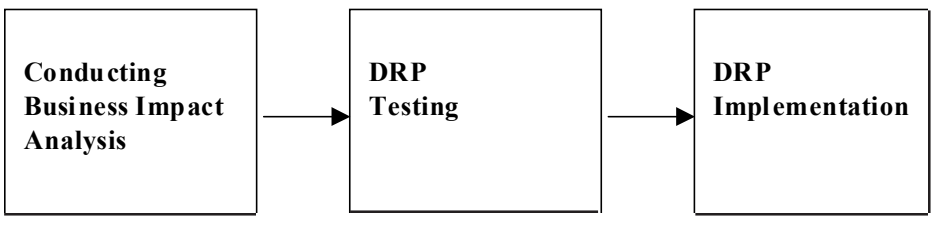
H2: The implementation of DRP by HMOs is positively associated with the testing of DRP.

Sample

Data was collected as part of a bigger study via a mail questionnaire sent to HMOs across the United States. Survey questionnaires were sent to 727 HMOs from a list of HMOs published by the American Hospital Association Guide. It was requested that the questionnaire be filled out by the disaster recovery planner, MIS director, CIO, or some other key employee in the HMO who was involved in BIA and Disaster Recovery Planning.

Altogether, 121 usable responses were received from the survey. This resulted in a net response rate of 18 %. Possible reasons for the somewhat low response rate could be one or a combination of the following: a) due to budget constraints, it was not

Figure 3. The Model



possible to notify the respondents in the sample by telephone before the survey questionnaires were sent; b) e-mail addresses of respondents were not available to provide notice of the survey and seek cooperation; c) no token monetary inducement could be given to the respondents; and d) some respondents might have been concerned about confidentiality even though it was guaranteed by the researcher. The confidentiality issue merits some thought. The HMOs might not have been enthusiastic about disclosing that they, even though they were totally dependent on the uninterrupted functioning of HMIS, had not taken adequate protection against disasters. They might have feared a potential loss of company image and customer confidence.

Measurement of Constructs

The three constructs measured (from H1 and H2 above) were: conducting of BIA, testing of DRP, and implementation of DRP. These constructs were captured in the following questions, respectively, included in the survey:

1. Has your organization completed a Business Impact Analysis (yes/no)?
2. If your organization has already developed a HMIS Disaster Recovery Plan, please describe the frequency of testing of the plan (any frequency mentioned other than 'never tested' indicated that a DRP was tested).
3. If your organization has already developed a HMIS Disaster Recovery Plan, describe the extent to which it is currently being applied to your organization (responses of 'fairly regularly' or 'has become a standard practice' indicated that DRP implementation had taken place).

Results

Hypothesis 1 examined the association between DRP testing and BIA. The hypothesis was tested using chi-squre tests of significance and the Phi coefficient from a cross-tabulation analysis. The cross tabulation analysis is shown in Table 2.

From Table 2, it is seen that the Pearson Chi-square statistic of 22.705 is significant at the level of $p < .001$. The Phi coefficient, which is a measure of the strength of association, is also significant at the $p < .001$ level with a value of .433. Thus, Hypothesis 1 is supported. There is a positive association between the conducting of BIA and DRP testing.

Table 2: Crosstabulation of Business Impact Analysis and DRP Testing

Business Impact Analysis Done?	**Testing Done?**		
	No	Yes	**Total**
No	44	12	56
Yes	23	42	65
	67	54	121

Pearson Chi-Square Statistic (1 degree of freedom) = 22.705, $p < .001$
Phi Statistic = .433, $p < .001$

Table 3: Crosstabulation of DRP Testing and DRP Implementation

DRP Testing **Done?**	**DRP Implementation Done?**		
	No	**Yes**	**Total**
No	61	6	67
Yes	15	39	54
	76	45	121

Pearson Chi-Square Statistic (1 degree of freedom) = 51.237, $p < .001$
Phi Statistic = .651, $p < .001$

Hypothesis 2 examined the association between DRP testing and implementation. This hypothesis was tested using a cross-tabulation analysis which is presented in Table 3.

From Table 3, the Pearson Chi-square is found to be 51.237, which is significant at the $p < .001$ level. The Phi coefficient of .651 is also significant at the $p < .001$ level. These results indicate strong support for Hypothesis 2. There is a positive association between DRP testing and DRP implementation.

MANAGERIAL IMPLICATIONS

The results of the study have several managerial implications for the implementation of DRP by HMOs. The study provides management with insights into some critical issues faced by HMOs today. The issues addressed are: 1) Are HMOs sufficiently aware of their dependence on the reliable functioning of HMIS?; 2) Are HMOs aware of the potential danger that the adverse effects of a disaster can inflict on them?; 3) Are HMOs protecting themselves in advance so that they can recover from a disaster with their critical applications running?

