# Disaster recovery planning: a strategy for data security

**Steve M. Hawkins**
Department of Decision Sciences and MIS, Miami University, Oxford, Ohio, USA
**David C. Yen**
Department of Decision Sciences and MIS, Miami University, Oxford, Ohio, USA
**David C. Chou**
Department of Business Computer Information Systems, St Cloud State University, St Cloud, Minnesota, USA

**Keywords**
Disaster recovery, Data security, Networks

**Abstract**
The migration from centralized mainframe computers to distributed client/server systems has created a concern on data security. If a disaster occurs to the organization that destroys a server or the entire network, a company may not be able to recover from the loss. Developing an effective disaster recovery plan will help an organization protect them from data loss.



## Introduction

The centralized computer systems are now replaced with or connected to the distributed systems. Also, multiple servers are connected to each other on a corporate network to balance their processing power. If one of the servers in the networked environment crashes, troubles will arise for both the users and the company.

There are a variety of reasons that cause systems to crash. For example, the lack of system security and employee sabotage are the main concerns. While computer hackers live outside of the company walls, this is not always the case. Although passwords and firewalls help keep viruses and intruders from entering the corporate systems, sometimes they are useless. Corporate management needs to recognize the necessity for data security.

A disaster could cause companies an interruption for a period of time. The Business Recovery Plan is the document used to assist an organization in recovering its business functions. A Disaster Recovery Plan (DRP), however, is a document designed to assist an organization in recovering from data losses and restoring data assets. A DRP should be a pro-active document, a living and breathing document. It does not document the tasks, it is an action plan that is used to identify a set of policies, procedures, and resources that are used to monitor and maintain corporate information technology (IT) before, during, and after the disaster. Possible IT disasters include (Semer, 1998):

- natural disasters, such as fires, earthquakes, lightning, storms, and static electricity;
- software malfunctions;
- hardware or system malfunctions;
- power outages;
- computer viruses;
- man-made threats, such as vandalism, hackers, and sabotage; and
- human error, such as improper computer shutdown, spilling liquids on the computer, and cigarette ash.

Disaster recovery was a term coined by computer vendors between 1960 and 1980 – the era of the centralized mainframe computer (Colraine, 1998). During that time, a disaster recovery plan was used to backup mainframe computers.

A disaster recovery plan was similar to an insurance policy that provided a protection from natural disasters, such as earthquakes, floods, hurricanes, and tornadoes. Disaster recovery plans during these years were typically used by organizations that have large mainframe computers and data sites for daily business operations. Since data recovery planning process was expensive, an alternative was to backup the data from the mainframe computer and store it at alternate locations. During the 1970s, providing backup data services was a lucrative business.

According to 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 (Panettieri, 1995).

Most companies hesitate to develop a disaster recovery plan until a disaster occurs. According to another survey (Patrowicz, 1998), 85 per cent of the *Fortune* 1,000 companies have disaster recovery plans. Within these companies which have disaster recovery plans:

- 80 per cent have plans that protect their data center resources;
- 50 per cent have plans that protect their networks; and
- less than 35 cent have plans that protect their data on PC LANs.

In an Ernst & Young/Computerworld Global Information Security Survey of 4,255 IT and information security managers, 84 per cent of

Information Management & Computer Security
8/5 [2000] 222–229

[ISSN 0968-5227]



Information Management &
Computer Security
8/5 [2000] 222–229



them said that their senior management believes that security management is "important" or "extremely important." Of these respondents, over 50 per cent 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.

The growth of distributed systems and the global business environment make corporate decision makers believe that having a backup or recovery plan is necessary. Many companies need to process the mission-critical information stored in distributed or client/server systems throughout entire enterprise networks. One of the success factors for a company's business operations is based on the continuance of these enterprise networks. Client/server systems have replaced the centrally located mainframe, residing at multiple sites in a building or across a corporate WAN. Consequently, protecting these client/server systems has become a major priority for corporations today (Colraine, 1998).

Distributed systems are becoming an architectural standard for networked organizations. These systems have diffused mission-critical data across local area networks which extend corporate resources to remote work sites. As distributed systems continue to replace the "glass house" environment of the mainframe, the data decentralization is going to increase in the future (Mello, 1996).

