

Information Security

Indra Tobing
STMIK Putera Batam

Information Security

Goal of Information Security class

To give us awareness of:

Existing serious threats of information system security

and

Knowledge of system vulnerabilities.

Information Security

Topics:

- People awareness;
- Recognize the various threats and its impact;
- Scrutiny the vulnerabilities of the objects, and;
- Security Key Aspects
- Learn how to cope with by examining the potential risk incorporated in the threats.

Earlier Issues

- Computer vandalism,
- Preserving the low operation temperature, and
- Maintaining the electricity.

Recent Issues

Recently, *Information security* flaws engage more complex problems, including:

- intruder attack;
- copyright infringement;
- privacy violation;
- natural disaster, and (even more extensive challenge);
- business continuity and disaster recovery plan.

What makes Information Security Different

Protecting information or computer, will be much different from protecting anything else.

Please observe this picture below.

© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com

What makes Information Security Different

They used moat to protect themselves. Why did they use such a security system?



What makes Information Security Different

A security system refers to:

What they fight for (the object they protect)

and

Who / what they prevent from (the threats).

What makes Information Security Different

What we are protecting now is a system contains information. As an object to protect, the information somehow, differs from tangible things in some manner.

What makes Information Security Different

What happen when it is	Tangible things	Information
stolen	It is notifiable, because it disappears.	No one aware, because nothing lessens
duplicated	The copied worth relatively cheaper than the original	The copied bring same value and price as the original
Dispersed widely and everyone has	Each still worth something and has price tag (minimum / least price)	It worth nothing. When everyone has it, it's not an information anymore.

Common Understanding

Information Security concerns mostly about;

- Ensuring that the information is protected along its life span;
- Maintaining 100% of data integrity, and;
- Protecting the computer operation against attacker, unintended human error, or natural disruption that could lead to malfunction or system fall down.

Other concerns are *access control*, *authenticity* and *non-repudiation*.

People Awareness

When an unprotected healthy PC is connected to the internet, how long will the PC can compromise before the first virus hits the PC ?

Do we realize that the first virus hits the “naked” PC, infects it, and abuses it to spread the disease to the internet in less than 60 seconds ?

So, what ??

What if one of These Happens

What can be worse than a leakage of customer data of a financial service ?

What will be the potential problem if your monthly spending is traceable by someone you don't even know ?

What if you are charged by your credit card provider for a pair of wedding ring you didn't buy ever ?

What can be more annoying than a jammed ticketing computer at the airport at day time?

