



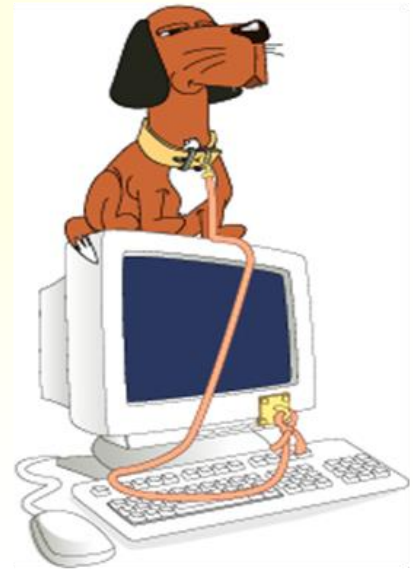
Chapter 1 – Introduction to Computer Security and Privacy

1.1 Overview

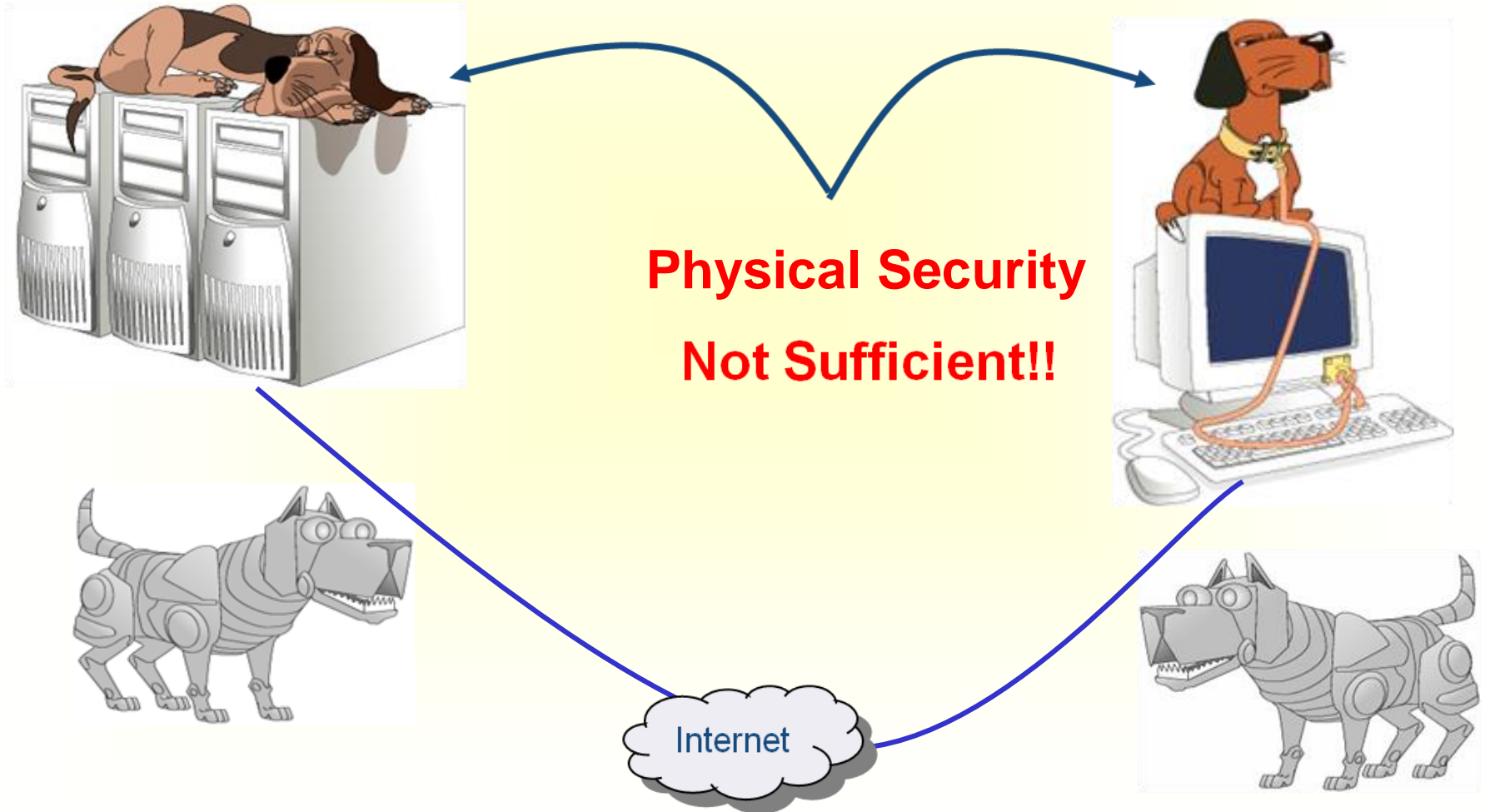
- **Computer security** is about provisions and policies adopted to protect **information and property** from unauthorized access, use, alteration, degradation, destruction, theft, corruption, natural disaster, etc. while allowing the information and property to **remain accessible** and productive to its intended use
- **Privacy**: The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family



