Computer Security

2022-2023

Required work

- Course
  - Be attentive, cooperative and dynamic
- Labs
  - Work in pairs (depending on the material available)

Course materials

- Bishop, M. (2018). Computer Security: Art and Science. Addison-Wesley Professional

- “Security Engineering,” Third Edition, Ross Anderson. Wiley, 2020.

https://drive.google.com/drive/folders/1I3Nv-AOqLzqCBz82Qya4xzSS_g-DhzZX?usp=sharing

Required Skills

- Programming knowledge
- Database knowledge (DBMS)
  - Oracle
  - MySQL
- Knowledge of operating systems
  - Windows
  - Linux

PLAN

- **Chapter I :** Intro to computer Security
- **Chapter II :** Access Control, Authorization, and Multi-Level Security
- **Chapter III :** Cryptography
- **Chapter IV :** System, Software and Web Security
- **Chapter V :** Operating System Security

Chapter I

Intro to Information system Security

What is Security?

- “The quality or state of being secure—to be free from danger”

- A successful organization should have multiple layers of security in place:
  - **Physical security**
  - **Personal security**
  - **Operations security**
  - **Communications security**
  - **Network security**
  - **Information security**

Examples…

What is Information Security?

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- **Necessary tools**: policy, awareness, training, education, technology
- C.I.A. triangle was standard based on **c**onfidentiality, **i**ntegrity, and **a**vailability
- C.I.A. triangle now expanded into list of critical characteristics of information

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
  - **Availability**
  - **Accuracy**
  - **Authenticity**
  - **Confidentiality**
  - **Integrity**
  - **Utility**
  - **Possession**

Critical Characteristics of Information

- **Availability** : enables users who need to access information to do so without interference or obstruction and in the required format. The information is said to be available to an authorized user when and where needed and in the correct format.

- **Accuracy :** free from mistake or error and having the value that the end-user expects. If information contains a value different from the user's expectations due to the intentional or unintentional modification of its content, it is no longer accurate.

Critical Characteristics of Information

- **Authenticity** : the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is the information that was originally created, placed, stored, or transferred.

- **Confidentiality** : the quality or state of preventing disclosure or exposure to unauthorized individuals or systems.

- **Integrity** : the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state.

