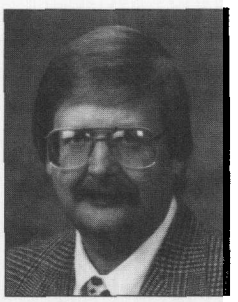
Disaster Recovery Planning and Accounting Information Systems

Steven J. Carlson, Assistant Professor of Accounting, University of North Dakota, Grand Forks, ND

D.J. Parker, Assistant Professor of Accounting, Western Washington University, Bellingham, WA



Steven J. Carlson

D.J. Parker

Disaster recovery planning is a crucial component in a company's efforts to minimize risk while maximizing long-term success and profitability. In this article, we discuss the deficiencies related to companies' current disaster recovery plans. Additionally, ideas on how to improve upon and implement disaster recovery plans are presented.

Introduction

The importance of computerized accounting information to the success of a business can be illustrated by the following facts:

- The average company experiencing a computer outage lasting ten days or more will never fully recover.
- Fifty percent of these companies are out of business within five years [1].

Incidents of floods, earthquakes and hurricanes are examples of disasters that can seriously compromise the availability of accounting information. Additional disasters include fire, employee sabotage, computer viruses, physical damage (e.g., static electricity or disks crashing) and theft. The dollar value of physical damage from a disaster can be staggering. The city of Chicago suffered over one billion dollars in damage from a 1992 flood [6].

Effects of disasters extend for a long period after the physical damage is repaired. The quicker a company recovers from such a disaster, the less extensive the long-term effects of the disaster. While the loss of sales during a disaster is harmful, the loss of customers, vendors, inventory and employee records extend recovery times from weeks and months to years. If a company has a well designed disaster recovery plan (DRP) in place, the plan will minimize the inconvenience of a disaster, while improper planning can result in a company experiencing bankruptcy.

The objective of this study is twofold: (1) provide insight as to how the importance of a disaster recovery plan can be communicated to management and throughout the organization and (2) survey accountants in private industries concerning the composition of their companies' DRPs for their accounting information systems. The results of the survey indicate a need for a better distribution of information concerning the benefits of a DRP and, more importantly, how to begin the process of formulating such a plan. Information from prior research is available referencing what factors are necessary components of a DRP [1,6,7]. However, research about which components are actually being implemented in business is scant.

Elements of a DRP

A disaster is generally defined as any interruption in a company's operations that will significantly affect employees and/or customers. A DRP is the method by which a company identifies critical resources, determines how these resources are negatively impacted by a disaster, and develops a plan to minimize and recover from the negative impact of a disaster [7]. The accounting information system component of a DRP focuses on the organization's accounting-related data requirements for making decisions.

Disruption in the continuity of a business for an extended period of time seriously affects the overall viability of a company and may eventually lead to bankruptcy. The comprehensiveness of a company's disaster recovery planning has a critical impact on how effectively and efficiently a company recovers from a disruption. A proper DRP satisfies the following objectives:

- Protection of assets and records
- Resumption of normal operations
- Protection of personnel
- Continuity of management
- Minimization of losses and recovery time [5].

There are numerous sources available describing the elements of a DRP [2,4,6,7]. These sources also contain lists of companies that provide disaster recovery planning and consulting services.

Communicating the Importance of a DRP

Management must accept ultimate responsibility for the success or failure of a DRP; therefore, communicating the importance of a DRP to management is the first step in establishing such a plan. The audit committee/board of directors and the comptroller are the most critical levels of management that need to support a DRP.

However, the entire company needs to be involved with the DRP process. Upper management needs to provide the strategic direction and financial resources for the DRP. Middle management is responsible for facilitating the coordination and effective execution of the plan. Lower management should understand the need for a DRP and provide insights into plan improvements and efficient execution.

There are two sources for initiating communication to management about the importance of a DRP. One source is external, the external auditor and/or computer consulting companies that provide services to the company. The external auditor is expected to provide advice concerning internal control structure weaknesses. An inability to recapture information, whether from a disaster or general system vulnerability, is considered an internal control weakness. The other source for initiating communication is internal, an employee of the company. This employee could be from one of several departments, e.g., internal audit, information systems, comptroller or a specific individual concerned about information security.