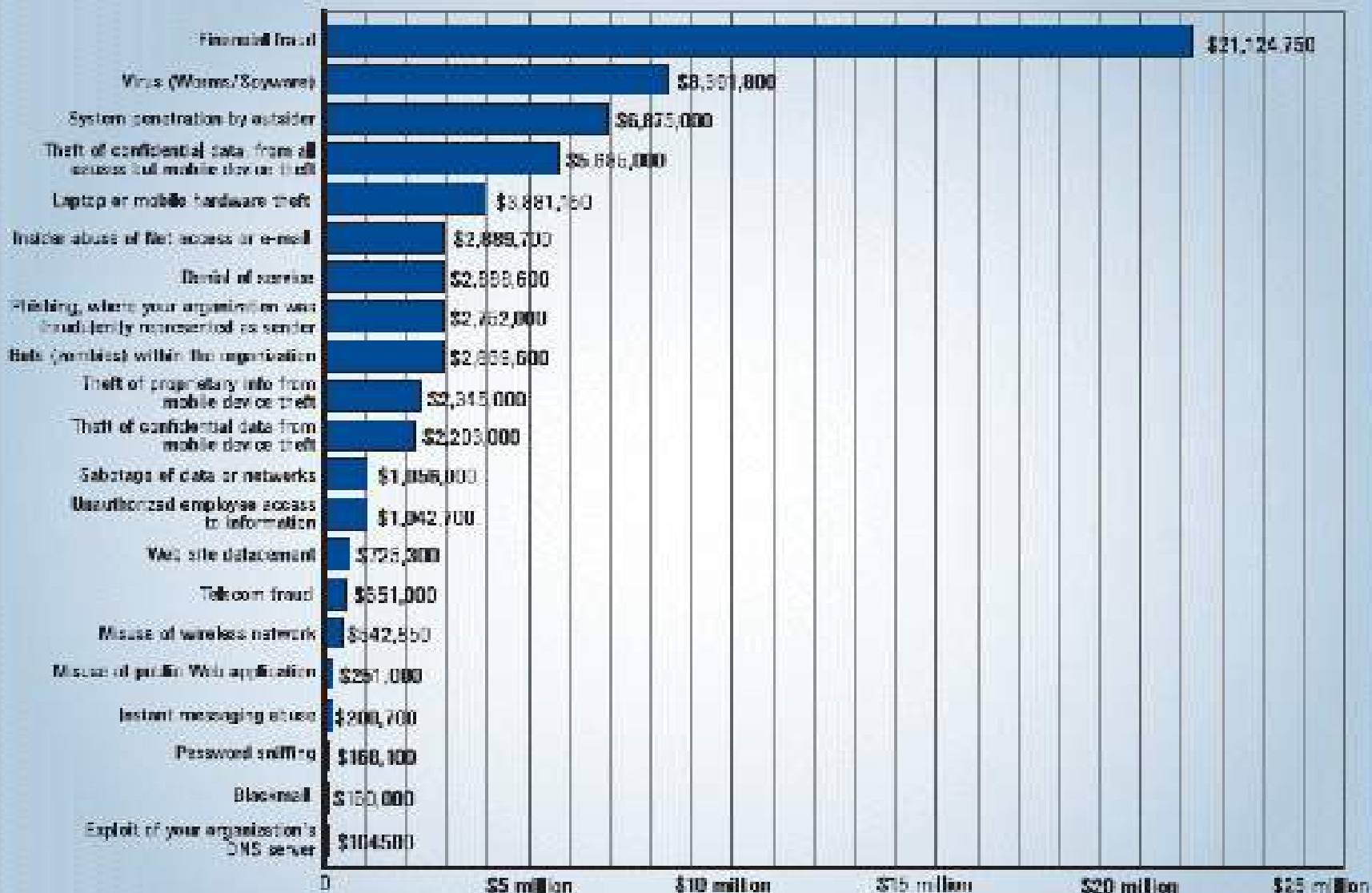
Recognize the Threats & Impacts

Name	Date	Impact
Morris Worm	'88	<ul style="list-style-type: none">• Stopped 10% of computers connected to Internet
Melissa Virus	May '99	<ul style="list-style-type: none">• 100,000 PCs in one week• \$1.5 billion impact
Explorer Virus	June '99	<ul style="list-style-type: none">• \$1.1 billion impact
Love Bug Virus (I Love You Virus)	May '00	<ul style="list-style-type: none">• \$8.75 billion impact

Recognize the Threats & Impacts

Name	Date	Impact
Sircam Virus	Jul '01	<ul style="list-style-type: none">• 2.3 million PCs infected• \$1.25 billion impact
Code Red Worm	Jul '01	<ul style="list-style-type: none">• 359,000 PCs infected in less than 14 hours• \$2.75 billion impact
Nimda Worm	Sep '01	<ul style="list-style-type: none">• 160,000 PCs infected at peak• \$1.5 billion impact
Klez	'02	<ul style="list-style-type: none">• \$750 million impact
BugBear	'02	<ul style="list-style-type: none">• \$500 million impact