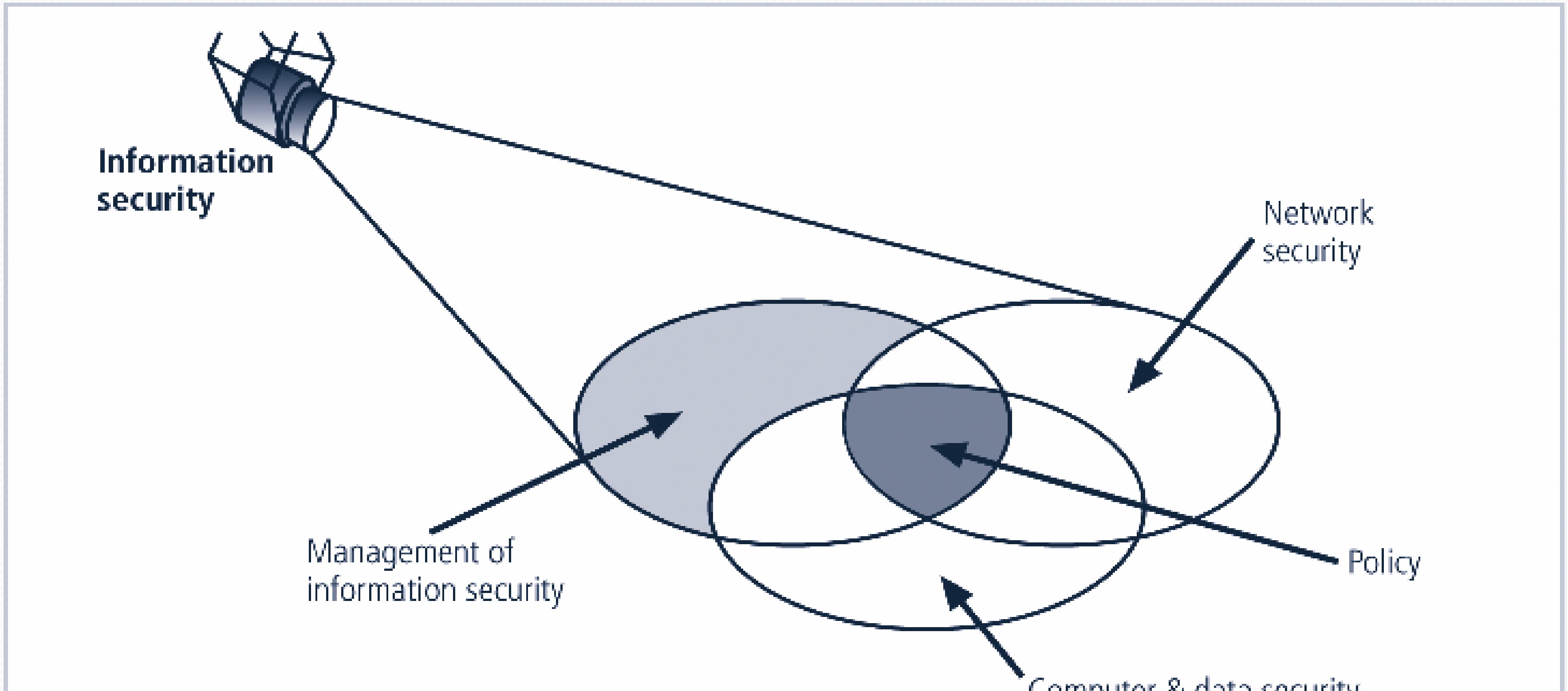
Critical Characteristics of Information

- **Utility** : the quality or state of having value for some purpose or end. Information has value when it serves a particular purpose. This means that if information is available, but not in a format meaningful to the end-user, it is not useful.

- **Possession** : the quality or state of having ownership or control of some object or item. Information is said to be in possession if one obtains it, independent of format or other characteristic.

