Chapter-:3

Types of Exploits:

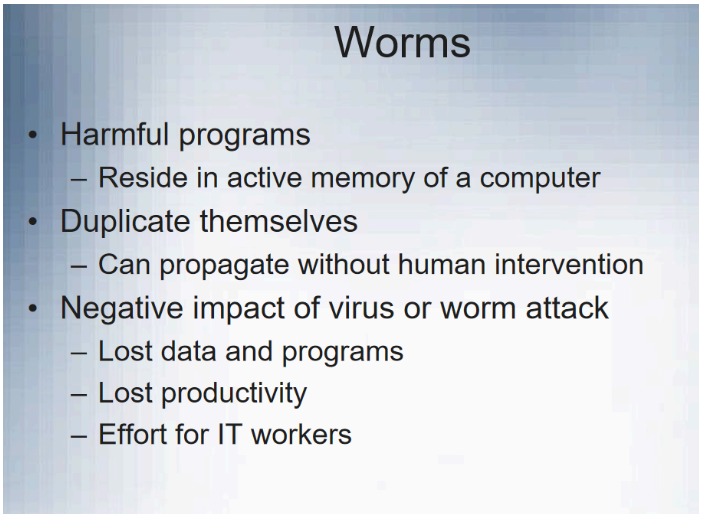
1. **Virus**

Computer virus has become an umbrella term for many types of malicious code. Technically, a virus is a piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner. Often a virus is attached to a file, so that when the infected file is opened, the virus executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies, or creates them. Most viruses deliver a "payload," or malicious software that causes the computer to perform in an unexpected way. For example, the virus may be programmed to display a certain message on the computer's display screen, delete or modify a certain document, or reformat the hard drive.

A true virus does not spread itself from computer to computer. A virus is spread to other machines when a computer user opens an infected email attachment, downloads an infected program, or visits infected Web sites. In other words, viruses spread by the action of the "infected" computer user.

Macro viruses have become a common and easily created form of virus. Attackers use an application macro language (such as Visual Basic or VBScript) to create programs that infect documents and templates. After an infected document is opened, the virus is executed and infects the user's application templates. Macros can insert unwanted words, numbers, or phrases into documents or alter command functions. After a macro virus infects a user's application, it can embed itself in all future documents created with the application.

2. Worm



Worms

- Harmful programs
  - Reside in active memory of a computer
- Duplicate themselves
  - Can propagate without human intervention
- Negative impact of virus or worm attack
  - Lost data and programs
  - Lost productivity
  - Effort for IT workers

3. Torjan Horse

A Trojan horse is a program in which malicious code is hidden inside a seemingly harmless program. The program’s harmful payload might be designed to enable the hacker to destroy hard drives, corrupt files, control the computer remotely, launch attacks against other computers, steal passwords or Social Security numbers, or spy on users by recording keystrokes and transmitting them to a server operated by a third party.
A Trojan horse can be delivered as an email attachment, downloaded from a Web site, or contracted via a removable media device such as a CD/DVD or USB memory stick.

Another type of Trojan horse is a logic bomb, which executes when it is triggered by a specific event. For example, logic bombs can be triggered by a change in a particular file, by typing a specific series of keystrokes, or by a specific time or date.

4. Email Spam

CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) is used to ensure that only humans create free accounts

5. DDos (Distributed Denial of Service)

   A DDoS attack involves a malicious actor taking control of multiple computers over the internet and using them to overwhelm a target website or server with requests for data or tasks. Unlike hacking, it doesn't involve infiltrating the target system. Instead, it floods the target with traffic, making it unavailable to legitimate users.

How DDoS Attacks Work:

- **Botnets:** Attackers use malware to create botnets, networks of compromised computers (zombies) controlled remotely.
- **Overwhelming Requests:** At the attacker's command, the botnet sends a massive volume of requests to the target, overwhelming its resources.
- **Denial of Service:** The target becomes so busy responding to the attack that legitimate users cannot access it.