Figure 16. Dollar Amount Losses by Type of Attack



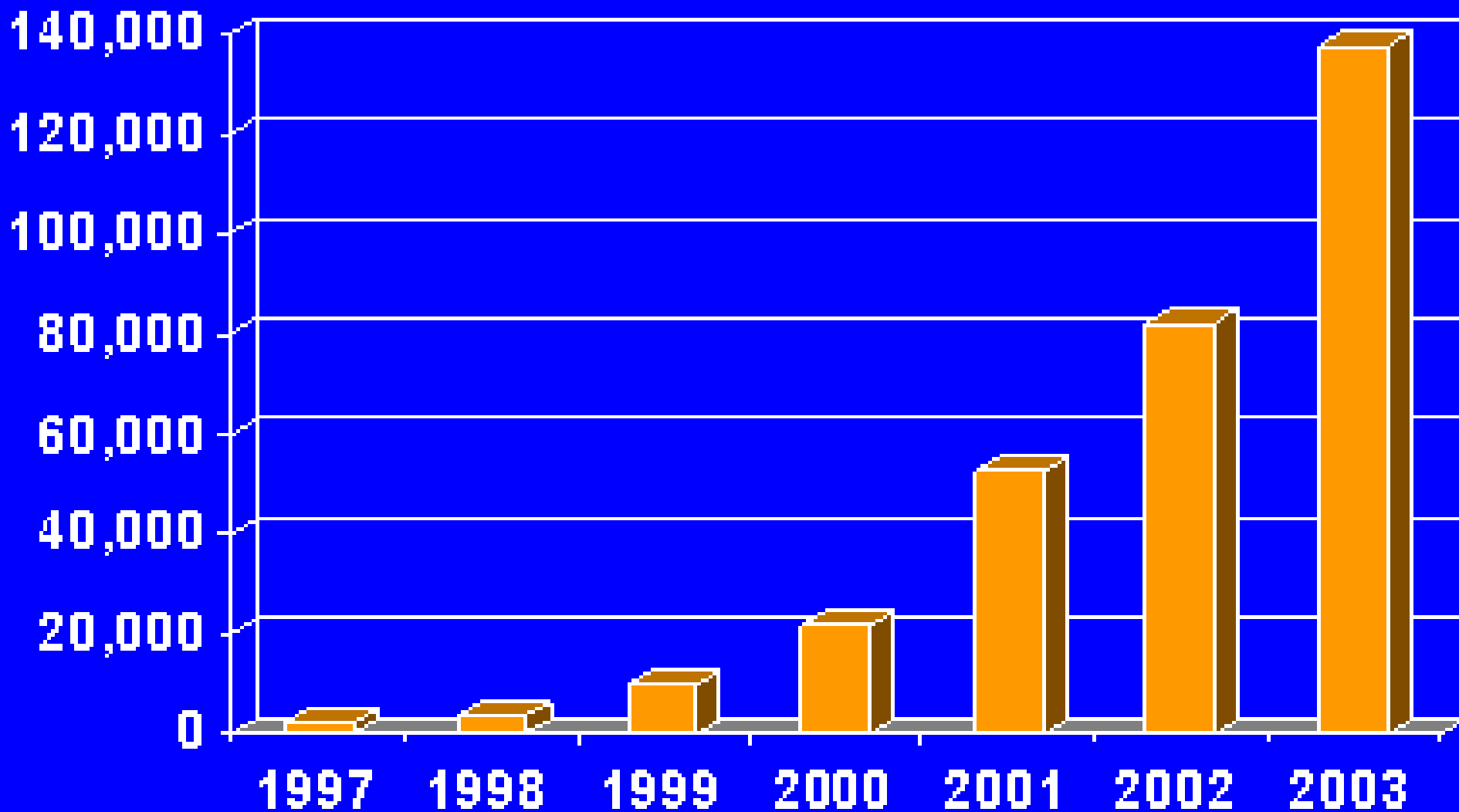
Total Losses for 2007 = \$66,930,950

(Numbers above do not equal total due to rounding.)

Do We Realize the Chance ?

What is the chance that things might happen to us ?

Reported Security Incidents / yr



Source: The Computer Emergency Response Team Coordination Center (CERT/CC)

Information Security Incidents

The Computer Emergency Response Team Coordination Center (CERT/CC) defines an incident as:

- unauthorized use of a computer system,
- an unwanted disruption of computer service, or
- changes to a system without the owner's knowledge.

Vulnerabilities

Recent PC is built of millions of transistors from numbers of manufacturers.

Inside, the software has hundreds of millions of lines of codes, hundreds of thousands of files and countless applications.

Chance has only to find a tiny inaccuracy “aperture” to jeopardize a whole complex costly system.

Vulnerabilities

In computer security, the term **vulnerability** is applied to a weakness in a system which allows an attacker to violate the integrity of that system. Vulnerabilities may result from weak passwords, software bugs, a computer virus or other malware, a script code injection, a SQL injection or misconfiguration.

A security risk is classified as a vulnerability if it is recognized as a possible means of attack.

Vulnerabilities, the causes

1. Password management flaws
2. Fundamental operating system design flaws
3. Software bugs
4. Unchecked user input

Vulnerabilities, the causes

1. Password management flaws:

The computer user uses weak passwords that could be discovered by brute force. The computer user stores the password on the computer where a program can access it. Users re-use passwords between many programs and websites.