Components of an Information System

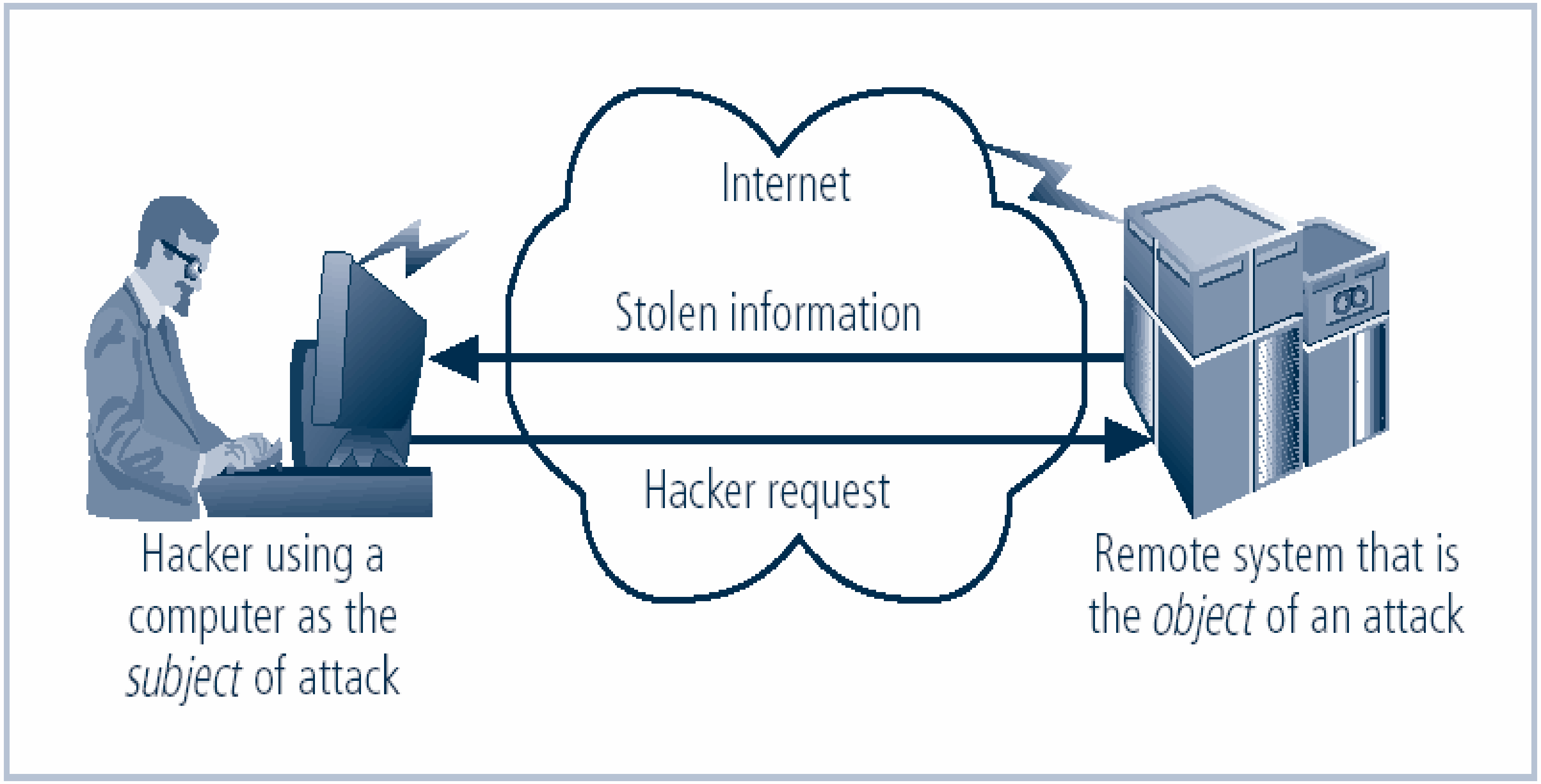
- Information System (IS) is entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization



Securing Components

- Computer can be subject of an attack and/or the object of an attack
  - When the subject of an attack, computer is used as an active tool to conduct attack
  - When the object of an attack, computer is the entity being attacked

