Sources and Types of Security Threats

By: Mallory Huth
Three Major Sources

- Human errors and mistakes
- Malicious human activity
- Natural events and disasters
Human errors and mistakes

- Caused by both employees and nonemployees
- Could be an actual physical error
  - catching the building on fire
- Input errors
  - email wrong person data
Malicious Human Activity

- Caused by employees/former employees/criminals
- Cause harm to others
  - infect computers system w worms
- Benefit themselves
  - steal valuable information
- Natural occurrence
- Not only causes initial problems but also stemming problems during recovery
- Include fire, storms, earthquakes, etc..
The Five Types of Security Threats

- Unauthorized Data Disclosure
- Incorrect Data Modification
- Faulty Service
- Denial of Service
- Loss Of Infrastructure
Unauthorized Data Disclosure

Human Error

- *Unauthorized data disclosure* can occur by human error when someone inadvertently releases data in violation of a policy.
- Employees who place restricted data on Web sites that can be reached by search engines may mistakenly publish proprietary or restricted data over the Web.

Malicious Human Activity

- computer crime includes breaking into networks to steal personal and confidential data.
- **Pretexting**, also called email spoofing, occurs when someone deceives by pretending to be someone else.
- **Phishing** is a similar technique for obtaining unauthorized data that uses pretexting via email.
- **Spoofing** is another term for someone pretending to be someone else.
- **IP spoofing** occurs when an intruder uses another site’s IP address as if it were that other site.
- **Sniffing** is a technique for intercepting computer communications.

Natural Event

- Safeguards are let down during recovery of event
Incorrect Data Modification

**Human Error**
- employees follow procedures incorrectly or when procedures have been incorrectly designed.

**Malicious Human Activity**
- Hacking occurs when a person gains unauthorized access to a computer system.

**Natural Event**
- Incorrect Data recovery from a natural event due to the circumstances.
Faulty Service

**Human Errors**
- Faulty service could include incorrect data modification, as previously described.
- It also could include systems that work incorrectly.

**Malicious Human Activity**
- *Usurpation*- occurs when unauthorized programs invade a computer system and replace legitimate programs.

**Natural Disaster**
- Faulty service can also result from mistakes made during the recovery from natural disasters.
Denial of Service

**Human Errors**
- Accidentally shut down a browser or system that was in use, no longer able to help the user.

**Malicious Human Activity**
- Denial-of-service attacks- hackers use things such as worms to clog up sites so they are unusable by customers

**Natural Event**
- Cause systems to fail denying service
Loss of Infrastructure

**Human Errors**
- Human accidents such as accidental fire or cutting of an important cable.

**Malicious Human Activity**
- Terrorist attacks could cause loss of building and physical equipment

**Natural Events**
- Present the biggest risk for loss of infrastructure
Tools and Techniques used for Malicious Human Activity (malware)

- **Adware** - watch user activities and produce pop-ups
- **Spyware** - unknown to user all actions are observed and reported to sponsor
- **Viruses** - a computer program that replicates itself consuming computers resources
- **Worms** - fastest spreading virus propagates using the internet
- **Trojan Horses** - masquerades as a useful program but is really a virus