What is Information Security?

DEFINING INFORMATION SECURITY

Before we continue on our security mission, you must know what information security is. You must know the terminology and you must know why it is critically important today.

In a nutshell, security is to protect oneself from harm.   Information security is also to protect oneself from harm, the only differences is the harm that we are trying to prevent comes in a digital format vs. a physical or verbal format. It is the digital format that computers and networks speak. This is called data and is what we must protect, hence the term Information Security.

THE **CIA** TRIANGLE

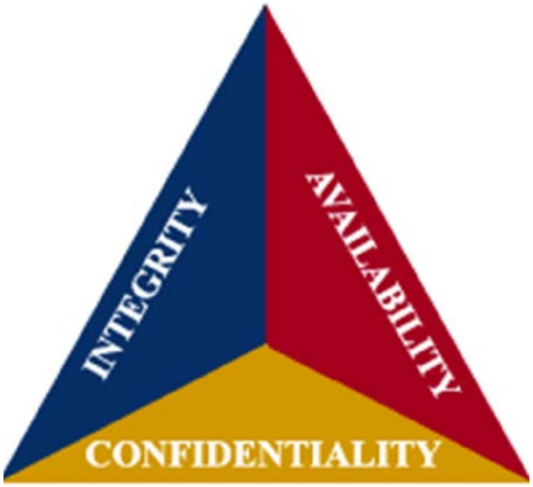
In a more granular sense, Information Security has three unique characteristics that have to be protected and will be the focus of this course, they include: **Confidentiality**, **Integrity** and **Availability** (CIA). Review the definitions of these three characteristics on the following page.

Integrity:

When digital information is allowed to be kept intact and not disturbed by unauthorized people or malicious software then the integrity of the information has been protected.

Availability:

Information certainly has to be secure, but it also has to be immediately available to you when you need it, if you have authorization to use it.



Confidentiality:

When a select group of people, which could be just you, are the only ones given authorization to view information, then the confidentiality of the information must be protected.

SUPPORT SYSTEMS

With the protection of information, the protection of support systems must also be included. These include the following major support system components:

