MALAYAN COLLEGES LAGUNA ONLINE | CCIS College of Computer and Information Science, Malayan Colleges Laguna

Threats to Information Security

TOPIC OBJECTIVE(S): Identify the threats posed to information security

Management must be informed of the various kinds of threats facing the organization.

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

Threats

We already defined what threat is -- **an object, person, or other entity that represents a constant danger to an asset.**

The 2002 Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI) survey on Computer Crime and Security found:

- *90% of organizations responding detected computer security breaches within the last year*
- *80% lost money to computer breaches, totaling over $455,848,000 up from $377,828,700 reported in 2001*
- *The number of attacks that cam across the Internet rose from 70% in 2001 to 74% in 2002*
- *Only 34% of organizations reported their attacks to law enforcement*

Threats to Information Security

Categories of Threat	Examples
• Acts of human error or failure	Accidents, employee mistakes
• Compromise to intellectual property	Piracy, copyright infringement
• Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
• Deliberate acts of information extortion	Blackmail of information disclosure
• Deliberate acts of sabotage or vandalism	Destruction of systems or information

Threats to Information Security

Categories of Threat	Examples
• Deliberate acts of theft	Illegal confiscation of equipment or information
• Deliberate software attacks	Viruses, worms, macros, denial-of-service
• Forces of nature	Fire, flood, earthquake, lightning
• Deviations in quality of service from service providers	Power and WAN service issues
• Technical hardware failures or errors	Equipment failure

Threats to Information Security

Categories of Threat	Examples
• Technical software failures or errors	Bugs, code problems, unknown loopholes
• Technological obsolescence	Anticipated or outdated technologies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 the greatest threats to information security -- they are the closest to the organization data

Who is the biggest threat to your organization?

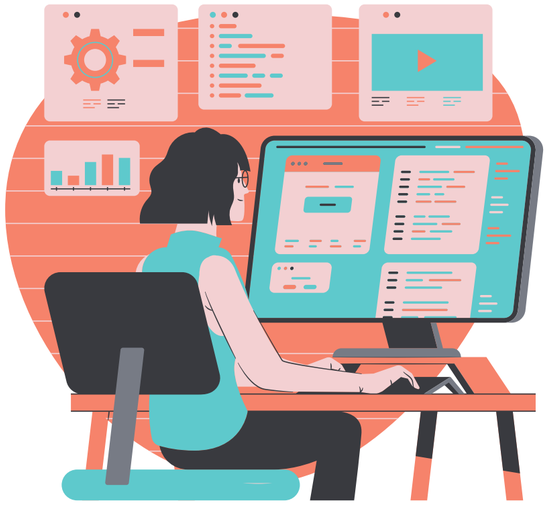
Employees tempted to steal from the company

Tom Twostory
convicted burglary

Employees who developed personal interests

Dick Davis a.k.a. "wannabe amateur hacker"

Employees who commits a purely honest mistake



Harriet Altthumbs
accidentally deleted the only copy of a critical report

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*

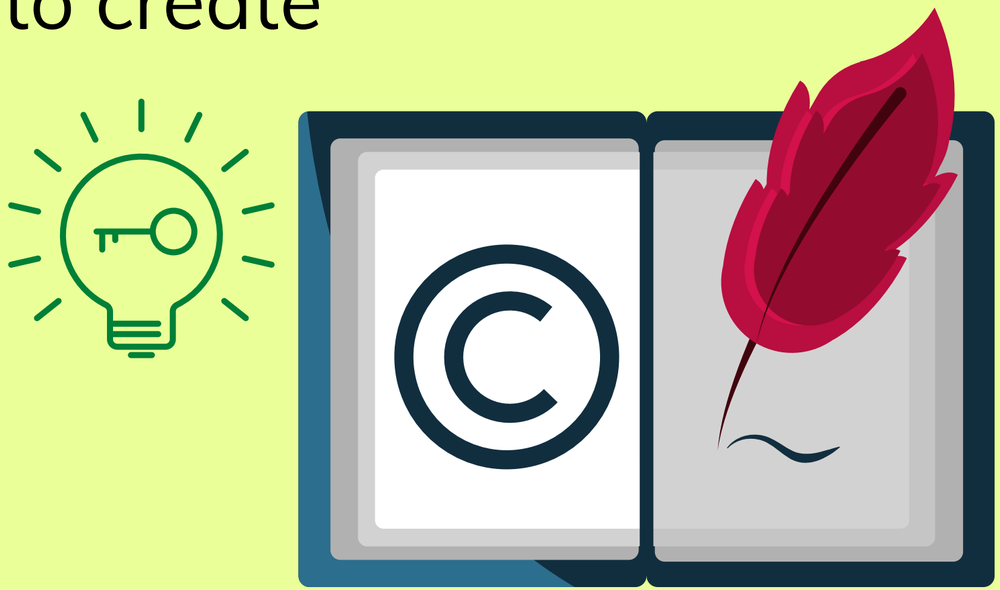
*Many of these threats *can be prevented with controls*

