CSE 265:
System and Network Administration

- Disaster Recovery
    - Why disaster recovery?
    - What is a disaster?
    - Risk analysis?
    - Legal obligations
    - Damage limitation
    - Preparation

- Backup and Restore is coming in a few weeks

Why Disaster Recovery

- A disaster recovery plan

  - considers what disasters could hit

  - implements ways to mitigate potential disasters

  - makes preparations to enable quick restoration of services

  - identifies key services and how quickly they need to be restored

- Need to understand the requirements

What is a disaster?

- A catastrophic event that causes a massive outage (affecting an entire building or site)

- Natural disasters

- Man-made disasters

Fire and Earthquake

Lightning and Tornadoes
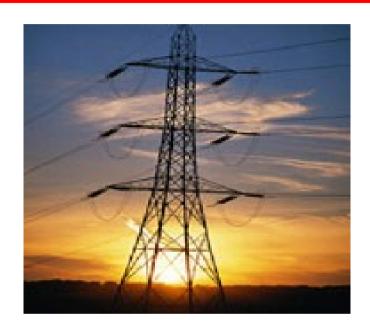
Bombings

CSE 265: System and Network Administration ©2004-2012 Brian D. Davison

Back-hoes

Power Outages

Electronic Break-In

What is a disaster?

- A catastrophic event that causes a massive outage (affecting an entire building or site)

- Natural disasters
  - Earthquake, hurricane, tornado, plague or other diseases, lightning strike, fire, or flood

- Man-made disasters
  - Bomb or other terrorism, massive loss of power, idiots with backhoes, security breaches

Risk analysis

- First step in disaster recovery planning (usu. outsourced)

- Determines budget for mitigation of disaster

  - (ExpCost(Disast) – ExpCost(MitigatedDisast)) * Prob(Disast)
  - Examples
    - Flooding chance is 1 in million, flood cost would be $10M, not worth spending > $10
    - Severe earthquake chance 1/3000, $60M loss, then budget of $20K

- Simpler case: single point of failure in major router

  - 70% chance of failure every 24 months
  - One day to repair, with estimated loss of productivity $68K
  - Redundancy budget could be $24K

Legal obligations

- In addition to costs to company, there may be legal obligations to vendors, customers, and shareholders

- Contracts may allow for delays of n days, which defines the amount of time available

- May require that individual parts of infrastructure be operational before the rest

  – Need to carefully track dependencies!

Damage limitation

- I.e., reducing the cost of the disaster (still subject to cost-benefit analysis)

- Relatively inexpensive, but specific to expected disaster
  - Put equipment above ground in flood plains
  - Mount equipment in earthquake areas
  - Use of lightning rods

- Other mechanisms
  - Fire protection systems that limit damage to computer systems (inert gases, delayed water systems)
  - Moisture detection for raised floors or UPS rooms
  - UPS for short power outages

Preparation

- In addition to damage limitation, you still need to be prepared for likely disaster scenarios

    - must be able to restore essential services to working order in a timely manner

- Need to

    - be able to rebuild data and services on new equipment if old equipment is not operational

    - arrange for replacement hardware in advance

    - arrange for a facility to put the replacement hardware

        - arrange for power, telephone, network connectivity at backup site

    - plan for time to get backup tapes from off-site storage