Impact and Targets:

- DDoS attacks can disrupt critical services, such as online banking and e-commerce.
- Banks and e-commerce websites are frequent targets.
- DDoS attacks can be used to distribute spam and malware.

Botnets and Spam:

Botnets are used for various malicious activities, including distributing spam and malicious code. The Grum botnet, for example, was responsible for a significant portion of global spam.

6. Rootkit: **A rootkit** is a set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge. Some symptoms of rootkit infection
    i. The computer locks up or fails to respond to input from the keyboard or mouse
    ii. The screen saver changes without any action on the part of the user
    iii. The taskbar disappears
    iv. Network activities function extremely slow
7. Phishing → Smishing, Vishing

Phishing:

Phishing is a fraudulent attempt to obtain personal data via email. Attackers send legitimate-looking emails urging recipients to click links or open attachments, leading to fake websites designed to steal information. Sometimes just visiting the site can download malware. Commonly spoofed websites include Citibank, eBay, and PayPal.

Spear-Phishing:

Spear-phishing is a targeted form of phishing aimed at specific organizations. Fraudulent emails, appearing to come from high-level executives, direct employees to fake websites to enter personal information. Botnets are often used for distribution. The Stratfor case exemplifies this, where stolen email accounts were used for targeted attacks.

Smishing and Vishing:

- **Smishing:** Phishing via SMS text messages. Recipients are told to call a number or visit a website, often under the guise of an urgent account problem. These are used to steal personal information or download malware.
- **Vishing:** Similar to smishing, but uses voicemail messages to instruct victims to call a number or visit a website.

Both smishing and vishing are used to steal financial information.

Preventative Measures:

- **Education:** Companies should educate customers about these scams through various channels.
- **Training:** Call center employees should be trained to detect and gather information about suspected scams.
- **Immediate Notification:** Customers should be notified immediately if a scam is detected via recorded messages, news articles, website banners, and physical posters.
- **Reporting:** Scams originating in the U.S. should be reported to the FBI.

- **Telecommunications Notification:** Companies should try to get the phone numbers used in the scams shut down by notifying the telecommunications carriers.

Perpetrators:

The people who launch these kinds of computer attacks include thrill seekers wanting a challenge, common criminals looking for financial gain, industrial spies trying to gain a competitive advantage, and terrorists seeking to cause destruction to further their cause. Each type of perpetrator has different objectives and access to varying resources, and each is willing to accept different levels of risk to accomplish his or her objective. Each perpetrator makes a decision to act in an unethical manner to achieve his or her own personal objectives.

Types of Perpetrators:

1. **Hackers (White hat hackers):** Hackers test the limitations of information systems out of intellectual curiosity—to see whether they can gain access and how far they can go. They have at least a basic understanding of information systems and security features, and much of their motivation comes from a desire to learn even more. They generally find loopholes in the system and help them to cover the loopholes.
   Three phases of hacking (1960 to present). Originally, *hackers* referred to creative programmers who wrote clever code.
2. **Crackers:** are kind of bad people who break or violate the system or a computer remotely with bad intentions to harm the data and steal it. Crackers destroy data by gaining unauthorized access to the network. Their works are always hidden as they are doing illegal stuff. Bypasses passwords of computers and social media websites, can steal your bank details and transfer money from the bank.

3. **Malicious Insiders:**

Malicious insiders are individuals within an organization (employees, consultants, contractors) who intentionally abuse their access for harmful purposes. They pose a significant security risk due to their authorized access and knowledge of internal systems. They can be motivated by financial gain, revenge, or publicity.

Types of Fraud:

Insiders can engage in various fraudulent activities, including:

- Diversion of company funds.
- Theft of assets.
- Bidding process fraud.

- Invoice and payment fraud.
- Computer fraud.
- Credit card fraud.

Challenges in Detection:

- **Authorized Access:** Insiders often have legitimate access to the systems they abuse.
- **Knowledge of Systems:** They understand system vulnerabilities, access procedures, and security protocols.
- **Collusion:** Frauds frequently involve collusion with outsiders, making them harder to detect.
- **Weak Internal Controls:** Many frauds are discovered by chance, not through established controls.

