# Global Information Assurance Certification Paper

# Disaster Recovery: Survivability & Security

Linda E. Ridgway
Version 1.4b GIAC Practical Assignment
27 October 2003



## Abstract

Since September 11, 2001, Disaster Recovery has become one of the hottest topics in businesses and governments. Disasters as defined in, “So-Called ‘Small Disasters’ Can Equal Big Trouble (Disaster Recovery Journal, Fall 2002, Vol. 15 No. 4) by Ron Levine [1] are, “natural weather storms, tornados, hurricanes, fires, earthquakes, and explosions”. The Disaster Recovery Guide goes on to name, contamination, environmental, epidemics, war, loss of utilities and fuel, mergers, and legal problems also under the heading of ‘disasters’ [2]. To this list we can now add disgruntled employees, thieves, manmade mayhem such as strikes, mobs, bombings, etc. and now… terrorism.

There have been a number of previously written books and articles, some more than 25 years ago, describing the mechanics of disaster recovery to include the survivability and security in a number of areas. ”Any crisis management plan prior to Sept. 11, 2001, is obsolete since it does not deal with many of the new potential terrorist activities that are now part of our consciousness” [3] as defined by Edward Moed. To meet these growing demands hundreds of new businesses have been started since the fall of 2001, in addition over 200,000 articles, videos, and CDs have been published on this subject. Today most Disaster Recovery Plans (DRP) handle the area of equipment, network, data, key personnel, and the organization in many types of disasters. In today’s environment, the following areas require a closer look: physical surroundings, data, key personnel, and the organization as an individual entity as well as where the coordination of the Business Continuity Plan (BCP) and DRP coordinator belongs in the organization. And why the BCP plan and DRP coordinator belong there where they are assigned in the organization.

**Survivability/Security of the Physical Surroundings**

Some initial questions to ask in the area of physical surroundings include:

- How strong are the structures after the disaster?
- Can the organization/government operate on the site or in the structures?
- How secure is the site or structures from additional manmade or natural disasters?
- Have any physical security measures been breeched due to the disaster?
- What will it take to make the physical surroundings and structures as secure as before the disaster?
- How secure is the structure from uninvited guests from freely entering the structure without proper authorization?
- How long and what will it take to resume business to the prior operational capabilities?
- What about the surrounding area? Is there any damage, danger, etc that will prevent key personnel from accessing the site or structures?
- What will it take to get power, water, and sewage back into operational order?
- How soon can we get our key personnel into place to put the site and/or structures back into operational order?
- And always, ensuring the safety before, during, and after a disaster has struck an organization.

All of these questions and others not thought of, until a physical disaster or simulation of, has taken place, should be placed into the organization's DRP as a checklist. Key personnel will only need to react quickly and accurately to each disaster as addressed in their DRP. Steve Davis developed a comprehensive emergency management program (CEMP) chart (see inset below) that assists an organization's DRP team to make the 'right call' [4]. For those disasters not previously defined, there should be enough information from other DRP checklists to be able to resolve to the best of the abilities of the DRP coordinator and their team.

CEMP Plan Components

| CEMP | Mitigation | Disaster Recovery | Business Continuity | Business Resumption | Contingency Planning |
|---|---|---|---|---|---|
| Objective | Prevent or Reduce Impact | Critical Computer Apps | Critical Business Processes | Process Restoration | Process Workaround |
| Focus | Prevention | Data Recovery | Process Recovery | Return to Normal | Make Do |
| Example Event | Flood Proofing | Mainframe or server failure | Labratory Flood | Building Fire | Loss of Application |
| Solution | Check Valve | Hot Site Recovery | Dry Out & Restart | New Equip. New Bldg. | Use Manual Process |

To determine the survivability of a structure these questions must be answered, along with key pieces of information that have been identified about the organization, its purpose, and its personnel be placed into an organization's DRP:

1. Which disaster risks are considered and addressed,
2. What are the building specifications/structure integrity as far as each risk is assessed,
3. What types of tests can/have been performed on the materials used in the testing of building structure materials.

Organizations must work with the local and national and in some cases international agencies to determine the operational survivability of a structure and the surrounding area once a disaster has occurred. It can be very helpful if the organization has already built a working relationship with the agencies that will be inspecting the damaged structures. Knowing these pieces of information can assist in determining what options should be considered when looking into the survivability and security of the physical structure as an entity. Each area of the site and physical structures must be considered, evaluated, and the recovery process to each MUST BE documented and/or revised in the organization's DRP.