When communicating the importance of a DRP several issues should be emphasized to management. The effect of even a short-term interruption in business on profits and cash flows should be stressed. Specific examples of disasters are the fire that destroyed the corporate headquarters of Steinberg, Inc., a Canadian company with $4.5 billion in retail sales, the bombing of the World Trade Center, the Con Edison fire and the Los Angeles and San Francisco earthquakes. These examples illustrate how quickly a company can be crippled by an uncontrollable event.

The average company experiencing a computer outage lasting ten days or more will never fully recover.

A competitive disadvantage for the company during even the shortest business interruption is that competitors will have the opportunity to sell to the company's customers. Management should be reminded of how detrimental this disadvantage will be to the company in both the short and the long term. Also, the potential exists for stockholder lawsuits for gross negligence related to safeguarding the company's assets. The underlying theme of these issues is that there are substantial costs associated with the risk of not implementing a DRP. The cost of not having a plan in place can be severe enough to cause bankruptcy. One question should be asked of upper management: "Are you willing to assume such risks when a relatively small investment of time and money can provide a solution?" The process of establishing a DRP is not costly and is successfully being performed by numerous companies, such as Steinberg, Inc.

When establishing a DRP, management should pay special attention to assigning responsibility to specific individuals. One approach is to hire a full time employee who is designated the disaster recovery person. Whether a full time employee is or is not hired, the responsibilities for a company's DRP should be distributed among several employees. The best approach would be to designate a disaster recovery team, with one member specified as team leader and another as assistant team leader.

The disaster recovery team should be responsible for establishing and documenting a DRP with the specific tasks associated with the plan divided among employees. Once a disaster occurs, one individual should be responsible for beginning the recovery process. This individual is responsible for communicating with employees, customers and suppliers. The communication process should include issues like how to contact the company (new phone numbers), where the temporary office is located and how payroll obligations will be satisfied.

Another employee should be assigned responsibility for maintaining the currency of the DRP. Tasks associated with maintaining currency of the plan include identification of the following items: critical data files, key employees, location of back-up sites and how to replace hardware and software. As part of the process of identifying key employees, it is crucial to identify and document the specific duties of these employees along with developing a hierarchical list of employees to take over these specific duties.

The effect of even a short-term interruption in business on profits and cash flows should be stressed.

An employee should be specifically assigned responsibility for backing up critical data files at specified intervals and securing these data files at an off-site location. Data represent the core function of an information system. Hence, the importance of this task cannot be overstated. Additionally, it is crucial that written documentation of all components of the DRP be maintained at locations outside the company. Homes of the DRP team members offer possible options for storing copies of the DRP.

Internal Control and Disaster Recovery Planning

The survey is concerned with corporate accountants' perceptions of how their company's DRP functions. Hence, in order to anticipate which objectives of a DRP are the concerns of an accountant, one must first understand which aspects of a company's accountants are viewed as the most important. Establishing and maintaining an appropriate internal control system is typically considered necessary to ensure relevant, reliable accounting information. Hermanson and Hermanson list the primary objectives of internal control as provided by the Institute of Internal Auditors [3]. The purpose of these objectives is to provide reasonable assurance of:

- Reliability and integrity of information
- Compliance with policies, plans and laws
- Safeguarding assets
- Efficient use of resources
- Accomplishment of goals.

The objectives of a DRP and a system of internal control are linked via the protection/safeguarding of assets and records concept. Thus, one would expect accountants to perceive the objectives of a DRP relating to protection of assets and records to be more important than the remaining objectives.

Demographics of Respondents

Surveys were sent to 400 accountants across the U.S. who are in managerial positions in their companies. The mailing list was obtained by random selection from the American Institute of Certified Public Accountants. An attempt was made to gather detailed information concerning all aspects of a DRP and resulted in a lengthy and unwieldy instrument. The questionnaire was designed to gather information concerning DRP issues perceived by accountants to be important to an accounting information system. The questionnaire addressed two types of respondents, those with and those without a DRP. The authors reviewed various DRP "how-to" articles and compiled a composite list of attributes relevant to an accounting information system. For companies without a DRP in place, information was gathered as to why such a plan was not adopted.