Preventative Measures:

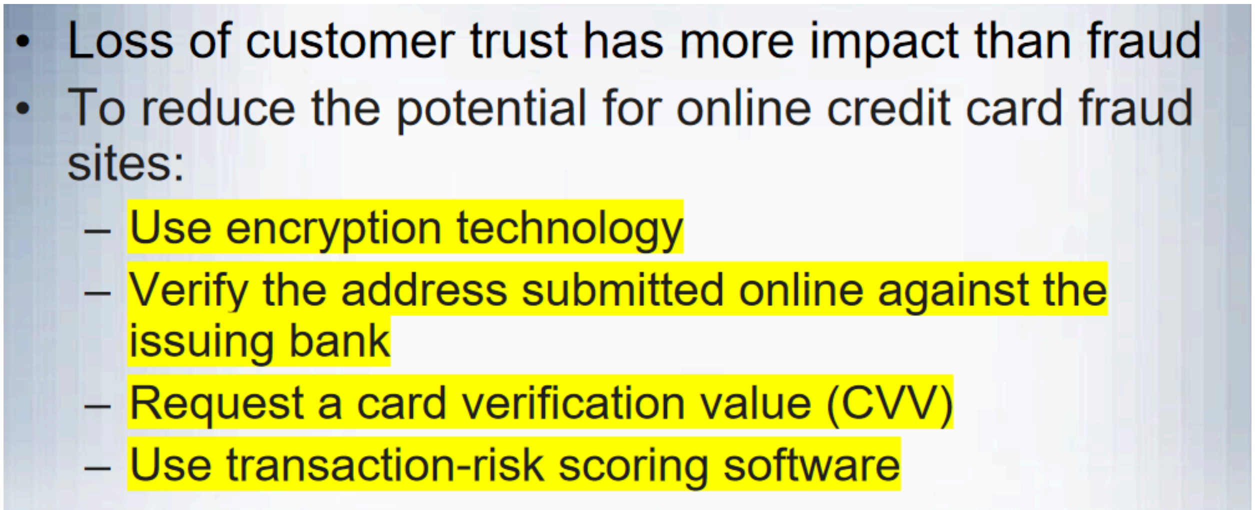
- **Thorough Background Checks:** Conduct background checks, psychological evaluations, and drug testing for sensitive positions.
- **Regular Testing:** Implement ongoing psychological and drug testing for employees in sensitive roles.
- **Limited Access:** Restrict access to sensitive operations and grant only necessary privileges.
- **Segregation of Duties:** Ensure that the same person cannot initiate and approve actions.
- **Job Rotation:** Periodically rotate employees in sensitive positions to detect unusual activities.
- **Immediate Access Revocation:** Revoke access privileges when employees change roles.
- **Ongoing Audit Process:** Implement regular audits of key actions and procedures.

Negligent Insiders:

Organizations must also address the risk of negligent insiders, who, despite good intentions, can cause significant damage due to poor training or management.

4. **Industrial Spies:** use illegal means to obtain trade secrets from competitors.

