Disaster Contingency Recovery Planning (DCRP): Management Role

Ku Maisurah Ku Bahador, Raudah Danila
Faculty of Accountancy, Universiti Utara Malaysia

ABSTRACT

This paper presents an analysis of selected MSC companies in a survey of Disaster Contingency Recovery Planning (DCRP). In particular, it examines the role of management in planning and setting priorities for contingency planning, especially in those organizations that have specified IT is vertical to business operations. At present, the level of adoption of DCRP in Malaysia is moderate. Only 40.4% of the companies are currently implementing the DCRP plan. However, it is believed that there would be a rapid development in DCRP in future based on the fact that the respondents perceived the benefits outweigh the barriers

1.0 PURPOSE AND OBJECTIVES OF STUDY

The increasing importance and sophistication of computer systems in data processing are spurring many organizations to emphasize information security practices aimed at helping them quickly regain access to data in the event of natural or man-made disaster. Getting management to understand the importance of information technology security measures is a big task faced by a security administrator. Many nontechnical managers often view IT contingency plan as a way to spend funds with little chance for a return on investment. Therefore, an IT security measures are often the first line items to be cut from the budget. However armed with the knowledge of the firm's IT and its greatest known vulnerability points, understanding how earthquake, floods, bombings and other natural and human-made disasters may occur throughout the firm and the rest of the world. Recovering from a disaster quickly is crucial to a firm's survival as a going concern, thus a disaster contingency and recovery plan must be prepared to survive a severe crisis. The plan provides guidelines that, if followed, enable a firm to minimize damage and restore both its computer operations and regular business operations.

A disaster contingency and recovery plan (DCRP) is a comprehensive plan for recovering from natural and human-made disasters that affect not only a firm's computer processing capabilities but also its critical business operations. Often these disasters completely shut down operations. The longer a firm's operations are shut down, the more likely it will never reopen the business. Studies have conclusively demonstrated that a comprehensive DCRP must be prepared to survive a severe crisis.

Several examples which in case of natural or man made disaster have highlighted the importance of the DCRP. The 11 September tragedy in the USA has provided a wake up call to remind businesses of the need for adequate disaster recovery and business continuity planning. The attack had also caused many organizations to move DCRP from nice to have to should have, some have even moved to must have and are starting to take actions. Some industry sectors which are more reliant on technology to run their business have leaded the way to have a comprehensive and up to date DCRP.

Therefore this study is conducted firstly to explore management awareness towards the importance of a DCRP in Malaysia setting. Secondly, this study examines the role of management in planning and setting priorities for contingency planning especially in those organizations that have specified that IT is critical to the business operations.

The results of this study are useful to explain whether Malaysian companies are taking the risks to their business and IT seriously. This study also provides an input to the regulator body such as Multimedia Development Corporation (MDC) on whether they should set DCRP as one of criterion of MSC status companies.

As for the industry, the findings are likely to provide awareness among the managers thus stimulate the companies to plan interventions such as education, workshops and self-assessment schedules on DCRP. Moreover, the outcomes of the study contribute in cultivating DCRP culture not only among the private sector but also the government bodies which are marching towards the era of Information, Communication and Technology (ICT). Furthermore, in Malaysia, few studies were done on the management perceptions and awareness of DCRP, therefore this study was conducted to fill the gap in DCRP research subsequently make some contribution to the accounting information systems literature.

2.0 LITERATURE REVIEW

Disaster recovery (DR) ensures that data are automatically backed-up, restored or recovered in the event of a disaster, accident or other failure. The ultimate goal is that historical data are automatically accessible and reside on the right media while storage space is consistently available. (Alberto Petroni, 1999).