Communication Systems

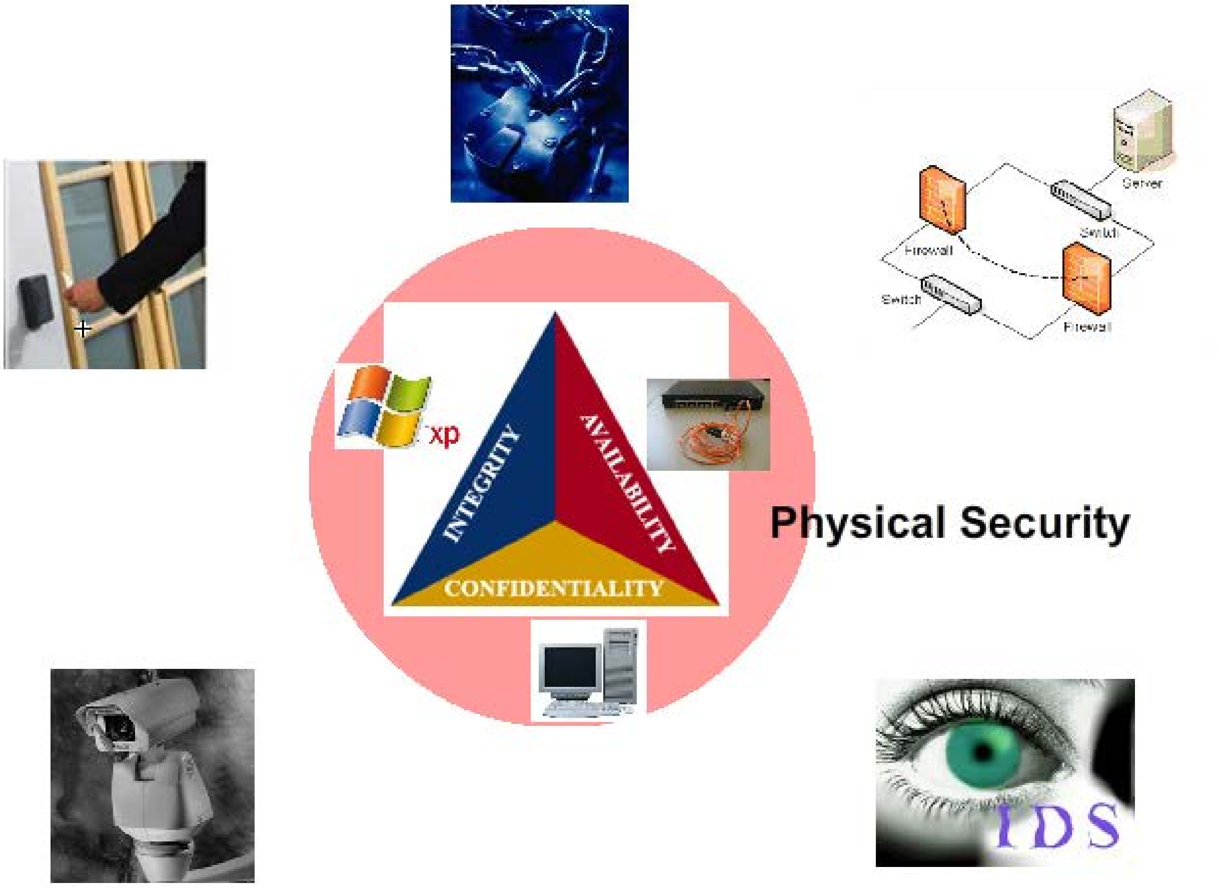
Operating Systems

Computer Systems

LAYERED PROTECTION

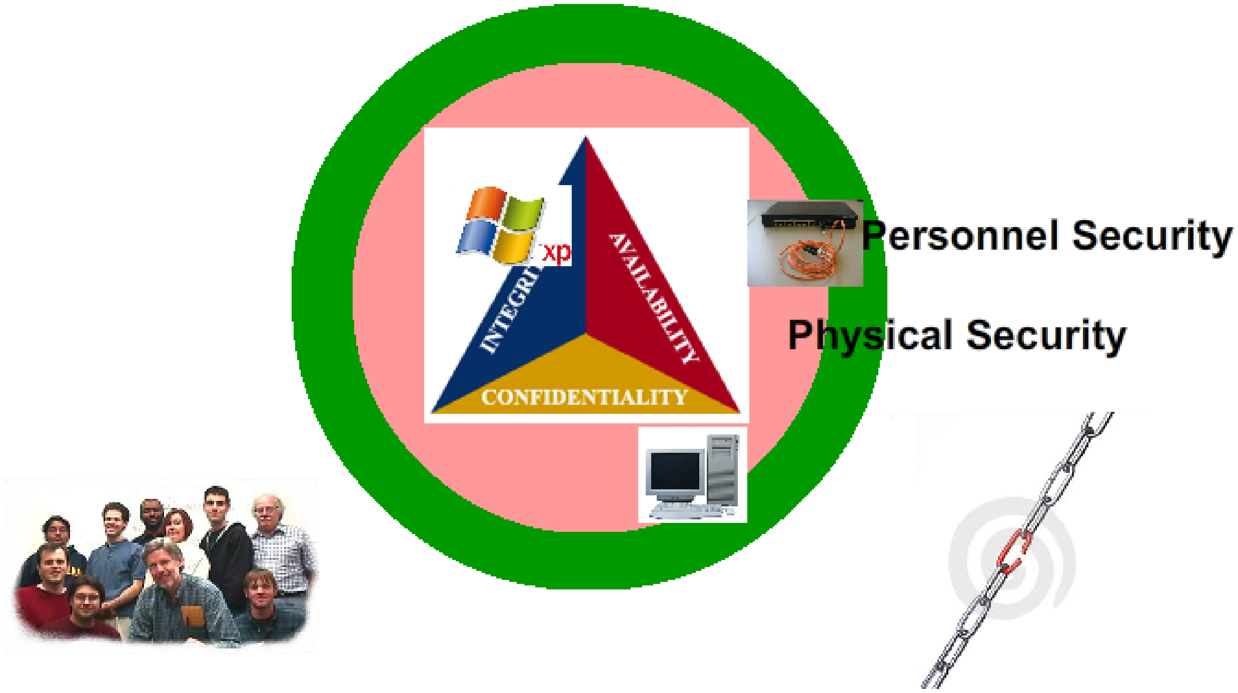
PHYSICAL SECURITY

Information and the hardware and software that support it are what is protected. The protection comes in multiple layers. The inner most layer is **physical security**. This includes door locks, surveillance cameras, intrusion detection systems, firewalls, and such.
See image below.



