Computer and Internet Crime

2ND LECTURE SLIDES

Overview

- ❑The security of information technology used in a business is of utmost importance.
- ❑Confidential business data and private customer and employee information must be safeguarded, and systems must be protected against malicious acts of theft or disruption.
- ❑**A security incident** is an event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed.
- ❑ **A security breach** pertains to data breaches only -- not a network or system access violations, or malware invasions where data is not involved.
- ❑Although the necessity of security is obvious, it must often be balanced against other business needs and issues

Security Terms

- Exploit
  - An attack that takes advantage of a particular system vulnerability
- Zero-day attack
  - Takes place before a vulnerability is discovered or fixed
- Patch
  - “Fix” to eliminate a problem
  - Problem: users responsible to install patches

Types of Exploits

- **A Virus** is a piece of programming code, usually disguised as something else, which causes a computer to behave in an unexpected and usually undesirable manner.
  - A true virus does not spread itself. It spread when a computer user opens an infected attachment, downloads an infected program, or visits infected websites.
  - Macro viruses can insert unwanted words, numbers, or phrases into documents or alter command functions

- **A worm** is a harmful program that resides in the active memory of the computer and duplicates itself. Worms differ from viruses in that they can propagate without human intervention.

- **A Trojan Horse** is a program in which malicious code is hidden inside a seemingly harmless program. Might be designed to enable the hacker to destroy hard drives, corrupt files, control the computer remotely, steal passwords, or spy on users by recording keystrokes. The logic bomb is another type of Trojan horse that is triggered by a specific event.

Types of Exploits

- **Email spam** is the abuse of email systems to send unsolicited emails to large numbers of people. Most spam is a form of low-cost commercial advertising.
  - Is spam legal?
  - It is legal, provided that the messages meet a few basic requirements-
    - Spammers cannot disguise their identity by using a false return address,
    - The email must include a label specifying that it is an ad or a solicitation, and
    - The email must include a way for recipients to indicate that they do not want future mass mailings.

- **Distributed Denial-of-Service (DDoS)** Attack is one in which a malicious hacker takes over computers on the Internet and causes them to flood a target site with demands for data and other small tasks. **Botnet** is a large group of computers controlled from one or more remote locations by hackers, without the knowledge or consent of their owners. Botnets are frequently used to distribute spam and malicious code.

Types of Exploits

- **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
  - The computer locks up or fails to respond to input from the keyboard or mouse
  - The screen saver changes without any action on the part of the user
  - The taskbar disappears
  - Network activities function extremely slow
- **Phishing** is the act of using fraudulently to try to get the recipient to reveal personal data. In a phishing scam, con artists send legitimate-looking emails urging the recipient to take action to avoid a negative consequence or to receive a reward. **Spear-phishing** is a variation of phishing in which the phisher sends fraudulent emails to a certain organization's employees. It is much more precise and narrow.

Types of Exploits

Smishing and Vishing variations of phishing involve the use of Short Message Service (SMS) and voice mail, respectively.

❑Recommended action steps

- Companies should educate their customers about the dangers of phishing, smishing, and vishing
- Call center service employees should be trained to detect customer complaints
- Customers should be notified immediately if a scam occurs
- Institutions can notify the telecommunications carrier for the particular phone number to shut down

Brute-Force Attacks

- Hackers use software to repeatedly and systematically attempt password combinations until they find one that works. Limiting login attempts and enabling two-factor authentication are better preventative measures against brute-force attacks.

Types of Perpetrator

Hackers and Crackers

- Hackers test the limitations of information systems out of intellectual curiosity.
- Three phases of hacking (1960 to present). Originally, *hackers* referred to creative programmers who wrote clever code.
- Hackers are kind of good people who do hacking for a good purpose and to obtain more knowledge from it. They generally find loopholes in the system and help them to cover the loopholes.
- **Hacktivism** is the use of hacking expertise to promote a political cause.

- **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.

