NASA IV & V ANNUAL WORKSHOP 2012

The 4th International Workshop on Independent Verification & Validation of Software

Disaster Recovery Planning

Divya Krishnamoorthy

Mailam Engineering College, Mailam.

(Affiliated to Anna University Chennai, India.)

AGENDA

- Introduction
- Types of Disasters
- Principle causes of Disasters
- Phases of Disasters
- Computer Disaster Planning
- Benefits of Computer Disaster Planning
- Conclusion

INTRODUCTION

- Anything that prevents access to key processes and activities can be defined as a disaster.

- Disaster recovery is a set of loosely related activities that occur before, during, and after a disastrous event.

- The ideal disaster recovery process recognizes the possibilities of the situation, and manages the necessary activities so that they are solutions, not additional problems.

TYPES OF DISASTERS

Disasters that have occurred in similar businesses and companies in the same area may be researched to ascertain the type of threats facing a company. They are,

- Natural or environmental disasters
- Technical or mechanical hazards
- Human Activities or Threads

NATURAL OR ENVIRONMENT DISASTERS

- A natural or environmental disaster could be anything from a fire, flood, earthquake, hurricane, lightning storm or an air crash.

- The location of the business premises and the local environment needs to be assessed to determine the exact external threats that the company faces.

TECHNICAL OR MECHANICAL DISASTERS

- Technical Disasters includes the computers problems, instrumental failures, industrial disasters, equipments problems, etc

- Examples of technical threats include viruses, worms, power outages, backup failure, system failure and hacker attacks such as denial of service attacks.

HUMAN ACTIVITIES OR THREADS

- These include accidental and intentional activities.
- Malicious attacks may originate from hackers, paid professionals, disgruntled employees or organised crime gangs.
- Unintentional threats may come from employees who accidentally delete or update information.
- Over dependence on one key person is also a threat to the system.

TYPES OF DISASTERS

Potential Types of Exposure		
Natural Threats and Hazards	Technical and Mechanical Hazards	Human Activities and Threats
Fire	Power outage/failure	Computer error
Flood	Gas leak	Lost or misfiled documents/records
Hurricane	Software failure/malfunction	Vandalism
Earthquake	Sewage failure/backup	Theft
Lightning strike	Building structural failure	Bomb threat
Tornado, wind storm	Electrical shortage/faulty wiring	Civil disorder
Snow and ice storms	Toxic spill	Strikes
Wind	Radiation contamination	Kidnapping
Tidal wave	Loss of physical access to resources	Terrorism
Typhoon	Biological contamination	Sabotage
Mold and mildew	Train derailment/airplane crash	Loss of key personnel
Insects and rodents		Epidemic

PRINCIPLE CAUSE OF DISASTERS

➢ A library or archives disaster is an unexpected event which puts collections at risk.

➢ Disasters can be classified into two types. They are as follows

❖Natural Disaster

❖Man-Made Disaster

NATURAL DISASTERS

- Rain and wind storms
- Floods
- Biological agents (micro-organisms, insect or vermin infestation)
- Earthquakes
- Volcanic eruptions