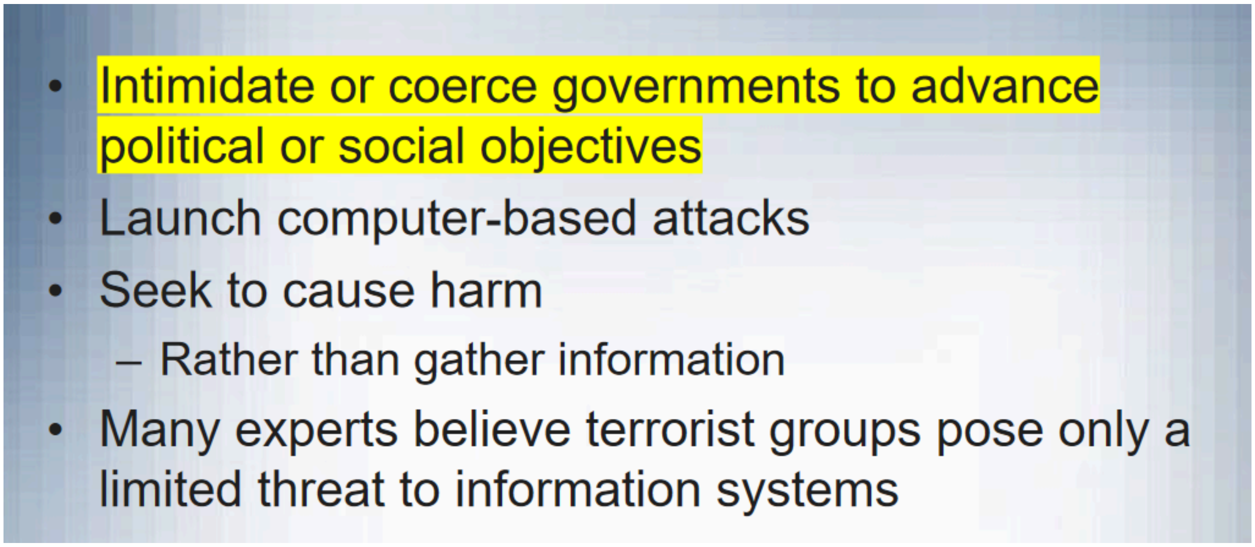
5. **Cybercriminals:** Cybercriminals are motivated by the potential for monetary gain and hack into computers to steal, often by transferring money from one account to another to another—leaving a hopelessly complicated trail for law enforcement officers to follow. Cybercriminals also engage in all forms of computer fraud—stealing and reselling credit card numbers, personal identities, and cell phone IDs. Because the potential for monetary gain is high, they can afford to spend large sums of money to buy the technical expertise and access they need from unethical insiders.



- Loss of customer trust has more impact than fraud
- To reduce the potential for online credit card fraud sites:
  - Use encryption technology
  - Verify the address submitted online against the issuing bank
  - Request a card verification value (CVV)
  - Use transaction-risk scoring software

6. **Hacktivists**: Hacktivism, a combination of the words hacking and activism, is hacking to achieve a political or social goal. People who do this are known as hacktivists. **Hacktivism** is the use of hacking expertise to promote a political cause.

7. **Cyberterrorists:** a criminal who uses computer technology and the Internet, especially to cause fear and disruption or in order to advance certain political or social objectives.

