

How to Protect against Terrorism, Disasters, and Disaster Recovery (An introduction class)

Victor G. Williams
Information Technology
Macon State College
100 College Station
Macon, GA 31206
(478)757-7087

vwilliam@mail.maconstate.edu

This paper will discuss the “what, why, how and results of a class on “How to protect against Terrorism, Disaster and Disasters Recovery that was presented at Macon State College. The paper will also discuss feedback from the students that attended the class.

In response to the necessities to utilize more security and protection against terrorism in the United States, it is very important that the Information Technology (IT) student learn what to do to protect against terrorism, protect against disasters and what they should do once a disaster happens to their organizational computer systems. With these objectives in mind, Macon State College has started looking into offering courses that will meet the criteria and goals of teaching IT students the importance of protecting against terrorism and disaster recovery.

Macon State College offers a Bachelor of Science degree in Information Technology. This has proven so successful that the program has increased from 50 students in the fall of 1998 to over 1300 students.

The Class Outline

During the class the overall objective was to teach students different ways to help protect against disasters and to also give the student as much real world cases to help with the understanding of the lesson. The instructor also wanted the student to understand what are some of the tools that could also help with the overall protection in everyday life.

Below is outline for a class on “How to Protect against Terrorism, Disasters, and Disasters Recovery”. This outline includes Disaster recovery techniques, security, and crimes that may cause disasters.

Week 1: Induction to Disaster recovery

Week 2: The need for Security in Disaster recovery

Week 3: Crimes that will cause a Disaster

Week 4: Developing a Disaster Recover Plan

Week 5: The organization’s role in the Disaster Recovery Plan

Week 6: Testing your Disaster Recovery plan

Week 7: Emergency Operations Center

Week 8: Understanding computers and Networks

Week 9: Protecting the Network from Disasters

Week 10: Continued Assessment of Needs, Threats, and Solutions

Week 11: Future trends in Disaster Recovery

Summary

Not having a disaster plan can be a devastating event for you and your business. The 9/11 nightmares have caused many to rethink having a disaster recovery plan or question if the one they have is acceptable. *President Bush recently signed the Homeland Security act into law, authorizing the formation of the Department of formation of the Department of Homeland Security, which will have the authority to develop a plan to inventory and protect the nation's critical in-frastructures, telecommunications, financial and banking, energy, and transportation. Safeguarding the IT infrastructure in both the public and private sectors is expected to be a key part of the new department's work. All the U.S. Department of Justice has proposed new legislation that will give it the power to prosecute computer crimes as acts of terrorism.* (The information Management Journal)

Appendix A

Why should I write a plan?

The primary objective of a Disaster Recovery Plan is to enable an organization to survive a disaster and to reestablish normal business operations. In order to survive, the organization must assure that critical operations can resume normal processing within a reasonable time frame. In developing a Disaster Recovery Plan, you should include the following:

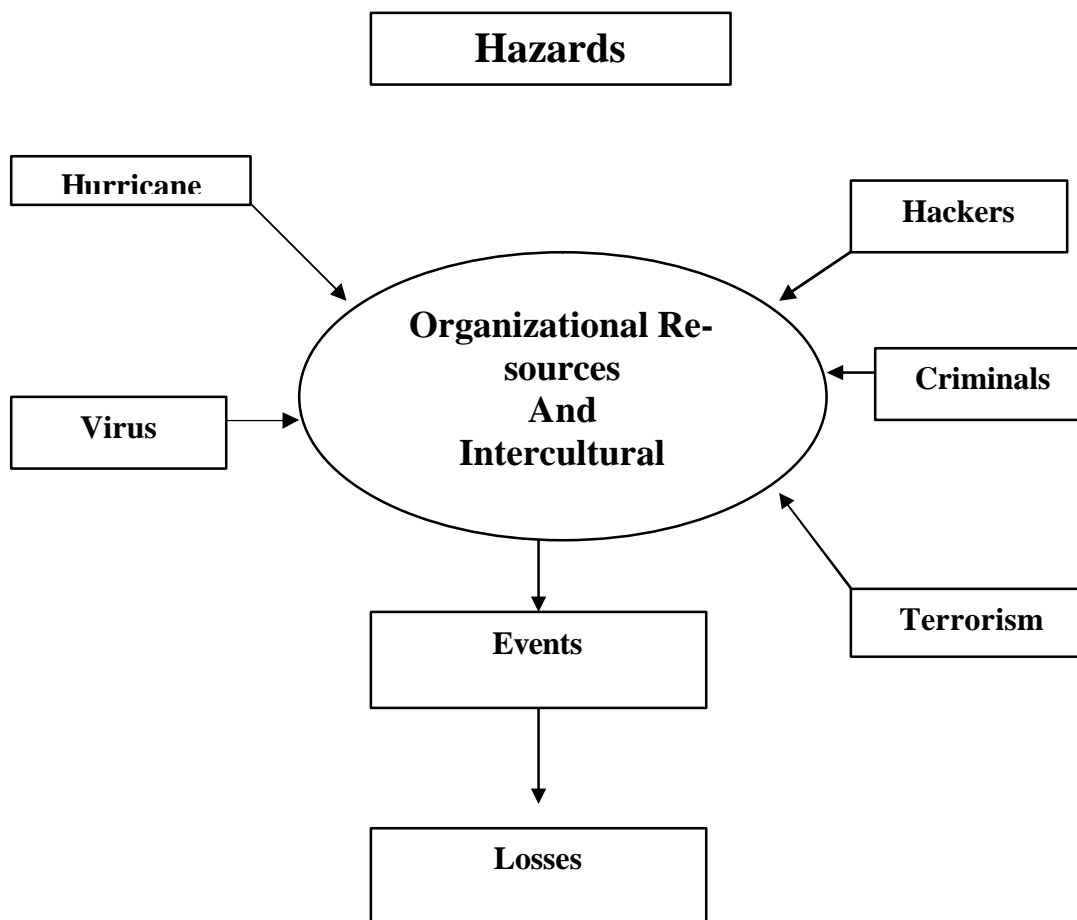
- Protecting all vital information from internal and external disasters.
- Restoring business to near normal operation without having major delays
- Facilitating an effective recovery tasks
- Developing an effective back up and recovery strategies to mitigate the impact of disruptive events