Department of Information Michigan (2003) defined A Disaster Recovery Plan (DRP) is the documentation that delineates all the roles and responsibilities for staff, along with the steps that must be taken to successfully move the production processing performed at the site of the disaster to the Disaster Recovery site. Kweku-Muata (Noel)

Bryson2002 explained DRP is made up of procedures and rules that utilize solution resources (e.g. hot sites) that are aimed at protecting and/or reviving target organizational resources, functions, or processes (e.g. information systems)

DCRP Awareness

In an Ernst & Young-Computerworld Global Information Security Survey of 4,255 IT and information security managers, 84 percent of them said that their senior management believes that security management is *important* or *extremely important*. Out of these respondents, over 50 percent of them stated that they lack a disaster recovery plan (Anthes, 1998). However, most of the problems stem from the lack of communication at the corporate level (Steve M.Hawkins, 2000).

Moreover, according to Panettieri (1995), in the third annual information security survey conducted by Information Week and Ernst & Young, nearly half of the more than 1,290 respondents representing information systems chiefs and security managers suffered security-related financial losses in the past two years. Most companies hesitate to develop a disaster recovery plan until a disaster occurs. According to another survey done by Patrowicz (1998), 85 percent of the Fortune 1,000 companies have disaster recovery plans. Within these companies which have disaster recovery plans, 80 percent have plans that protect their data center resources, 50 percent have plans that protect their networks, and less than 35 percent have plans that protect their data on PC LANs.

McGaughey *et a*l.(1994) said that despite contingency planning, top management control concerns that continue to increase in importance. Moreover, although many companies rely increasingly on computer systems to run critical elements of their businesses, managers' awareness is somehow still inadequate as some have not taken steps to ensure continuous access to their systems. Traditions abound about the problems in instituting disaster recovery or business continuity plans is that there are small and even medium-sized businesses often dismiss the need prematurely. A recent study by Eastwood (1995), found that less than one in four senior managers rate systems security as extremely important. Over 40 percent view it as somewhat important or not important at all.

Hoffman (1998) in his study found that another survey done in 1993 of 200 senior executives at companies with average annual revenue of $2.5 billion, 41 percent did not have a disaster recovery plan in place at their organizations. Furthermore, nearly half of the IS professionals who responded to a recent Business Research Group survey said their companies must have their mission-critical applications running 24 hours a day, but roughly 30 percent of the survey's respondents do not have a disaster recovery plan in place. On average, larger corporations spend up to 6 percent of their information technology budget on consulting, applications software or outsourcing that is related to disaster recovery planning. Finally, it is also worth mentioning the empirical findings of a survey conducted by the Defense Information Systems Agency, that after evaluating recovery plans at 16 Defense Department data processing mega-centers, concluded that most of the centers were not prepared for large scale disasters.

Benefits of developing a DCRP

According to Steve M. Hawkins (2000), in his article *Disaster recovery planning: a Strategy for data security*, developing of DRP or DCRP is to identify various steps to assist an organization in recovering from data losses and restoring data assets. This process generates the at least seven benefits. Firstly, it helps to e*liminating possible confusion and error.* Secondly, it helps in *reducing disruptions to corporate operations.* Besides, DRP also *provides alternatives during a disastrous event.* needed to consider all of the alternatives and choices for disaster recovery. Furthermore, having a DRP can assist an organization to *reduce the reliance on certain key individuals.* The most critical benefit is *protecting the data of the organization.*

When a disaster demolishes the building, corporate offices need to be relocated. A DRP could also include a logistical support group that would provide comprehensive support to employees. A disaster recovery plan covers most of the problems that could happen during a disaster and it provides the necessary resources to solve those problems, while management can focus its attention to other critical issues. In other words, a DRP assists in e*nsuring the safety of company personnel*

3.0 INDUSTRIAL PROFILE

This research is carried out as a market based research. The subject that made up the study population are all the MSC listed companies. The Multimedia Super Corridor (MSC) is an initiative by the Government of Malaysia to create the world's first integrated environment with all unique elements and attributes needed to build a global multimedia hub.