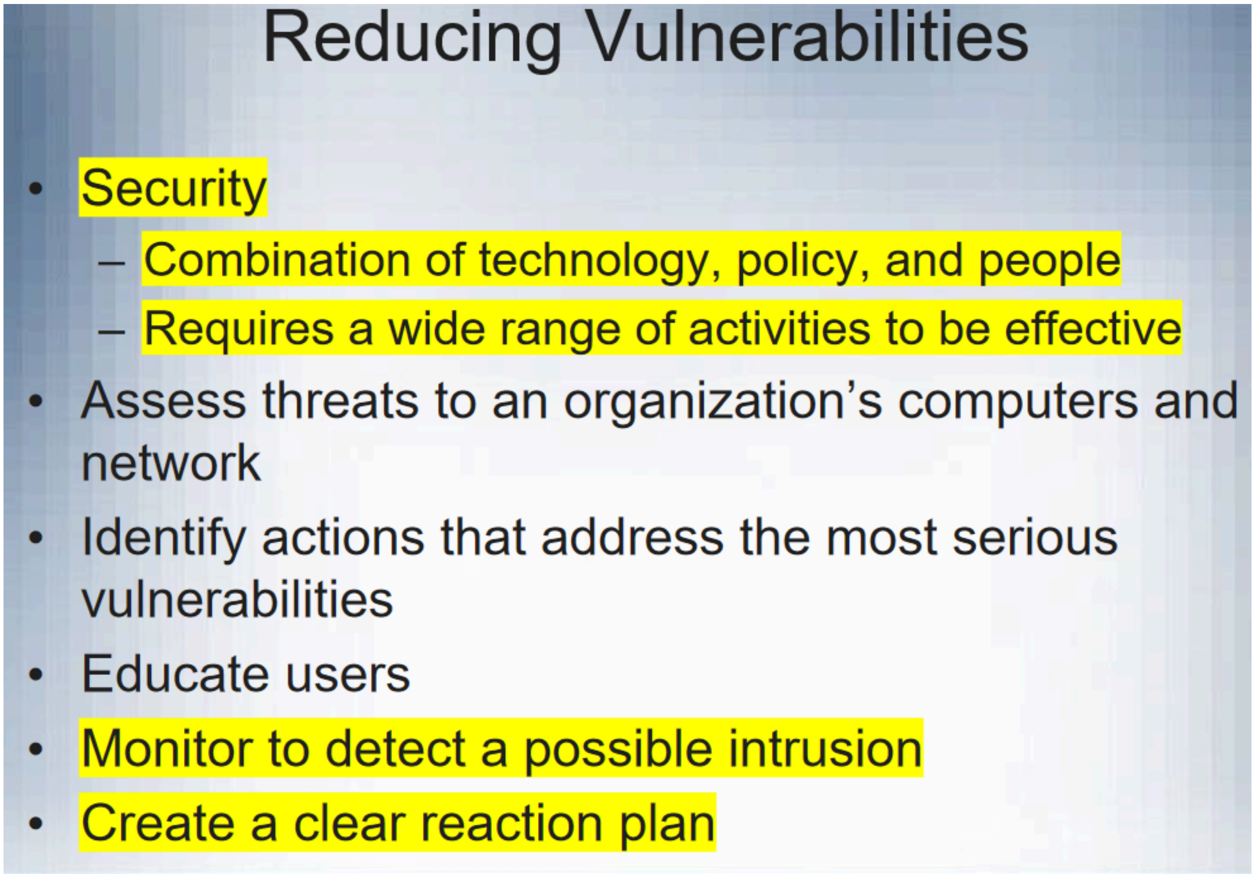


- Intimidate or coerce governments to advance political or social objectives
- Launch computer-based attacks
- Seek to cause harm
  - Rather than gather information
- Many experts believe terrorist groups pose only a limited threat to information systems

