# Transcript: IT Podcast - Ep 112 - C836 Lesson 9 - with Arthur Moore and Jessica Galterio

*The following transcript is a verbatim account of the video or audio file accompanying this transcript.*

Speaker # 1: Arthur Moore

WGU IT audio series; flexible, portable, profound.

Hey, this is Arthur with WGU. I'm one of the course instructors for C836, fundamentals of information security. Just as a quick note, this series is there to enhance the learning material, not meant to replace it. Let's go on ahead and jump into Chapter 9. Physical security. Physical security is largely concerned with the protection of three main categories: people, equipment, and data.

Our primary concern, of course, is always to protect people. People are considerably more difficult to replace than equipment or data, particularly when they are experienced in a particular field and they are familiar with the process and task that they perform. In short, with no physical security, there is no security.

Disaster recovery, business continuity planning, and physical security threats. In many larger organizations, protection of people, data, and equipment is covered under a specific set of policies and procedures collectively referred to as business continuity planning and disaster recovery planning. Often referred to as one entity, BCP, DRP. Business continuity planning refers to specifically the plans we put in place to ensure that the critical business functions, keyword, critical business functions, can continue operations through the state of emergency. Disaster recovery and planning covers the plans that we put in place in preparation for a potential disaster and what exactly we do during and after particular disaster strikes to replace infrastructure.

The way I like to remember it is business continuity planning is a subset of the disaster recovery planning. Major categories are physical threats, extreme temperature, gases, liquids, living organisms, projectiles, movement, energy anomalies, people, toxins, smoke, and fire.

Physical security controls. Physical security controls are 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 security controls. They are deterrents, 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 internal or external. Detective controls serve as a way to detect and report undesirable events that are taking place. Preventive controls are used to physically prevent unauthorized entities from breaking into our physical security.

Protecting people. The primary concern of physical security is to protect the individuals in our business. Physical concerns for people. People are relatively fragile in comparison to equipment, so they are susceptible to the entire scope of threats that 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 is one of the best methods that we can use to keep our people safe and almost any dangerous situation and orderly evacuation away from the source of danger is the best thing that we can do. There are a few principles in order to consider when we're doing an evacuation: where, how, who, and practice. Where. Whether or not we are evacuating from a commercial building or residence, we need to make sure that there's a rally point to ensure that we are at a safe distance and everyone is accounted for. How. Make sure we have planned routes to the nearest exit. Who is a vital importance to an evacuation. We need to make sure everyone is out of the building, and we need to make sure that we have an account for everyone, at least two people are responsible for the group; one to ensure that he or she is responsible that nobody is left in the building and the other one to make sure that everybody has arrived safely. Practice. You have to practice so that way in an event of a disaster an evacuation can go smoothly.

Protecting data. Physical concerns for data. Depending on the type of physical media on which our data is stored on, there can be any number of adverse physical conditions that might be problematic to the integrity. Availability. One of our larger concerns that we discuss when protecting data is, as the data format gets older, it often hinges on our equipment and our facilities being in the right condition and making sure that it is available. Residual data is data that is leftover or rendered inaccessible after a time being. For example, when you delete data. When you delete a particular file, it might be overwritten a certain amount of times in the future, but there's still residual data that's left.

Backups are in order to ensure that we maintain the highest level of availability in our data. We like to maintain backups and just making sure that's where we actually backup our data and store it, hopefully, offsite in another facility so that way if disaster strikes our facility, we are still able to get to our backups and restore from them. RAID is a redundant array of inexpensive disks, that's what the course material calls it, but it can also be a redundant array of inline disk. But the point of RAID is we are making sure that we have more than one hard drive, so that way, if we have a hard drive that fails on our devices, the other disk that are a part of that RAID will pick up until you can get that drive repaired.

You're not in a state of where the equipment isn't usable because of the disk being down or faulty at that point.

Protecting equipment. Physical concerns for equipment, physical threats that might harm our equipment are fewer than those that might harm people but are still numerous. Extreme temperatures, liquids, living organisms. Funny story, living organisms are very true, I have worked in the field for many years and I have come across many pest inside of a PC or server that I was working on and one instance comes to mind in particular, where there was a PC that was overheating and come to find out a baby snake, again, into the cooling fan of the PC and had become stuck and died and the corpse of the little snake was actually preventing the fan from turning and the PC started to overheat. That is a real-world example of how living organisms can actually damage your equipment.

Environmental conditions. The term debugging actually comes from when a bug was actually on a computer system, in September 1947, it was actually a moth and it was shorting out the circuits on the mainframe. The technician just said, I am debugging the system and it has always been a part of the IT community ever since. A couple of more environmental conditions that you might want to think of when selecting your site is where your site is, how secure the access is for your site and other environmental conditions. I want to pick on my state of South Carolina. It is a humid subtropical environment, so we do have several hurricanes and we have high humidity. You can pick any particular area in South Carolina, there's most likely a lot of land that we have, so that would be a plus for the site selection here. Securing access, you could build it away from the city so you wouldn't need to worry as much of foot traffic when you're securing access for your facility.

Environmental conditions would be the negative depending on where you are located in the state. You might only have one or two Internet service providers and power providers and so on and so forth, so you wouldn't have a great deal of redundancy when it comes to that. Then we go back to those environmental factors as well as the humidity. You're going to spend more dehumidifying the air in this particular state than you would in, let's say, a more dryer state. Let's go out with maybe California, where you would actually have to do the exact opposite and actually add humidity to the air to keep it in between that range. With all that, I bring our physical security conversation to a close. This has been Arthur Moore. You have a wonderful day.

Schedule time with your course instructor to explore more deeply. WGU, a new kind of you.