According to a survey conducted by the research group of David Michaelson & Associates, the respondents stated that 43 per cent of the data housed on corporate PC LANs today is mission related (Mello, 1996). Of these respondents, 77 per cent employ a continuous or daily backup for their PC LANs, and 89 per cent of them follow some kinds of backup procedures. It is a dramatic increase from a similar 1993 survey, in which only 45 per cent of the organizations stated that they backed up their PC LANs on a continuous or daily basis. As the distributed system model continues to become the de facto standard in most corporate networks today, companies will eventually learn – either by proper planning or their own unfortunate experience – that having a disaster recovery plan is vital for their survival in today's networked environment.

This paper identifies the importance of disaster recovery planning in the business world. The benefits and limitations of developing a disaster recovery plan are identified in the next section. An analysis framework for developing a disaster recovery plan is introduced next. It follows by illustrating a step-by-step strategic planning process that an organization could follow to develop their own DRP. Finally, conclusions are stated.

## Benefits and cost of disaster recovery plans

Corporate decision makers must look at every aspect of a DRP before implementing it within their organization. Listed below is a culmination of the benefits and costs of developing a DRP.

### Benefits of developing a DRP

Developing a DRP is to identify various steps to assist an organization in recovering from data losses and restoring data assets. This process generates the following seven benefits:

1 *Eliminating possible confusion and error*. By organizing the response teams to take care of specific responsibilities during a disaster, management can focus their attention on other critical issues related to disaster recovery. Depending on the nature and scope of the disaster, managers need to handle customer relations, company liability, vendor issues, additional staffing needs, and legal issues.

2 *Reducing disruptions to corporate operations*. As tactical response teams or qualified personnel are in place and an alternate site is available within a short amount of time, corporate operations can be re-established quickly with minimal delays.

3 *Providing alternatives during a disastrous event*. By developing a DRP before disaster strikes, top-level management can take the time needed to consider all of the alternatives and choices for disaster recovery.

4 *Reducing the reliance on certain key individuals*. If the responsibilities of re-establishing a LAN were left to the systems administrator or network administrator, and that particular individual was injured during the disaster, the corporate network would have a difficult time re-establishing itself in the shortest amount of time. By delegating recovery responsibilities to key individuals who know exactly what to do in an emergency situation, the company can develop redundancy within its corporate hierarchy so that they can replace those individuals who are unavailable in the disaster.

5 *Protecting the data of the organization*. Data are one of the most important assets in an organization. Data are stored in many different forms, including

databases, spreadsheets, and documents. The data that are vital to the organization may include customer databases, financial documents, mailing lists, and EDI forms from vendors and customers. Most of this data could be stored on magnetic media, such as tape backup or on hard drives in LAN servers. If a company locates in an area that is vulnerable to floods or severe weather, its DRP may include elevating computer equipment off the floor and onto wall-mounted racks where initial flooding will not damage the computer equipment.

6 *Ensuring the safety of company personnel.* 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.

7 *Helping an orderly recovery*. 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, management can focus its attention to other critical issues.

### Costs of developing a DRP

Developing a DRP is not easy. It needs to consume corporate resources to make it successful. It has at least the following two types of costs:

- *Cost of DRP preparation.* Corporate management could spend a long time identifying mission-critical systems that must be implemented after a disaster. This project could cost a company a tremendous amount of man-hours. If a company chooses a third party vendor to develop their disaster recovery plan, the costs could be considerably higher. The challenge to developing a DRP is to convince top-level management that the plan is worth the investment.

  The New York World Trade Center bombing in 1993 displaced thousands of workers for weeks, causing a financial impact on 350 firms located within the trade center (Stefanac, 1998). By performing some risk analyses to corporate management, they may well consider adopting a DRP.

  A disaster recovery plan does not have to be an elaborate framework of policies, procedures, and hardware. In fact, preparing a disaster recovery plan may simply outline the procedures for performing nightly data backups to a mirror site via a telephone line. The minimum goal of developing a DRP is to protect the data.
- *Cost of corporate resources.* Implementing a DRP requires a strong commitment. It needs the support from top-level management, the cooperation from employees in the company, and the availability of an inventory of all the mission-critical resources of information technology.

