Success factors for IS disaster recovery planning in Hong Kong

Wing S. Chow
Hong Kong Baptist University, Hong Kong

Keywords
Information systems,
Disaster recovery,
Contingency planning, Hong Kong

Abstract
The organization of information technology components into effective enterprise information systems is fast becoming a basic infra-structural and operational necessity for every organization and business sector. These information systems must be well managed, cost-efficient, legal, and safe. There is a growing reliance upon IT in many organizations to the point of mission-criticality. Ideas from disaster recovery planning (DRP) can and should be applied to installed information systems and the new information services whose continuous and reliable functioning may be vital to the organization. This paper reviews the literature concerning the factors that have been identified as essential to the development of DRPs in organizations. As a result of a survey study of four business sectors in Hong Kong: banking, manufacturing, trading, and hotels – the top five critical factors for a successful DRP in information systems are identified with the preferred patterns of DRP identical for three of these sectors.

Information Management & Computer Security
8/2 [2000] 80–86

[ISSN 0968-5227]

Introduction

Information technology and the design, installation, and management of enterprise information systems (ISs) are becoming a basic infra-structural and operational necessity for every organization and business sector. Two factors have played an important role in information service functions (ISF) in organizations. Firstly, the improvement of the cost and power of computer hardware and software has elevated the demand for computer-based IS for organizations. Secondly, organizations are coming to realize the competitive advantage which IS offer to them. As organizations become increasingly dependent on IS for daily operations, mechanisms for dealing with malfunctions, crashes, and disruptions must be factored in. A malfunction may lead to degradation of services or even permanent loss of business if the duration and extent of the disruption are extensive (Yiu and Tse, 1995). Banking, for example, is heavily reliant on on-line systems to process transactions, so that when the system fails, business is halted. Other consequences include loss in profits, and damage to the reputation of that organization, its competitive advantage, and market share (Wong *et al.*, 1994). These potential losses consequent upon failure of and reliance upon an IS cannot be overlooked by an organization and what is required is a pragmatic combination of awareness and planning.

As a result of increasing dependence on IS in the business environment, a serious threat can become a disaster. The term "disaster" here goes beyond natural disaster. Snoyer and Fischer (1993) have defined disaster as "an event that is likely to cause significant disruption in an organization's operations for a period of time". Arnell (1990) defined disaster as "any event that can cause a significant disruption in the information services capabilities for a period of time and affect the operation of the organization" and suggested that "the purposes of DRP are to minimize financial losses, maintain the continuity of operations, ensure the integrity of data, and restore normal operations in a timely, cost-effective manner".

The quality of the decisions made in a crisis and under pressure is not likely to be as good as when made with time to consider all possible options. Disaster recovery planning (DRP) must become figured as a necessity for businesses that become heavily dependent on IS, since it can help to prevent the losses that are caused by a disaster. The (pre-emptive) development and testing of an effective DRP, in advance, is the most critical element in helping organizations to survive a disaster (Paradine, 1995). Thus, the development of DRP in ISF plays a crucial role in business continuity.

This paper reports on the critical success factors for the development of DRP in ISF. Specifically, this paper proposes to identify and rank the top five critical success factors of DRP by surveying the IS professionals from a number of different industries in Hong Kong. The following sections present the DRP literature survey, the study method, results and discussion, and conclusion.

Disaster recovery planning

The term DRP is defined in many different forms in the literature. Hutt *et al.* (1988) have defined it as a concern for computer security that provides alternatives for businesses facing contingency events that could be detrimental to the functions normally performed. Rosenthal and Sheinink (1993) regarded DRP as an arrangement for emergency business and data center operations together with recovery planning following a disaster. According to Paradine

(1995), DRP is a plan, which allows installation to former business status when it suffers some kind of major damage or other disastrous event. Yiu and Tse (1995) have defined DRP as a set of procedures that are used to ensure the recovery of relevant information within an affordable downtime when a disaster strikes.

Although there are many references in the literature describing procedures for the development of DRP, it is not the intention of this paper to review them all in detail here. Rather, this section is intended to identify and cluster common ideas gleaned into a proper category of DRP success factors.