In Nancy Green's article "Life after Death", she uses Dr. Judith Herman's model of recovery for individuals and applies it to an organization's recovery process [5] to demonstrate how the recovery process can be used in the organization as well as the individuals:

- The first stage of her model, deals with safety and control of the environment after the disaster.

- The second stage deals with remembrance and mourning, this allows the individuals and the organization to establish control over the disaster that has beset the organization [5] and its employees.
- The last stage is to reconnect to normal life for the individual and the organization [5].

This is key for an organization to returning to normal operations as they were before the disaster or crisis.

For the physical surroundings, some natural disaster risk assessments can include the pre-planning of actions to take before the 'storm' strikes and while it is upon the organization's physical surroundings to include the land, buildings, and nearby roads, which could be obstructed by water, fire, or debris. Then the DRP team must come in (if not already onsite) after the disaster has struck (and it is safe), assess the roads leading to the area and the physical structures, determine what actions need to be taken, and in which order, based upon the organization's DRP to include securing the area from unauthorized personnel and protecting key personnel while they are onsite.

This may also include:

1) The installation or repairing of a perimeter fence to protect the physical surroundings and structures,
2) The hiring of additional security force, as necessary, to protect the site and physical structures,
3) Working with the local agencies to open and/or repair roads, as needed, leading to the site,
4) Assessing and repairing, if possible, of structures on the site,
5) Purchasing/Leasing of temporary structures (onsite or offsite), if structures cannot be occupied immediately,
6) The installation of and/or repairing locks and gates,
7) Building/repairing protective barriers from natural disasters for the site and structures, if needed,
8) The hiring of temporary contractors as needed to repair and/or replacing of parts on the site and/or structures,
9) Assessing and determining the timeline, purchases, repairs, and associated costs with putting the site and/or structures to full operating conditions, and
10) The temporary placement of electronic surveillance cameras and warning signs as needed.

Assessing and reviewing each of these questions, within the scope of each disaster, will allow the DRP team, agencies, contractors and/or business partners to pre-plan for many types of disasters and the responses that can affect an organization's physical surroundings and structures survivability and in the nearby community as a whole.

**Survivability/Security of the Data**

Some initial questions to ask in the area of data include:

- How much data was lost?
- What would it take to get the data back to operating condition?
- How good are the Business Continuity Plan (BCP) procedures (backups, data replication, sister sites, etc.) to use as part of the data recovery process?
- What about key access points to the system or data?
- Has there been any security breech in the system or data?
- Has any data been compromised?
- Do we have the key personnel to restore the data (onsite, offsite, sister site)?

To also include some simple or inherent questions in the DRP risk assessment like:

- How often is the computer room cleaned?
- Are cleaning personnel cleared or escorted?
- How is the computer room cleaned; swept, wet mopped, dusted, vacuumed?
- Does the equipment have preventive maintenance (PM) performed?
- If yes, how often and what type of PM is performed on the equipment?
- If not, is there a repair or maintenance contract in place to bring in parts and equipment to put the systems and data back to operational conditions?
- Is the organization's data stored on a centralized system or in a distributed environment (many buildings, many sites, mirrored, duplicated)?
- How is the data protected (cipher locks, controlled access) and backed up (data replication, tape/disk copies)?
- How is the data output safeguarded if the data is business sensitive or classified?
- How is bad or old media destroyed to prevent the data from being compromised?

As defined in Ron Levine's article "How critical is the data to the organization?" [1] Knowing the answers to these questions and many others as defined in an organization's DRP will help the DRP team determine the recovery approach to take (lease/repair/purchase) and the time it will take to recover from the disaster.

Most publications today, define data replication as the preferred method to preserve the data [1, 2, 6]; but disaster recovery plans need to be tailored to each specific organization/government operation. In the Hitachi Data Systems white paper by Mikkelsen and Attanese, "Addressing Federal Government Disaster Recovery Requirements with Hitachi Freedom Storage", their figure 2

(see inset below) is very useful in assisting decision makers in determining the best approach, for data restoration planning investigation which includes data replication locally and remotely [6] based upon financial systems such as the Securities Exchange Commission (SEC).