Types of Perpetrator

Malicious insiders can be employees, former employees, contractors or business associates who have legitimate access to your systems and data, but use that access to destroy data, steal data or sabotage your systems. It does not include well-meaning staff who accidentally put your cyber security at risk or spill data. CERT describes the classification of malicious insider activities:

- **IT sabotage** is abusing information technology to direct specific harm to an organization or individual. These types of attacks are usually performed by system administrators, programmers, or other technically savvy employees who can hide their malicious actions and disable an organization's operations.
- **Data theft** is stealing intellectual property or sensitive data from an organization for monetary gain or personal benefit. Insiders who steal data are usually current employees: engineers, programmers, scientists, salespeople, etc.
- **Insider fraud** is unauthorized access or modification of an organization's data. Usually, the motivation for fraud is personal gain or data theft. These attacks are usually committed by lower-level employees like administrative assistants, customer service specialists, or data entry clerks.

Types of Perpetrator

Industrial spies use illegal means to obtain trade secrets from competitors.

Competitive intelligence is legally obtained information gathered using sources available to the public.

Competitive advantages?

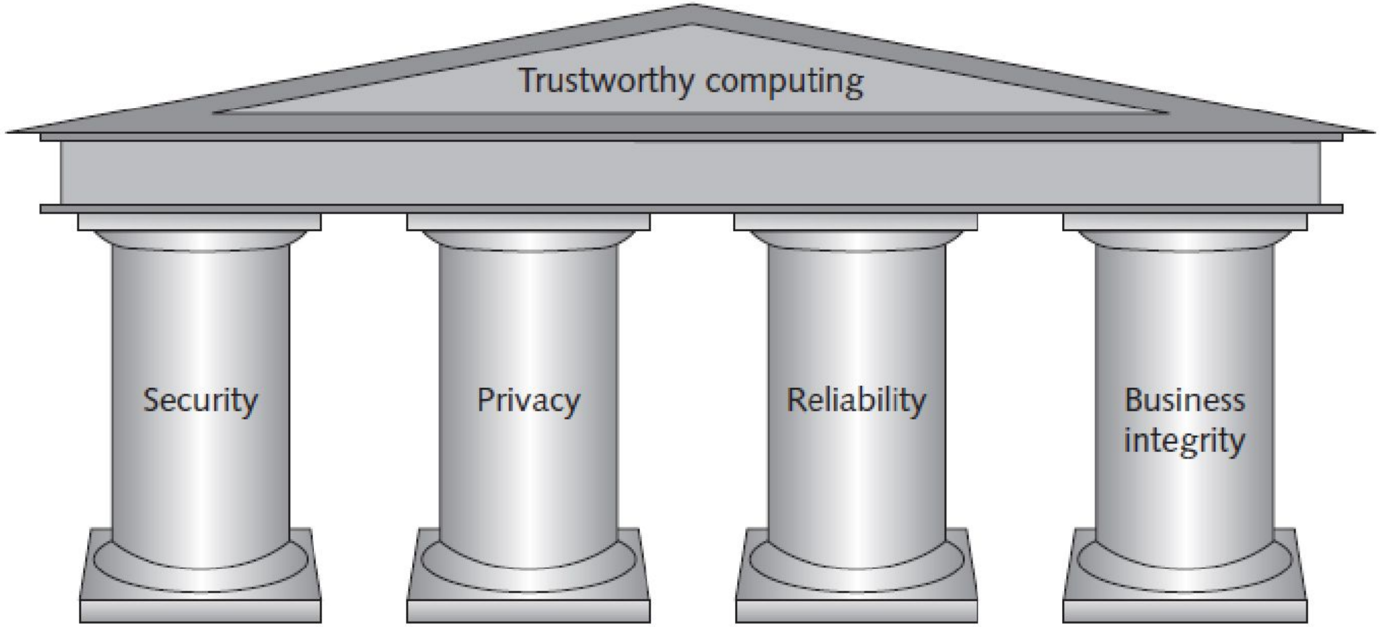
A *cyber-terrorist* is a criminal who uses computer technology and the Internet, especially to cause fear and disruption or in order to advance certain political or social objectives.