Awareness of Reliance on HMIS

The results indicated that 114 out of 121 (94.2%) HMOs in the sample were either heavily or totally dependent on HMIS. In other words, 94 percent of HMOs would either go out of business soon or could run with severe difficulty in the event of complete loss of support from HMIS (Figure 1). Also, 26.8 percent HMOs could withstand the loss of HMIS support for only 24 hours, and as high as 79.5 percent of HMOs would be in critical condition if the outage should last for a week (Figure 2). These figures can help HMO executives to become more aware of their organizations' dependence on the reliable functioning of HMIS.

Awareness of Threats

The study indicated that only 65 out of 121 HMOs (53.72%) completed a BIA (Table 2). The study also indicated that out of 65 HMOs that conducted BIA, 42 (64.6%) decided to test a disaster recovery plan; whereas out of 56 HMOs that did not conduct BIA, only 12 (21.4%) decided to test such a plan. This clearly points toward the fact that HMOs that conducted BIA were more aware of the impact of the potential unavailability of HMIS on the entire organization and its environment. The implication is to persuade HMO managers to conduct BIA. Without BIA, managers will not comprehend the degree of reliance their organizations have on HMIS, the risks associated with disasters, and how vulnerable their organizations are to these risks. The understanding of the impact of unavailability of HMIS on HMOs should provide management with the awareness of risks associated with disasters which, in turn, will kindle interest toward protecting their HMIS environment.

Degree of Protection

HMOs that implement DRPs are able to protect themselves against HMIS disasters better than those that do not. It is also necessary to periodically test installed DRPs. Effective functioning of DRP depends on periodic testing. Testing facilitates the process of DRP implementation. The study indicated that out of 54 HMOs that tested a DRP, as many as 39 (72%) implemented it (Table 3). Only six HMOs implemented a disaster recovery plan without test-

ing it. Therefore, it is important to stress that the chances of implementing DRP successfully increase if it is tested periodically.

CONCLUSION

First, this paper illustrates the dependence of HMOs on the reliable functioning of HMIS and the subsequent need for disaster recovery planning to safeguard the HMIS environment. Next, the paper discusses BIA and testing as two major antecedent elements to successful implementation of DRP. An empirical test shows that HMOs that conduct BIA are more likely to test DRP, and HMOs that perform DRP testing are more inclined to implement them. Also, the results of the empirical test indicate that, of 121 HMOs that responded to the survey, only 45 (37%) have actually implemented a DRP to protect their HMIS environment from possible disasters. This shows that the majority of HMOs do not currently have adequate protection against disasters possibly interrupting their businesses. It is hoped that the facts outlined in this article will awaken managers to reality and make them conduct BIA to assess the impact of unavailability of HMIS and exercise testing of a DRP to ensure its effectiveness and reliability before eventual implementation. These actions will enable HMOs to better prepare for any possible information systems disaster and leave them ready to face the aftermath.

REFERENCES

Anderson, T., Arbetter, L., Benavides, A., Longmore-Etheridge, A., "Recovery Made Easy," *Security Management*, 38(9), September 1994, 25-26.

Andrews, W.C., "Contingency Planning for Physical Disasters," *Journal of Systems Management*, July 1990, 28-32.

Asbrand, D., "Are You Ready for a Disaster?," *Infoworld*, 17(24), June 12 1995, 45-49.

Balas, J. and Brockman, D.R., "Disaster Planning for DP Operations: The Choice Between Wipe-Out and Recovery," *CA Magazine*, 118(8), August 1985, 46-49.

Brown, M., "The Disaster Business," *Management Today*, October 1993, 42-48.

Christensen, S.R., and Schkade, L.L., *Financial and Functional Impacts of Computer Outages on Businesses*, Arlington Texas: The University of Texas at Arlington, Center for Research on Information Systems, 1987.

Coleman, R., "Six Steps to Disaster Recovery," *Security Management*, 37(2), February 1993, 61-64.

Dellecave, T., "Informationweek 500: Technology: The Best Remedy," *Informationweek*, 545, September 18, 1995, 126-130.

Effgen, K.F., "Presenting the Business Case for a Network-Based Disaster Recovery Planning Program," *Telecommunications*, 26(11), November 1992, 28-31.

Epich, R. and Persson, J.A., "Fire Drill for Business," *Information Strategy: The Executive's Journal*, Winter 1994, 44-47.

Keehn, K., "Networks Need Place in Contingency Plans," *Systems Management 3X/400*, 21(7), July 1993, 83-84.

Terry, R.J., "Organizing a Contingency Plan for Success," *Disaster Recovery Journal*, 8(2), 1995, 43-46.

Toigo, J.W., *Disaster Recovery Planning: Managing Risk and Catastrophe in Information Systems*, Yourdan Press Computing Services, Prentice Hall, Englewood Cliffs, NJ, 1992.

Wong, B.K., Monaco, J.A., and Louise S.C., "Disaster Recovery Planning: Suggestions to Top Management," *Journal of Systems Management*, 45(5), May 1994, 28-34.