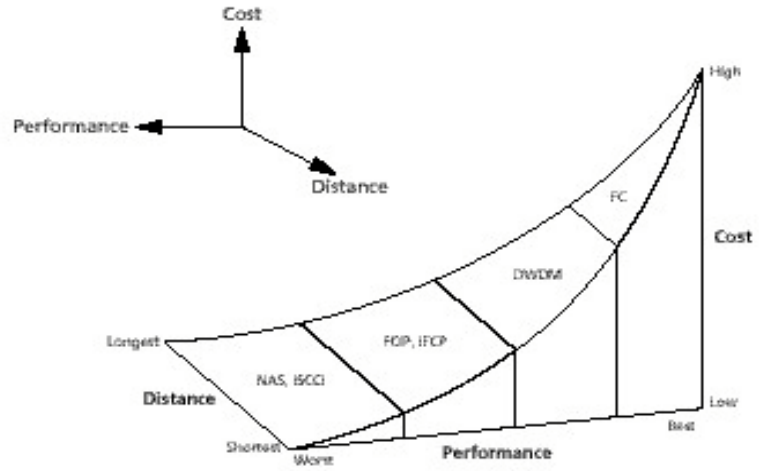


*Figure 2: Solution Area (Under The Curve) of Cost, Performance, and Distance.*

For many organizations data replication is a very affordable BCP option in their DRP. "According to a Needham & Company investment analysis, a common benchmark among Information Technologies (IT) managers is that one cent of data backup is worth $2,500 of data re-entry [7]." Some organizations are mom and pop businesses that cannot necessarily afford the equipment, or cost associated with data replication on duplicate hardware at another site, or on a data warehouse system where space can be 'rented' nor afford the $2,500 associated with data re-entry costs [7]. These organizations must look at what type of data disaster recovery methods will meet the cost replacement and benefits of their organization. Some government organizations cannot replicate their organization's data to data warehouses where sensitive or classified data could be compromised; again, another strategy must be investigated and implemented to meet these needs.

The Disaster Recovery Planning Guide produced by the University of Toronto provides a good quick reference checklist for the DRP Coordinator and team to use as a guide in creating an organization's DRP. But, if no other type of disaster recovery is performed, by any size organization --- back up your data! This can prevent the loss of as small as a minute/hour of an organization's work if the data is replicated. If an organization cannot implement data replication of data to another building or an offsite location, then some type of backup strategy should be developed and implemented. For small organizations such as a mom and pop business, backups of their small system(s) to a zip drive(s), tape drive(s), CD(s) or even floppies and taken to another structure on the site, to a sister site -- if available, or to a company that might specialize in the secure storage of your data, might be enough. For all types of storage selected, the media must be kept

in an environmentally safe and controlled storage area. Media cannot be stored in someone's desk drawer and expect to work 100% if a fire, flood, or tornado has struck the office; it may (if you are lucky) and then it may not; as Clint Eastwood's character Harry Callahan asks in the movie 'Dirty Harry' (1971), "Are you feeling lucky, punk?" [8]

Security of the data can be vital to an organization's survival. A cleaning formula for a small cleaning company that falls into a competitor's hands because the waste paper was not properly shredded could be a disaster; so proper media handling and security of the data is a critical part of data security.

The proper inventory control, and audit of sensitive documents and media are critical for all organizations, from a cosmetics company to an aerospace agency. Periodic sightings and inventory should be performed regularly and always after a significant happening or changeover of personnel, as well as, a disaster that could have affected the site, structure, personnel, or data of an organization.

Computer room cleaning is often overlooked for possible system/data loss causes. Some cleaning issues that could have an impact on the systems and/or data integrities, are:

- Ensuring that the computer room is cleaned regularly,
- Ensuring the old media is properly disposed of
    - Shredded if paper,
    - Degaussed/magnetized if magnetic,
    - Smashed/crushed if optical disks [CDs]),
- Ensuring that all cleaning personnel have the required authorization to access the computer facility or offices where data may be present,
- Escorting all cleaning personnel who are not cleared for access, and
- Verifying, if possible, that the appropriate computer room cleaning supplies are used (low lint sweepers and mops, appropriate floor cleaners, etc.).