Vulnerabilities, the causes

2. Fundamental operating system design flaws:

The operating system designer chooses to enforce sub optimal policies on user/program management. For example operating systems with policies such as default permit grant every program and every user full access to the entire computer. This operating system flaw allows viruses and malware to execute commands on behalf of the administrator.

Vulnerabilities, the causes

3. Software bugs:

The programmer leaves an exploitable bug in a software program. The software bug may allow an attacker to misuse an application.

Vulnerabilities, the causes

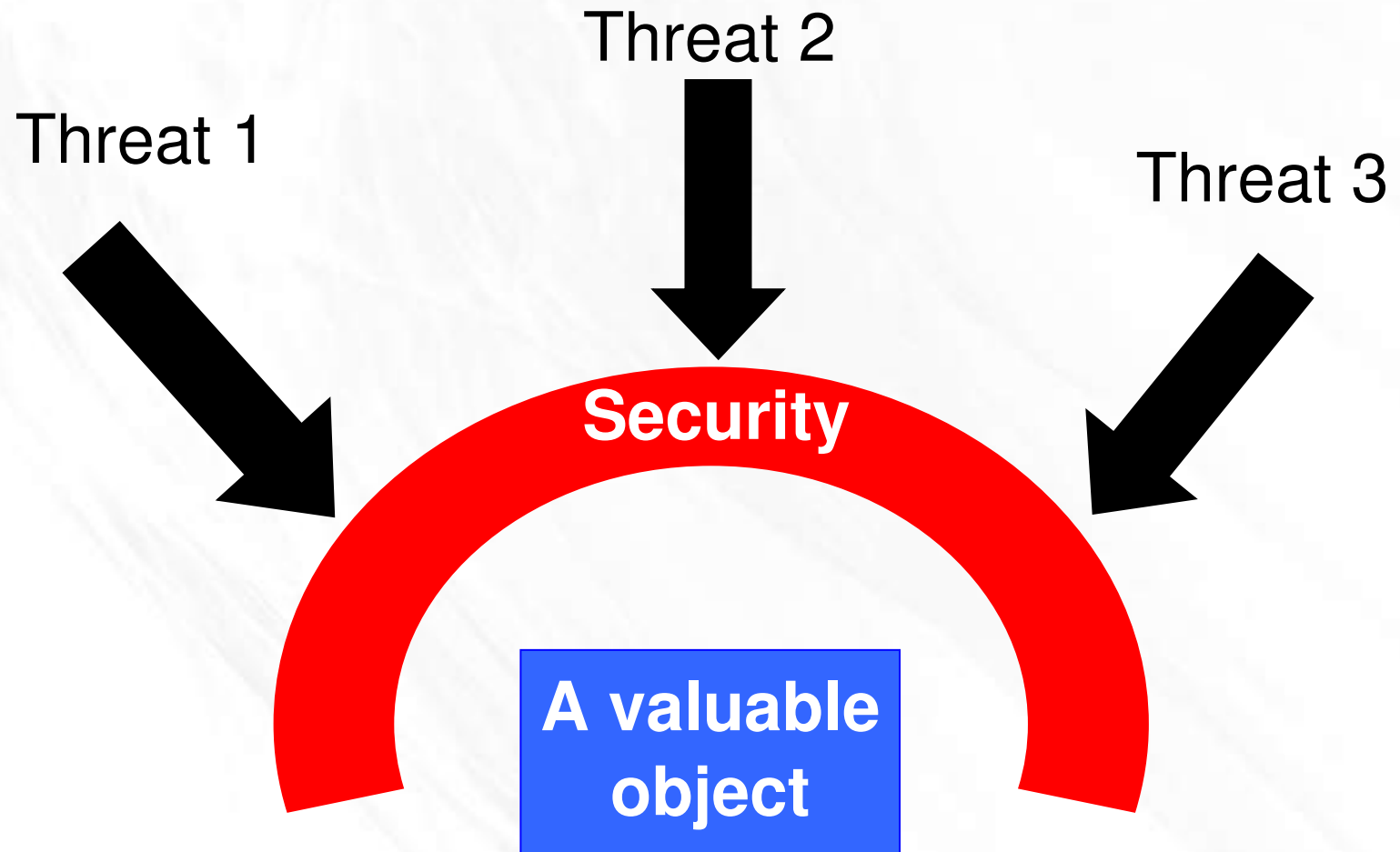
4. Unchecked user input:

The program assumes that all user input is safe. Programs that do not check user input can allow unintended direct execution of commands or SQL statements (known as Buffer overflows, SQL injection or other non-validated inputs).