In general, the following 17 success factors of DRP can be summarized from literature:

1 *Top management commitment*. DRP is a long-term planning activity that involves a significant capital investment by an organization, thus only top management commitment can ensure the ongoing provision of resources and money for developing, maintaining, and testing the DRP plan (Rothstein, 1988). Rohde and Haskett (1990) claim that staff will only take DRP seriously if it is clear that management has made a total commitment to the plan.

2 *Adequate financial support*. The greatest barrier to launching a successful DRP is the cost associated with the development and maintenance of the DRP. The reason is that the associated cost of DRP is deemed too great and DRP has no immediate return on investment. Therefore, adequate financial support must be obtained so as to make DRP a success (Lee and Ross, 1995). Rosenthal and Sheiniuk (1993) also concurred that the initial step in any DRP program is to obtain the substantial funding normally required.

3 *Alignment of DRP objectives with company's goals*. The initial phase of DRP must define and establish the objectives that are aligned with the goals of company (Hutt *et al.*, 1988). The objectives of DRP can serve as a basic guide for the development of the plan whose detail and manner are effective and consistent with management's intentions. Snoyer and Fischer (1993) have further explained that DRP is a corporate-wide issue which incurs much cost, thus it is essential to set the scope and objectives of the plan aligned with the corporate mission so that this will prevent a loss of focus which can result in a plan that deviates from its mission.

4 *Adoption of project management techniques*. A work plan and schedule must be formulated to manage the DRP properly. The purpose of project management techniques is to clearly identify events such as project tasks to be completed, person-in-charge for the completion of project, the time frame or schedule of tasks, start and completion activities, and the budgets for each task. Thus, the planning process would be properly controlled and completed within the schedule and the budget (Snoyer and Fischer, 1993).

5 *Presence of a formal recovery planning committee*. A formal recovery planning committee must be appointed by top management because some issues of the DRP development may affect a number of functions in a company and that integration and coordination between functional units is needed (Rohde and Haskett, 1990). In addition, Hutt *et al.* (1988) also concluded that it is important to establish an authority to be responsible for developing and implementing the plan and to foster co-operation across all organizational functions.

6 *Participation of representatives from each department*. Representatives from various departments throughout the organization should participate in a formal recovery planning committee because the respective representatives are more familiar with the functions of their own functional unit (Wong *et al.*, 1994).

7 *Engagement of external consultant*. The appointment of the external consultant is crucial to the integrity of the plan because the use of external consultant to review the technical, technological, business, or organizational aspects of the DRP may detect weaknesses that may not be too obvious to the internal staff. The involvement of a combination of in-house staff and outside consultants to develop the plan is often effective since it will offer the opportunity to capitalize on outside expertise (Hutt *et al.*, 1988).

8 *Risk assessment and impact analysis*. DRP must be specific and tailor-made for a particular company. In order to have a cost-effective DRP, risk assessment and impact analysis must be performed prior to choosing a recovery strategy. The risk assessment considers all possible threats to the IS, such as natural disaster, hardware and software failure, and human error. The impact analysis evaluates the consequences of an IS disaster in each functional area of the business and assesses the maximum allowable IS downtime (Wong *et al.*, 1994). Management must assess the

vulnerability of the business and the importance of the IS by conducting risk assessment and impact analysis, and then decide the type of effort that should be put into the backup of the computer function (Arnell, 1990).

9 *Determination of maximum allowable IS downtime*. When the maximum allowable IS downtime is determined, management will be much more inclined to defend the resources required to maintain the recovery facilities, and to plan as necessaryto enable recovery within the tolerance period. By knowing the maximum allowable IS downtime, organizations will either not over-invest or under-invest in recovery facilities such as hot sites and cold sites (Wong *et al.*, 1994).

10 *Prioritization of IS applications*. All IS applications are not equally important and susceptible to disruption, thus each IS application should have a different degree of protective level in the DRP. Due to the heavy cost requirement for maintaining a complete duplication of all hardware, software, and people, it is necessary to prioritize IS components (Lee and Ross, 1995). The prioritization should be based on how each application affects the ability of an organization to achieve its mission. Mission-critical applications should be given the highest priority.

