III- Risk assessment

Objectives

At the end of this lesson, students will be able to:

- make a correlation with disaster management
- make a procedure of recovery

Prerequisites

To be able to understand this lesson, students need notions on :

- management

Keywords

DISASTER, MANAGEMENT, DISASTER PREVENTION
DISASTER RESPONSE, DISASTER RECOVERY
DISASTER RECOVERY PLANNING, CRITICAL
ASSETS, NOTIFICATION PLAN, RANKING DISASTER

Literature

Kizza, J. M. : Guide to Computer Network Security, Third Edition. Computer Communications and Networks. Springer 2015

Stallings, W.: Cryptography and Network Security: Principles and Practice, Sixth Edition. Pearson, USA 2014

Further readings

1. A Correlation with the Disaster Management (1)

Webster' s Dictionary defines *disaster* as a sudden misfortune, a catastrophe that affects society

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

Information Technology

Big security problems to the enterprise information systems that must be handled with skills

- 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 (availaibility)

2. A Correlation with the Disaster Management (2)

Information Technology

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.

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

Disaster management as a major information systems' security problem

Disaster Prevention

The monitoring devices, in case of an enterprise information system

Disaster Response

Makes a response to a disaster is vital and of critical importance
Is a set strategies used to respond to both the short-term and long-term needs of the affected community

In IT

- Restoring services
- Identifying high-risk system resources

Disaster Recovery

Ability to react to the threat shifty and efficiently.
An informed staff, disaster suppliers, and planned procedures

Disaster Recovery Planning:

It involves risk assessment, developing, documenting, implementing, testing, and maintaining a disaster recovery plan

3. Procedure of recovery (1)

Identifying and Prioritizing the Disaster

- 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

Identifying Critical Resources

The ranking of critical assets may be based on the money amount spent on acquiring the item or on the utility of the item.

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

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

4. Procedure of recovery (2)

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

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**.

	Low level disaster	Medium level - disaster	High level disaster
Level 1 – critical assets	System admin.	System admin.	System admin., management, law, the media
Level 2 – critical assets	System admin.	System admin., management	System admin., management, law, the media
Level 3 – critical assets	System admin.	System admin., management	System admin., management, law, the media

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.

5. Procedure of recovery (3)

Make Your Network Disaster Ready

Training of Employees

Priorities for the Restoration of Essential Functions

- Always Be Ready for a Disaster
- Always Backup Media
- Risk Assessment

6. Questions and 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. 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.

Check to see if your university has a disaster plan (http://palimpsest.stanford.edu/bytopic/disasters/plans/). 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.