To have a feasible recovery plan strategy is not only the job of the business owner but the organization's data processing division, communications and operations divisions. It is also the users of those services and management personnel who have responsibility for the protection of the organization's assets. Many businesses have the misconception that disaster recovery planning is just for the IT department. Technology as well as business areas supported by Information Systems all must be play a significant roll throughout the project for the planning process to

be successful. Disaster recovery planners must keep in mind that the aim of the planning process is to:

- Evaluate existing weaknesses
- Implement disaster prevention procedures
- Develop a comprehensive plan that will enable the organization to react properly and in a timely manner if disaster strikes.

Potential Hazards That Impact Organizational Resources and Infrastructure



When is it time for a disaster plan?

The start of recovery must begin immediately. Advanced planning, in the form of a Disaster Recovery Plan, puts you in a position to do just that; plan. It will enable you to act appropriately to assure that a minor occurrence does not spiral into a major disaster.

Disaster recovery, when properly documented, addresses not only the recovery of core businesses, but also realizes the importance of support functions. A solid disaster recovery plan will

include the entire business. It was reported that 40% of companies that suffer a disaster goes out of business. Another survey sponsored by National Association of Corporate Treasurers, shows that more than 50% of CFO's felt that their companies were inadequately prepared for coping with disasters. Some business believe that creating an effective plan is time consuming process and one that requires expensive system change. What you need to do will depend on your business situation and structure and risk you may face. When building an effective disaster recovery plan, there are at least five questions you must ask yourself.

What are the mission critical functions?

What are my risks if this happens?

What are my current contingency measures and how effective is it?

What corrective actions must I take?

What are the action priorities and timelines?

You will find below an example of a disaster recovery plan. They also have software that is available to help you create and implement your plan.

Sample outline Of a Disaster/Contingency Plan

1

Introduction

- A. Policy Statement
- B. Purpose
- C. Overview
 1. Definitions
 2. Scope
 3. Objectives
 4. Structure of plan
- D. Planning Process Description (use of flow chart)
- E. Organization Documents
 1. Organization description
 2. Security/backup systems
 3. Floor plans of electrical, water, exits
 4. Insurance documents
 5. Resource lists/contracts
 - a. Equipment vendors
 - b. Water-related recovery
 - c. Supply/forms/blank checks
 - d. Storage companies
 6. Organization inventory
 7. Vital records listing
 8. Location of operating procedures
 9. Distribution of the plan
 10. Maintenance of the plan

F. Testing/Training

1. Program description
2. Types of tests
3. Testing frequency/schedules

2

Risk Assessment

- Description
- Detailed risk assessments
- Results

3

Introduction

- A. Level One/Category One
- B. Level Two
- C. Level Three
- D. Level Four
- E. Level Five

4

Team Responsibilities/Organization

- A. General
- B. Management
- C. Logistics
- D. Users
- E. Records and information systems (computers)

5

Restoration Procedures

- A. Specific procedures for handling each type of probable disaster
- B. Equipment and supply lists with phone numbers