11 *Off-site storage of backup*. Off-site storage, such as backup hardware, software, data files, and source documents, is a vital part of effective DRP because it allows a company to recover their relevant information if a disaster strikes. Arnell (1990) further pointed that the location of such an off-site storage should be located in a place that is far enough from the company so that the likelihood of being affected by the same disaster is greatly reduced. Another issue which needs to be addressed in off-site storage is that a dispatching system for transfer materials should also be carefully established.

12 *Presence of emergency response procedures*. Emergency response procedures, which is a set of prepared actions to cope initially with disruption, is an important element of DRP since the initial response to an emergency can be the critical factor affecting its ultimate outcome. The entire staff should know who is responsible and what action is expected in an emergency. In addition, the format and presentation of the procedures must be clear enough to assure ease of use by all users (Hutt *et al.*, 1988).

13 *Training of recovery personnel*. Recovery team members must clearly understand their responsibilities and must be adequately trained beforehand to ensure smooth and quick implementation of the DRP. The key personnel to carry out the procedures must be adequately trained and kept up to date as the procedures have changed (Hutt *et al.*, 1988). The recovery personnel must be knowledgeable of their own specific duties and must be adequately trained beforehand so that they have the ability to act independently to solve problems in the event of a disaster (Lee and Ross, 1995).

14 *Appropriate backup site*. Selecting an alternative site for computer operations is crucial in DRP since the original site is no longer feasible in the event of a disaster (Yiu and Tse, 1995). There are various backup site options, such as hot site, cold site, service bureau, and reciprocal agreements. All options have their own trade-off. It is possible to choose an appropriate backup site depending on the degree of business dependency on computers and the length of maximum allowable downtime (Wong *et al.*, 1994).

15 *Periodical testing of DRP*. A DRP becomes obsolete very quickly if it is not periodically tested. Therefore, a series of test programs needs to be developed and conducted to make sure the DRP is complete and accurate. Snoyer and Fischer (1993) pointed out that changes in personnel, job function, technology, physical site layout, and the social-economic environment might alter various emergency policies and procedures within the plan. Therefore, a continuous review and evaluation of the DRP is necessary in order to keep the plan as valid and effective at all times.

16 *Maintenance of DRP*. An effective DRP should be maintained on an ongoing basis. The plan would become outdated when new applications or changes of business strategy are introduced. Therefore, the plan should be updated to reflect the changes. Due to ever changing IS technology, the DRP should be reviewed as often as possible. With an obsolete plan, an organization may not recover when disaster strikes (Lee and Ross, 1995). Changes in business strategy, hardware, or software will demand a review of the plan soon after the implementation of the changes.

17 *Insurance coverage for IS loss*. Insurance on its own does nothing to prevent disaster, but it can help to compensate for some forms of losses incurred in the

disaster (Paradine, 1995). The benefit of insurance is that it will provide funds to reduce the financial impact of a loss in information processing. When a disaster strikes, the "ability to pay" to emergency supplies comes into question. If an effective insurance policy is in place, concerns about "ability to pay" will be overcome.

The study method

Data collection procedures

A structured questionnaire with a covering letter was used to collect data through direct mail. The sample for this study consisted of 400 companies from a cross-section of four industries: banking, hotel, trading, and manufacturing. A total of 98 completed questionnaires (i.e. 24.5 per cent) were returned. All of our respondents were the managers of MIS/EDP departments who were actively participating in DRP in their firms. Table I reveals the general background of our respondents.

Measures

The list of measurement was developed based on 17 factors that were reviewed from the last section. All these factors were identified as the relevant issues in literature. Therefore, instead of evaluating its relevance, we asked our respondents to rate them according to the following criterion: respondents were asked to identify the top five critical success factors when a DRP is developed in their company, and rank them accordingly. To ease a better understanding of the result, we further split the original factor of "risk assessment and impact analysis" into two separated factors, namely "risk analysis" and "impact analysis". In conclusion, a total of 18 factors were adopted in our questionnaire. Each of these 18 factors is clearly denoted in the respective tables in the following sections.

Data analysis

All collected data were saved into a database. In analyzing the data, a ranking method proposed by Chow and Luk (1996) was adopted. They have proposed an effective method in identifying the top five ranking orders of voted factors. The proposed ranking method by the latter paper can be generally described in the following four steps.