Physical Security



- **Computer Security**: when there is connection to networks (**Network security**) it deals with provisions and policies adopted to **prevent and monitor** unauthorized access, misuse, modification, or denial of the computer **network and network-accessible resources**



- “The **most secure** computers are those **not connected** to the Internet and **shielded** from any interference”

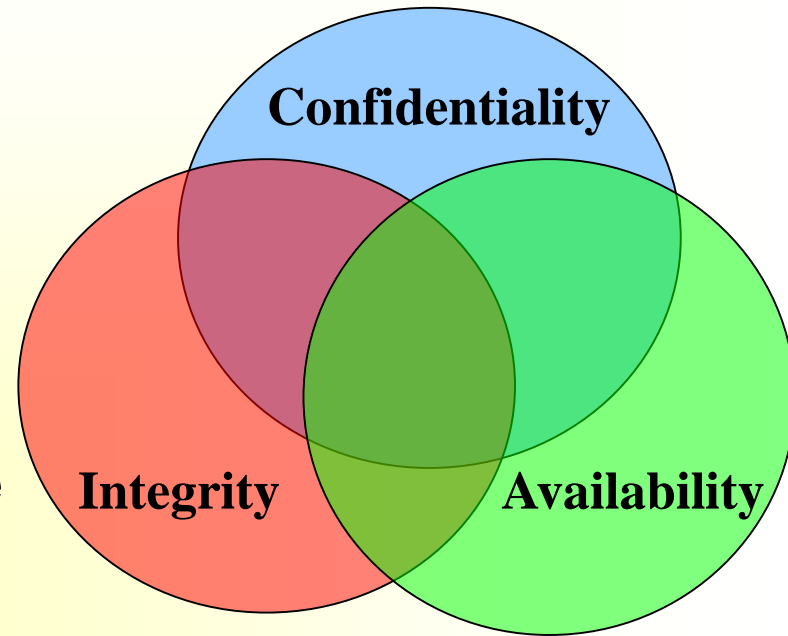


- Two extreme attitudes regarding computer security
 - There is no real threat; they believe that
 - Much of the negative news is simply unwarranted panic
 - If our organization has not been attacked so far, we must be secure
 - This is a **reactive** approach to security; wait to address security issues until an incident occurs
 - The opposite viewpoint overestimates the dangers
 - They tend to assume that talented, numerous **hackers** are an imminent threat to a system
 - They may believe that any teenager with a laptop can traverse highly secure systems at will
 - Such a worldview is unrealistic
 - The reality is that many people who call themselves hackers are less knowledgeable than they think they are. These people have a low probability of being able to compromise any system that has implemented even moderate security precautions

- This does not mean that skillful hackers do not exist
- However, they must balance the costs (financial, time) against the rewards (ideological, monetary)
- “Good” hackers tend to target systems that yield the highest rewards
- Keep in mind, too, that the greatest **external threat** to any system is not hackers, but malware and denial of service attacks. Malware includes viruses, worms, Trojan horses, logic bombs, etc.