Compromises to Intellectual Property

Intellectual property is "the ownership of ideas and control over the tangible or virtual representation of those ideas"

Many organizations are in business to create intellectual property (IP):

- *Trade secrets*
- *Copyrights*
- *Trademarks*
- *Patents*



Compromises to Intellectual Property

Most common IP breaches involve ***software piracy***

Watchdog organizations investigate:

- *Software and Information Industry Association (SIIA)*
- *Business Software Alliance (BSA)*

Espionage or Trespass

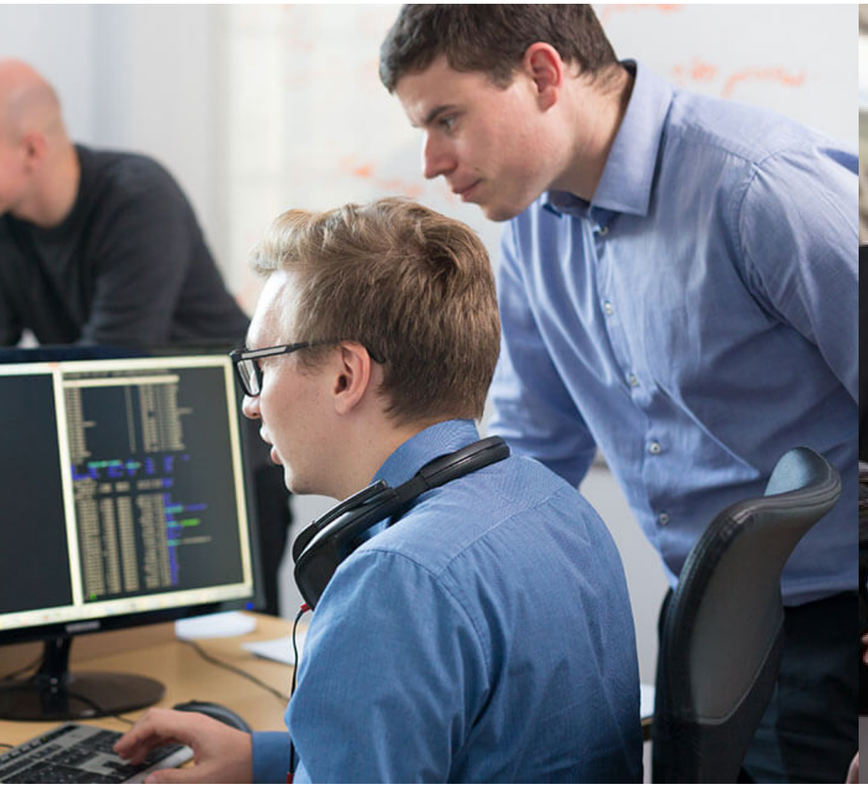
These are broad category of activities that breach confidentiality.

- *Unauthorized accessing of information*
- *Competitive intelligence (the legal and ethical collection and analysis of information regarding the capabilities, vulnerabilities, and intentions of business competitors) versus espionage*
- *Shoulder surfing can occur in any place a peron is accessing confidential information*

Espionage or Trespass

- *Controls are implemented to mark the boundaries of the organization's virtual territory giving notice to trespassers that they are encroaching on the organization's cyberspace*
- *Hackers use skill, guile, or fraud to steal the property of someone else*

Shoulder surfing takes many forms.
Some may not be obvious.



Hacker Profiles

Traditional hacker profile: Age 13-18, male with limited parental supervision spends all his free time at the computer

Modern hacker profile: Age 12-60, male or female, with varying technological skill levels; may be internal or external to the organization

Espionage or Trespass

Generally, two skill levels among hackers:

- *Expert hacker* - develops software scripts and codes exploits; usually a **master of many skills**; will often 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