TABLE 3-5 Classifying perpetrators of computer crime

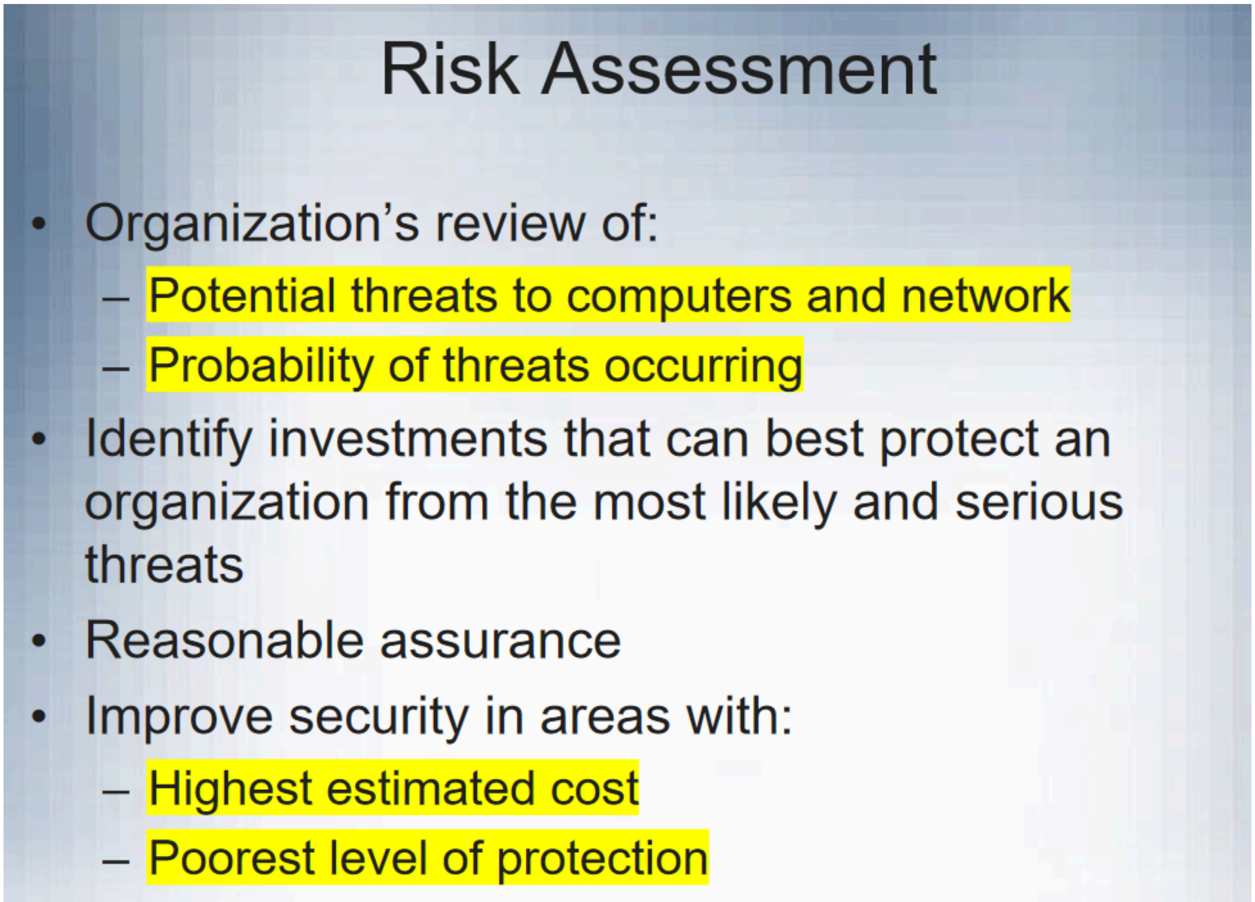
Type of perpetrator	Typical motives
Hackers	Test limits of system and/or gain publicity
Crackers	Cause problems, steal data, and corrupt systems
Malicious insiders	Gain financially and/or disrupt company's information systems and business operations
Industrial spies	Capture trade secrets and gain competitive advantage
Cybercriminals	Gain financially
Hacktivists	Promote political ideology
Cyberterrorists	Destroy infrastructure components of financial institutions, utilities, and emergency response units

Source Line: Course Technology/Cengage Learning.