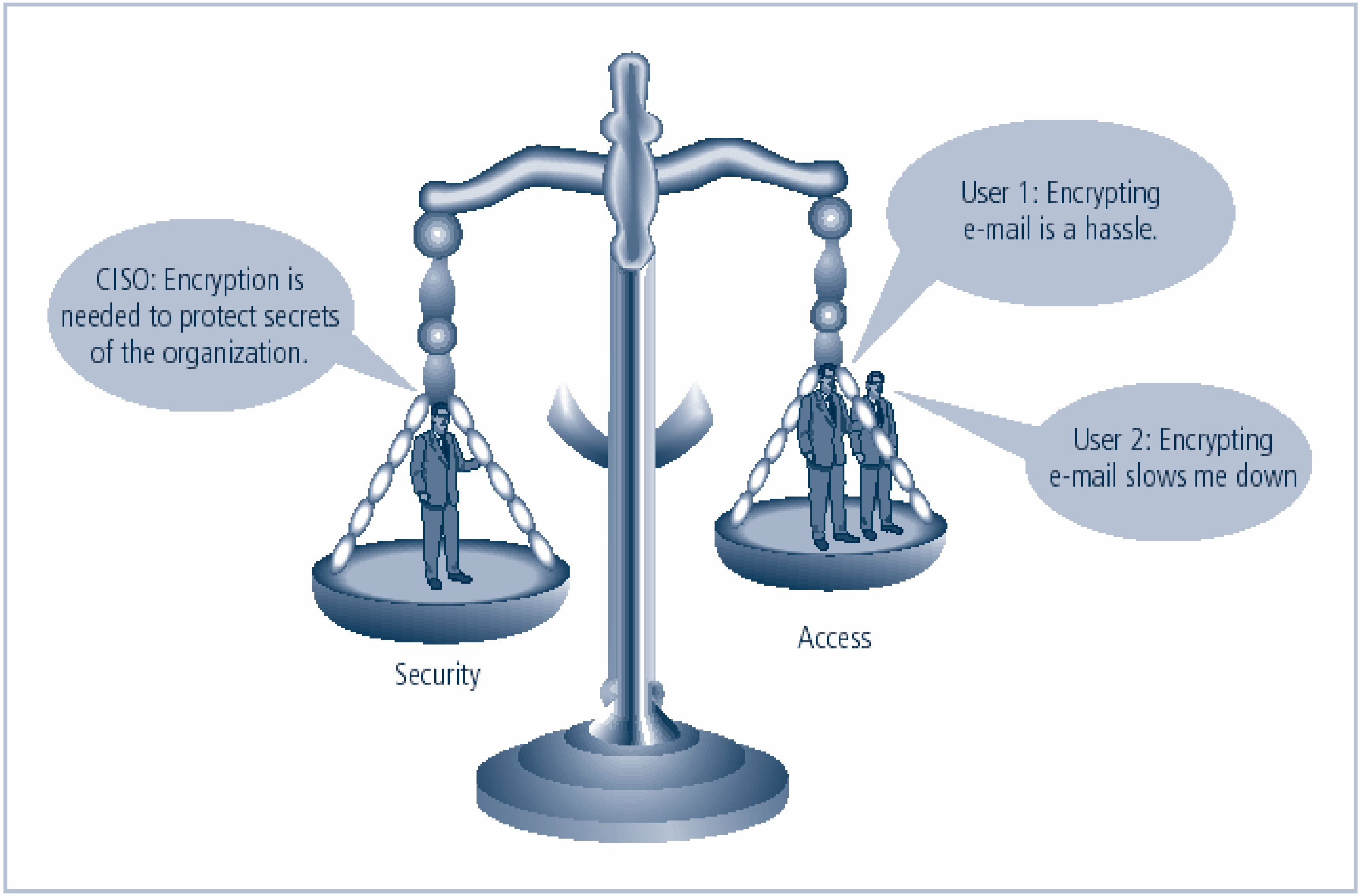
Figure 1-5 – Subject and Object of Attack


Internet
Stolen information
Hacker request
Hacker using a computer as the *subject* of attack
Remote system that is the *object* of an attack

Computer as the Subject and Object of an Attack

Balancing Information Security and Access

- Impossible to obtain perfect security—it is a process, not an absolute
- Security should be considered balance between protection and availability
- To achieve balance, level of security must allow reasonable access, yet protect against threats


CISO: Encryption is needed to protect secrets of the organization.
User 1: Encrypting e-mail is a hassle.
User 2: Encrypting e-mail slows me down
Security
Access

Balancing Information Security and Access

Protecting Data

- One of the most valuable assets is **data**

- Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers

- An effective information security program is essential to the protection of the integrity and value of the organization’s data

