Key Terms & Principles in InfoSec

CISC 3325 — CUNY Brooklyn College
Lecture Notes

Key Terms & Principles in InfoSec

In this chapter, we will:

1. Learn what types of assets shall be secured.
2. Find out what types of security threats and types of attackers exist.
3. Introduce the "CIA" security concepts that we'll use throughout our course.
4. Speak about security control methods and countermeasures.
5. List the 8 fundamental principles of information security.

What Assets to Keep Secure

In Topic 1, we learned that information security is about defending information from unwanted actions like disruption, modification, etc.

Information, however, isn't an independent entity existing by itself: it is kept or held in a physical storage device as data, transmitted through cable or wireless means, and processed by computer programs.

As such, we must provide adequate security to the following categories of assets:

- Hardware
- Software
- Data

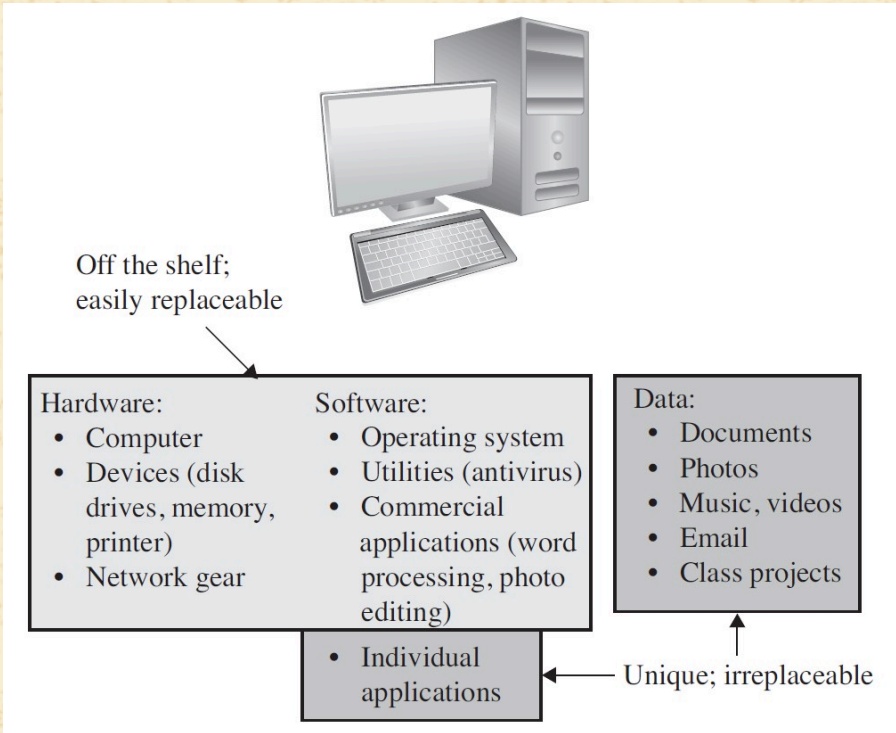
The value of each asset depends on (1) the **ease and cost of replacement** (in case of damage/loss) and (2) **how unique and personally valuable it is** to the asset's owner.

What Assets to Keep Secure

Hardware:	Software:	Data:
• Computer	• Operating system	• Documents
• Devices (disk drives, memory, printer)	• Utilities (antivirus)	• Photos
• Network gear	• Commercial applications (word processing, photo editing)	• Music, videos
	• Individual applications	• Email
		• Class projects

Hardware, software, and data assets to keep secure. "Figure 1-2: Computer Objects of Value" (page 3), Pfleeger, Charles P., et al. *Security in Computing*. Prentice Hall, 2015.

What Assets to Keep Secure



Values of assets. "Figure 1-3: Values of Assets" (page 4), Pfleeger, Charles P., et al. *Security in Computing*. Prentice Hall, 2015.

What Assets to Keep Secure

Another important aspect of information security to consider is **People**.

Many vulnerabilities emerge because of uncareful human behavior (for example: using a weak account password,) and can be prevented by providing adequate training and by raising the awareness of information security risks resulting from uncarefulness.

Keeping the employees of the workplace motivated and aware of security risks and involving them in the implementation of information security measures is an important aspect of information security that cannot be forgotten at any cost.