In preparing for disasters the DRP team should review the organization's PM contracts to see:

- What type of response is defined for emergency repairs,
- What type of response is defined for normal repairs,
- Is the system covered by routine PMs to reduce the risk of hardware failure,
- If routine PMs are scheduled, what is checked/covered under them and how often are they performed, and
- Does the organization have any type of contracts and/or business partners to analyzed 'crashed media' for possible reclamation, if so, at what cost.

Using available DRP tools to assess the risks and disasters associated with system/data loss will allow the DRP team, managers, agencies, and contractors

or business partners to pre-plan for many types of disasters and the appropriate response for the organization's system/data.

**Survivability/Security of an Organization's Personnel**

Some initial questions to ask in the area of personnel include:

- Was anyone lost or injured? If so, who and what was their position in the organization?
- Where are key personnel (onsite/offsite/vacation/injured/killed)?
- How about key personnel families (anyone injured or lost that would have an impact on the key personnel's ability to respond)?
- What type of security is afforded key personnel?
- Is there physical security still in place onsite?
- During the recovery process, what part of the DRP team is needed, at what point, during the recovery?
- What level of depth is required for each key personnel team's position?

Whenever a disaster strikes, the appropriate DRP is put into action. The initial assessment of the disaster, should define who the key personnel are by name and/or position within the organization for that type of disaster. There could be different key personnel on the DRP team depending upon the type of disaster that has struck the organization. An auto mechanic for a delivery business may not be required to be a member of the DRP team if there is a fire in the accounting building whereas most financial managers may be. A secretary may not be required to be a member of the DRP team if a flood has struck the warehouse of a toy company whereas the inventory control manager may be.

Once the initial assessment has been defined, are the key personnel already onsite and available to execute the recovery process?

Part of the DRP that has been given little to no mention is the welfare of the key personnel's families and homes that may be affected by the same disaster. Each organization should develop a DRP plan that will address:

1) How the key personnel are determined for each type of disaster,
2) Are there areas that are deemed to be 'safe and secure' for key personnel to occupy during a disaster (if needed or required to be onsite during the disaster),
3) Are key personnel to be onsite before a natural disaster strikes or to report immediately after the danger has pasted,
4) If key personnel are to be stationed onsite before and during a natural disaster how and when will key personnel receive personal information about their families and homes while recovering the organization's facilities, equipment, and their data, and
5) What type of assistance (food, lodging, transportation, etc.) will be provided to key personnel (and their family) during the recovery

process so that they can concentrate on the organization's recovery to normal operations?

Some Disaster Recovery Plans implement crisis and trauma counseling as part of the recovery process for their employees. These types of counseling can also be used within the organizational structure providing mental health to the individuals and the operational functioning capabilities of the organization as they recover [5]. In Dr. Judith Herman's model, the second stage deals with remembrance and mourning, this allows the individuals and the organization to establish control over the disaster that has beset the organization [5] and its employees.

In the event that key personnel are lost or cannot quickly respond to the disaster, backup personnel should be identified in the DRP. These key personnel (and backups) should be identified in the DRP to include:

- Their name,
- Home phone,
- Cell phone,
- License tag numbers of their vehicles (in the event of accidents),
- Their email,
- Their address, and
- Directions to their residences.

This section should be one of the appendices of the DRP that can be quickly updated without revising the whole document every time any information changes. For some key personnel positions in the DRP, critical areas, may need to be defined three layers deep to be able to have the appropriate personnel with the knowledge and skills to recover from the disaster readily available. Offsite or sister site key personnel are very useful with business partners in disaster recovery plans that have created partnerships in the community for quick recovery of an organization's operations. The ability for key personnel to be able to receive and provide information on their well being of their families and as well as themselves during the crisis can have a dramatic effect on the organization's recovery time. Depending upon how this sensitive topic is reviewed, prior to a crisis with key personnel, will determine how well key personnel can/will perform on the job during the crisis

The physical security of key DRP personnel should be covered under the physical surroundings section of the DRP. The security access level of key personnel would be performed before the disaster by the necessary background requirements and checks of the organization; or escorts, pre-defined to escort key personnel not cleared for sensitive area recovery.

Using available DRP tools, managers and organizations should assess the risks and disasters with respect to the DRP team, managers, employees, and contractors or business partners to pre-plan the assignment of key personnel for

many types of disasters and the appropriate response of the organization's DRP team and the team makeup for each type defined.

