Physical Security

Types of Threats

- Human Intrusion
  - Attackers looking to perform some sort of damage or obtain useful information
- "Natural" Disasters*
  - Fire
  - Flood
  - Earthquake/Seismic Vibrations
  - Power Outages/Fluctuations

Physical Protection from Human Attackers

- One example why physical security should be taken very seriously
  - The only tools you need to break into an unsecured PC:
    - A Phillips-head screwdriver
    - USB Thumbdrive or an external hard drive
    - Knoppix CD
    - Knoppix Floppy
  - BIOS password can be bypassed.
    - Remove the machine's hard drive and put it in another machine
    - Reset the BIOS password via jumpers on the motherboard
    - Simply remove the CMOS battery to reset
  - Once accomplished, boot off CD or floppy (in this example, KNOPPIX), and copy.

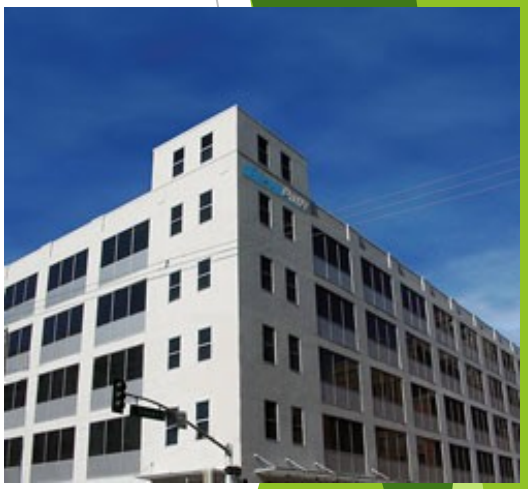
- Resetting admin passwords has never been easier
  - Insert the Windows XP installation on a healthy installation
  - Choose to repair the installation
  - While “Setup is copying files”, simply press Shift+F10
    - This brings up a console in which the user has administrative rights and can, for example, reset the current administrator’s password.

Risk Assessment

- Determine your primary threats and act accordingly
- A very large company participating in the global market obviously has more at stake than John Q's Computer Store.
- While their susceptibility of attack is the same, the large company will house more profitable information and technology.
- FBI statistics indicate that approximately 72% of all thefts, fraud, sabotage, and accidents are caused by a company's own employees.
- Only about 5% is done by external sources.

The "How-Tos" of Protection

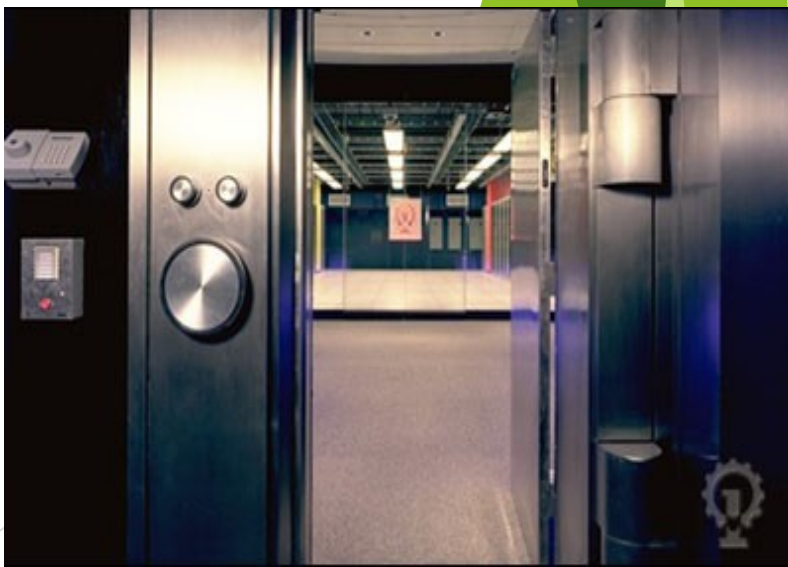
- Guarding the Outer Perimeter*
  - Disguise
    - Out of sight, out of mind
  - If disguising is not possible
    - High fences
    - Barbed wire
    - Round-the-clock security guard
    - Security Cameras
    - Motion Sensors



The ServPath building, located in San Francisco, is a datacenter that houses "supernodes" for both AT&T and MCI.

- The Workstations
  - Workstations should ALWAYS be logged off or locked out whenever unattended
  - Screens positioned such that they cannot be seen through the windows
    - Hackers with telescopes to record keystrokes
  - Workstations should be secured and physically locked while unattended
    - Steel cable that runs through the computer case and attaches to an "anchor" to prevent the tower from being removed

- Safeguarding the Computer Rooms
  - Keep the doors locked
  - Tuck networking cables out of sight
    - Keep networking cables inaccessible from outside room
  - Secure items in the room according to value
  - Intrusion detection systems
  - Ensure walls extend to the physical ceiling versus ceiling panels
    - Attackers can gain access to the room via scaling the wall
  - Access Control Methods
    - Biometrics
    - Key Card access w/ PIN #s
    - Security Guard presence at all times
      - Watchdogs if the assets merit
    - Security Cameras