1.1.1 Basic Security Objectives (Pillars) - CIA

- **Confidentiality**: This term covers two related concepts:
 - **Data confidentiality**: Assures that private or confidential information or **resources** (**resource** and **configuration hiding**) are not made available or disclosed to unauthorized individuals
 - Is compromised by **reading** and **copying**
 - In network communication, it means only sender and intended receiver should “understand” message contents
 - **Privacy**: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed



- **Integrity**: This term covers two related concepts
 - **Data integrity**: Assures that information and programs are changed only in a specified and authorized manner
 - In network communication, sender and receiver want to ensure that the message is not altered (in transit or afterwards) without detection
 - **System integrity**: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
 - Is compromised by **deleting**, **corrupting**, and **tampering with**
- **Availability**: Assures that systems work promptly and service is not denied to authorized users
- **Authenticity**: Some say it is a missing component of objectives in CIA. It is the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator; or sender and receiver want to confirm the identity of each other

1.1.2 Policy and Mechanism

- A **security policy** is a statement of what is, and what is not, allowed by users of a system
- A **security mechanism** is a method, tool, or procedure for enforcing a security policy
- More on this in Chapter 5 - Security Mechanisms and Techniques and Chapter 6 – Information Security

1.1.3 Goals of Security

- Given a security policy's specification of “secure” and “nonsecure” actions, security mechanisms can **prevent** (**defend**) the attack, **detect** the attack, or **recover** from the attack
 - **Prevention/Defence**: take measures to prevent the damage; it means that an attack will fail; e.g., passwords to prevent unauthorised users or Intrusion Prevention Systems (IPSs)
 - **Detection**: if an attack cannot be prevented; when, how and who of the attack have to be identified; e.g., when a user enters a password three times; Intrusion Detection Systems (IDSs)
 - **Recovery/Reaction**: take measures to recover from the damage; e.g., restore deleted files from backup; sometimes retaliation (attacking the attacker's system or taking legal actions to hold the attacker accountable)
- The three strategies are usually used together
- A fourth approach is **deterrence**; involves active steps to beat off attacks; discourage them even to try attacking

- **Example 1:** Protecting valuable items at home from a burglar
 - **Prevention:** locks on the door, guards, hidden places, etc.
 - **Detection:** burglar alarm, guards, Closed Circuit Television (CCTV), etc.
 - **Recovery:** calling the police, replace the stolen item, etc.
- **Example 2:** Protecting a fraudster from using our credit card in Internet purchase
 - **Prevention:** Encrypt when placing order, perform some check before placing order, or don't use credit card on the Internet
 - **Detection:** A transaction that you had not authorized appears on your credit card statement
 - **Recovery:** Ask for new card, recover cost of the transaction from insurance, the card issuer or the merchant

1.2 Brief History of Computer Security and Privacy

- Until the 1960s computer security was limited to physical protection of computers (Physical Security)
- In the 60s and 70s (System/Information Security)
 - Evolutions
 - Computers became interactive
 - Multiuser/Multiprogramming was invented
 - More and more data started to be stored in computer databases
 - Organizations and individuals started to worry about
 - What the other persons using computers are doing to their data
 - What is happening to their private data stored in large databases

- In the 80s and 90s (Network Security)
 - Evolutions
 - Personal computers were popularized
 - LANs and the Internet invaded the world
 - Applications such as E-commerce, E-government and E-health started to be developed
 - Viruses became majors threats
 - Organizations and individuals started to worry about
 - Who has access to their computers and data
 - Whether they can trust a mail, a website, etc.
 - Whether their privacy is protected in the connected world

■ Famous Security Problems

■ Morris worm – Internet Worm

- On November 2, 1988 a worm attacked more than 60,000 computers around the USA
- The worm attacks computers, and when it has installed itself, it multiplies itself, freezing the computer
- It exploited UNIX security holes in Sendmail and Finger
- A nationwide effort enabled to solve the problem within 12 hours
- Robert Morris became the **first person** to be indicted under the **Computer Fraud** and Abuse Act
 - He was sentenced to 3 years of probation, 400 hours of community service and a fine of \$10,500



*Robert Morris
in 2008*

- **Bank theft**

- In 1984, a bank manager was able to steal \$25 million through un-audited computer transaction

- **NASA shutdown**

- In 1990, an Australian computer science student was charged for shutting down NASA's computer system for 24 hours