**Survivability/Security of the Organization & the Business Continuity Plan**

Some initial questions in the area of the organization include:

- How much down time is possible before an organization/government project is determined to be a loss?
- What is the cost of replacement of the process, structure, personnel, data, and/or organization?
- Should the DRP coordinator be placed in the security department?
- Should the DRP coordinator be placed in the IT department?
- Should the DRP coordinator be placed in the human resources (HR) department?

In Dr. Judith Herman's model, the last stage is to reconnect to normal life for the individual and the organization [5]. This is key to returning to normal operations as they were before the disaster or crisis.

What might be the key for a small baking company to resume to normal operations might not be the same key for a large stock brokerage firm. A loss of a small baking company's receipts caused by a corrupt disk might be the end of the company, if, there is no backup or paper copy from which to re-key the information. While the loss of a stock broker's account transactions for the day from a corrupt disk might be an inconvenience while the data is recovered from online data backup or replication site, the transactions are not lost nor have to be re-keyed in.

Investment in backups can prove to be a vital lifeline for any company. An organization can spend from several hundred of dollars for a small tape library & the needed tapes to maintain adequate backups of a small organization to several hundreds of thousands of dollars investment in backup systems, software, and media to maintain for a mammoth organization. Remembering that with tape/disk backups that there will be a replacement cost that will need to be computed into the equation when the media has reached/exceeded its life expectancy. This replacement cost can range from several hundred to thousands of dollars per year depending upon life expectancy of media and how often it is used.

Within the DRP, must be the Business Continuity Plan, which defines the remedies for each of the key elements of the organization and its ability to resume normal operations within a reasonable timetable [9] from a disaster. Many books and articles say that the coordinator of the Business Continuity Plan should be assigned to the top of the organization while others believe that the DRP coordinator should be part of the Organization's IT, HR, or Security

departments. No matter where the DRP coordinator is placed he/she must have top-level support [10] to develop, test, implement, and maintain the organization's DRP and BCP as a viable plan that will guarantee the survivability of the organization as an entity.

Should the DRP coordinator be placed in the security department? It depends. If the security department should be one of the first members already onsite before a natural disaster strikes or one of the first members to arrive during a manmade disaster like a fire or explosion. Also the security department should be the team that secures the site from unauthorized personnel from entering.

Should the DRP coordinator be placed in the IT department? It depends, some reasons for a yes response, it might be that the IT department knows what data is critical to the organization's and needs to be recovered quickly. This might be true if the disaster is just a system or disk failure, but may not be true if the disaster is a fire or explosion.

Should the DRP coordinate be placed in the HR department? It depends, some reasons for a yes response, it might be that the HR department knows each employee's position and what their work positions detail in respect to the organization's structures, data, security, public relations, and management and can quickly identify those employees key to disaster recovery for the type of disaster that has occurred. This might especially be true if the organization has a high duty to be open to the public on anything that could impact the surrounding community with respect to the disaster that has occurred at the organization's site.

Without the dedicating the necessary resources (personnel, data, physical surroundings, etc.) to implement and maintain, thoroughly tested, periodic reviews, and updates to a disaster recovery plan the organization will not successfully survive a disaster [11]. Without reviewing in detail the survivability and security for key personnel, data, physical surroundings, and the DRP and BCP, the organization will not survive! Organizations should take the necessary time and resources to review their DRPs and BCPs for layers of protection and coverage of critical positions, so their organization will not fail, while there is still ample time for creating, editing, reviewing, and testing. Even though an organization has a documented DRP, it should be reviewed at least once a year for any updates (system replaced, application upgraded, key personnel changes, more data requirement needs) at a minimum.

Many organizations have DRPs, BCPs, and some have CEMPs that have been developed and written addressing their organizations operations. Once an organization has selected an overall coordinator of their Disaster Recovery and Business Continuity Plans and the position location within their organization; then the process should be that the key personnel of each critical process and area of

the organization be identified and selected. Once the team has been established, it will be their role (with key management support) to begin the process of:

- Looking at what each component of the organization is,
- Working to identify what the critical operations and/or processes of the organization are,
- Updating key personnel assignments as needed during the review cycle,
- Creating and/or revising their organization's DRP, BCP and CEMP as needed,
- Testing (as much as possible) each process identified in the plan for the various disasters identified,
- Revise the DRP, BCP, and CEMP as needed,
- Test again, once updates are incorporated into the DRP, BCP, and CEMP, and
- Determine the criteria that will be used to trigger an update (new application, new process, new disaster identified, changeover of personnel, time cycle limit reached).