The collection of all the measures that we take to secure hardware, software, and data and to convey security principles to employees is considered a **layered approach** to security. An effective implementation of information security should consider all the layers without omitting any of them.

What Assets to Keep Secure

Any questions?

Types of Threats

Security threats are divided into two categories: External Threats and Internal Threats.

External Threats are threats that originate outside of an organization or system, primarily from the environment in which the organization or system operates.

Conversely, **Internal Threats** emerge from inside the system or company, with the primary contributors being employees, contractors, or suppliers to whom work is outsourced. Internal Threats mainly have a form of fraud, misuse of information, and/or destruction of information, and account for about **80%** of all security incidents.

The following slides divide External and Internal threats into groups and provide examples of each group of threats.

Some of the attack examples / names on slides 10 – 12, especially under the Network, Software, and Human threat groups might be unfamiliar to you yet; no worries, as we will cover those terms in the upcoming topics!

External Threats: Groups

Kinds of external threats. "Figure 3-2: External threats" (page 32), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.

External Threats: Groups and Examples

Physical Threats

- Natural disasters: hurricanes, floods, earthquakes, etc.
- Fire or arson
- Terrorist threats: bombs, hostage situations, etc.
- Hardware destruction & damages
- Physical intrusion, e.g., vandalism
- Sabotage, e.g., by company's rivals
- Theft of sensitive assets/information

Network Threats

- Sniffing or Eavesdropping
- Snooping, authentication attacks, or hijacking
- Spoofing
- "Man in the middle" attacks
- "Denial of service" attacks
- SQL injection
- Exploitation of weak passwords
- Exploitation of weak encryption

External Threats: Groups and Examples

Software Threats

- Defects leading to errors
- Defects being exploited
- Malware: viruses, worms, etc.
- Bots or Botnets
- Invalidated inputs
- Authentication attacks
- Exploitation of misconfigurations

Software Threats – Cont'

- Login and session-related issues
- Inappropriate error handling by apps
- Buffer overflow issues
- Mishandled cryptography by apps
- Variable manipulations/abuse
- OS-related issues and flaws

Human Threats

- Social engineering
- Hacker attacks
- Blackmail, extortion
- Espionage (= spying)

Compliance Threats

- Fees, penalties, and closure of a company when it doesn't follow security laws and rules.

Internal Threats: Groups and Examples

Human Threats

- Misuse of assets or information
- Mistakes by employees
- Espionage (= spying)
- Employee Social Engineering
- Employees' lack of knowledge
- Weak password breaking
- Theft
- Unfollowed policies / rules

Human Threats – Con't

- Fraud due to role abuse
- Malware from infected devices
- Disallowed software downloads

Internal Application Threats

- Invalidated inputs
- Misconfigured apps
- Wrong error handling in apps

Internal Application Threats – Con't

- Variable manipulation & abuse
- Unauthorized access

Other Threats

- Data theft from USB disks
- System corruption: power surge
- Hardware failure due to errors
- Infrastructure failure: bad maintenance

Types of Attackers

Movies, caricatures, and websites usually depict computer attackers as secretive, shady, hoody-dressed geniuses sitting in front of a computer and typing or running a significant amount of code (such as the image on slide 14.) This depiction, however, is far from reality since attackers are very diverse in their personality, cognitive ability, socio-economic status, reasons for attacking, attacking resources available to them, and how they unleash their attacks.

Studies about the nature of attackers usually analyze cyber-criminals and convicts (because they are the ones 'at hand'.) Not surprisingly, the characteristics of non-criminal attackers, such as hackers who do it for fun or frustrated individuals who wish to get revenge, may be different from those of criminal attackers.

In general, no single exact profile would capture the traits of a "typical" computer attacker, and the traits of some famous attackers also match many people who are not attackers.

In the next slides, we present a few common categories of attack and their attack motives (= reasons / goals).

Types of Attackers

The (wrong) depiction of a typical attacker. Image by Drazen Zigic on Freepik.