- **Airline computers**

- In 1998, a major travel agency discovered that someone penetrated its ticketing system and has printed airline tickets illegally

- **The list continues ...**

- **Does anyone know any security problem stories in Africa and Ethiopia? Most incidents in Africa are not usually reported**

- Early Efforts
 - 1960s: Marked as the **beginning** of true computer security
 - 1970s: Tiger teams
 - Government and industry sponsored **crackers** who attempted to break down defenses of computer systems in order to uncover vulnerabilities so that patches can be developed
 - 1970s: Research and modeling
 - Identifying security **requirements**
 - Formulating security **policy** models
 - Defining **guidelines** and controls
 - Development of **secure systems**
 - Standardization
 - 1985: Orange Book for Security Evaluation (or **TCSEC** - Trusted Computer System Evaluation Criteria) - Chapter 7
 - Describes the evaluation criteria used to assess the level of trust that can be placed in a particular computer system
 - 1978: DES selected as encryption standard by the US

■ Legal Issues

- In the US, **legislation** was enacted with regards to computer security and privacy starting from late **1960s**
- The European Council adopted a **convention** on Cyber-crime in **2001**
- The World Summit for Information Society considered computer security and privacy as a **subject of discussion** in **2003** and **2005**
- In Ethiopia
 - The **Ethiopian Penal Code** of **2005** has articles on data and computer related crimes
 - **Computer Crime Proclamation 2016**

1.3 Computer Security Controls

- Security controls refer to mitigation techniques to achieve security goals (prevention, detection, recovery)

a. Authentication (Password, Card, Biometrics) - For Prevention

(What the entity knows, has, is!)



- Authentication is the binding of an identity to a subject
- An entity must provide information to enable the system to confirm its identity. This information comes from one (or a combination) of the following
 - What the entity knows (such as passwords or secret information)
 - User name: serves to identify user data stored in the system
 - Password: establishes authenticity
 - Password file contains not passwords, but their hash values (see later in Chapter 3)

- What the entity **has** (such as a **badge** or **card**)
- What the entity **is** (such as **fingerprints** or **retinal characteristics - Biometrics**)
 - Such attributes are suitable for biometric identification if the following requirements are met:
 - **Pervasiveness**: everybody has this attribute
 - **Uniqueness**: any two people differ in their values of this attribute
 - **Permanence**: attribute value does not change with time
 - **Measurability**: attribute can be measured
 - Biometric system practices pattern recognition or comparison
 - Attributes of a human are measured, and the measured data are compared with stored data

- The goal is either
 - **verification**: is it actually Alice? (comparison with Alice's stored data - typically for authentication) or
 - **identification**: who is it? - typically for fighting crime
- Practical Systems



(a) Fingerprint system for computer authentication

(b) Fingerprint system for authentication of customers, prior to charging a credit card

(c) Lock with fingerprint system

- Benefits with biometrics as opposed to passwords
 - Simple and intuitive usage
 - Forgery is difficult
 - No oblivion (not forgettable like passwords), loss, theft
 - The user must be present for authentication
- b. Encryption - For Prevention and Detection
- c. Auditing - For Recovery
 - Auditing is essential for recovery and accountability
 - Auditing is the process of analyzing systems to determine what actions took place and who performed them; It is the analysis of log records to present information about the system in a clear and understandable manner
 - Logging is the basis for most auditing; It is the recording of events or statistics to provide information about system use and performance

- d. Administrative procedures - For Prevention, Recovery and Deterrence
- e. Standards and Best Practices - For Prevention
- f. Physical Security - For Prevention
- g. Laws - For Deterrence
- h. Intrusion Detection/Prevention Systems - For Detection/Prevention
- i. Software Patches - For Prevention
- j. Anti-malware - For Prevention
- k. Access Control Technologies (Firewalls, Authentication and Authorization Technologies) - For Prevention