The MSC is physically located in a Greenfield corridor of 15km wide by 50 km long, stretching from the Kuala Lumpur City Centre (KLCC) to the Kuala Lumpur International Airport (KLIA). Among others, the MSC houses 5 MSC Cybercities – Cyberjaya, Technology Park Malaysia (TPM), Kuala Lumpur City Centre (KLCC), UPM_MTDC and KL Tower (MDC, 2003).

The reason we chose the MSC status company is because it is assumed that these companies are equipped with significant computer configuration. In other words, they are highly dependent on IT that should be protecting their business most thoroughly. In relation to this, the listing of MSC company (http://www.msc.com.mt/cs/company) were reviewed.

Subjects and Population

From the existing records, as at December 1, 2004, it appears that there are a total of 1146 listed companies, 67 of which are world class. Out of 1146 MSC status companies, 481 companies which are located at the five Cybercities area were sent online questionnaires. Only a total of 6 companies responded to the survey. 97 questionnaires were bounced due to technical reasons while 397 remain unreplied. The reason for the silence may due to the fact that some of these companies were either moved elsewhere or changed their e-mail address.

After receiving such a poor response, we decided to run the fieldwork by sending the questionnaires by hand. Because of financial and time constraints, we limit our visit to only two cyber cities area namely Cyberjaya and UPM_MTDC. At least 100 questionnaires were sent door to door. As a result, we managed to interview 9 companies and collected 44 completed questionnaires. After went through the replied questionnaires, 12 were considered incomplete.

Hence, only 47 companies were successfully surveyed in this study. Since the number of MSC companies located in both Cyberjaya and UPM_MTDC is 277, this make the response rate touched 16.9%. to make this study valid, we thus changed our strategy; instead of analyzing the population of MSC companies, we only focused on companies that are located in Cyberjaya as well as the UPM_MTDC area.

From the survey, the companies are owned by both Bumiputra and non-Bumiputra companies (who consisted of Chinese, Indians and foreigner from the USA, Canada and Russia). All the companies were involved in the Multimedia Super Corridor with a maximum capital of RM500,000 each and all were registered under private companies. Their entrepreneurial products and services mostly varied from application software, call center and data center services, internet services, industry specific software application, engineering design services, telecommunication products and services, entertainment content and programs as well as software integration, implementation and support services.

4.0 RESEARCH DESIGN

To achieve the study objectives, data were collected using both online and manual questionnaires. We intended to go online due to the facts that we believe that being fully IT based companies, the respondents have all the facilities that enable them answering online. In fact, this paperless method would be more convenience and time saving to researchers as well as the respondents. Somehow, due to the poor response rate , we went to the company ourselves.

It contains questions in the following categories; demographic, experienced contingencies, attitudes to planning, actual planning and backup procedures. We also looked this matter through consideration of three main aspects; experienced contingencies, plan management and relationship to other risks. The target person were the CEO or the MD since in our opinion the overall business contingency planning needs will be the responsibility of the senior executives. The questionnaires were also extended to the IT manager or contingency manager.

5.0 DATA ANALYSIS

This study employed descriptive analysis to analyze the data. Statistical techniques such as frequency tables and figures were used to describe the information such as the percentage of companies that have and do not have DCRP and other relevant information.

The responses of the 47 companies to the questionnaire were scored and raw data obtained using the online database (Microsoft Acces). These data were then converted to Microsoft excel spreadsheet to enable these data to be imported to SPSS.

This study examines the awareness and experiences of MSC listed companies on DCRP. A total of 481 questionnaires have been sent through online to MSC listed companies. Unfortunately, only 97 questionnaires were bounced due to technical problem or changes of email address. After sending in manually, we managed to get 41 completed questionnaires. As a result, 47 companies were effectively surveyed in this study representing a respond rate of 16.9%.

In chapter 4, the findings of the survey are discussed. Section 1 explains the demographic details of the companies that responded. Section 2 provides findings for DCRP implementation. The interruptions experienced by the companies are then discussed in Section 3. Next, Section 4 elaborates the management awareness towards DCRP.