Exhibit 1 provides demographic information relating to 61 respondents. The respondents are relatively experienced within their company and industry (seven and 11 years, respectively). Additionally, almost all of the respondents have some type of certification. This evidence indicates that the respondents are both knowledgeable and technically competent about the importance and requirements of an accounting information system, and they have the requisite amount of experience to impact decisions concerning corporate policy within their company.

Data relating to the respondent's individual business indicate that the companies involved in the study are, for the most part, small to medium sized. It should be noted that only 71 percent of the companies responded to the question relating to annual sales. Therefore, average sales may not be representative of the sample as a whole. Respondents that did not rely extensively on computerized accounting data (ten percent) were excluded from the rest of the study, primarily because these respondents answered relatively few questions.

Exhibit 1. Demographics of Respondents and Their Companies

Certified Public Accountant (%)	92
Certified Management Accountant (%)	5
Other Accountant (%)[1]	33
Average Number of Years, Current Position	7
Average Number of Years, Current Industry	11
Average Number of Employees	210
Average Yearly Dollar Value of Sales ($ mil)[2]	33
Self-Classification (%):	
Small	57
Medium	34
Large	8
Rely Extensively on Computerized Accounting Data (%):	
YES	90
NO	10
Have a DRP in place (%)[3]:	
YES	87
NO	13

[1] The total does not add to 100 percent because a respondent can have more than one type of certification. [2] Only 71 percent of the companies responded to this question. [3] This response is only for companies who rely extensively on computerized accounting data.

Survey Results

Survey results indicate over 90 percent of respondents are dependent on computerized information systems. Computerized

Exhibit 2. Factors Influencing the Decision to Have a DRP

	Agree/ Strongly Agree (%)	Neutral (%)	Disagree/ Strongly Disagree (%)
Cost/Benefit	63	23	15
Ease of Implementation	81	6	13
Maintenance	72	17	11
Flexibility	66	23	11
On-Site Recovery	77	13	10
Off-Site Recovery	50	27	23
Vendor Support/Service	44	37	20

systems increase communications and the flow of information between and among divisions in an organization. Businesses rely on the ability to integrate and communicate information to make effective decisions. Hence, the respondents were asked three questions relating to how their company protects the data used for the communication of information throughout the organization.

Factors Influencing a Company's Decision. Factors important in influencing a company's decision to have a DRP in place are listed in Exhibit 2. A cost/benefit analysis was found to be important by 63 percent of the respondents. What is interesting is that 38 percent of the companies were neutral or disagreed that a cost/benefit analysis was important in their company's determination to have a plan. Typically, companies are reluctant to make decisions that do not have a known positive benefit. It should be noted that because of the downside risk and potential large-scale costs involved with not having a DRP, companies might decide to implement a plan with no formal cost/benefit analysis.

The most important factor that influences the decision to adopt a DRP is ease of implementation (81 percent). If the implementation of a plan is perceived to be relatively easy, the associated costs may be perceived to be relatively low. Given the potential downside of a disaster and if a company believes this downside can be avoided via the relatively simple implementation of a plan, the decision to execute a DRP becomes easier.

Ease of maintenance (72 percent) and flexibility (66 percent) were the next most important factors that influenced a decision to have a DRP. However, the authors expected higher percentages for these two factors. This finding implies that companies may not be willing to continuously evaluate and update a DRP to meet the informational needs of the various divisions within the organization. A DRP needs to be dynamic in nature. Hence, flexibility of a DRP will directly affect a company's ability to modify and maintain the DRP in response to changes in an information system.

On-site recovery was more important than off-site recovery (77 versus 50 percent). One reason for the increased emphasis concerning on-site recovery could be the lower cost associated with this type of plan relative to off-site recovery. It has been estimated that off-site recovery systems are two to three times as expensive as on-site recovery plans [8].