  If a company lacks the experience of developing its DRP, outsourcing could be a good choice. Consultants such as IBM, Comdisco Inc., and SunGard Recovery Services Inc. could provide assistance to all of its needs.

## Analysis framework of DRP

Any company beginning a DRP project should perform a risk assessment for its information technology. This involves checking their network inventory and identifying the resources needed to maintain daily business operations. After analyzing the resources, they must develop a plan of action. This could be a set of procedures or the multiple-volume instruction manual. After developing this plan, the company could integrate it into its business strategies. Also, this company needs to train its employees about specific tasks to be done and how each employee is involved in the process. This implementation process should be reinforced by the company at least once a year by conducting mock disaster scenarios. This process will ensure each employee keeps his or her skills up-to-date in the event of a disaster.

The DRP development involves three process stages: construction, adoption, and evaluation. The DRP development starts with the construction process. During this process, ideas and concepts are transformed into tangible tasks and procedures. A DRP planning committee is formed to include representatives from all functional areas of the company. This committee performs risk analysis for each functional area of the company in order to determine the consequences and potential damages caused by a disaster. When the analysis is complete, a plan of action is developed and presented to top management for approval.

After management's approval, a DRP is adopted and integrated into the company's daily business functions. This process stage includes the activities such as employee training and awareness, modification of job descriptions, and integration of DRP into normal operating procedure.

Finally, management plays a main role in supporting the new plan by conducting regular evaluations. If new computers are installed into a particular department, the plan should be re-evaluated and modified to provide an additional security blanket to the company's assets.

Steve M. Hawkins,
David C. Yen and
David C. Chou
*Disaster recovery planning: a strategy for data security*
Information Management & Computer Security
8/5 [2000] 222–229



Preparing a disaster recovery plan is not a solitary effort. It requires the expertise, ingenuity, and cooperation of corporate employees and top-level decision makers. A well-planned DRP requires three main functional areas (management, information technology, and human resources) to participate and prepare themselves for subjects such as employee awareness, and safety of computer technology and data security. Activities and involvement of three functional areas are discussed in the following sections.

## Management involvement and activities

### *Keeping current with IT knowledge*

The top-level decision makers may not want to be confronted with computer technology for three reasons. First of all, they may not consider themselves as "computer people," and consequently leave the computer problems to either their subordinates or their IT staff. Second, they may want to learn more about computer technology, but are overwhelmed and confused by all of the literature available in bookstores or in the library. Finally, they may feel intimidated by IT counterparts who know and understand something that they cannot understand. As executives, they may feel intimidated by their lack of understanding and avoid the issue altogether. If, however, they take the initiative to learn how computer technology can help them make better decisions and protect their data, they will become better managers and be able to communicate with their IT counterparts.

### *Employing qualified professionals to develop and maintain the company's DRP*

Individuals who are certified can prove their value and knowledge. Certifications such as the Microsoft Computer Systems Engineer (MCSE) for Windows NT or the Certified Novell Engineer (CNE) for Novell networks are examples. If a company's future plans involve an enterprise network that will include hubs, routers, and bridges, it might also consider employing Cisco trained professionals with Cisco Certified Network Associate (CCNA) or Cisco Certified Internetwork Engineer (CCIE) certifications. Employing MCSEs, CNEs, and CCIEs to run a company's network also saves time and money on IT training.

Similarly, there is training and certification available for disaster recovery. An organization such as the Disaster Recovery Institute offers training and certification on disaster recovery.

### *Ensuring insurance coverage for LAN*

A comprehensive insurance policy may cover data restoration, business interruption, recovery costs, and damage to computer hardware from natural disasters, such as flooding, tornadoes, and earthquakes. Also, a company needs to make sure that they have the proper coverage for all geographical areas.

