Disaster Management 8

8.1 Introduction

Webster's Dictionary defines *disaster* as a sudden misfortune, a catastrophe that affects society [1]. It is the effect of a hazardous event caused by either man or nature. Man-made disasters are those disasters that involve a human element like intent, error, or negligence. Natural disasters are those caused by the forces of nature like hurricanes, tornados, and tsunamis. Disasters, natural or man-made, may cause great devastation to society and the environment. For example, the 2006 tsunami in Southeast Asia caused both huge human losses and environment destruction. The effects of a disaster may be short lived or long lasting. Most disasters, both man-made and natural, have long-lasting effects. To mitigate disaster effects on society and businesses, disaster management skills are needed.

In information technology, disaster situations are big security problems to the enterprise information systems that must be handled with skills just like other security problems we have discussed so far in this book. To understand how this is a very big security problem for a modern society, one has to understand the working of a modern business entity. Modern businesses have moved away from the typewriter and manila folders to desktops and large databases to process and store business day-to-day data and transactions. This growing use of computers in businesses, the ever-increasing speed of data transmission, and the forces of globalization all have forced businesses into a new digitized global corner that demands high-speed data access to meet the demands of the technology-savvy customers in a highly competitive global environment. In response, high-volume and high-speed databases have been set up.

For the business to remain competitive and probably ahead of the competitors, all business systems must remain online and in service 24/7. No modern business can afford a disaster to happen to its online systems. Failing to achieve that level of service would mean the failure of the business. Thousands of businesses close or lose millions of dollars every year depending on the level of attention they give to their online systems and failing to protect them against disasters like fire, power outage, theft, equipment failure, viruses, hackers, and human errors. No business

J.M. Kizza, *Guide to Computer Network Security*, Computer Communications and Networks, DOI 10.1007/978-3-319-55606-2_8

can succeed in today's environment without plans to deal with disasters. The September 11, 2002 attack on New York financial district was an eye-opener to many businesses to be prepared for disasters. For a quick recovery of these enterprises, good disaster management principles are needed.

Also as company databases grew in size and complexity and the demand for their online fast access grew, the need for the protection of business-critical and irreplaceable company data is also growing in tandem. These developments are forcing business information system managers to focus on disaster prevention, response, and recovery. The importance of disaster planning and recovery can be born by the fact that 93% of the companies that did not have their data backed up properly when a disaster struck went out of business, according to DataSafe, Inc., one of the leading companies involved with data backup services [2].

The goal of chapter, therefore, is to treat disaster management as a major information systems' security problem and start a discussion of ways, tools, and best practices of dealing with disasters and mitigating their long-term effects on business information systems. We will break the discussion into three parts: disaster prevention, response, and recovery.

8.1.1 Categories of Disasters

Before we do that, however, let us look at the categories of disasters that can affect business information systems [3].

8.1.1.1 Natural Disasters: Due to Forces of Nature

- Tsunami
- Tornados
- Hurricanes (same as tsunami)
- Cyclone (same as tsunami)
- Flood
- Snowstorm
- Landslides
- Drought
- Earthquake
- Electrical storms
- Snowslides
- Fire

8.1.1.2 Human-Caused Disasters

- Terrorism
- Sabotage
- Theft

- Viruses
- Worms
- Hostile code
- War
- Theft
- Arson
- Loss of:
  - Power supply (both electric and gas). This can result in a large number of related failures like cooling system and machines.
  - Communications links.
  - Data.
- Cybercrime (many types)

8.2 Disaster Prevention

Disaster prevention is a proactive process consisting of a set of control strategies to ensure that a disaster does not happen. The controls may be people, mechanical, or digital sensing devices. Times and technology have improved both disaster prevention and recovery strategies. The elements of effective disaster prevention are the early detection of abnormal conditions and notification of persons capable of dealing with the pending crisis, for example, if you have a temperature detector to report on an air-conditioning failure as soon as the temperature starts to rise or a fire detector to gracefully power down all computing equipment before fire systems discharge. By detecting and treating minor problems early, major problems can be avoided.

Every system, big and small, needs a disaster prevention plan because the cost of not having one is overwhelming. According to Intra Computer, Inc., a disaster prevention and recovery company, in one of its surveys, 16% of those responding to the survey reported that a system-stopping event caused by environmental conditions occurred at least six times annually, and 12% of respondents put the minimum estimated dollar cost of each of these incidents at over $50,000 [4]. Also according to DataSafe, Inc. [2], thousands of businesses lose millions of dollars worth of information due to disasters like fire, power outage, theft, equipment failure, and even simple operator mistakes.

In past years, system disaster prevention depended entirely upon an on-site person's ability to detect and diagnose irregular conditions based on experience. This experience was based on one's knowledge and ability to analyze conditions created by unusual events such as high temperature, presence of smoke, water, and interruption in power to equipment that could lead to the likely corruption or destruction of the enterprise's information system's resources including active data files.