Demographic

Table 1: Summary of the respondent's details, n=47

	Variables	Frequency	%
Gender	Male	35	74.5
	Female	12	25.5
Race	Malay	11	23.4
	Chinese	20	42.6
	Indian	5	10.6
	Others	11	23.4
Religion	Muslim	11	23.4
	Buddha	12	25.5
	Hindu	4	8.5
	Christian	7	14.9
	Others	13	27.6
Age	Under 30	23	48.9
	30 - 39	17	36.1
	Above 40	7	14.8
Education	Diploma	2	4.2
	Bachelor Degree	35	74.5
	Masters	10	21.3
Post	Top Management	7	14.9
	IT Manager	25	53.2
	Staff Members	15	32
Working Experience	Less than 5 years	22	46.8
	5 - 9 years	20	42.5
	10 - 15 years	2	4.2
	More than 15 years	3	6.3

A summary of the respondent's details is reported in Table 1. The sample suggests that about 74.5 % of the respondents are males and 25.5% of them are females. 42.6% of the sample are Chinese, 23.4% are Malays, 10.6% are Indians and another 23.4% are from others likes foreigners from another countries. The age ranges for respondents were that 48.9% of them had age below 30 years, 36.1% had age ranged between 30 to 39 years, and 14.8% had age over 40 years.

The education levels of respondents are 74.5% per cent had obtained Bachelor Degree while 21.3% had obtained Master Degree. The remaining 4.2% score for Diploma holder. Finally, the findings on working experience shows that most of respondents had 46.8% per cent of less than 5 years while 42.5% per cent were had 5 to 6 years. However the remaining had 6.3% working experience on more than 15 years and only 4.2% on 10 to 15 years.

DCRP Implementations

Based on our survey results, of the 47 respondents, 40.4% of the companies claimed they have DCRP while remaining 59.6% are found not having DCRP.

Table 2: Companies having or not having DCRP plans, n=47

	Frequency	Percent
Yes	19	40.4
No	28	59.6
Total	47	100

Table 3: Companies have started implementing DCRP plans, n=19

Variables	Frequency	Percent
Less than 1 year	11	57.9
1 - 5 years	6	31.6
6 - 10 years	2	10.5
Total	**19**	**100**

In terms of duration, only 10.5% company with DCRP established for a period of 6-10 years, 31.6% has been established between one to five years, while majority of the respondents (59.7%) are with DCRP established for a period less than one year. A summary of the respondents' demographic profiles is reported in table 4.

Table 4: Cross-tabulation Between Business Industries and Companies implement DCRP, n=19

Industries		Company implement DCRP		Total
		Yes	No	
Industry specific software application	Count	7	6	13
	% within Industries	53.8	46.2	100
	% within Comp have DCRP	36.8	21.4	27.7
	% of Total	14.9	12.8	27.7
Telecommunication products and support services	Count	4	7	11
	% within Industries	36.4	63.6	100
	% within Comp have DCRP	21.1	25	23.4
	% of Total	8.5	14.9	23.4
Internet services	Count	3	3	6
	% within Industries	50	50	100
	% within Comp have DCRP	15.8	10.7	12.8
	% of Total	6.4	6.4	12.8
Software integration and support services	Count	2	3	5
	% within Industries	40	60	100
	% within Comp have DCRP	10.5	10.7	10.7
	% of Total	4.3	6.4	10.7
Others	Count	3	9	12
	% within Industries	25	75	100
	% within Comp have DCRP	15.8	32.1	25.6
	% of Total	6.4	19.2	25.6
Total	Count	19	28	47
	% within Industries	40.4	59.6	100
	% within Comp have DCRP	100	100	100

Management roles of implementing DCRP

In terms of industry, this survey revealed that out of 19 companies' with DCRP, 27.7% are industry specific software application companies, 23.4% are telecommunication products and support services companies, 12.8% are internet services companies, 10.7% are software integration and support services and 5.6% are other companies.