MAN – MADE DISASTERS

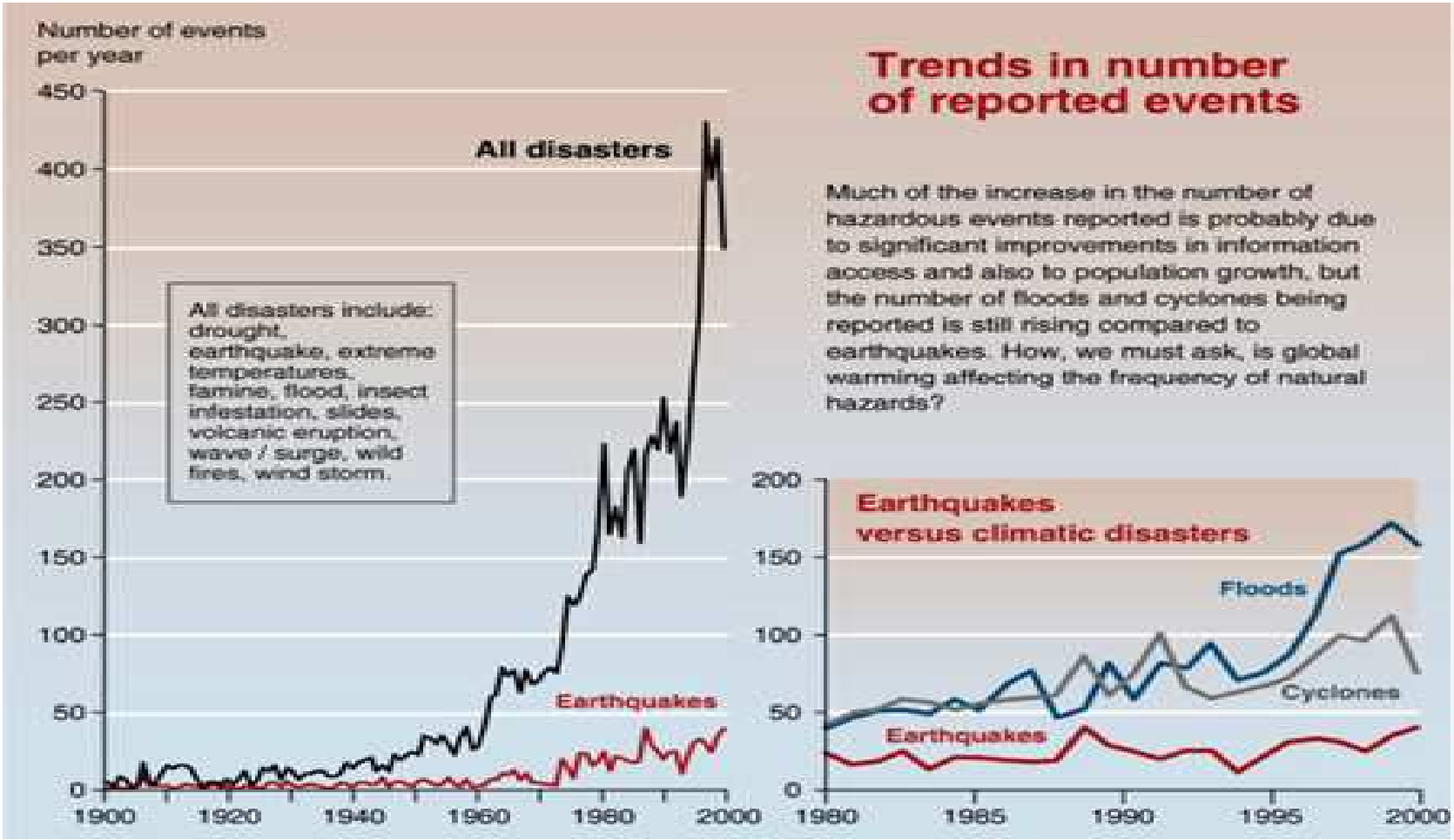
- Acts of war and terrorism
- Fires
- Water (broken pipes, leaking roofs, blocked drains, fire extinguishing)
- Explosions
- Liquid chemical spills
- Building deficiencies (structure, design, environment, maintenance)
- Power failures

SOME MAJOR EFFECTS OF DISASTERS

- Regardless of the many forms a disaster may take, the actual damage to collections is usually caused by fire or water.

- Even when they are not the initial factor, fires and floods almost invariably occur as secondary causes of library and archives disasters.

NATURAL DISASTER RATING



PHASES OF THE DISASTER

- The Disaster has four main phases. They are as follows,

  - Prevention
  - Preparedness
  - Response
  - Recovery

PHASE 1:

PREVENTION

- Identify and minimize the risks posed by the building, its equipment and fittings, and the natural hazards of the area.

- Carry out a building inspection and alter factors which constitute a potential hazard.

- Establish routine housekeeping and maintenance measures to withstand disaster in buildings and surrounding areas.

PHASE 1:

PREVENTION

- Install automatic fire detection and extinguishing systems, and water-sensing alarms.

- Take special precautions during unusual periods of increased risk, such as building renovation.

- Make special arrangements to ensure the safety of library or archival material when exhibited.

PHASE 1:

PREVENTION

- Provide security copies of vital records such as collection inventories, and store these off-site.

- Protect computers and data through provision of uninterrupted power supply.

- Have comprehensive insurance for the library or archives, its contents, the cost of salvage operations, and potential replacement, re-binding and restoration of damaged materials.

PHASE 2:

PREPAREDNESS

- Develop a written preparedness, response and recovery plan.

- Keep the plan up-to-date, and test it.

- Keep together supplies and equipment required in a disaster and maintain them.

PHASE 2:

PREPAREDNESS

➢Establish and train an in-house disaster response team. Training in :

✓Disaster response techniques

✓Identification and marking on floor-plans and enclosures of irreplaceable and important material for priority salvage.

PHASE 2:

PREPAREDNESS

- Prepare and keep an up-to-date set of documentation

- Distribute the plan and documentation to appropriate locations on- and off-site.

- Institute procedures to notify appropriate people of the disaster and assemble them rapidly.

PHASE 3:

RESPONSES

- Follow established emergency procedures for raising the alarm, evacuating personnel and making the disaster site safe

- Contact the leader of the disaster response team to direct and brief the trained salvage personnel

- When permission is given to re-enter the site, make a preliminary assessment of the extent of the damage, and the equipment, supplies and services required.