Technology has, however, through intelligent monitoring devices, helped and improved the process of disaster prevention. Monitoring devices nowadays are capable of quickly responding to unusual and irregular conditions caused by a disaster event. The monitoring devices, in case of an enterprise information system, monitor a variety of conditions from a given list. The list includes [4]:

- Temperature
- Humidity
- Water
- Smoke/fire
- Airflow
- AC power quality
- UPS AC/battery mode
- Personnel access security
- Halon triggering state
- State of in-place security/alarm systems
- Hidden conditions undetectable by security personnel
  - In air-conditioning ducts
  - Under raised floors
  - Inside computer chassis

During the monitoring process, if and when an event occurs that meets any one of the conditions being monitored, an immediate action is triggered. The choice of action taken is also predetermined by the system manager and is selected from a long list that includes [4]:

- Activating local or remote alarms indicators like sirens, bells, light signals, and synthesized voice.
- Taking over control of the affected resource to isolate it, cut it off from the supply line, or maintain the declining supply line. The supply line may be power, water, fuel, and a number of other things.
- Interfacing with existing or cutting off from existing security system as dictated by the event.
- Sending a signal to designated personnel. Among the designated personnel are [4]:
  - System users
  - Site managers
  - Security personnel
  - Maintenance personnel
  - Service bureaus and Alarm Co. central offices
  - Authorities at remote sites
- Gracefully degrading the system by terminating normal operations, closing and protecting data files, and disconnecting AC Power from protected equipment.

After one or more of the actions above have been taken, the system will then wait for a response. The response usually comes from the human component. Let us discuss this in the next section.

8.3 Disaster Response

As we pointed out earlier in this chapter, the rapid development in computer and information technology and the ever-growing society's dependence on computers and computer technology have created an environment where business-critical information, irreplaceable business data, and transactions are totally dependent and are stored on computer systems. This being the case makes a response to a disaster vital and of critical importance. Disaster response is a set strategies used to respond to both the short-term and long-term needs of the affected community. In dealing with business information system disasters, the strategies involve quick and timely response to the disaster prevention system (DPS) signals with directed action. The essential steps in disaster response include:

- Restoring services
- Identifying high-risk system resources

Six factors govern a quick disaster response. According to Walter Guerry Green [5]:

- Nature and extent of the destruction or risk in case the disaster occurs. This is based on either prior or a quick assessment of the situation.
- The environment of the disaster. The environment determines the kind of response needed. Take a quick inventory of what is in the room or rooms where the systems are. Make a note of how the chosen action to meet the needs is going to be carried out successfully.
- Make note of the available resources. The degree and effectiveness of the response to the disaster is going to depend on the available resources on the ground that can be used to increase and enhance the success rate of the chosen response.
- Time available to carry out the chosen response action. Time is so important in the operation that it determines how much action can be taken and how much effort is needed to control the disaster.
- Understanding of the effective policy. Every chosen action taken must fall within the jurisdiction of the company policy.

The degree of success in observing this success determines the effectives of the disaster recovery efforts.

8.4 Disaster Recovery

The value of a good disaster recovery plan is its ability to react to the threat shifty and efficiently. In order for this to happen, there must be an informed staff, disaster suppliers, and planned procedures. These three make up the disaster recovery plan. Every system manager must be aware and confident with the system's disaster recovery plan. The plan must not only be on the books and shelved but must be rehearsed several times a year. For example, since the September 11, 2001 attack on the World Trade Center, companies learned the value of off-site storage of data. And since then, rehearsed procedures for retrieving archived data media from off-site facilities are common. There are several other outsourced options to disaster recovery in addition to the in-house one we have so far discussed. These include maintenance contracts and services that offer from routine planned disaster testing to full extended warranty services, standby services that usually do only the storage and recovery of your data services and delivery very quickly, and distributed architectures that are companies that sell you the software that stores your data on their network and you can move it back and forth at a moment's notice. All these, when used effectively, help to continue business as usual in the hours during and immediately following a disaster.

8.4.1 Planning for a Disaster Recovery

Disaster recovery planning is a delicate process that must be handled with care. It involves risk assessment, developing, documenting, implementing, testing, and maintaining a disaster recovery plan [6]. For starters, the plan must be teamwork of several chosen people that form a committee—the Disaster Recovery Committee. The committee should include at least one person from management, information technology, record management, and building maintenance. This committee is in charge with deciding on the what, how, when, and who are needed to provide a good solid recovery that your company will be proud of. Such a plan must sustain critical business functions. The planning process, therefore, must start with steps that identify and document those functions and other key elements in the recovery process. According to [7], these steps include:

- Identifying and prioritizing the disaster
- Identifying and prioritizing business-critical systems and functions
- Identifying business-critical resources and performing impact analysis
- Developing a notification plan
- Developing a damage assessment plan
- Designating a disaster recovery site
- Developing a plan to recover critical functions at the disaster recovery site
- Identifying and documenting security controls
- Designating responsibilities

Because disasters do not happen at a particular time in a given month of a known year, they are unplanned and unpredictable. This makes disaster recovery planning an ongoing, dynamic process that continues throughout the information system's life cycle.