The Vulnerabilities

When we have a valuable object, it is natural, that threats could emerge in its surrounding. The threats will apparently rummage around for any possible potential vulnerability system of the object to burglarize it. Such threats could possibly harm our valuable object. Security action will consequently be required, and it will take place in between, just as a shield.

The Vulnerabilities



The Vulnerabilities

As security is a shield placed between an object and its threats, each security system naturally has its adapted form and structure which compromises with the object and its progressive threats.

So, as it is apparent, security and threats constantly evolves in order to compete against each other

The Vulnerabilities

The “toughness” of the shield is mostly depends on at least two factors;

- 1.How harmful the risk (of the threat) will be, for not taking any security action, and
- 2.How much the security action and/or tools will cost.

1. How harmful the risk of the threat, for not taking any security action

There are 3 aspects:

Confidentiality

Information has potential lost of its secrecy by intruder threats.

Ex.: Customer private data spilled

Integrity

Data may have potential problem of lost integrity by virus threats.

Availability and Reliability

System has potential problem of disruption by intruder, unintended human action and natural disaster threats.

2. How much the security action and/or tools will cost.

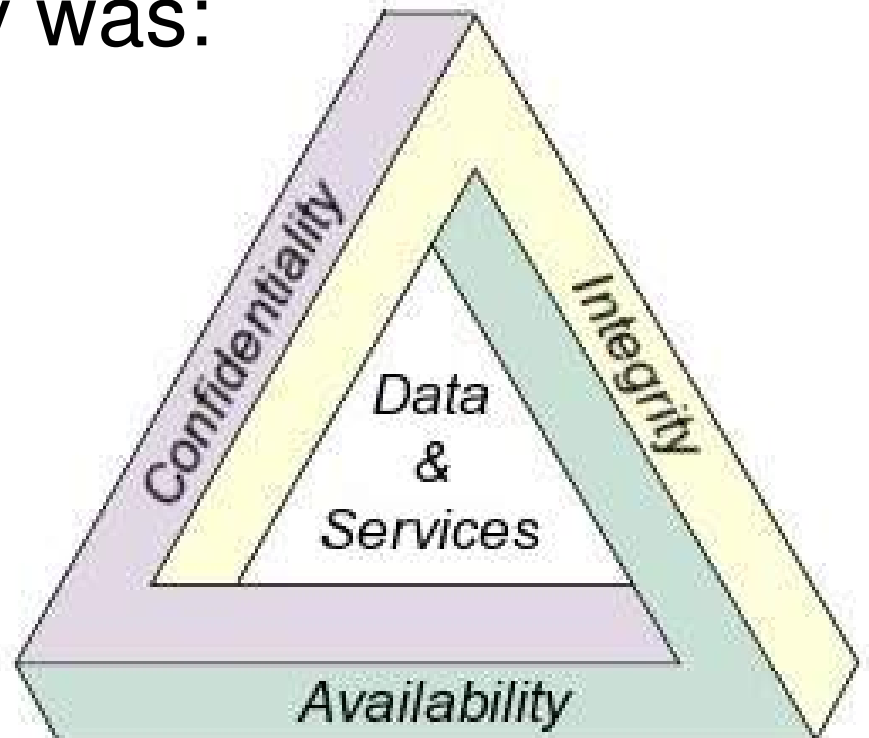
- Costs us money,
- Trades off our valuable expediency,
- Reduces our priceless freedom and
- Diminishes our precious privacy.

So the *Computer Security* is apparently not just updating anti-virus, having an expensive firewall, planting backup system and placing a UPS. Further, the *Computer Security* is analyzing threats and their risks and finding the equilibrium among safety, risk, convenience and privacy.

Security Key Aspects

A previous key concept of information security has been around for more than twenty years. It is called as **CIA Triad**, the three aspects of information security initially was:

- Confidentiality,
- Integrity, and
- Availability.



CIA Triad: Confidentiality

Information that is considered to be confidential in nature must only be **accessed, used, copied, or disclosed** by persons who have been authorized to access, use, copy, or disclose the information, and then only when there is a genuine need to access, use, copy or disclose the information.

