Fundamentals of Information Security Series

C836

Instructor: Arthur Moore

Event time: Every Thursday at 6:00PM MST

# Instructor intro

- Contact info: Arthur.Moore@wgu.edu
- Number: 1-877-435-7948 Ext. 1554
- Office Hours:
- Monday: 8AM-5PM
- Tuesday: 8AM-5PM
- Wednesday: 8AM-5PM
- Thursday: 8AM-12PM AND 7PM-10PM
- Sunday: 6PM-10PM

# As a reminder

- This web series is only to enhance/supplement the course material not to replace it please follow the guidelines as posted below.
- ***It's Highly recommended that you Don't schedule the first assessment until all the materials are covered***.
- -take the preassessment until constantly passing
- -review lessons 1-14 readings (pay close attention to chapters 1 – 6.)
- -complete lessons 1-14 quizzes.
- -complete lessons 1-14 exercises (pay close attention to chapters 1 – 6)
- -watch the videos that are posted in the course tips
- -go over the PowerPoints that are posted in the course tips

# Physical Security

- Physical security is largely concerned with the protection of three main categories of assets: people, equipment, and data. Our primary concern, of course, is to protect people. People are considerably more difficult to replace than equipment or data, particularly when they are experienced in their particular field and are familiar with the processes and tasks they perform.
- In short with no physical security there is no security.



# DRP/BCP Physical Security Threats

- In many larger organizations, protection of people, data, and equipment is covered under a set of policies and procedures collectively referred to as business continuity planning (BCP) and disaster recovery planning (DRP), often referred to as one entity called BCP/DRP. BCP refers specifically to the plans we put in place to ensure that critical business functions can continue operations through the state of emergency. DRP covers the plans we put in place in preparation for a potential disaster, and what exactly we will do during and after a particular disaster strikes to replace infrastructure.
- **Major categories of physical threats**
  - Extreme temperature
  - Gases
  - Liquids
  - Living organisms
  - Projectiles
  - Movement
  - Energy anomalies
  - People
  - Toxins
  - Smoke and fire



# Physical Security Controls

- Physical security controls are the devices, systems, people, and other methods we put in place to ensure our security in a physical sense. There are three main types of physical controls **deterrent**, **detective**, and **preventive**.
- **Deterrent:** controls are designed to discourage those who might seek to violate our security controls from doing so, whether the threat is external or internal.
- **Detective:** controls serve to detect and report undesirable events that are taking place. The classic example of a detective control can be found in burglar alarms and physical intrusion detection systems.
- **Preventive:** controls are used to physically prevent unauthorized entities from breaching our physical security. An excellent example of preventive security can be found in the simple mechanical lock.

# Protecting People

- The primary concern of physical security is to protect the individuals on which our business depends and those that are close to us.
- **Physical Concerns for People**: As people are rather fragile in comparison to equipment, they can be susceptible to nearly the entire scope of threats we discussed at the beginning of this lesson.
- **Safety**: the safety of people is the first and foremost concern on our list when we plan for physical security.
- **Evacuation**: Evacuation is one of the best methods we can use to keep our people safe. In almost any dangerous situation, an orderly evacuation away from the source of danger is the best thing we can do. There are a few main principles to consider when planning an evacuation: where, how, and who.
  - **Where**: Whether we are evacuating a commercial building or a residence. We need to get everyone to a rally point to ensure that they are at a safe distance and that we can account for everyone.
  - **How**: When planning such routes, we should consider where the nearest exit from a given area can be reached, as well as alternate routes if some routes are impassable in an emergency. We should also avoid the use of areas that are dangerous or unusable in emergencies, such as elevators or areas that might be blocked by automatically closing fire doors.
  - **Who**: The most vital portion of the evacuation, of course, is to ensure that we actually get everyone out of the building, and that we can account for everyone at the evacuation meeting place. This process typically requires at least two people to be responsible for any given group of people: one person to ensure that everyone he or she is responsible for has actually left the building and another at the meeting place to ensure that everyone has arrived safely.
  - **Practice**: Particularly in large facilities, a full evacuation can be a complicated prospect. Practice to pervent injury or loss of life.

# Protecting Data

- **Physical Concerns for Data**: depending on the type of physical media on which our data is stored, any number of adverse physical conditions may be problematic or harmful to their integrity. Such media are often sensitive to temperature, humidity, magnetic fields, electricity, impact, and more, with each type of media having its particular strong and weak points.
- **Availability**: one of our larger concerns when we discuss protecting data is to ensure that the data is available to us when we need to access it. The availability of our data often hinges on both our equipment and our facilities remaining in functioning condition, as we discussed earlier, and the media on which our data is stored being in working condition.
- **Residual Data**: when we look at the idea of keeping data safe, we not only need to have the data available when we need access to it, but we also must be able to render the data inaccessible when it is no longer required.
- **Backups**: In order to ensure that we can maintain the availability of our data, we will likely want to maintain backups. Not only do we need to back up the data itself, but we also need to maintain backups of the equipment and infrastructure that are used to provide access to the data.
- **Raid**: We can utilize redundant arrays of inexpensive disks (RAID) in a variety of configurations to ensure that we do not lose data from hardware failures in individual disks, we can replicate data from one machine to another over a network, or we can make copies of data onto backup storage media, such as DVDs or magnetic tapes.

# Protecting Equipment

- **Physical Concerns for Equipment**: The physical threats that might harm our equipment, although fewer than those we might find harmful to people, are still numerous.
  - •Extreme temperatures can be very harmful to equipment.
  - •Liquids can be very harmful to equipment, even when in quantities as small as those that can be found in humid air.
  - •Living organisms can also be harmful to equipment, although in the environments with which we will typically be concerned, these will often be of the smaller persuasion. Insects and small animals that have gained access to our equipment may cause electrical shorts, interfere with cooling fans, chew on wiring, and generally wreak havoc.

# Environmental Conditions

- **Debugging**: The term ***bug*** being used to indicate a problem in a computer system originated in September 1947. In this case, a system being tested was found to have a moth shorting two connections together and causing the system to malfunction. When the moth was removed, the system was described as having been debugged.
- **Site Selection**: When we are planning a new facility, or selecting a new location to which to move, we should be aware of the area in which the facility will be located. A number of factors could cause us issues in terms of protecting our equipment and may impact the safety of our people and data as well. If the site is located in an area prone to natural disasters such as floods, storms, tornadoes, mudslides, or similar issues, we may find our facility to be completely unusable or destroyed at some point.
- **Securing Access**: When we discuss securing access to our equipment or our facility, we return again to the concept of defense in depth. There are multiple areas, inside and outside, where we may want to place a variety of security measures, depending on the environment.
- **Environmental Conditions:** For the equipment within our facilities, maintaining proper environmental conditions can be crucial to continued operations. Computing equipment can be very sensitive to changes in power, temperature, and humidity, as well as electromagnetic disturbances. Particularly in areas where we have large quantities of equipment, such as we might find in a data center, maintaining the proper conditions can be challenging, to say the least.