- Control the flow of people in the building
  - Employee and visitor badges
  - Access restricitions to visitors and maintenance
  - Any unscheduled dropoffs or deliveries should be verified with vendors
  - You don’t want the wrong people getting in

Physical Protection from "Natural" Disasters

- Physical security is more than "guns, gates and guards"

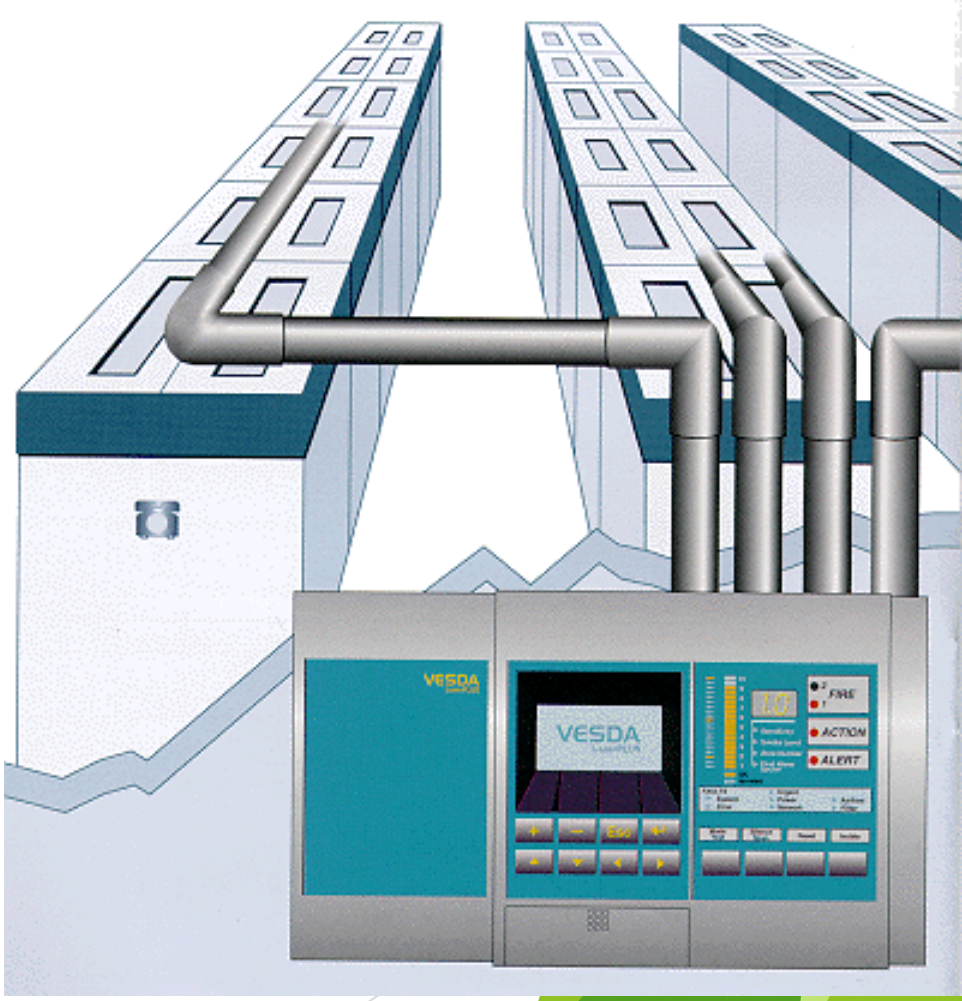
- Risk Assessment
  - Proper security solutions require a proper threat assessment
  - The likelihood of tsunami's is very low in Phoenix

Security Mechanisms

- Fire*
  - Extinguishers
    - Carbon Dioxide
      - Harmful to Humans
    - Halon
      - Preferred Choice, but very expensive to refill
      - Binds with available oxygen molecules to starve the fire
      - Harmful to the ozone
    - Inergen
      - Safer and cleaner alternative to Halon
      - Allows a breathable atmosphere and starvation of the atmosphere without ozone harm

Fire Detectors/Alarms

- Detectors
  - VESDA
  - Laser smoke detection
  - Dry pipe suppression



- Flood/Water
  - "Go to the high ground"
  - Locate sensitive equipment on the second story or above
  - Don't allow water pipes to run through or around computer room

- Earthquake/Seismic Vibrations
  - Airports, railroads, major thoroughfares, industrial tools, and road construction are common sources of vibration
  - Common solutions involve supporting the foundation of computers with springs, gel-filled mats, or rubber pads.
  - THE most effective solution:
    - Don't position your data center near a source of seismic vibrations

- Power Outages/Fluctuations
  - UPS
    - Large solutions available to large power consumption
  - Generator
    - When UPS just isn't enough
  - Extreme Temperature/Humidity
    - Control must be maintained over the environment
    - Larger computers run hotter and thus more susceptible to heat in the room
    - Humidity problems with moisture developing on the inside of the machine
      - Redundant HVAC unit (Heating, Ventilation, and Air Conditioning) that can handle temperature and humidity control of the computer room, sheltered from the weather

THANKYOU

Physical Security