8.4.1.1 Disaster Recovery Committee

This committee is responsible for developing the disaster recovery plan. The committee must represent every function or unit of the business to ensure that all essential business information and resources are not left out. Before the committee starts its job, members must all be trained in disaster recovery. Each member of this committee is assigned responsibilities for key activities identified and duties outlined within their departments and as defined within the disaster recovery plan. The committee is also responsible for bringing awareness to the rest of the employees.

8.4.2 Procedures of Recovery

The procedures followed in disaster management and recovery are systematic steps taken in order to mitigate the damage due to the disaster. These steps are followed based on the rankings (above) of the nature of the disaster and the critical value of the items involved.

8.4.2.1 Identifying and Prioritizing the Disaster

These may be put in three levels: low, medium, and high:

- Low-level disasters may be local accidents like:
  - Human errors
  - High temperature in room
  - Server failure
- Medium-level disasters may be less local including:
  - Virus attack
  - Long power failures—may be a day long
  - Server crush (Web, mail)
- High-level disasters—this level includes the most devastating disasters like:
  - Earthquakes
  - Hurricanes
  - Big fire
  - Terrorism

8.4.2.2 Identifying Critical Resources

The ranking of critical assets may be based on the dollar amount spent on acquiring the item or on the utility of the item. Some examples of these critical assets include [2]:

- Servers, workstations, and peripherals
- Applications and data
- Media and output
- Telecommunication connections
- Physical infrastructure (e.g., electrical power, environmental controls)
- Personnel

Rank them in three levels:

- Low level—these include:
  - Printer paper, printer cartridges, and media
  - Pens, chairs, etc.
- Medium level—these include relatively costly items:
  - All peripherals
  - Switches
  - Workstations
  - Physical infrastructures
- High level—these include valued items and high ticket items like:
  - Servers
  - Disks (RAID)/application data
  - Workstations
  - Personnel

8.4.2.3 Developing a Notification Plan

This requires identifications of all those to be informed. This can also be done based on the previous levels of the disaster and the level of critical resources. This plan is represented into a matrix form below.

	Low-level disaster	Medium-level disaster	High-level disaster
Level 1—critical assets	System adm.	System adm.	System adm., management, law enforcement, the media
Level 2—critical assets	System adm.	System adm., management	System adm., management, law enforcement, the media
Level 3—critical assets	System adm.	System adm., management	System adm., management, law enforcement, the media

For each cell in the matrix, chose an acceptable method of transmitting the information to be transmitted. Determine how much information needs to be transmitted and when it should be transmitted. For each group of people to be informed, choose a representative person. For example, for management, who should be informed, the vice president for information or the chief executive officer?

Keep in mind that prompt notification can reduce the disaster's effects on the information system because it gives you time to take mitigating actions.

8.4.2.4 Training of Employees

Since disaster handling is a continuous process in the life cycle of an enterprise system, the training of employees about possible disasters and what each one has to do is desirable. However, the training of the select people on the Disaster Recovery Committee is critical. Plan ahead of time how this training is to be carried out.

There are several ways of doing this in a work environment depending on the number of people to be trained:

- Professional seminars for all those on the Disaster Recovery Committee
- Special in-house education programs for all those on the Disaster Recovery Committee, heads of departments, and everybody else

The choice of the type of training also requires to determine who will be conducting the training and who is responsible for the arranging the training. Somebody responsible for training could be somebody well trained to do that if available in-house or by using a vendor to come on the component premises or by sending people to vendor-designated sites.

8.4.2.5 Priorities for the Restoration of Essential Functions

One of the most critical and vital bit of information in disaster planning is to prioritize the order of critical resources as they come back online. Follow that order because it was chosen by the Disaster Recovery Committee for a reason.

8.5 Make Your Business Disaster Ready

In the introduction, we talked about the importance of a recovery plan for a business. In fact, the statistics we quoted indicate that almost 90% of all companies that did not have a disaster recovery plan did not survive are indicative of the importance of a business disaster recovery plan. Also in the introduction, we indicated that disaster planning is an ongoing process that never ends. This means that for your company to remain in business and remain competitive, the disaster recovery plan must be in place and must keep changing to meet the developing new technologies. Among the things to help you refresh your evolving business disaster plan are being disaster ready all the time; making periodic drills of checking the storage media to make sure that they are already ready for the big one to happen, for those working with databases, working with a base-function script for the capability of your interfaces; and always periodically doing a risk assessment for the disaster.