Factors Provided by an Outside Source. The results for which factors should be provided by an outside source are reported in Exhibit 3. It should be noted that outsourcing is not a permanent solution to a lack of internal disaster recovery planning. The data may be stored in a format that does not allow for the most efficient recovery of vital information. For data backup purposes, 35 percent of the respondents agreed that outsourcing is important. Respondents may not be outsourcing more data backups because of the relative ease with which data can be backed up on-site via disk or tape drive.

Insurance coverage could be a reason why more respondents agreed that it is important for an outside source to replace hardware (61 percent) and software (50 percent). However, companies need to remember that insurance claims

Exhibit 3. Factors Important for an Outside Source to Provide a DRP

	Agree/ Strongly Agree (%)	Neutral (%)	Disagree/ Strongly Disagree (%)
Data Backup	35	24	41
Hardware Replacement	61	13	26
Software Replacement	50	22	28
Re-installation Service	51	16	33

are not satisfied in one business day. Hence, even with adequate insurance, a company will experience some delay in doing business. The fact that companies may rely on the competence and knowledge of their own employees who were responsible for the original installation of a system could explain why approximately one-half of the respondents did not agree that re-installation service should be outsourced.

Exhibit 4. Important Components of a DRP

	Agree/ Strongly Agree (%)	Neutral (%)	Disagree/ Strongly Disagree (%)
Plan to Backup Data	100	0	0
Plan to Restore Data	98	0	2
Plan to Resume Normal Business	94	0	6
Protect Customer Records	90	6	4
Protect Financial Statement Data	90	8	2
Protect Personnel Records	58	18	24
Protect Vendor Records	62	19	19
Protect Inventory Records	55	21	23
Plan to Restore LAN	53	25	23
Protect Hardware	60	28	13
Plan to Restore Damaged Hardware	65	24	11
Listing of Key Employees	26	48	26
Administrator to Oversee	57	35	9
Backup Power Source	55	28	17
Listing of Necessary Software	22	54	24

Components of a DRP. Exhibit 4 illustrates the components of a DRP that accountants consider most important. The respondents universally agreed that backup of all data is paramount (100 percent) with restoration of data (98 percent) also of vital importance. Without data as an input to the decision-making process, a firm lacks guidance and direction with respect to achieving specific goals and objectives. A major problem with systems that are designed to recover all information is the lack of specific attention to data that is critical to resuming normal operations. Cathey and Phillips point out the need for building a system with low, medium and high priority levels for recovery of data [1].

Protection of accounting records is crucial, because these records are a critical input to the decision-making process. Survey responses revealed that other important components of a DRP are backups of financial statements (90 percent) and backups of customer records (90 percent), followed by vendor records (62 percent), personnel records (58 percent) and inventory records (55 percent). No clear pattern emerges indicating a prioritized approach to planning a disaster recovery system. The importance of backing up each of these records may depend on a company's ability to recreate the information from a third party source. For instance, vendors are more likely than customers to inform a company of what is owed between the two parties. Also, personnel records can be recreated by having employees fill out a survey and by providing old paycheck stubs. Unless warehouse facilities are completely destroyed, inventory records can be partially restored by taking a physical count/estimate of remaining inventory.

The respondents strongly agree (94 percent) that backup systems should be designed to resume normal business. However, the respondents did not indicate strong support for the need of a plan to protect and restore computer-related hardware (range of 53 to 65 percent). It is possible that respondents believe their firm has adequate insurance coverage to compensate for such a loss. However, one cannot necessarily assume computers will be readily available during a disaster. Hence, even though a firm is financially reimbursed for replacing computer-related hardware, the actual acquisition of such hardware may take days or even weeks. Thus, a firm's reliance on insurance coverage may result in its DRP failing to meet the plan's objective of minimizing losses and recovery time.

Backup of all data is paramount, and restoration of the data is of vital importance.