### *Organizing specialized response teams to execute the DRP during an emergency*

A DRP should be up-to-date and every team member involved in the recovery process should be familiar with it. The implementation of a DRP should involve specialized teams to be responsible for certain areas of expertise, including initial response team, restoration team, recovery operations team, and logistical support team (Semer, 1998):

- *Initial response team*. This team is the first set of eyes to evaluate the nature and extent of the damage. These people will determine whether or not business operations can continue on-site or should be moved to an alternate location. If the damage is severe, this team will contact additional response teams for further assistance.
- *Restoration team.* This team coordinates the damage control, restoration, and reactivation of network resources, which include data files, software, network infrastructure, and communication lines.
- *Recovery operations team*. If the initial response team determines that operations need to be re-established at an alternate location, the recovery operations team will set up and run the operations at the new location. Their responsibilities include re-establishing the distributed network infrastructures, retrieving backup files, setting up hardware and communication lines, and other related activities.
- *Logistical support team.* During the transfer of operations to an alternate site, the logistical support team provides logistical support by ensuring that employees can access alternate offices and facilities. They also provide personal support for employees, which includes travel and relocation assistance, cash advances for emergency expenses, crisis counseling, and employee family assistance.

## Information technology involvement and activities

### *Developing a detailed network blueprint*

When a disaster destroys most or all of the building, the network will have to be rebuilt. The blueprint of the company's network architecture will allow the IT staff to rebuild the network quickly.

*Gaining management's support to the disaster recovery plan*
Senior management is recognizing the outcomes of losing corporate data. An effective CIO could understand both IT and management needs, thereby translating the schematics of the technology into management's language.

*Monitoring employees' Internet accesses*
While the Internet provides the worldwide information at a moment's notice, it also brings with it the threat of sabotage from hackers and viruses. Many of the security concerns regarding the Internet stem from the design of the Internet itself, making it difficult to identify and trace where data are coming from or where they are going (Garfield and McKeown, 1997). Consequently, the best way IT can protect their organization from hackers and viruses is to monitor employees' Internet accesses through firewalls. This will greatly reduce the dangers from hackers outside the company.

*Standardizing hardware and software*
Any organization having heterogeneous hardware and software will create difficulties of rebuilding the network. For example, if some departments are using Macintosh computers while others are using PCs, the rebuilding process will take even longer. Therefore, having a homogeneous enterprise system can reduce the complexity of rebuilding the network.

*Securing support from IT vendors*
Implementing a DRP needs to secure support from both routine vendors and specialized vendors. Routine vendors are suppliers who provide daily services, such as hardware and software support, e-commerce support, and telecommunications service. Specialized vendors are companies that provide specific disaster recovery services. Their services include data salvage and restoration, alternate office space, alternate backup sites, and emergent lease of hardware and equipment.

*Performing routine backups*
A backup procedure should be performed in order to ensure that all mission-critical systems are stored on LAN servers instead of users' workstations, floppy disks, or ZIP disks, which are not subject to system backups. This ensures that the data are centrally located in one place to facilitate backup and recovery procedures.

*Ensuring smooth interface between client/server and mainframe systems*
Interface applications that allow data to be exchanged between mainframe and networks will need to be identified and included in the backup and recovery procedures. Any failure of backing up these applications may complicate the recovery process and the integrity of data and system.

*Using redundant array of independent disks (RAID) technology to capture on-line transaction activity*
RAID provides mirrored copies of data on multiple disk drives that create up-to-date copies of data files. RAID also provides capability of fault tolerance, providing accessibility to data in the event of a partial disk failure.

*Preventing LAN from viruses' attack*
Choosing the right anti-virus software for the LAN is imperative for protecting the data. After selecting suitable programs, system administrators should make regular sweeps of the LAN to ensure system integrity at all times.

*Protecting hardware from environmental damage*
Make sure that surge protector and anti-static mats are installed on all LAN servers in order to protect them from static electricity. According to a report, computer users in the Midwest and North Central USA suffer the most data loss due to static electricity during the winter dry air (Sutton, 1998).

*Connecting uninterruptable power supplies (UPS) to key servers and equipment*
The power-related problem is one of the major causes of losing data. If a server suddenly loses its power, there is a chance that the data on the hard drive will be lost. By installing UPS and/or a backup power supply on the entire LAN servers could maintain the integrity of the data on the server.