Espionage or Trespass

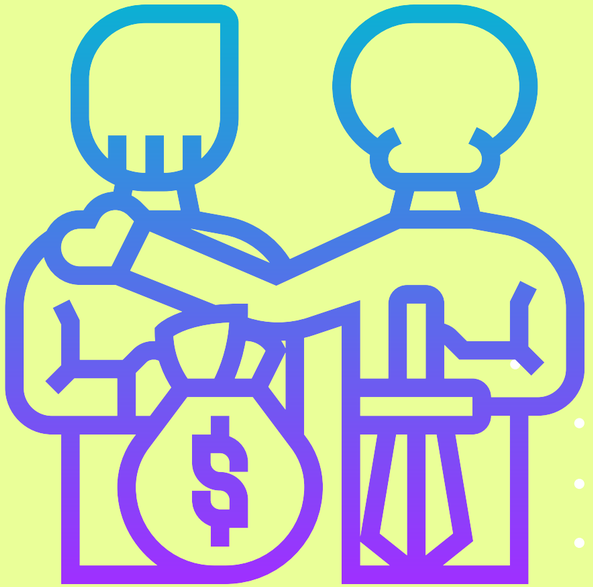
Other terms for system rule breakers:

- *Cracker* - an individual who "cracks" or removes protection designed to prevent unauthorized duplication [of apps, programs, software packages]
- *Phreaker* - hacks the public telephone network to gain access [usually to use it for free]

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.

- *Hackers* hold your data, website, computer systems, or other *sensitive information* hostage until you meet their demands for payment



Sabotage or Vandalism

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.

- These threats can range from petty vandalism to organized sabotage
- Organizations rely on *"image"* -- so web defacing can lead to dropping of consumer confidence, even sales

Deliberate Acts of Theft

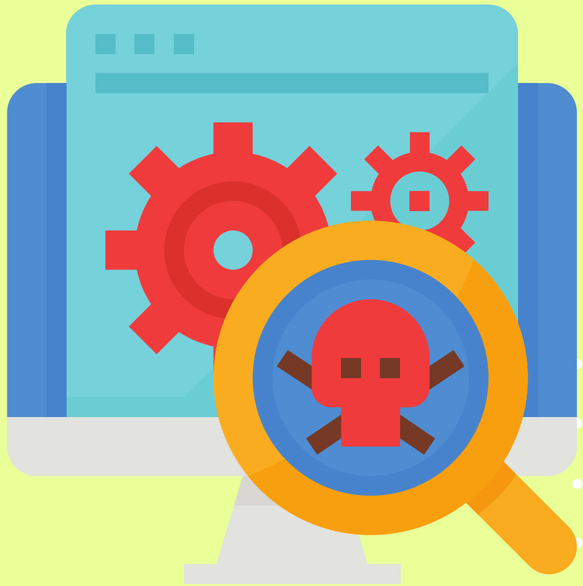
Illegal taking of another's property -- physical, electronic, or intellectual

- *Physical theft* -- can be controlled with a wide variety of measures used from locked doors to guards or alarm systems
- *Electronic theft* -- 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.

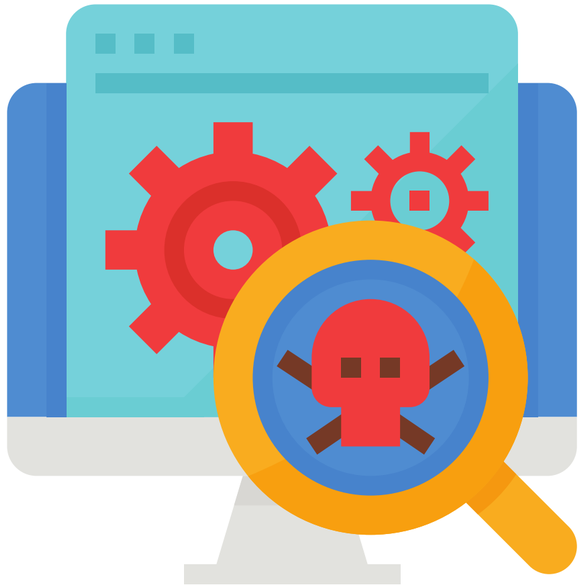
- Designed to *damage*, *destroy*, or *deny service* to the target systems



Deliberate Software Attacks

Includes:

- *Macro viruses*
- *Boot virus*
- *Worms*
- *Trojan horses*
- *Logic bombs*
- *Back door or trap door*
- *Denial-of-service (DoS) attacks*
- *Polymorphic*
- *Hoaxes*



Trojan horse arrives via email or software such as free games

Trojan horse is activated when the software or attachment is executed

Trojan horse releases its payload, monitors computer activity, installs backdoor, or transmits information to hacker

Forces of Nature

Forces of nature (force majeure), or acts of God, are dangerous because they are unexpected and can occur with very little warning.

- Can disrupt not only the lives of the individuals, but also the storage, transmission, and use of information
- Include *fire*, *earthquake*, *lightning*, as well as *volcanic eruption* and *insect infestation*

*Since it is not possible to avoid many of these threats, management must implement controls to limit damage and also prepare ***contingency plans*** for continued operations

Deviations in Quality of Service

Pertains to situations of product or services not delivered as expected.