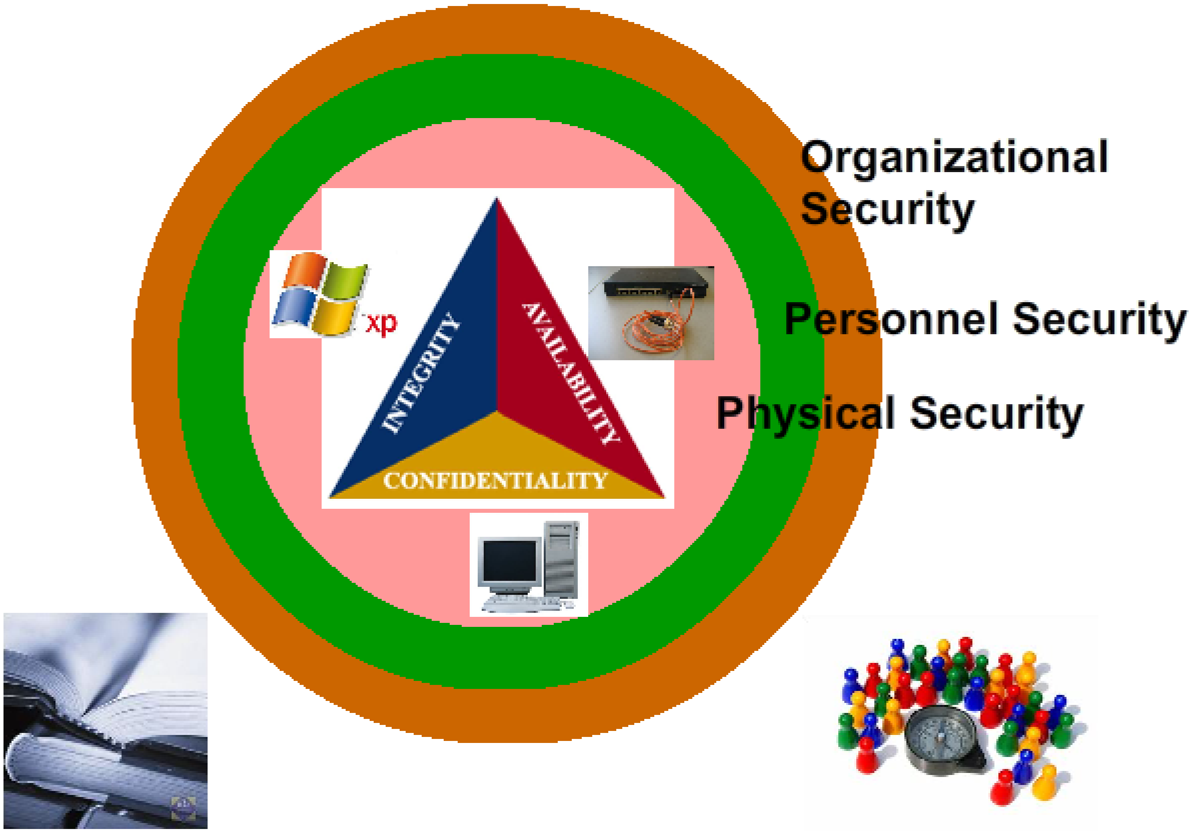
PERSONNEL SECURITY

The next layer is **personnel security** – this of course deals with people. People must use the proper tools and techniques and follow corporate guidelines regarding security; otherwise absolutely NOTHING can be kept secure. It is said time and time again that this layer is the weakest of all the protection layers. See image below.



ORGANIZATIONAL LAYER

The last layer is the **organizational layer** – this is the layer where the policies and procedures are located. This is the layer that essentially guides the personnel security layer, and it is the personnel layer that implements the physical layer. You can see that these are all connected and interact. Securing the center requires that all three layers are implemented consistently and correctly. See image below.



INFORMATION SECURITY TERMINOLOGY

This tutorial has already given you some terms that are likely new to you. There are terms, however, that are very commonly referred to when discussing information security. These are defined in user-friendly terms below.

ASSET AND RISK

Let's assume that one day I park my car in the parking lot. I purposely leave my laptop in the car and lock the car; however, I forget to close my window before I walk off to my office.   In this scenario I just defined both an **asset** and a **risk**.   See the images below.

Asset (with open window - vulnerability)

Risk - of losing both my car and my laptop. I have insurance, so some of the risk is transerred to my insurance agent.

Asset - something I want protected, so I lock it up in my car.

THREAT AGENT

That day a man dressed like a thief (maybe that's because he was one) approached my car. This man is a **threat agent**.   He has the power and potential to steal my assets from me if he so chooses. See image below.

VULNERABILITY

Normally, the parking lot is very secure, however, that day the parking lot security man was sleeping. This sleeping man created a **vulnerability** or weakness in the security of the parking lot that will allow the threat agent (the man looking like a thief) to bypass security and rip me off. See image below.

Vulnerability in the security of the parking lot.
+
Threat Agent
Assets

EXPLOIT

Well, the man that looked like a thief actually became one. He chose to steal my laptop by **exploiting** the security weakness (vulnerability). Fortunately, he did not steal my car. See image below.

Exploit

IMPORTANCE OF INFORMATION SECURITY

It is important to everyone...

- To prevent data theft
- To protect your identity.
- To avoid the legal consequences of not securing information.
- To maintain productivity.
- To foil cyber terrorism.

Mission
/mi-shun/
def: A task or purpose that needs to be carried out by a group of people or the people who are given the task.

Mission Assignment: MP1-2

Type: Group - Blackboard Discussion Board Forum: **MP1-2: Importance of Information Security**
Resource: Internet, personal experience, assigned reading.

Description:

Businesses and individuals are at risk of losing (in total) billions of dollars due to losses created because of breaches to data and personal information, illegal use of information, and loss of productivity.

This group assignment will require that you define one of the areas of importance as listed above, some suggested discussion points will be detailed in the discussion board.