**Human resources services**

*Providing employee-training programs on computer uses and computer ethics*
Any employee could carry viruses from his/her home computers to work computers, which can destroy the integrity of corporate network. Human resources departments need to alert employees to this risk by educating them to keep their home PC applications off their work computers. Therefore, virus attacks could be kept at a minimum level.

Some disasters may be caused by unethical practices. Practicing proper ethics on the computer is also becoming an issue within many organizations today. In an era where computers have become an integral part of society, many organizations discovered that employees who use their computers inappropriately could cause companies a significant loss in information, time, and

Information Management &
Computer Security
8/5 [2000] 222–229



money. As a result, many organizations are implementing corporate codes of ethics as part of their employee agreement.

*Promoting employee safety awareness programs*

A DRP can cover a broad range of scenarios, from a corrupted LAN server to complete destruction of a corporate building. Depending on the location of the organization, management should implement safety awareness programs into their DRP in order to train employees on how to take care of himself or herself during a natural disaster, such as an earthquake, tornado, or hurricane. These programs might include classes in CPR and first aid training that can benefit employees inside and outside the company. Other types of training may include fire drills, using a fire extinguisher, and locating safe shelter during a disaster. While many organizations may view a DRP as an insurance policy of their corporate assets, it is a good idea to include one of the most important company assets, that is, their employees.

## Development strategies for DRP

Developing a disaster recovery plan could be a simple set of procedures describing how to backup a server to a tape drive, or a multiple-volume instruction manual describing procedures for earthquake damage. Companies need to identify certain suitable development strategies for DRP. The procedures and strategies for developing a disaster recovery plan are discussed as follows:

### Performing a risk assessment

This process begins by checking inventory of the organization and identifying the systems and resources that are most critical to their business operations. The two methods which can be used to identify these resources are "Business impact analysis" and "Risk assessment analysis" (Semer, 1998).

Business impact analysis identifies the mission-critical resources in the company – the resources that are absolutely essential for keeping the organization running every day. Once these resources have been identified, the next challenge is to estimate how long the company can continue their business operations after suffering major losses.

After identifying the mission-critical resources, it needs to analyze the potential risks to these resources. Risk assessment analysis identifies corporate resources development, including the infrastructure of the network. The statistics gathered from this assessment provide a blueprint of risk assessment.

In many cases, departmental managers are familiar with their department's day-to-day operations and, therefore, they are in a better position to decide how their mission-critical resources should be restored.

### Identifying possible vulnerabilities

Monitoring the vulnerability will prevent a problem before it occurs. For the most companies, the main areas of vulnerability may include (Rothstein, 1998):

- backup storage locations for data;
- security;
- physical security;
- the room or building that is housing the computers,
- electrical power;
- fire detection and suppression;
- depending upon one person for information;
- management controls; and
- reliability of telecommunication services.

Other areas of vulnerability include employee resignation, repairing a roof leak in the computer room, computer virus infection, and so on.

### Developing a plan of action

One way of developing a disaster recovery plan is to conduct a brainstorming session for management and corporate employees. Each department could develop their own recovery plan that provides directions on how to quickly resolve a site crisis. The plan should include phone numbers of people who must be notified immediately after a disaster occurs, all of the vendor contact names and phone numbers, and the location of an alternate site. The plan should include but not be limited to the following possible scenarios (Jackson, 1997):

- employees can access the building but the computer systems are down; and
- employees cannot access the building and must drive to an alternate site.

### Choosing an alternate recovery site

If the cause of the disaster was due to a flood, tornado, or fire, travelling to an alternate site may be required. Mission-critical resources should also be considered when relocating business functions to an alternate site (Rothstein, 1998). Possible recovery strategies are discussed as follows:

- *Vendor maintenance agreement.* This is an essential strategy, particularly for organizations having computer networks of small size. Under vendor maintenance agreement, computer hardware vendors are responsible for equipment recovery, repair, and replacement. If a standard

agreement could not cover damages caused by external factors such as a fire or flood, a supplemental agreement may be necessary to cover these expenses.