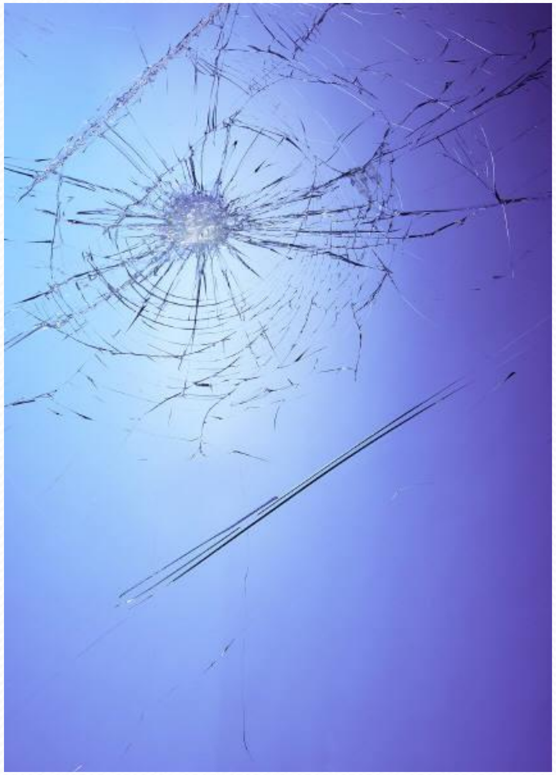
Definitions

- Risk: Probability that an intentional or unintentional act will harm resources
- Threat: Any accidental or intentional event that negatively impacts company resources
- Vulnerability: Inherent weakness that may enable threats to harm system or networks

Risks, threats, and vulnerabilities affect confidentiality, integrity, and availability (CIA).

Types of Threats

- Malicious software
- Device failure
- Application failure
- Natural disaster
- Intrusive cracker



Types of Vulnerabilities

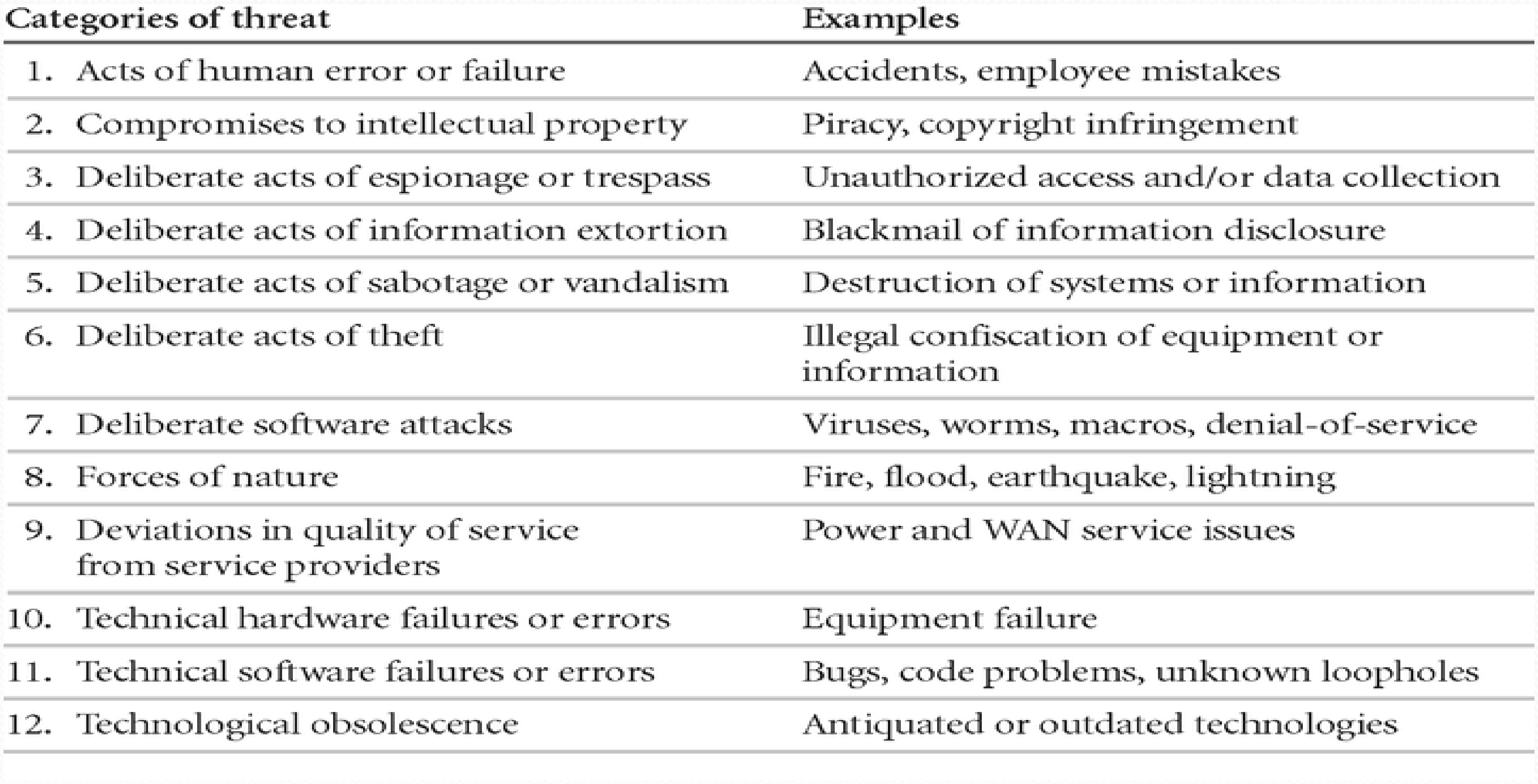
- Insecure servers or services
- Exploitable applications and protocols
- Unprotected system or network resources
- Traffic interception and eavesdropping
- Lack of preventive and protective measures against malware or automated attacks