1. Step 1: tabulate all cast votes for each ranking.
2. Step 2: select the factor that has the highest cast vote and denotes it as the top rank order.
3. Step 3: add the cast votes of those unchosen factors in the above step to the second rank.
4. Step 4: repeat the above two steps until all ranking orders are identified.

This procedure is further illustrated in the following section. Readers who are interested in the rationale and justification of the proposed procedure may refer to the paper of Chow and Luk (1996).

Table I
Background information of our samples

	No. of respondents	Percentage #
Type of industries		
Banking	30	30.6
Manufacturing	18	18.4
Trading	23	23.5
Hotel	27	27.6
Educational level		
Post-secondary	7	7.1
Degree holders	52	53.1
Post graduate degree	39	39.8
Years of experience		
Less than 1 year	7	7.1
1 to 3 years	40	40.8
4 to 6 years	27	27.6
7 to 10 years	18	18.4
Over 10 years	6	6.1
Size of companies		
Less than 200	31	31.6
200 to 500	32	32.7
Over 500	35	35.7

sample size = 98

Results and discussion

Table II shows the votes cast for each success factor. The columns and rows in this table represent the respective DRP success factors and rank orders. In this table, each rank order (except for rank order 1) represents three values. Value "a" represents the total of cast votes; value "b" is the grand total number of cast votes summed up from the rank order 1 to the present rank. Value "c" with a symbol "*" denotes the factor that was chosen for that rank. The top five critical success factors for the development of DRP were reported in the following orders:

1 "F1" = top management committee,
2 "F17" = adequate financial support,
3 "F11" = appropriate backup site,
4 "F8" = off-site storage of backup; and
5 "F13" = training of recovery personnel.

The top five critical success factors identified in Table II were reported as coherently meaningful and logical. For instance, the "top management support" is a crucial factor for the success of DRP for two reasons. First, it is a form of long-term planning because information is now a corporate asset for which the development of DRP for IS becomes a corporate-wide issue. Second, DRP involves an ongoing capital expenditure that may be in a form of acquisition of software, hardware, workplace, and/or manpower. Therefore, "adequate financial support" is a must. An additional requirement for launching the DRP in our findings is a safe location in which the valuable information should be kept so that it can be retrieved when needed. The two most common storage places are:

1 on-site location – that is, information is kept within the company;
2 off-site location – that is, information is kept at a place where the location does not inherit a similar environment condition as the present company.

The result showed that both of these storage places are considered as significant.

We further elaborate the results of Table II to include the pattern of preferred order for each industry by manipulating the database. We believe that the latter result provides us with an in-depth understanding of the behavior in each industry. Table III illustrates the preferences for the proposed four industries. The "overall" in this table represents the result of Table II.

Despite the ordering, there are two sets of preference lists that can be clearly identified from Table III. The first set, which applied to the industries of banking, manufacturing, and trading, is reported as "F1" = top management commitment, "F11" = appropriate backup site, "F8" = off-site storage of backup, "F13" = training of recovering personnel, and "F17" = adequate financial support. Whereas, the second set which only applied to the hotel industry is shown as "F1" = top management support, "F17" = adequate financial support, "F12" = presence of emergency response procedures,

Table II
The top-five critical success factors of DRP in ISF success factors #

Rank order		F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14	F15	F16	F17	F18	Total
1	**a**	48	2	3	3	0	2	0	5	0	0	9	6	0	2	2	2	11	3	98
	c	*																		
2	**a**	0	8	2	5	5	4	2	12	0	3	14	6	9	6	0	6	16	0	98
	b	–	10	5	8	5	6	2	17	0	3	23	12	9	8	2	8	27	3	
	c																	*		
3	**a**	9	2	0	18	5	2	3	10	0	0	9	9	12	9	0	3	0	7	98
	b	–	12	5	26	10	8	5	27	0	3	32	21	21	17	2	11	–	10	
	c											*								
4	**a**	7	0	12	7	4	4	0	9	4	0	8	2	13	7	14	2	5	0	98
	b	–	12	17	33	14	12	5	36	4	3	–	23	34	24	16	13	–	10	
	c								*											
5	**a**	6	0	0	3	6	5	3	11	2	6	4	10	5	10	14	0	13	0	98
	b	–	12	17	36	20	17	8	–	6	9	–	33	39	34	30	13	–	10	
	c													*						

where: F1 = top management commitment; F2 = presence of formal recovery planning; F3 = prioritisation of critical applications; F4 = risk assessment; F5 = impact analysis; F6 = determination of maximum allowable IS downtime; F7 = insurance coverage for IS loss; F8 = off-site storage of backup; F9 = participation of representatives from each department; F10 = engagement of external consultant; F11 = appropriate backup site; F12 = presence of emergency response procedures; F13 = training of recovery personnel; F14 = periodical testing of DRP; F15 = maintenance of the DRP; F16 = alignment of DRP objective with goals of company; F17 = adequate financial support, and F18 = adoption of project management techniques