- The Human Factor

- The **human factor** is an important component of computer security
- Some organizations view **technical solutions** as “their only solutions” for computer security
 - Technology is **fallible** (**imperfect**)
 - e.g., UNIX holes that opened the door for Morris worm
 - The technology may **not** be **appropriate**
 - e.g., It is difficult to define all the security requirements and find a solution that satisfies those requirements
 - Technical solutions are usually (very) **expensive**
 - e.g., Antivirus
- Given all these, someone, a **human**, has to be there to **implement** the solution

- **Competence** of the security staff
 - e.g., Crackers may know more than the security team
- Understanding and **support** of **management**
 - e.g., Management does not want to spend money on security; difficult to convince them based on Return on Investment (ROI); a better approach is to view this investment as insurance
- Staff's **discipline** to follow procedures
 - e.g., Staff members choose simple passwords
- Staff members may **not** be **trustworthy**
 - e.g., Bank theft

1.4 Physical Security

“The most robustly secured computer that is left sitting unattended in an unlocked room is not at all secure !!” [Chuck Easttom]

- Physical security is the use of **physical controls** to protect premises, site, facility, building or other physical asset of an organization [Lawrence Fennelly]
- Physical security protects your **physical computer facility** (your building, your computer room, your disks and other media) [Chuck Easttom]
- Physical security was overlooked in the past few years by organizations because of the emphasis placed on improving cyber security

- In the early days of computing, physical security was **simple** because computers were big, standalone, expensive machines
 - It was almost **impossible to move** them (not portable)
 - They were very few and it is **affordable** to spend on physical security for them
 - Management was **willing** to spend money
 - Everybody **understands** and accepts that there is restriction

- Today
 - Computers are more and more **portable** (PC, laptop, Smart phone)
 - There are **too many** of them to have good physical security for each of them
 - They are not “too expensive” to **justify** spending more money on physical security until a major crisis occurs
 - Users **don't accept restrictions** easily
 - Accessories (e.g., network components) are **not** considered as **important** for security **until there is a problem**
 - Access to a single computer may **endanger many** more **computers** connected through a network
- ⇒ **Physical security is much more difficult to achieve today than some decades ago**

1.4.1 Types of Vulnerabilities

- Physical vulnerabilities (e.g., Buildings)
- Natural vulnerabilities - disasters (e.g., Earthquake)
- Hardware and Software vulnerabilities (e.g., Failures)
- Media vulnerabilities (e.g., Disks can be stolen)
- Communication vulnerabilities (e.g., Wires can be tapped)
- Inherent Technological weaknesses: Computer and network technologies have intrinsic security weaknesses. These include TCP/IP protocol weaknesses, operating system weaknesses, and network equipment weaknesses

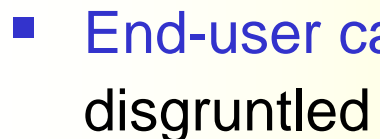


Not in the area of physical security

- **Configuration weaknesses:** These include mis-configured hardware or software and poor network design. The major ones are the following.
 - **Unsecured user accounts:** User account information might be transmitted insecurely across the network, exposing usernames and passwords to snoopers
 - **System accounts with easily guessed passwords:** This problem is the result of poorly selected and easily guessed user passwords

- Security policy weaknesses

- Lack of written security policy: A policy that is not written cannot be consistently applied or enforced
- Software and hardware installation and changes do not follow policy: Unauthorized changes to the network topology or installation of unapproved applications create security holes
- Disaster recovery plan nonexistent: Lack of a disaster recovery plan creates chaos, panic, and is a cause for confusion to occur when someone attacks the organization

- 
- End-user carelessness and intentional end-user acts (that is, disgruntled employees or the insider threat)

- **Some of the vulnerabilities in brief**

- 1. Natural Disasters

- a. Fire and smoke

- Fire can occur anywhere
 - Solution – Minimize risk
 - Good policies: No Food and Drinks, No Smoking, etc.
 - Fire extinguisher, good procedure and training
 - Fireproof cases (and other techniques) for backup tapes
 - Fireproof doors

b. Climate

- Heat
- Direct sun
- Humidity
- Hurricane, storm, cyclone
- Earthquakes
- Water
 - Flooding can occur even when a water tap is not properly closed
- Electric supply
 - Voltage fluctuation (Solution: Voltage regulator)
- Lightning

Avoid having servers in areas often hit by Natural Disasters!