Threats

- A threat is an object, person, or other entity that represents a constant danger to an asset

- By examining each threat category in turn, management effectively protects its information through policy, education and training, and technology controls

Threats to Information Security



Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Acts of Human Error or Failure

- Includes acts done without malicious intent

- Caused by:
  - Inexperience
  - Improper training
  - Incorrect assumptions
  - Other circumstances

- Employees are greatest threats to information security – They are closest to the organizational data

Acts of Human Error or Failure

- Employee mistakes can easily lead to the following:
  - revelation of classified data
  - entry of erroneous data
  - accidental deletion or modification of data
  - storage of data in unprotected areas
  - failure to protect information

- Many of these threats can be prevented with controls

Why Systems are Vulnerable

- Unauthorized access
  - by Hackers or Employees
  - to destroy, steal or alter data, hardware or software
- Denial of Service (DOS) Attack
  - Flooding a server with bogus requests in order to crash the network
- Computer Viruses
  - self-replicating, malicious code
- Disasters
  - flood, fire, power loss etc.
- Errors
  - in Data Entry, Hardware or Software

Espionage/Trespass

- Broad category of activities that breach confidentiality
  - Unauthorized accessing of information
  - Competitive intelligence vs. espionage
  - Shoulder surfing can occur any place a person is accessing confidential information
- Controls implemented to mark the boundaries of an organization’s virtual territory giving notice to trespassers that they are encroaching on the organization’s cyberspace
- Hackers uses skill, guile, or fraud to steal the property of someone else

Shoulder Surfing

PINs 0123
abcd
Passwords
CAMERA
1 2 3
4 5 6
7 8 9
0

Espionage/Trespass

- Generally, two skill levels among hackers:
  - **Expert hacker**
    - develops software scripts and codes exploits
    - usually, a master of many skills
    - will often create attack software and share with others
  - **Script kiddies**
    - hackers of limited skill
    - use expert-written software to exploit a system
    - do not usually fully understand the systems they hack

Information Extortion

- Information extortion is an attacker or formerly trusted insider stealing information from a computer system and demanding compensation for its return or non-use

- Extortion found in credit card number theft

Sabotage

- Individual or group who want to deliberately sabotage the operations of a computer system or business, or perform acts of vandalism to either destroy an asset or damage the image of the organization

- Organizations rely on image so Web defacing can lead to dropping consumer confidence and sales

- Rising threat of hacktivist or cyber-activist operations – the most extreme version is cyber-terrorism

Deliberate Acts of Theft

- Illegal taking of another’s property - physical, electronic, or intellectual
- The value of information suffers when it is copied and taken away without the owner’s knowledge
- Electronic theft is a more complex problem to manage and control - organizations may not even know it has occurred

Deliberate Software Attacks

- When an individual or group designs software to attack systems, they create malicious code/software called malware
  - Designed to damage, destroy, or deny service to the target systems

- Includes:
  - macro virus
  - boot virus
  - worms
  - Trojan horses
  - logic bombs
  - back door or trap door
  - denial-of-service attacks
  - polymorphic
  - hoaxes

Deliberate Software Attacks

- Virus is a computer program that attaches itself to an executable file or application.
- It can replicate itself, usually through an executable program attached to an e-mail.
- The keyword is “attaches”. A virus can not stand on its own.
- You must prevent viruses from being installed on computers in your organizations.