Types of Attackers

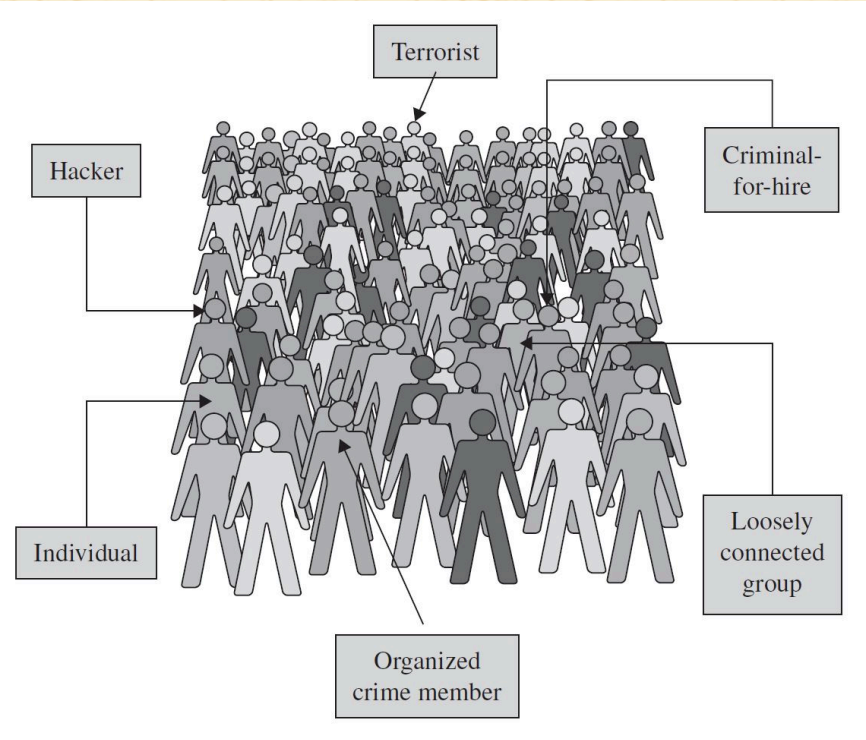
Speaking in a very generalizing way, below are some common types of attackers:

1. **Individuals**. The very first computer attackers were individuals, who committed these actions for fun, to show off, for challenge, to test their own abilities, and sometimes out of revenge. Two famous individual attackers are Robert Morris and Kevin Mitnick.
2. **Organized, Worldwide Groups**. Groups of loosely-connected international groups of hackers conducted more recent attacks. "Loosely-connected" means that the attackers don't know other attackers in that group very well and that they aren't restricted from leaving the group whenever they want and joining other such groups. The motives of such groups in unleashing attacks are mostly financial: they 'join forces' to attack systems or companies to steal money, e.g., by stealing customer credit card information.
3. **Organized Crime Groups**. The goal of such criminals isn't damaging a computer or system but turning that computer into a money-making target. For instance: by secretly stealing credit card information over a period of time without being detected or demanding ransom for data they stole and encrypted, and also selling the data.

Types of Attackers

3. Organized crime groups realize that computer crime can be lucrative: their motives may include fraud, extortion, money laundering, and drug trafficking, among other financial-related reasons. Furthermore, they often use the money they steal during cyberattacks to finance other types of crimes they engage in.
4. **Terrorists**. The term **terrorism** is defined as bringing fear and damage to people amid ideological views. Terrorists may use a computer in several ways to accomplish their attack:
    1. Setting computers as targets of attack, such as when destroying power plant and hospital computers.
    2. Using computers as methods of attack, e.g. by writing a virus and running it on a victim's computer.
    3. Using computers as enablers of attack, e.g. to communicate and coordinate with other terrorists.
    4. Using computers as enhancers of attack, e.g. by recruiting additional terrorists to amplify the attack.
5. **Governments**. As technology gets commonplace and many vital services and infrastructures increasingly depend on computers, governments realize the potential of using cyber-attacks for warfare and as a measure of defense from enemy countries. Governments, though, often avoid taking responsibility and keep such actions secret.

Types of Attackers



Attackers being diverse and hard to distinguish in a crowd. "Figure 1-10: Attackers" (page 17), Pfleeger, Charles P., et al. *Security in Computing*. Prentice Hall, 2015.