8.5.1 Always Be Ready for a Disaster

Because disasters can happen at any time and while some customers will understand, the majority will not wait for you to learn the tricks of handling a disaster.

They will move to your competitor. Do always be prepared for the big one by doing the following [3]:

- Periodically check and test your backup and recovery procedures thoroughly to ensure that you have the required backups to recover from various failures, that

your procedures are clearly defined and documented, and that they can be executed smoothly and quickly by any qualified operator.
- Always secure, keep, and periodically check and review all system logs and transaction logs. This will help you to backtrack if you have to and to find anything you might have missed out.

8.5.2 Always Back Up Media

There is no better way to deal with a disaster than having a backup. We have been told since we were kids to keep a copy of everything important. You are doing the same thing here. In a computing system environment, also consider:

- A schedule to revisit the saved materials
- Whether to store at a location but in a different place or in a different location
- A chart of which data needs to be stored, where it is to be stored, and for how long

8.5.3 Risk Assessment

Risk assessment is a systematic process of evaluating a system's potential hazards and corresponding analysis of ways to mitigate damage if such hazards were to occur. One way of doing this is to use a matrix model consisting of all types of disasters that can happen to a system in a row and all the system resources that may be affected in each column. Each entry in the matrix cell is potential risks to the organization which could result to the resource in case of the disaster in that row occurring. This matrix model must have been done by the Disaster Planning Committee. There are tools on the market to help you achieve this, including COBRA [3].

8.6 Resources for Disaster Planning and Recovery

As businesses begin to see disasters as a huge security problem to the day-to-day running of the business, there is going to be a high demand for tools and services from vendors to manage disasters. These resources fallow into two categories: public agency-based and vendor-based resources. Also whether public- or private-based resources, these resources can be obtained quickly because they are local or they may take time because they are some distance off. Always start with local resources when you need them.

8.6.1 Local Disaster Resources

These resources can be freely obtained locally:

- Police
- Civil defense

- Fire department
- Ambulatory services

These resources can be obtained on the business premises:

- Paper
- Fire extinguisher
- Small capacity tapes and disks

These resources can be obtained from vendors (online or offline):

- Specialized computer equipment
- Specialized software tools like COBRA

Exercises

1. List as many of the emergency agencies in your community.
2. Of these listed in (1) above, which are dealing with information security?
3. We pointed out that the development of a good disaster recovery plan requires risk assessment. Design a matrix for the risk assessment of your security lab.
4. Using your security lab as your fictitious company, develop a disaster plan for the lab.
5. Study vendor tools in disaster recovery. Write about five of them, listing their merits and costs involved.
6. Study and develop a list of companies offering disaster recovery services in your area or state. Write about five, listing their merits and fees charged.
7. Based on your plan in (4) above, develop a rescue plan for the lab by developing a list of tools needed by the lab for disaster recovery, when needed.

Advanced Exercises: Case Studies

1. Check to see if your university has a disaster plan. Prepare a disaster plan for your university. Note that it should have the major headings as follows: (1) Introduction, (2) Emergency Procedures, (3) Response Plan, (4) Recovery Procedures, (5) Other Emergencies, and (6) Local Supplies.
2. Form a committee, whose size depends on the size of your college. Empower the committee to develop a disaster recovery plan for the college.
3. Consider the following company. HHR is a company involved with retail advertising. Major national chains use it to host their online catalogs. Every day, HHR gets about 5000 hits. It has four departments (Human Resources, Accounting, Advertising, IT), and employs about 2000 people nationally. The company is just getting started with disaster recovery and they have hired you to do it for them. Write a two-page document to the CEO of HHR selling your services.

4. Draw a plan of how you will go about setting up a Disaster Recovery Committee, indicating who will be in it and why. Also send a memo to the committee members telling them about the first organizing meeting, and list out the items to be discussed by the committee.
5. Develop a disaster recovery plan for HHR.

References

1. John Gage Allee (ed) (1998) Webster's dictionary. Literary Press, 1958
2. DataSafe, Inc., What is disaster planning? http://www.amarillodatasafe.com/abstracts.htm
3. The Disaster Recovery Guide (2002) http://www.disaster-recovery-guide.com/risk.htm
4. Intra Computer, Inc. Elements of an effective disaster prevention system. http://www.intracomp.com/page5.html
5. Walter Guerry Green (2001) Command and control of disaster operations, Universal Publishers, Inc/uPUBLISH.com
6. Erbschloe M (2003) Guide to disaster recovery. Course Technology, Boston
7. USAID. Disaster recovery planning procedures and guidelines. http://www.usaid.gov/policy/ads/500/545mal.pdf