- *Quick shipping program.* The maintenance contract could ask vendors to deliver hardware replacement to original site or alternate site within three to five days. This quick shipping program works well for companies that can afford to have networks down for a week or longer. Also, the maintenance costs would be as low as $300 a month (Rothstein, 1998).
- *Hot sites.* A hot site is provided and supported by a disaster recovery plan vendor. It is a fully equipped facility furnished with the computer resources required by the organization, including FAX, computer hardware and software, telecommunications, office supplies, and other needed peripherals. A hot site provides a ready-to-go computer system in a prepared location with a minimizing network downtime (Rothstein, 1998). A hot site is usually located within 30 miles of a client site to facilitate employees' travel (Patrowicz, 1998). Since the site could be a distance away from many employees, it also provides living amenities including sleeping areas, showers, and cafeteria (Leary, 1998).

  An additional function for a hot site is to provide a practice model for training personnel during corporate disaster recovery planning (Semer, 1998). Management could practice their disaster recovery plan in a setting that will not disrupt normal business operations. By practicing a disaster scenario on a regular basis, management and employees would be prepared for any disaster that could occur in the future.
- *Cold sites.* A cold site is simply an empty building that is wired, air-conditioned and computer ready (Patrowicz, 1998). Because of the time factor involved with setting up the equipment and becoming fully functional, cold sites should only be considered if the organization is not pressed for time (Semer, 1998).

  The cost of leasing a cold site ranges from $500 to $1,500 a month, depending on the complexity of the computer system. Many companies use their cafeterias as an on-site cold site or use a company-owned warehouse as an off-site cold site. If any disaster damages their facilities, a company would choose a vendor-provided cold site as their alternative (Leary, 1998).

  However, choosing a cold site encounters a few disadvantages. Since computer equipment has to be shipped to the site, a close coordination between the company security and the computer vendors is required in order to ensure safe and timely delivery. Also, the replacement equipment may take several hours to deliver, which may result in an increase of the system downtime (Leary, 1998; Rothstein, 1998).
- *Mobile recovery facilities.* This recovery site is a self-contained mobile trailer that houses all of the computer equipment. Most of these trailers are equipped with backup power generators, and can be equipped with all of the necessary computer equipment as needed. Although it may vary, the usual recovery time for a mobile recovery facility is typically a week or more (Rothstein, 1998).
- *Mirrored site.* Similar to a hot site, a mirrored site is equipped with all of the hardware and communications equipment needed to assume immediate operations. Since the company usually owns these sites, data are transmitted concurrently to these sites as they are being processed at main facility, so they can be ready to go at a moment's notice. Some companies send their nightly backup tapes to their mirrored site so that recovery will only involve the current day's transactions. Whether data are mirrored or sent to the site, the startup time is usually on the same day (Rothstein, 1998).
- *Winging it.* This choice involves no alternative site location or a backup plan for the organization. Organizations that use this method usually fail more than they succeed in rebuilding their computer systems.

## Selecting a backup strategy

Selecting a backup strategy could speed up the process of disaster recovery. There are two backup strategies that are currently used today, including the in-house backup and the offsite backup.

1. *In-house backup systems.* These are backup servers strategically at different locations inside the organization. Using in-house hardware to remove the dependence toward outside vendors could save the company a lot of expenses on leasing equipment. If the backup servers are used for other purposes, however, special procedures should be included in the disaster recovery plan for relocating these systems (Semer, 1998).
2. *Offsite backup systems with data encryption.* Data are encrypted and backed up to a remote site for offsite backup system. Since the communications to the backup site are on the leased line, the data transmission is virtually secure. Organizations that use this backup

method include financial institutions, the military, hospitals, large corporations, and the FBI (Sutton, 1998).

### Conducting a verbal walk-through

Those employees involved in the recovery plan need to participate in a verbal walk-through process, in which they talk through "what if" scenarios and outline individual tasks and responsibilities. This will provide each employee with a working knowledge of the plan, rather than simply reading it on paper (Jackson, 1997).

### Testing the plan on a regular basis to ensure its integrity

Companies need to update their disaster recovery plan on a regular basis. As the company grows, so does its data. If a DRP is not updated to keep up with the growing needs of the company, the company may soon discover that it will not be capable of recovery operations.