CIA Triad: Confidentiality

A breach of confidentiality occurs when information that is considered to be confidential in nature has been, or may have been, accessed, used, copied, or disclosed to, or by, someone who was not authorized to have access to the information.

CIA Triad: Confidentiality

For example:

Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it would be a breach of confidentiality if they were not authorized to have the information.

If a laptop computer, which contains employment and benefit information about 100,000 employees, is stolen from a car (or is sold on eBay) could result in a breach of confidentiality because the information is now in the hands of someone who is not authorized to have it.

Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information.

CIA Triad: Integrity

The concept of integrity means that data can **not** be created, changed, or deleted without authorization. It also means that data stored in one part of a **database** system is in agreement with other related data stored in another part of the database system (or another system).

CIA Triad: Integrity

For example:

A loss of integrity can occur when a database system is not properly shut down before maintenance is performed or the database server suddenly loses electrical power.

A loss of integrity occurs when an employee accidentally, or with malicious intent, deletes important data files.

A loss of integrity can occur if a computer virus is released onto the computer.

A loss of integrity can occur when an on-line shopper is able to change the price of the product they are purchasing.

CIA Triad: Availability

The concept of availability means that the information, the computing systems used to process the information, and the security controls used to protect the information are all available and functioning correctly when the information is needed.

CIA Triad: Availability

For example:

An attack of availability may result in a denial of service (DOS).

Other aspects has been added to this CIA Triad concept recently, they are;

1. Access Control,
2. Authenticity, and
3. Non Repudiation.

1. Access Control

The concept of access control means that the computer system **can and only be accessed by authorized persons.**

An access control is a mechanism, built to regulate a physical and software access to critical and sensitive resources of information system. This includes the authentication and authorization practices of the entry right. For entry barrier, the access control may incorporate tools such encryption, password, digital signatures, metal locks, biometric scan, surveillance cam and more coming yet.

1. Access Control

To share the responsibility of this task among management, the mechanism is constructed in a written procedure. This is also to impel the access control to become the standard procedure. As the responsibility is shared, the **access control** is built as a trilogy;

- **Administrative / Procedure control;**
- **Logical / Technical control;** and
- **Physical control.**

1. Access Control

Administrative control,

is an official procedure that regulates human or non-human access to all predefined computer and information system facilities. This procedure is approved by management, often is like a white book company. The procedure depicts the **technical (or logical) control** and the **physical control**, which is technically conducted by IT team.

1. Access Control

Logical or technical control,

uses software or application programs to guard and limit the access of unauthorized person to the computer system.

For example: password, finger print, firewall, network intrusion detection system, data encryption and access control lists. Any access that is awarded to individuals or programs through **logical / technical control**, should have **principle of least privilege**. The principle means that the access should not unlimited in time or period. Example: A contract employee should be awarded the access only as long as contract period; there are some facilities that could only be accessed in working hour.

1. Access Control

Physical control,

is explicitly understandable. At the minimum level, security system naturally uses **physical control**. It uses physical things to protect the perimeter. Such as doors and chain locks, smoke detection and fire alarms, camera, even security guards.

2. Authentication

While the **access control** holds the unauthorized access off, and allows the access right owner to enter the resource, the **authentication** is a method of verifying that the one who owns the access right is truly the one he / she claims to be.

3. Non-Repudiation

A condition that protects a circumstance, against denial of receiving (by receiver) or sending (by the sender) of some information across a communication line.

Social Engineering in Information Security

A very good, multi layered, and expensive security system means nothing without a proper person behind the gun.

AWARENESS:

the key to avoiding social engineering



Social Engineering in Information Security

It doesn't matter how strong and expensive your security system is, the attacker only needs to find a little tinny "hole" to melt the robust computer security system.

An unaware and untrained employee could naturally be the weakest chains of the security system, and could spill sensitive information. This employee will potentially become the target of the attacker.

Social Engineering in Information Security

Social engineering is a method of manipulating circumstance to get unauthorized access without technical effort, instead by socializing with the man behind the gun, and then influencing him.

Social engineering is about inducing someone who owns an authorized access to relief it for certain purpose. This inducing technique approaches the target through *familiarity, sympathy, Comfort and Trust.*

Example of social engineering case to get an unauthoriz

▪