Table 5: Person who most frequently cited as having responsibility for planning and maintaining, n=19

Variables	Frequency	Percent
IT manager	14	73.7
Top Management	1	5.3
Staff members	4	21.1
Total	**19**	**100**

In case of planning and maintaining, substantially 73.7% of the companies have put the responsibility to the IT manager. This findings are inline with the findings done by the Earnest Jordan (1999) where IT manager is the most responsible people for planning and maintaining DCRP. Only 21.1% companies indicated that the staff members should carry the responsibility. However, only 5.3% have the top management conducting the DCRP planning and maintenance.

Table 6: Person who takes responsibility when interruption occurs, n=19

Variables	Frequency	Percent
Top Management	7	36.8
IT Manager	8	42.1
Staff Members	4	21.1
Total	**19**	**100**

The survey questionnaire also asked the in charge person when interruption occurs. It was found that 36.8% positioned top management as the captain at the wheel of the shipwreck (Earnest Jordan, 1999). 42.1% of the companies has put the responsibility on the IT manager while the remaining 21.2% rests it to the staff members.

Table 7: Level confidence has an unreasonable correspondence to the level of preparedness, n=19

Variables	Frequency	Percent
Strongly agree	8	42.1
Agree	10	52.6
Disagree	1	5.3
Total	**19**	**100**

On the questions about how they felt or perceived their DCRP performance/capability, almost half (42.1%) has strongly agree that their DCRP has the high level of readiness to encounter disaster. However, only 5.3% felt that their DCRP are still not reliable enough to protect their companies when disaster occurs. The rest has sensible feeling that their companies can rely on the DCRP in case of emergency.

Experiences of Interruptions

There are wide ranges of interruption that may occur in the operation of a company. Some of them are common interruptions such as power failure, communication line failure and others are extremely rare such as extensive fires, major accidents or bombs (Earnest Jordan, 1999).

Table 8: Types of interruptions, n=47

Variables	Frequency	Percent
Technical Interruption	25	53.2
Man Made Interruption	2	4.2
No Interruption	20	42.6
Total	**47**	**100**

In the survey, the companies were asked whether they have experienced any technical or man made interruptions. Study found that, 25 out of 47 companies (53.2%) had experienced man made interruption while only 2 companies had experienced man made interruption. 20 companies claimed that they never experienced any kind of interruption so far.

Table 9: Experienced of interruptions
Panel A: Technical Interruption, n=25

Technical	Variables	Frequency	Percent	Mean
Number of interruptions in a year	1 - 3 times	19	76	3.06
	4 - 6 times	3	12	
	7 - 10 times	3	12	
	Total	25	100	
Interruptions duration	Less than 1 hour	16	64	3.13
	More than 4 hrs	7	28	
	More than 12 hrs	1	4	
	More than 1 day	1	4	
	Total	25	100	
Time taken to recover	1 day	23	92	2.91
	1 week	2	8	
	Total	25	100	
Area affected	Operational	19	76	3.06
	Others	6	24	
	Total	25	100	

Technical Interruptions

We discussed the technical interruptions experienced by the companies from four aspects as below;

i) Number of interruptions in a year

76% had encountered 1 to 3 times technical interruptions in a year, 12% had 4 to 6 times interruptions and the remaining 12% had 7 to 10 times in a year. From the results, we assumed that the situation is still under control where most of the companies having experienced not more that 3 interruptions in a year. The mean for the year interruptions is 3.06.

ii) Interruptions duration

Survey revealed that 64% of companies had experienced less than one hour technical interruptions, while 28% had more than 4 hours interruptions. Eventually, only 2 companies had experienced long interruptions which is more than 12 hours and 1 day respectively. The mean for interruptions duration is 3.13.

iii) Time taken to recover

92% companies took one day to fully recover from the technical interruptions while 8% took one week to recover form the same interruptions. The mean for recovery time for technical interruptions is 2.91.

iv) Area affected

For most companies, the technical interruptions affected their operational job. The study pointed out that 76% of the interruptions affects operational areas and only 24% affects other area such as customer care and maintenance area. The mean is 3.06.