Deliberate Software Attacks

- There is no foolproof method of preventing them from attaching themselves to your computer
- Antivirus software compares virus signature files against the programming code of know viruses.
- Regularly update virus signature files is crucial.

Deliberate Software Attacks

- A worm is a computer program that replicates and propagates itself without having to attach itself to a host.
- Most infamous worms are Code Red and Nimda.
- Trojan Programs disguise themselves as useful computer programs or applications and can install a backdoor or rootkit on a computer.
- Backdoors or rootkits are computer programs that give attackers a means of regaining access to the attacked computer later.

Attacks

- An attack is the deliberate act that exploits vulnerability

- It is accomplished by a threat-agent to damage or steal an organization’s information or physical asset
    - An exploit is a technique to compromise a system
    - A vulnerability is an identified weakness of a controlled system whose controls are not present or are no longer effective
    - An attack is then the use of an exploit to achieve the compromise of a controlled system

Malicious Code

- This kind of attack includes the execution of viruses, worms, Trojan horses, and active web scripts with the intent to destroy or steal information

Attack Descriptions

- **IP Scan and Attack** – Compromised system scans random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits

- **Web Browsing** - If the infected system has write access to any Web pages, it makes all Web content files infectious, so that users who browse to those pages become infected

- **Virus** - Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection

Attack Descriptions

- **Unprotected Shares** - using file shares to copy viral component to all reachable locations
- **Mass Mail** - sending e-mail infections to addresses found in address book
- **Simple Network Management Protocol** - SNMP vulnerabilities used to compromise and infect
- **Hoaxes** - A more devious approach to attacking computer systems is the transmission of a virus hoax, with a real virus attached

Attack Descriptions

- **Back Doors** - Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource
- **Password Crack** - Attempting to reverse calculate a password
- **Brute Force** - The application of computing and network resources to try every possible combination of options of a password
- **Dictionary** - The dictionary password attack narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords (the dictionary) to guide guesses

Attack Descriptions

- **Denial-of-service (DoS)**
  - attacker sends a large number of connection or information requests to a target
  - so many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service
  - may result in a system crash, or merely an inability to perform ordinary functions

- **Distributed Denial-of-service (DDoS)**
  - an attack in which a coordinated stream of requests is launched against a target from many locations at the same time

Attack Descriptions

- **Spoofing** - technique used to gain unauthorized access whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host
- **Man-in-the-Middle** - an attacker sniffs packets from the network, modifies them, and inserts them back into the network
- **Spam** - unsolicited commercial e-mail - while many consider spam a nuisance rather than an attack, it is emerging as a vector for some attacks

Attack Descriptions

- **Mail-bombing** - another form of e-mail attack that is also a DoS, in which an attacker routes large quantities of e-mail to the target

- **Sniffers** - a program and/or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information from a network

- **Social Engineering** - within the context of information security, the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker

Attack Descriptions

- **Buffer Overflow**
  - application error occurs when more data is sent to a buffer than it can handle
  - when the buffer overflows, the attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure
  - Usually the attacker fill the overflow buffer with executable program code to elevate the attacker's permission to that of an administrator.

Attack Descriptions

- **Ping of Death Attacks**
  - A type of DoS attack
  - Attacker creates an ICMP packet that is larger than the maximum allowed 65,535 bytes.
  - The large packet is fragmented into smaller packets and reassembled at its destination.
  - Destination user cannot handle the reassembled oversized papcket, thereby causing the system to crash or freeze.

Attack Descriptions

- **Timing Attack**
  - relatively new
  - works by exploring the contents of a web browser's cache
  - can allow collection of information on access to password-protected sites
  - another attack by the same name involves attempting to intercept cryptographic elements to determine keys and encryption algorithms