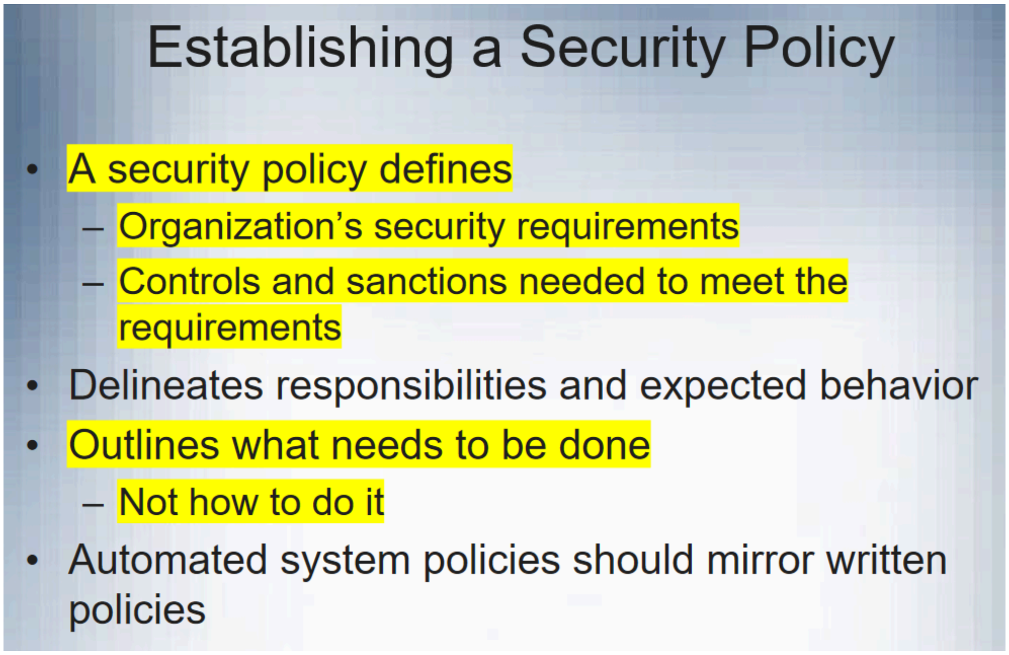
Reducing Vulnerabilities

- Security
  - Combination of technology, policy, and people
  - Requires a wide range of activities to be effective
- Assess threats to an organization's computers and network
- Identify actions that address the most serious vulnerabilities
- Educate users
- Monitor to detect a possible intrusion
- Create a clear reaction plan



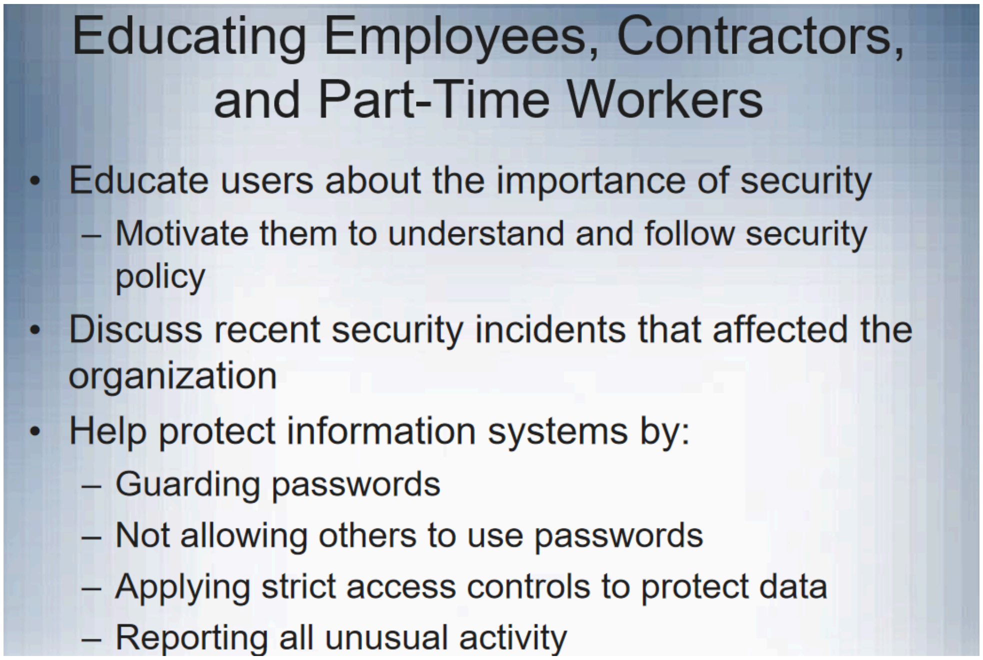
Risk Assessment

- Organization’s review of:
  - Potential threats to computers and network
  - Probability of threats occurring
- Identify investments that can best protect an organization from the most likely and serious threats
- Reasonable assurance
- Improve security in areas with:
  - Highest estimated cost
  - Poorest level of protection



Establishing a Security Policy

- A security policy defines
  - Organization’s security requirements
  - Controls and sanctions needed to meet the requirements
- Delineates responsibilities and expected behavior
- Outlines what needs to be done
  - Not how to do it
- Automated system policies should mirror written policies



Educating Employees, Contractors, and Part-Time Workers

- Educate users about the importance of security
  - Motivate them to understand and follow security policy
- Discuss recent security incidents that affected the organization
- Help protect information systems by:
  - Guarding passwords
  - Not allowing others to use passwords
  - Applying strict access controls to protect data
  - Reporting all unusual activity

From here Follow the slide of chapter 3