Panel B: Man Made Interruption, n=2

Man Made	Variables	Frequency	Percent	Mean
Number of interruptions in a year	1 - 3 times	2	100	4.83
	4 - 6 times	0	0	
	7 - 10 times	0	0	
	Total	2	100	
Interruptions duration	Less than 1 hour	0	0	4.96
	More than 4 hrs	0	0	
	More than 12 hrs	0	0	
	More than 1 day	2	100	
	Total	2	100	
Time taken to recover	1month	1	50	4.94
	3 months	1	50	
	Total	2	100	
Area affected	Operational	2	100	3.91
	Others	0	0	
	Total	2	100	

Man Made Interruptions

However, as for man made interruptions, study showed relatively small portion of the companies (4.2%) were involved and the mean is 4.96. These companies experienced at least 1 to 3 times interruptions per year (mean = 4.83) and all the interruptions went on more than 24 hours. With mean 3.91, operational is the area affected and they took one to three months to pick up with the normal condition. (mean = 4.94).

Management Awareness towards DCRP

The main objectives of the survey on this section was to determine the management awareness and their perception towards DCRP.

Table 10: Awareness about DCRP, n=47

	Variables	Frequency	Percent
Heard of DCRP	Yes	26	55.3
	No	21	44.7
Should have DCRP	Yes	41	87.2
	No	6	12.8
Government should regulate DCRP	Yes	29	61.7
	No	18	38.3
Have DCRP	Yes	19	40.4
	No	28	59.6
Total		47	100

The questionnaire asked the respondents to indicate whether they conscious about DCRP and how they perceived the subject. The result discovered that more than half of the respondents (55.3%) apparently claimed that they are aware of DCRP and 44.7% said that they have not heard about DCRP before. However, out of 47 companies interviewed, 40.4% claimed that they do have DCRP while the rest does not even have guideline on what to do in case of disaster occurs. After providing a simple explanation on DCRP, in a different questions, they were asked whether a company should or should not have DCRP, 87.2% of felt that a company should have DCRP. They believe the advantages of having DCRP can aid a company to recover from either natural, technical or man made interruptions. Furthermore, the survey questionnaire asked whether the government should or should not regulate all MSC status companies to have DCRP, 38.3% of the respondents think that the government should not put DCRP as one of requirements on MSC status.. Anyway, the rest have no problem with the issue.

Table 11: Reasons for companies not implementing DCRP plans, n=28

Variables	Frequency	Percent
Insufficient resource	11	39.3
Plan exist but not documented	3	10.7
Being developed but not ready	5	17.9
Low priority	9	32.1
Total	**28**	**100**

Based on the findings in Table 10 above, 51.1% of the respondents found not to have DCRP. When asked what is the reason for not having DCRP, majority of the companies (39.3%) stated because of insufficient resources. Other reasons are low priority on protecting business operations (32.1%), the DCRP is still in development phase (17.9%), and finally DCRP exist but not documented (10.7%).

6.0 DISCUSSION

This study seeks to explore the role of management in planning and setting priorities for DCRP. The results showed that only 19 (40.4%) companies have DCRP plans to protect their business operations. It is assumed that this moderate level mirrored their attitudes towards risky securities issues.

Looking into the Malaysian Government effort through the MSC flagships implementation, the number of MSC companies will increase in the coming years. The greater they depend on the information system, the greater risk they are facing. All companies should have DCRP plan to survive when any form of disaster strikes. They must not wait and see until one of them is attacked by any kind of interruption or disaster.