Many organizations may not know how to begin this process and just throw up their hands and say, 'we do backups therefore we have disaster recovery'. This can be seen, by recent natural and manmade disasters, is not a true statement. For a small business, looking from the top-down may be the logical approach since the management level might be small and compact enough to be able to objectively see the organization's survivability and security without too many obstructions. For a large organization, looking from the top-down, may decide it is too large to try a top-down approach all at once. They may determine it is best to take one piece of the organization's business plan/goal and work thru each type of disaster, then move onto another department and repeat the process. This type of approach to disaster recovery could produce a multitude of different disaster recovery plans that will then need to be coordinated into one DRP with the survivability and security of the organization as a whole as the final goal. Whichever approach is taken by the organization and whichever department the DRP coordinator is placed it MUST HAVE TOTAL MANAGEMENT BUY-IN to be a successful DRP.

## Conclusion

While much investigation and research has been completed in these areas, investigation and research should continue in all of these areas more is still needed. Each organization must determine if they have fully addressed these and other issues that are critical to the survivability and security of their organization.

Some organizations may determine during their review cycles that they have adequately addressed these areas and other questions/answers not detailed in this paper, some may determine that there is still much revision work to be completed. Whichever decision is reached, September 11, 2001 has taught us that we need to be ever vigilante in creating, maintaining, testing and reviewing our Disaster Recovery Plans to preserve our businesses and government agencies.

By using the available resources (books, journals, articles, software packages, seminars, classes, conferences, and the internet) as a resource guide each organization can develop a an individual DRP that will assist their organization in it's survivability and security as an entity with respect to key areas, functions, and processes of their organization. The organization's DRP can include the organization's BCP and CEMP as tools and resources in assessing the risks and responses to each defined disasters.

Keeping always in their organization's mind:

**D**evelop a plan,
**I**dentify the disasters,
**S**eek out the key personnel,
**A**ssess the risks of each type of disaster,
**S**ecure the recovery process,
**T**est the plan (dry runs – paper or actual drills),
**E**valuate the test,
**R**evise and retest after updates
(Results from simulations, time cycle, personnel changes, technology updates, etc).
**S**urvivability and security of the organization is the goal!

## References


[1] Levine, Ron. “So-Called ‘Small Disasters’ Can Equal Big Trouble.” Disaster Recovery Journal Fall 2002. http://www.drj.com/articles/fall02/1504-16.html

[2] The Disaster Recovery Guide, Disaster Recovery Planning From A-Z. The Disaster Recovery Guide. 2002 http://www.disaster-recovery-guide.com/start.htm

[3] Moed, Edward. “A Crisis Plan is a ‘Must Have’ For Every Company.” Disaster Recovery Journal Fall 2002. http://www.drj.com/articles/fall02/1504-03.html

[4] Davis, Steve. “Developing Continuity in Government Planning.” Disaster Recovery Journal. Spring 2003. http://www.drj.com/articles/spr03/1602-01p.html

[5] Green, Nancy. “Life After Death.” Disaster Recovery Journal Fall 2002. http://www.drj.com/articles/fall02/1504-02.html

[6] Mikkelsen, Claus and Tom Attanese. Addressing Federal Government Disaster Recovery Requirements with Hitachi Freedom Storage. Hitachi Data Systems. November 2002 http://www.hds.com/pdf/fed_gov_wp_peri_128.pdf

[7] Real, Frank. “Tick … Tick … Tick … Time is Money When Recovering Lost Data.” Disaster Recovery Journal Fall 2002 http://www.drj.com/articles/fall02/1504-01.html

[8] The Dirty Harry Series. Dir. Don Sigel. 1974. Videocassette. Warner Studios, 2001.

[9] Herriott, Larry. “Business Contingency Planning Is…” 4 Dec 1997. http://www.drj.com/new2dr/w3_0006.htm

[10] Dato, Jeff. “Where Does Business Continuity Belong In Your Corporation.” Disaster Recovery Journal Fall 2002. http://www.drj.com/articles/fall02/1504-11.html

[11] Disaster Recovery Planning. Computing and Networking Services, University of Toronto. 1996-2002 http://www.utoronto.ca/security/drp.htm