Table III
DRP priority list for the four different industries

Rank order	Overall	Success factors# Banking	Manufacturing	Trading	Hotel
1	F1	F1	F1	F1	F1
2	F17	F11	F11	F17	F17
3	F11	F8	F13	F11	F12
4	F8	F13	F17	F8	F4
5	F13	F17	F8	F13	F15

where: F1 = top management commitment; F2 = presence of formal recovery planning; F3 = prioritisation of critical applications; F4 = risk assessment; F5 = impact analysis; F6 = determination of maximum allowable IS downtime; F7 = insurance coverage for IS loss; F8 = off-site storage of backup; F9 = participation of representatives from each department; F10 = engagement of external consultant; F11 = appropriate backup site; F12 = presence of emergency response procedures; F13 = training of recovery personnel; F14 = periodical testing of DRP; F15 = maintenance of the DRP; F16 = alignment of DRP objective with goals of company; F17 = adequate financial support, and F18 = adoption of project management techniques

"F4" = risk assessment, and "F15" = maintenance of the DRP. The two common factors reported from the two lists are "F1" = top management support, and "F17" = adequate financial support. In the following, reasons for which the different sets of preferred top five DRP success factors were chosen by the two groups of industries are provided.

In the first group of industries, the nature of competition in their businesses is rather keen. Their survival is dependent on how well they can compete. One way of reaching a competitive advantage over their competitors is implementing computerization. The latter practice enables them to gain access to valuable information so that effective decision making or transactions can be made. In fact, the companies of all the participants in this study are fully committed to computerization. The ability to retrieve valuable information when a disaster strikes becomes a crucial element of retaining their competitive power. Therefore, it is not a surprise to reveal in our result that this group of industries chooses the following factors as three of the top five critical success factors for DRP: "F11" = appropriate backup site, and "F8" = off-site storage backup, "F13" = training of recovery personnel. The ranking order of these factors is quite dependent on the nature of industry. For instance, banking is heavily dependent on their databases for daily transactions, thus factors "F11" and "F8" are ranked as more critical than factors "F13" and "F17". On the other hand, factor "F8" (= off-site storage of backup) is ranked as fifth place for manufacturing because such a practice is not commonly adopted in this industry. One note for the trading industry in Hong Kong is that their computer systems are mostly provided by and designed by a software house, which trains in-house recovery personnel. Although this is considered as significant, it is ranked as the fifth place.

The above explanation for the first group of industries, also applies to the hotel industry except that their meanings are placed in reverse. This observation is further elaborated here. The nature of business for the hotel industry is dependent on the performance of the local tourism industry as well as the demand for its hotel accommodation. In a report, the Hong Kong Tourist Association (HKTA) indicated that the total number of visitors for 1996 was estimated at 11 million and its annual growth rate was about 8 per cent. It was also further estimated that the total number of rooms available in 1996 was less than 350,000 a day. (Note: this figure is confined to HKTA member hotels, hostels' and guesthouses only). In other words, the hotel occupancy rate is reached at 85 per cent a year. Given the fact that land is costly in Hong Kong, and there is nothing to indicate that the growth rate of available rooms would be increased substantially, the competition in this industry is thus concluded to be very low. In this respect, the adoption of computerization to improve their competitive power is less important. In Hong Kong, the only hotels that are noticeably implementing computerization are those hotels that are newly built and owned by a corporation; otherwise only computer-based accounting systems are used. Since the operational functions of the hotel industry are not fully computerized, the awareness of DRP in IS is also not fully appreciated. It is therefore revealed in our result that the method of data storage is not considered as one of the five most important DRP success factors (Tobin, 1995).