2. People

- Intruders
 - Thieves
 - People who have been given access unintentionally by insiders
 - Employees, contractors, etc., who have access to the facilities
- External thieves
 - Portable computing devices can be stolen outside the organization's premises

3. Loss of a computing device

- Mainly laptop

1.4.2 Safe Area

- **Safe area** is often a locked place where only authorized personnel can have access
- **Organizations** usually have safe area for keeping computers and related devices
- **Challenges**
 - Is the area **inaccessible** through other opening (window, roof-ceilings, ventilation hole, etc.)?
 - Design of the building with security in mind
 - Know the architecture of your building
 - **During opening hours**, is it always possible to detect when an unauthorized person tries to get to the safe area?
 - Surveillance/guards, video-surveillance, automatic doors with security code locks, alarms, etc.
 - Put signs so that everybody sees the safe area

- Are the **locks** reliable?
 - The effectiveness of locks depends on the design, manufacture, installation and maintenance of the keys
 - Among the attacks on locks are
 - Illicit keys
 - Duplicate keys
 - Avoid access to the key by unauthorized persons even for a few seconds
 - Change locks/keys frequently
 - Key management procedure
 - Lost keys
 - Notify responsible person when a key is lost
 - There should be no label on keys
 - Circumventing of the internal barriers of the lock
 - Directly operating the bolt completely bypassing the locking mechanism which remains locked
 - Forceful attacks
 - Punching, Drilling, Hammering, etc.

- Surveillance with Guards
 - The most common in Ethiopia
 - Not always the most reliable since it adds a lot of human factor
 - Expensive in terms of manpower requirement
 - Not always practical for users (employees don't like to be questioned by guards wherever they go)

- Surveillance with Video
 - Use of Closed Circuit Television (CCTV) that started in the 1960s
 - Became more and more popular with the worldwide increase of theft and terrorism
 - Advantages
 - A single person can monitor more than one location
 - The intruder doesn't see the security personnel
 - It is cheaper after the initial investment
 - It can be recorded and be used for investigation
 - Since it can be recorded the security personnel are more careful
 - Today's digital video surveillance can use advanced techniques such as face recognition to detect terrorists, wanted people, etc.
 - Drawback
 - Privacy concerns

1.4.3 Internal Human Factor - Personnel

- Choose employees **carefully**
 - Personal integrity should be as important a factor in the hiring process as technical skills
- Create an atmosphere in which the levels of employee **loyalty**, **morale**, and **job satisfaction** are high
- Remind employees, on a regular basis, of their **continuous responsibilities** to protect the organization's information
- Establish procedures for **proper destruction** and **disposal** of obsolete programs, reports, and data
- Act **defensively** when an employee must be discharged, either for cause or as part of a cost reduction program
 - Such an employee should not be allowed access to the system and should be **carefully watched** until s/he leaves the premises
 - Any **passwords** used by a former employee should be immediately disabled

- Guard Against Disgruntled Employees and Angry Former Employees
 - Many organizations have suffered damage by disgruntled employees or angry former employees. This is often referred to as the **insider threat**, or **former insider threat**
 - In situations where employees plan to do damage to the facilities or equipment of an organization, they have several advantages compared to **outsiders** who want to inflict physical damage
 - Knowledge of facility layout and design
 - Familiarity with the location of sensitive or expensive equipment
 - Duplicate keys that allow them easy access to buildings
 - Knowledge of access codes for alarm systems
 - The ability to gain access to buildings with the aid of a friend or relative who is still employed by the organization
 - Knowledge of organizational habits such as shift changes or which doors are not secured during working hours

- Some basic steps that can be taken to reduce those advantages
 - Notify security staff when an employee has been terminated or suspended
 - When you do not have a security staff, notify all managers and supervisors when an employee has been terminated or suspended
 - Maintain strict policies on access to facilities by nonemployees, and train all employees on those policies
 - If terminated or suspended employees had been issued keys, ensure that keys are returned
 - Change the locks for which any angry former employee had keys
 - Change key codes to electronic doors immediately after an employee has been terminated or suspended
 - Disable user rights for computers or communications systems held by a former or suspended employee