Types of Attackers

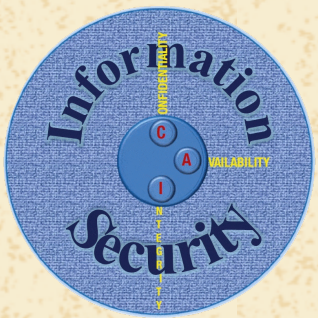
Any questions?

The CIA Triad

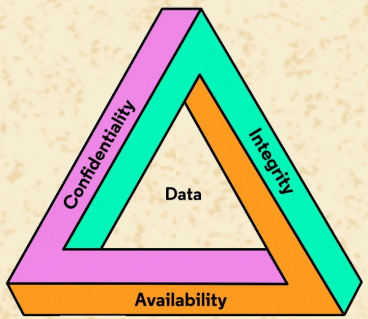
So far, we discussed what assets we shall secure, what threats we shall secure those from, and what kinds of perpetrators impose such threats. However, we haven't talked about *how* to secure the assets (that is, what action we are supposed to take to keep them secure.)

To address this question, we introduce an information security model called **CIA**, whose principles will direct us on how to secure information-related assets we care about.

The name "CIA" is an acronym, not for the Central Intelligence Agency, but for the three pillars of this model: Confidentiality, Integrity, and Availability. It is, therefore, often referred to as the **CIA Triad**. We'll explore it next.



CIA logo (from the book). "Figure 3-7: CIA Triad" (page 51), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.



CIA logo (triangle). Taken from Codeacademy's "What is Cybersecurity?" worksheet here.

The CIA Triad

1. **Confidentiality** means "avoiding the disclosure of information to those who aren't allowed or wanted to view it." That is, only those who are authorized to view this information can access it.

   Confidentiality is related to privacy, but information can be confidential also due to its national strategic importance, loss of business opportunities, and copyright and trademark issues.

   Each type of data/information has its own level of confidentiality: for example, our lecture notes are viewable by anyone with an Internet connection (no confidentiality at all,) while your medical information can/should be viewed only by healthcare professionals (a higher confidentiality level.)

   Accessing confidential info by an unauthorized person or computer program isn't the only way to violate confidentiality: accessing any partial detail or metadata about that confidential info is a violation as well.

The CIA Triad

Ways to Enforce Confidentiality:

1. **Access Control** (covered in Topic 3) is a set of policies that dictate who can access what information. These designations are assigned based on an employee's role in a company or, in the case of a computer system, the username. As part of Access Control, we will discuss:
   - **Authentication**, which is the confirmation of a person's identity and that they don't impersonate someone else to access information, and
   - **Authorization**, which is a "yes" or "no" answer that a computer system gives each time a user requests to access information depending on whether they are or aren't allowed to access it.
2. We also have to enforce **Physical Security** measures (also covered in Topic 3), such as keeping a computer in a locked room or keeping curtains closed, to physically limit access to confidential information.
3. Another method to enforce confidentiality is via **Encryption** (covered in Topic 4), in which characters in an information piece are scrambled to prevent unwanted people from understanding that info and can be recovered to its original form only by someone who has the decryption key (= authorized people.)

The CIA Triad

2. **Integrity** means "keeping a piece of information from being modified in an unauthorized / unwanted way." That is, only those who are authorized to make any changes to this information can do so.

   A system follows the Integrity principle when its data and information aren't unwantedly changed, neither while being stored on a computer, during transmission, nor while being processed by apps / programs on the system.

   Unwanted changes may also happen accidentally, such as when data get corrupted due to a system's or app's crash. Since the results are as grave as with intentional changes, we must secure information from any unwanted modification, whether intentional or unintentional.

   Example: Hank downloaded Minecraft from a pirate website run by hackers who implanted spyware in the game that will, from now on, record Hank's voice and video without his consent and without him even knowing it.

The CIA Triad

Ways to Enforce Integrity:

1. **Authentication** doesn't help only in preserving confidentiality but also for integrity because, but verifying the identity of, for example, the developer of a game you download online, you ensure that no one besides only the people you expected to develop this game touched it.
2. **Application Security** (covered in Topics 5-6) is needed to verify that the applications one runs on their device don't intentionally or unintentionally modify data in an unwanted way.
3. Similarly, **Network Security** (covered in Topic 8) ensures that data isn't modified while being transmitted from one device to another in a way we don't want.
4. Detecting if an error occurred (**Error Detection**) or even correcting errors that were detected (**Error Correction**) (covered in Topic 10) will help keep information unmodified.
5. Performing **Data Backups** periodically (covered in Topic 12) is a way to make sure that, even if data is destroyed on one device, we can recover it from the backup we made.