Furthermore, the awareness towards this matter is still at moderate level and this does not appear to be likely to change in the near future. In Malaysia, the development of contingency plan among companies is still considered at slow pace. This is due to some factors such as insufficient resources (39.2%) and low priority (32.1%). These factors indicate that the management perceptions. In spite of IT being critical to the companies, DCRP is still seen as a cost as well as extra burden rather than a necessity. Adding security measure to the IT simply increases the costs. Most of them agreed that the DCRP benefits the company only during emergency. From this study, most of the companies (76%) experienced only 1 to 3 times technical interruptions within a year and only 2 companies had experienced man-made interruptions within a year. These results showed a big reason why most of the company's managements are not serious in implementing DCRP plans.

As a matter of fact, the costs of implementing DCRP plan are considered high to some companies. Besides incurring the hardware and the software costs, other related costs such as training, maintaining, etc, are also involved in ensuring the implementation of DCRP plan. Thus, many companies tend to be more conservative in spending such big allocation on security of data and information system.

7.0 CONCLUSION

The findings of this study are useful to provide a platform for the present and future study on the DCRP. This study showed that most MSC companies in Cybercities area are adopting DCRP at a slow pace. Only 40.4% of these companies are currently having DCRP plan. However, we do not know much details of how they implement DCRP in their workplace. Fortunately, there are no major interruptions occurred had affect their business operations. So far they only experienced minor interruptions such as power and server failure and theft of information. These factors lead to a moderate development of DCRP plan among the MSC companies. However, it is believed that there will be rapid development in DCRP in future due to the fact that the respondents perceived the benefits outweigh the barriers. An interesting research in the future would include a study on the level of DCRP implementation i.e. simple, medium or more complex structure and policy, by DCRP adopters may shed some lights on the current state of disaster and recovery planning in Malaysia.

REFERENCES

Alberto Petroni (1999) Managing information systems' contingencies in banks: a case study. *Disaster Prevention and Management* Volume 8 · Number 2 · 1999 · pp. 101–110

Brancheau, J.C., Janz, B.D. and Wetherbe, J.C. (1996), "Key issues in information systems management: 1994-5 SIM Delphi results", MIS Quarterly, Vol. 20 No. 2, pp. 225-42.

Coopers and Lybrand (1992), Corporate Security and Contingency Planning, Coopers and Lybrand, Sydney

Eastwood, A. (1995), "End-users: the enemy within?", *Computing Canada*, Vol. 21 No. 1, p. 41.

Ernest Jordan (1999) "IT Contingency Planning: Management Roles". Information *Management & Computer Security* 7/5 [1999] 232±238

Ernst and Young (1996) Information Security Survey 1996, October, Ernst and Young, New York.

Hardy, K (1992), "Contingency planning", Business Quarterly, Vol. 56 No. 4, Spring, pp. 26-8. IBM (1996), A Risk too Far, IBM, London, with Cranfield University, Cranfield, UK.

Hoffman, T. (1998), "Denial stalls disaster recovery plans", Computerworld, Vol. 32 No. 8, p. 10.

Kearvell-White, B. (1996b), "National (UK) computer security survey 1996", Information Management and Computer Security, Vol. 4 No. 3, pp. 3-17

Kelly, C. (1995), "A framework for improving operational effectiveness and cost efficiency in emergency planning and response", *Disaster Prevention and Management*, Vol. 4 No. 3, pp. 25-31.

Kletz, T.A. (1996), "Disaster prevention: current topics", *Disaster Prevention and Management*, Vol. 5 No. 2, pp. 36-41.

Maslen, C. (1996), "Testing a plan is more important than the plan itself", Information Management and Computer Security, Vol. 4 No. 3 pp. 26-9.

McGaughey, R.E., Snyder, C.A. and Carr, H.H. (1994), "Implementing information technology for competitive advantage: risk management issues", *Information and Management*, Vol. 26 No. 5, pp. 273-80.

Steve M.H,David C.Y, David C.C (2000) Disaster recovery planning: a Strategy for Data Security. *Information Management & Computer Security* 8/5 [2000] 222±229