Why a Company Does Not Have a DRP in Place. Of the companies surveyed, 13 percent of the respondents who rely extensively on computerized accounting data do not have a DRP in place. Reasons as to why a company does not have a DRP in place is found in Exhibit 5. There is no single reason why nearly all of the respondents agree on why their company does not have a plan in place. Instead, a combination of reasons provides the best explanation for a company not having a DRP. In general, the percentage of respondents agreeing with a statement is approximately equal to the percentage of respondents disagreeing.

Communicating the importance of a DRP to management is the first step in establishing such a plan.

Overall, a lack of knowledge concerning DRPs is the central theme relating to why a company has not implemented a DRP. Where to start the process (54 percent), hardware and software needed (46 percent), and the belief that a disaster will not happen (55 percent) are all areas where companies profess to have a lack of knowledge concerning DRPs. A general lack of knowledge about DRPs supports the result that 31 percent of the respondents agree that the benefits of a DRP are one reason why their company did not have a DRP in place. This result further reinforces the conclusion that a better effort needs to be made to communicate the associated benefits of a DRP.

Exhibit 5. Why a Company Does Not Have a DRP in Place

	Agree/ Strongly Agree (%)	Neutral (%)	Disagree/ Strongly Disagree (%)
Lack Knowledge About:			
Where to Start	54	15	31
Benefits of a DRP	30	39	31
Hardware Needed	46	15	38
Software Needed	46	15	38
Cost/Benefit	14	43	43
Do Not Anticipate Disaster	55	23	23
Lack Management Support	33	27	40
Too Many Choices	15	31	54

There is a two-step solution to the problem of communicating the need for a DRP. First, an individual, either internally or externally, needs to accept responsibility for initiating the DRP. The devastating effects of previous disasters cannot be overstated. Second, resources are available in the references to this study that will provide guidance to an organization wishing to implement a DRP. With proper planning, the successful implementation of a DRP is a cost-benefit strategy.

A major obstacle to overcome in the successful implementation of a DRP is corporate accountants' perception of a lack of support from management for a DRP (33 percent agreeing). The establishment of a DRP team is one solution for this perceived lack of support. At a minimum, written documentation of the DRP should be made available to all employees.

Conclusion

Despite the fact that DRPs are important to the success and longevity of a business, the evidence indicates that companies are either failing to implement a DRP or have neglected to take full advantage of their DRP. Companies that have a DRP in place need a better understanding of the importance of the specific individual components of the DRP. While some records are perceived as crucial, other records and assets are considered to be less important.

The evidence provided here suggests a need for improvement in three areas relating to a DRP. First, corporate accountants perceive a lack of support from upper management for DRPs. Without the support of management, a DRP will not be successfully implemented. Second, companies need to do a better job of identifying the components most critical to the success of their company. Documentation of these components, along with a plan of substitution for these components is crucial to the success of a DRP. Third, while DRPs are designed to retrieve data, there appears to be a lack of planning on reinitializing the information system after a disaster. A recovery system should have the ability to integrate retrieved information to facilitate rapid communication between departments. ■

References

1. Cathey, J.M. and R.H. Phillips, Jr. "Don't Panic! Armed with the Right Strategies You Can Recover from a System Crash." *Management Accountant,* October 1994, pp. 49-54.
2. *Disaster Area Practice Guide.* American Institute of Certified Public Accountants, AICPA, New York, 1993.
3. Hermanson, D.R. and H.M. Hermanson. "The Internal Control Paradox: What Every Manager Should Know." *Review of Business,* Winter 1994, pp. 29-32.
4. Hunt, A.E., S. Bosworth and D.B. Hoyt. *Computer Security Handbook,* Third Edition. New York: John Wiley & Sons, 1995.
5. Lesmeister, J. Presentation to the Association of North Dakota Teachers of College Accounting, April 1992.
6. Powell, D. "Planning to Avoid Disaster." *Network Reliability,* June 1992, pp. 19-23.
7. Seibold, J. "Preventing Disasters: Whipping Up an Emergency Response Plan." *Network Computing,* February 1992, pp. 81-89.
8. Semilof, M. "Disaster-Recovery Options." *Communications Week,* August 12, 1994, pp. 18-19.