Information Management & Computer Security
8/2 [2000] 80–86

Conclusion

Modern organizations are nowadays becoming heavily dependent on IS that are provided by ISF to achieve competitive advantage. Awareness and the pre-emptive development of operational strategies for recovery from the failure in IT systems is vital and becoming more important. The development of DRP in ISF becomes an important issue.

The paper identified the top five critical success factors for developing a DRP in ISF. The preferred order of top five critical success factors may vary for different industries. This paper compares the preferred pattern of DRP in four industries; namely banking, manufacturing, trading, and hotel. It was generally reviewed in this paper that the first three types of industries chose a similar set of priorities; however the hotel industry selects a different pattern because of its unique environment in our sampling. It is, however, clear that other factors which did not fall into our selection criterion should also be considered when developing a DRP.

With many enterprise IS becoming based on networks of PCs, the importance of issues such as hardware and software quality and reliability must be confronted in any serious planning. PCs are not very manageable; mainframes are more reliable than PC-based client-server systems. The first PCs were more reliable because they were simpler; the problem started when PCs became more complex – users seem to have an insatiable demand for more bells and whistles whether they use them or not (see *Byte Magazine* cover story "Crash-proof computing", April 1988, reported by Tom R. Halfhill). Alternative, more robust client-server hardware and the Unix OS provide a viable alternative. The standardization on C/C++ 10 years ago in the IT industry for commercial software development has created a mountain of buggy software; too much beta-test software and too little quality assurances in the race to update modern languages – Delphi, VB etc. and purer object-oriented languages such as Java and Eiffel include memory management and garbage collection and are superior and safer. Realistically however – developers will continue to write bigger programs that ship before they are ready. Operating Systems will continue to grow more complicated. Users will continue to vote with their dollars for feature-laden software. Established platforms and applications will continue to overshadow radical alternatives. The shortest path to stability is simplicity; simpler hardware, simpler software, simpler user interfaces – demanding a whole new way of thinking, as claimed by the Director of MIT Lab for Computer Science. A better management on this aspect of hardware and software will also help a better planning for DRP in ISF.

References

Arnell, A. (1990), *Handbook of Effective Disaster/Recovery Planning*, McGraw-Hill Pub. Co., New York, NY, p. 333.

Chow, W.S. and Luk, V.W.M. (1996), "Management in the 1990s: a comparative study of women managers in China and Hong Kong", *Journal of Managerial Psychology*, Vol. 11 No. 1, pp. 24-36.

Hutt, A.E., Bosworth, S. and Hoyt, D.B. (1988), *Computer Security Handbook, 2nd ed.*, Macmillan Pub. Co., New York, NY, p. 399.

Lee, S. and Ross, S. (1995), "Disaster recovery planning for information systems", *Information Resources Management Journal*, Summer, pp. 18-23.

Paradine, T.J. (1995), "Business interruption insurance: a vital ingredient in your disaster recovery plan", *Information Management & Computer Security*, Vol. 3 No. 1, pp. 9-17.

Rohde, R. and Haskett, J. (1990), "Disaster recovery planning for academic computing centers", *Communications of the ACM*, Vol. 33 No. 6, pp. 652-7.

Rosenthal, P.H. and Sheiniuk, G. (1993), "Business resumption planning exercising the disaster management team", *Journal of Systems Management*, June, pp. 12-16, 38-42.

Rothstein, P.J. (1988), "Up and running: how to ensure disaster recovery", *Datamation*, Vol. 34 No. 20, pp. 86-96.

Snoyer, R.S. and Fischer, G.A. (Eds) (1993), *Managing Microcomputer Security,* Business One, Irwin, Homewood, IL, p. 431.

Tobin, M. (1995), "Keep a network disruption from becoming a workgroup computing disaster", *Managing Office Technology*, Vol. 40 No. 10, pp. 36-7.

Wong, B.K., Monaco, J.A. and Sellaro, C.L. (1994), "Disaster recovery planning: suggestions to top management and information systems managers", *Journal of Systems Management*, Vol. 45 No. 5, pp. 28-33.

Yiu, K. and Tse, Y.Y. (1995), "A model for disaster recovery planning", *IS Audit & Control Journal*, Vol. 5, pp. 45-51.