The CIA Triad

3. **Availability** means "ensuring that information is available to authorized people whenever they need to access, view, or even modify it."

   A computer system that crashes when too many users access it at the same time or crashes to due a cyber attack, due to which access to information isn't provided to the authorized users, violates the Availability principle.

   Example: You are required to carry out certain work and your reference documents are in a particular database and that particular database is down for technical reasons.

Ways to Enforce Availability:

1. **Physical Security** can also keep a system from natural disasters and vandalism that reduce availability.
2. Just as with integrity, **Data Backups** help keep posting data that were lost or damaged.

The CIA Triad

A beautiful 5-min video on the CIA Triad:

https://www.youtube.com/watch?v=432IHWNMqJE

The CIA Triad

Fun Class Activity: Match the incidents to the principles that are violated (one principle per incident:)

	Incidents
1	You want to register for classes on CUNYfirst, but it is undergoing unexpected maintenance.
2	Tom, your neighbor, uses his binoculars to look thru your window and see what you are doing.
3	A bug in a browser causes dates & times of Incognito browsing to show in your history.
4	A bug in your email server led to your reception of only a part of an email message.
5	You are working on a Word document when it suddenly stops responding.
6	A banker unlawfully sets up a transfer of $1000 from each of his clients, whose accounts info he is allowed only to view, to his bank account.

	Principles
A	Confidentiality
B	Integrity
C	Availability

Reminder: **Confidentiality** is the ability to view information, **Integrity** is the ability to change information, and **Availability** is the ability to access and use information whenever needed, all by authorized people/programs only.

The CIA Triad

A security model similar to and building up on CIA has not three but five principles.

It is named **The Five Pillars Of Information Assurance**, and it was proposed by the U.S. Department of Defense.

The five principles are listed below and are defined as follows:

1. **Confidentiality** is defined the same way as on slide 20.
2. **Integrity** is defined in a similar way to the one on slide 22, except that Integrity here doesn't assume the confirmation of a person's identity.
3. **Availability** is defined the same way as on slide 24.
4. **Authenticity** is the ability to confirm a person's (such as a computer user's or a message sender's) identity.
5. **Non-Repudiation** is the ability to obtain proof of a message's delivery in a way that prevents the sender from denying that he or she sent or wrote the message (repudiation = denial of one's actions.)

The CIA Triad

Any questions?

Control Methods

As we defined it in Topic 1, a control is a way to counter or address threats.

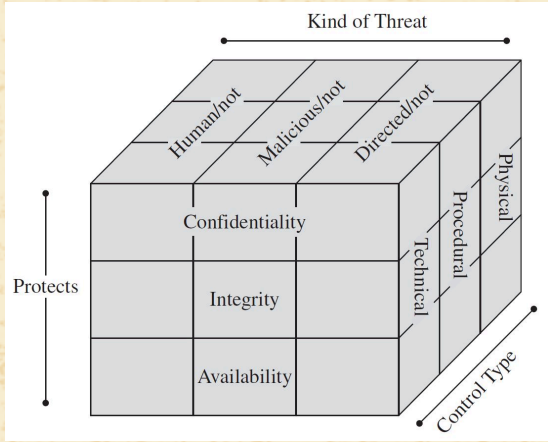
An organization can take the following courses of action as a means of controlling threats:

a. Fully block an attack by removing an underlying vulnerability.
b. Make the attack difficult to be carried out (e.g., to save more time and reduce damages.)
c. Make the target computer system less attractive to hackers, such as by removing confidential information from it or encrypting the data using a difficult-to-break key.
d. Plan ahead on what countermeasures to use to make the attack less severe in case it happens.
e. Train information security specialists to detect attacks that are in progress and take countermeasures.
f. Have a plan to recover with as minimal damages as possible from an attack in case such happens.

Control Methods

Controls are divided into 3 types:

1. **Physical Controls**, which are tangible objects that can be used for protection, e.g., doors, walls, locks, etc.
2. **Administrative Controls** that prescribe how a company behaves in each situation, e.g., policies and laws.
3. **Technical Controls** using hardware and software for control implementation, e.g., passwords and encryption.