Also, as the company grows, it eventually needs more computers, hubs, and routers, among other things. The new need requires some modifications to the disaster recovery plan. Companies need to modify their disaster recovery plan on a regular basis, especially if the company is growing at an accelerated pace (Leary, 1998).

## Conclusion

A disaster causes an event that halts the critical business functions within an organization. It can be as simple as a power disruption to a data server or as serious as a threat to the entire building. Disaster recovery is the process of correcting the problem and getting the critical business functions back online. A disaster recovery plan is, therefore, a predetermined set of instructions that describes the process of disaster recovery.

Developing a DRP needs some hard work such as planning, brainstorming, and cooperation from both corporate management and employees. The plan can be as simple as describing how to back up a server, or as complicated as describing what to do after a hurricane destroys the building. The main source of developing a DRP is to understand the particular needs of the organization.

There are advantages and costs of having a DRP. Some of the advantages are the reduction in data loss, minimizing the need of decision-making process during a disaster, and the protection of company employees. It also causes extra expenses and requires manpower. Despite the questions that arise when considering a DRP, companies should focus on the most important commodity: company data. Depending on the importance of the data, developing a DRP can be more economical than replacing the lost data.

As corporations become increasingly dependent on computers and the Internet for their daily activities, the data generated from their work are becoming critical. Companies that rely on their computer systems and networks to do their business can suddenly lose everything if their computer systems go off-line or are corrupted by a virus. In this electronic age where computers are enhancing the talents and skills of people, the data are now filling the seats of executive boardrooms and corporate offices. At one moment in our country's history, the battle cry used to be "survival of the fittest." Today, as computer technology and data are becoming the important commodities of the future millennium, the new battle cry is "survival of the data." Consequently, data are protected from corruption and it is one of the major functions of top-level management and IT professionals today.

## References

Anthes, G.H. (1998), "Lots talk, little walk", *Computerworld*, Vol. 32 No. 38, pp. 70-1.

Colraine, R. (1998), "Protect more, recover faster is the rule", *Computing Canada*, Vol. 24 No. 30, p. 35.

Garfield, M.J. and McKeown, P.G. (1997), "Planning for Internet security", *Information Systems Management*, Vol. 14 No. 1, pp. 41-6.

Jackson, J. (1997), "Give your LAN a hand", *Security Management*, Vol. 41 No. 8, pp. 44-52.

Leary, M.F. (1998), "A resource plan for your LAN", *Security Management*, Vol. 42 No. 3, pp. 53-60.

Mello, J.P. Jr (1996), "Taking a crack at backup", *Software Magazine*, Vol. 16 No. 10, pp. 85-8.

Panettieri, J.C. (1995), "Security", *Information Week*, 27 November, pp. 32-40.

Patrowicz, L.J. (1998), at http://www.cio.com/archive/040198_disaster_content.html

Rothstein, P.J. (1998), "Disaster recovery in the line of fire", *Managing Office Technology*, Vol. 43 No. 4, pp. 26-30.

Semer, L.J. (1998), "Disaster recovery planning for the distributed environment", *Internal Auditor*, Vol. 55 No. 6, pp. 41-7.

Stefanac, R. (1998), "When it comes to disaster, it's pay now or later", *Computing Canada*, Vol. 24 No. 30, p. 35.

Sutton, G. (1998), "Backing up onsite or online: 25 smart ways to protect your PC from disaster", *Computer Technology Review*, Vol. 18 No. 2, pp. 38 and 42.