Implementing a trustworthy computing

Trustworthy computing is a method of computing that delivers secure, private, and reliable computing experiences

The security of any system or network is a combination of technology, policy, and people and requires a wide range of activities to be effective

Microsoft’s four pillars of trustworthy computing

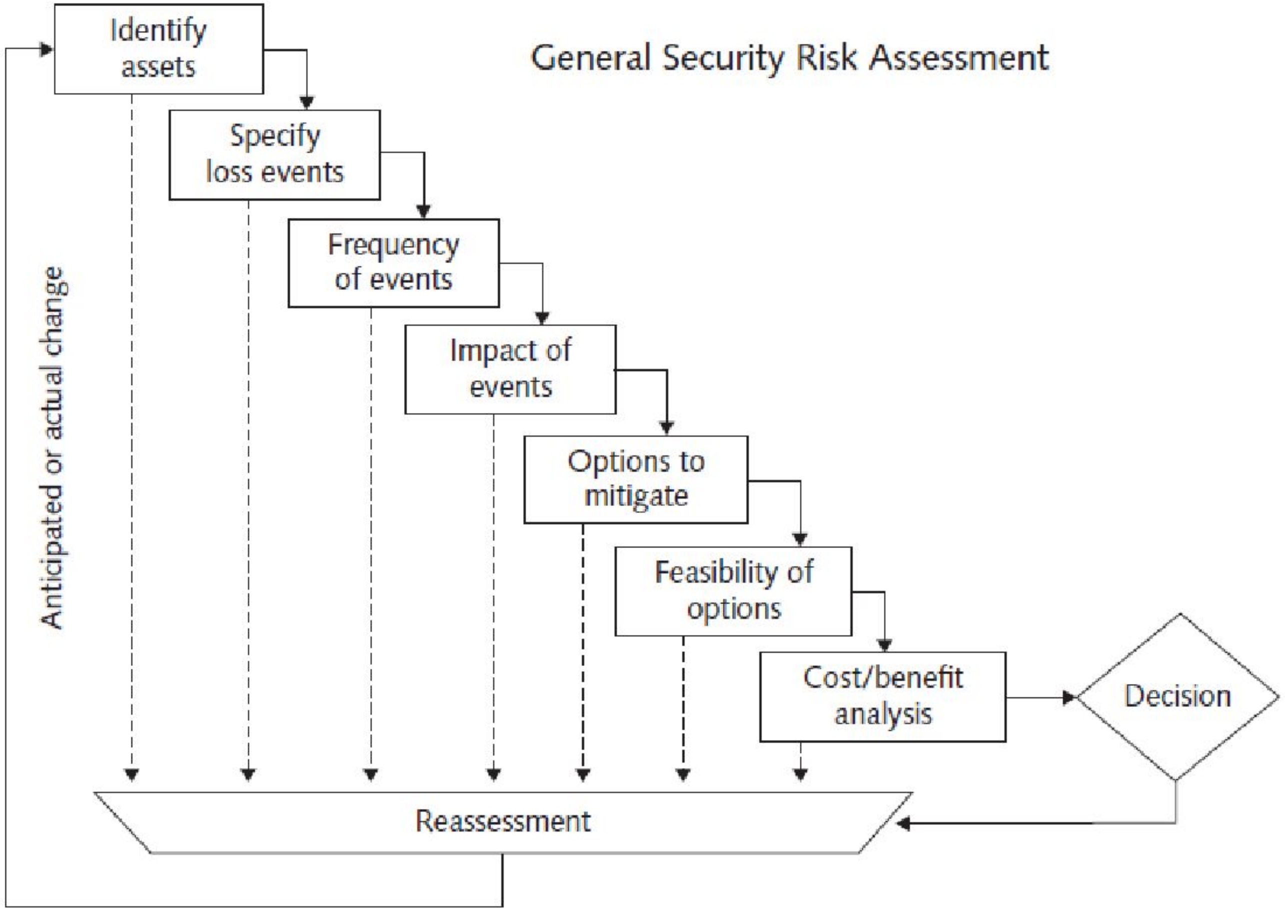


Risk Assessment

Risk assessment is the process of assessing security-related risks to an organization's computers and networks from both internal and external threats

In the context of an IT risk assessment, an asset is any hardware, software, information system, network, or database that is used by the organization to achieve its business objectives.

A loss event is any occurrence that has a negative impact on an asset, such as a computer contracting a virus or a Web site undergoing a distributed denial-of-service attack.



Prevention

The is to implement a layered security solution (e.g., two-factor authentication)

- Installing a corporate firewall
- Intrusion detection system
- Addressing the most critical internet security threats
- Conducting periodic IT security Audits

Detection and Response

Organizations often employ an intrusion detection system

Response

- Incident Notification
- Protection of evidence and activity logs
- Incident containment
- Eradication
- Incident follow-up

Computer Forensics

- Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.
- The goal of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.