A control per each threat type and each CIA principle. "Figure 1-13: Types of Countermeasures" (page 31), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.

Risk Management

It is *impossible* to have protection from 100% of all possible threats.

- Such a goal will require a skyrocketing budget just for security measures, which companies can't afford.

As such, each organization should do its research on what types of threats are the most relevant and can bring significant damage to the company, and direct its budget towards controlling these selected threat types. This procedure is called **Risk Management**, as part of which the organization will assess a risk level as follows:

$$\text{Risk} = (\text{probability that a threat is realized through an attack}) * (\text{cost of the damaged asset})$$

The higher a calculated risk is, the more resources the company should devote to controlling that threat.

Risk Management assists an organization in maximizing protection and minimizing costs and damages, as well as minimizing the probability or impact of unfortunate events.

Risk Management

Example: Given information on two threat types in the table below, an organization should prioritize protection against Threat 2 because its risk, which we calculate to be 0.02 * 550,000 = 11,000, is greater than the risk imposed by Threat 1, which is 0.91 * 10,000 = 9100, despite Threat 1's probability to occur being much higher:

Threat	Probability of Happening	Cost of Damage
Threat 1	0.91	$10,000
Threat 2	0.02	$550,000

Fun Class Activity: Which two of the following three threats should receive a company's greatest attention?

Threat	Probability of Happening	Cost of Damage
Threat X	0.36	$100,000
Threat Y	0.59	$89,000
Threat Z	0.21	$250,000

Risk Management

Risk management is about balancing off probabilities of threats and costs of assets. Adapted from image by Clker-Free-Vector-Images from Pixabay.

The list of threats that can affect a company, their risk levels, the decisions on which threats to prioritize, and the tools (hardware, software, etc.) that the company plans to use to control the threats are collectively called a **threat model**.

8 Fundamental Principles of Information Security

The principles below were published back in 1966 by the National Institute of Standards and Technology (NIST) as part of "Special Publication 800-14". These fundamental expectations are valid and relevant even in today's context:

1. **Principle 1: Computer Security Supports the Mission of an Organization**
   Without enforcing computer security, the organization will suffer damages from cyberattacks, which, in turn, undermines the goals and mission of the organization.
2. **Principle 2: Computer Security is an Integral Element of Sound Management**
   A sign of strong organization management is when the business secures itself from cyber attacks. Ignoring computer security is an organization's big mistake.
3. **Principle 3: Computer Security Should Be Cost-Effective**
   Every business has its own needs. It can't protect itself from all possible attacks, so it must decide which threats should have the highest focus priority and address them within the budget limits. The company should purchase a security system only if its benefits supersede, or at least equal, the costs of its purchase and implementation.

8 Fundamental Principles of Information Security

4. **Principle 4: Systems Owners Have Security Responsibilities Outside Their Own Organization**
   Since an organization serves private and commercial users, it should provide security to systems accessed from the outside by users, and not only to its own employees.
5. **Principle 5: Computer Security Responsibilities and Accountability Should Be Made Explicit**
   An organization should avoid hiding security incidents and should take responsibility for them, both to avoid loss of reputation from its customers and legal actions.
6. **Principle 6: Computer Security Requires a Comprehensive and Integrated Approach**
   To maximize efficiency, all the business's systems and related departments must work in perfect harmony.
7. **Principle 7: Computer Security Should Be Periodically Reassessed**
   Because technology changes rapidly, and because new flaws are discovered now and then, a company must re-think its security approaches from time to time and decide if any changes / updates should be applied.
8. **Principle 8: Computer Security is Constrained by Societal Factors**
   E.g.: tracking geolocation for security purposes may be limited by privacy laws, which the company must respect.

Any questions?

Key Terms & Principles in InfoSec: Sources

Rao, Umesh Hodeghatta, and Umesha Nayak. "Chapter 3: Key Concepts and Principles." *The InfoSec handbook: An introduction to information security.* Springer Nature, 2014, pp. 29-62. URL: https://link.springer.com/content/pdf/10.1007/978-1-4302-6383-8.pdf#chapter+3:+key+concepts+and+principles