**This article has been cited by:**


1. Parul Zaveri SHPT School of Library Science, SNDT Women's University, Mumbai, India . 2015. Digital disaster management in libraries in India. *Library Hi Tech* **33**:2, 230-244. [Abstract] [Full Text] [PDF]
2. Nik Zulkarnaen Khidzir, Azlinah Mohamed, Noor Habibah ArshadEvaluation of Vulnerability Risk Factor: Critical ICT Outsourcing project characteristics 1-5. [CrossRef]
3. Fuda Zheng, Fei WangModeling location problem of the regional disaster recovery centers for emergency platform system 889-892. [CrossRef]
4. Nik Zulkarnaen Khidzir, Azlinah Mohamed, Noor Habibah Arshad. 2013. ICT Outsourcing Information Security Risk Factors: An Exploratory Analysis of Threat Risks Factor for Critical Project Characteristics. *Journal of Industrial and Intelligent Information* **1**:10.12720/jiii.1.4, 218-222. [CrossRef]
5. Alan R. PeslakPenn State University, Dunmore, Pennsylvania, USA. 2012. An analysis of critical information technology issues facing organizations. *Industrial Management & Data Systems* **112**:5, 808-827. [Abstract] [Full Text] [PDF]
6. Young-Hee Jeong, Jung-Hoon Lee, Eun-Young Kim. 2011. A Study on the Critical Success Factors and Practical Method of Information System Disaster Recovery : Assuring Business Continuity of Information System Interface Specification Modeling. *Journal of the Korea society of IT services* **10**, 83-101. [CrossRef]
7. Barry A. Cumbie, Chetan S. Sankar. 2010. The Need for Effective Network Interconnectivity Among Multiple Partners in a Disaster-Embattled Region: A Content Analysis of an Exploratory Focus Group Study. *Journal of Contingencies and Crisis Management* **18**:10.1111/jccm.2010.18.issue-3, 155-164. [CrossRef]
8. Stuart B. Murchison. 2010. Uses of GIS for homeland security and emergency management for higher education institutions. *New Directions for Institutional Research* **2010**, 75-86. [CrossRef]
9. Bhaskar ChoudhuriThe Management School, Sheffield University, Sheffield, UK Stuart MaguireThe Management School, Sheffield University, Sheffield, UK and Udechukwu OjiakoDivision of Project Management, University of Northumbria, Newcastle upon Tyne, UK. 2009. Revisiting learning outcomes from market led ICT outsourcing. *Business Process Management Journal* **15**:4, 569-587. [Abstract] [Full Text] [PDF]
10. Wing S. ChowDepartment of Finance and Decision Sciences, Hong Kong Baptist University, Kowloon Tong, Hong Kong, China Wai On HaDepartment of Finance and Decision Sciences, Hong Kong Baptist University, Kowloon Tong, Hong Kong, China. 2009. Determinants of the critical success factor of disaster recovery planning for information systems. *Information Management & Computer Security* **17**:3, 248-275. [Abstract] [Full Text] [PDF]
11. Ali H. Al-BadiInformation Systems Department, Sultan Qaboos University, Al-Khoudh, Oman Rafi AshrafiInformation Systems Department, Sultan Qaboos University, Al-Khoudh, Oman Ali O. Al-MajeeniSchool of Computing Sciences, University of East Anglia, Norwich, UK Pam J. MayhewSchool of Computing Sciences, University of East Anglia, Norwich, UK. 2009. IT disaster recovery: Oman and Cyclone Gonu lessons learned. *Information Management & Computer Security* **17**:2, 114-126. [Abstract] [Full Text] [PDF]
12. Tao Xie, Abhinav SharmaCollaboration-Oriented Data Recovery for Mobile Disk Arrays 631-638. [CrossRef]
13. Dong-Her ShihAssociate Professor, Department of Information Management, National Yunlin University of Science and Technology, Yunlin, Taiwan Hsiu-Sen ChiangMaster's Student, Department of Information Management, National Yunlin University of Science and Technology, Yunlin, Taiwan. 2004. E-mail viruses: how organizations can protect their e-mails. *Online Information Review* **28**:5, 356-366. [Abstract] [Full Text] [PDF]
14. Jacques BothaDepartment of Information Technology, Port Elizabeth Technikon, Port Elizabeth, South Africa Rossouw Von SolmsDepartment of Information Technology, Port Elizabeth Technikon, Port Elizabeth, South Africa. 2004. A cyclic approach to business continuity planning. *Information Management & Computer Security* **12**:4, 328-337. [Abstract] [Full Text] [PDF]
15. Oscar Imaz-MairalBusiness Continuity Planning 163-172. [CrossRef]