Information system depends on many inter-dependent support systems.

Three sets of service issues that dramatically affect the availability of information and systems:

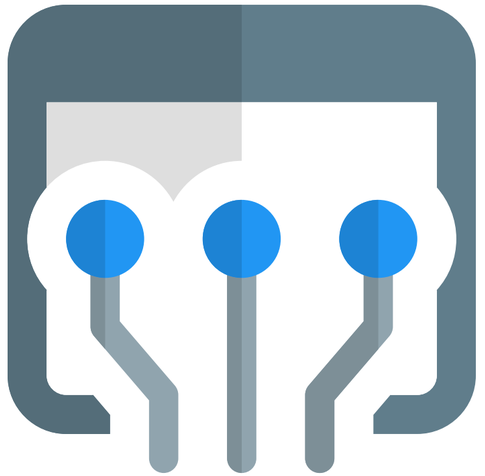
- *internet service*
- *communications*
- *power irregularities*

Internet Service Issues

Loss of internet service can lead to considerable loss in the availability of information -- especially in these times -- for most organizations who allow their employees to *telecommute*, or work at remote locations (***work-from-home setup***).

When an organization outsources its web servers, the outsourcer (or provider) assumes responsibility for:

- *all internet services*
- *the hardware and OS used to operate the website*

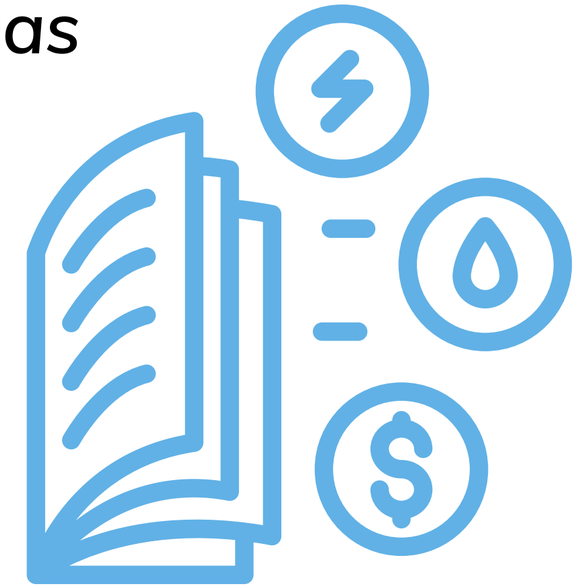


Communications and Other Services

Other utility services have potential impact as well.

Among these are;

- *telephone*
- *water and wastewater*
- *trash pickup*
- *cable television*
- *natural or propane gas*
- *custodial services*



The threat of loss of services can lead to **inability to function properly.**

Power Irregularities

Voltage levels can *increase*, *decrease*, or *cease*:

- *Spike* -- momentary increase
- *Surge* -- prolonged increase
- *Sag* -- momentary low voltage
- *Brownout* -- prolonged drop
- *Fault* -- momentary loss of power
- *Blackout* -- prolonged loss

Electronic equipment is susceptible to fluctuations, controls can be applied to manage power supply and quality.

Technical Hardware Failures and Errors

Technical hardware failures or errors occur when a manufacturer distributes to users equipment containing flaws.

- These defects can cause the system to perform outside of expected parameters, resulting in unreliable service, or lack of availability
- Some errors are *terminal*, in that they result in the unrecoverable loss of the equipment
- Some errors are *intermittent*, in that they only periodically manifest themselves, resulting in faults that are not easily repeated

Technical Software Failures and Errors

This category of threats comes from purchasing software with unrevealed faults.

- Large quantities of computer code are written, debugged, published, and sold only to determine that not all bugs were resolved
- Sometimes, unique combinations of certain software and hardware reveal new bugs
- Sometimes, these items aren't errors, but are purposeful shortcuts left by programmers for honest or dishonest reasons

Technological Obsolescence

When infrastructure becomes antiquated or outdated, it leads to unreliable and untrustworthy systems

- Management must recognize that when technology becomes ***outdated***, there is a *risk of loss of data integrity* to threats and attacks
- Ideally, proper planning by management should prevent the risks from technology obsolescence, but when obsolescence is identified, management must take action

Topic Summary

- Identified the threats that posed to information security

Threats to Information Security

IT128: Information Assurance and Security

~eldiem~

MALAYAN COLLEGES LAGUNA ONLINE

CCIS College of Computer and Information Science
Malayan Colleges Laguna