PHASE 3:

RESPONSES

- Stabilize the environment to prevent the growth of mould.

- Photograph damaged materials for insurance claim purposes.

- Set up an area for recording and packing material which requires freezing, and an area for air- drying slightly wet material and other minor treatment.

- Transport water-damaged items to the nearest available freezing facility.

PHASE 4:

RECOVERY

- Establish a programme to restore both the disaster site and the damaged materials to a stable and usable condition.

- Determine priorities for restoration work and seek the advice of a conservator as to the best methods and options, and obtain cost estimates.

- Develop a phased conservation programme where large quantities of material are involved.

PHASE 4:

RECOVERY

- Discard items not worth retaining, and replace or re-bind items not justifying special conservation treatment.
- Contact insurers.
- Clean and rehabilitate the disaster site.
- Replace treated material in the refurbished site.
- Analyse the disaster and improve the plan in the light of experience.

COMPUTER DISASTER PLANS

- To protect vital accounting information from loss, destruction, theft, and other threats, a company should prepare a comprehensive computer contingency plan.

- The computer contingency plan should have the following component plans:

  * Emergency
  * Back-up
  * Recovery
  * Test
  * Maintenance

COMPUTER DISASTER PLANS

EMERGENCY

- The emergency plan indicates actions to be taken immediately after a disaster.
- An important aspect of this plan is the preparation of a contingency organization chart, showing the name of the contingency manager and coordinators.
- The responsibilities of the contingency manager and contingency coordinators should be explained clearly.

COMPUTER DISASTER PLANS

BACKUP

- The second critical aspect of a computer contingency plan is the preparation of a back-up plan.

- The company should consider the following alternatives: utilization of data processing service bureaus, another company's computers, or a vendor's computers.

- To ensure a compatible computer is available on short notice, a mutually agreeable contract between the company and the other organization providing back-up facilities should be prepared.

COMPUTER DISASTER PLANS

RECOVERY

- The company should assess its ability to restore critical accounting information within an acceptable time period.
- A competent recovery team is a significant part of any recovery plan.
- The names, telephone numbers, specific assignments, special or alternative training needs, and other essential information of each team member must be shown on the recovery plan.

COMPUTER DISASTER PLANS

RECOVERY

- A section should indicate which recovery team members are responsible for establishing the timetable for the recovery operations and who decides if outside, temporary personnel are needed to complete the recovery on schedule.

- Also, the recovery plan should include procedures for coping with the non-availability of data processing personnel.

COMPUTER DISASTER PLANS

TESTING

- The computer contingency plan must be periodically tested to discover and eliminate problems.

- Many potential problems can be eliminated by developing a test strategy.

- The most effective way to determine if the contingency plan works is to conduct simulations of actual disasters.

- The results of the review should be utilized to identify any flaws in the contingency plan.

COMPUTER DISASTER PLANS

MAINTENANCE

- Finally, the company should ensure procedures are devised to keep the contingency plan current.

- Any necessary changes should be integrated into the documented plan, based on the simulated disasters.

- A plan of action should be prepared for the implementation of changes to ensure even greater protection from disasters.

BENEFITS OF COMPUTER DISASTER PLANS

- Enables a company to quickly restore its capabilities to process critical accounting information.

- Provide services and products for its customers efficiently and effectively.

- Preparation of such a plan forces a company to prioritize accounting applications into critical and non-critical categories.

- Thus, the company is able to continue processing critical accounting information, ensuring that it will not temporarily nor permanently cease operations.

CONCLUSION

- Although many sources claim a similar methodology for creating a disaster recovery plan, the plan must be heavily customized to the specifics of an organization.

- This may involve disregarding or combining multiple disaster recovery development phases.

- The success of a plan depends on its readability just as much as its comprehensiveness.

- Therefore, it is extremely important that a plan continues to be tested and maintained.

ACKNOWLEDGEMENT

- I would like to thank entire NASA IV & V team members for organizing such a Successful Workshop

- Also I would like to thank Mrs. Lisa Downs, NASA IV&V Annual Workshop Committee Chair for guiding me and helping me to present this paper in a successful ways.

REFERENCES

✓Hazards and Risk Virtual Library - by Impacts - Cultural Heritage
http://life.csu.edu.au/hazards/9CulturalHeritage.html

✓Disaster Preparedness and Response
http://palimpsest.stanford.edu/bytopic/disasters/

✓Disaster Planning for Libraries and Archives : Understanding the Essential Issues
http://www.nla.gov.au/nla/staffpaper/lyall1.html

✓Symantec Corporation. 2001. “Assets, Threats and Vulnerabilities: Discovery and Analysis.
A comprehensive approach to Enterprise Risk Management”.
http://enterprisesecurity.symantec.com/PDF/AxentPDFs/RiskMgmt.pdf

QUESTIONS
?