# Transcript: IT Podcast - Ep 104 - C836 Lesson 1 - 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's IT audio series, flexible, portable, profound.

Hey, this is Arthur Moore, one of the CIs for C836 fundamentals of information security, and this is Lesson 1. Just a note that this is meant to supplement the material for the course and not meant to replace it. Let's get to it. It's highly recommended that you do not schedule your first assessment until all materials are covered. Take the pre-assessment, review Lessons 1 through 12, pay a close attention through Chapters 1 through 6, complete Lessons 1 through 12 flashcards, paying close attention again through Lessons 1 through 6. Complete Lessons 1 through 12 quizzes and tests mode and learn mode, scoring 100 percent and paying close attention again to Chapters 1 through 6.

What is information security? Is it a state of data? Is it an action that the organization needs to take? Or is it industry best practices against unknowned and unnamed threats? The answer is D, all of the above, no device is ever truly 100 percent secure. The only device that is completely secure is off, unused, locked away in a vault somewhere, and even then there are speculations of how secure it is, but it offers no value to the organization. We as security professionals have to be willing to work with production and not stand in the way of production. Information security is keeping data, software and hardware secure against unauthorized access use, disclosure, disruption, modification, or destruction. What's worth protecting? Every business has assets both tangible and intangible.

Hardware, software, data, people. Now I wanted to pick on Jim, but this could be insert hard to deal with co-worker here. That hard to deal with coworker is more important than your software data, your security data, your hardware that runs all your servers. Because all of those items can be replaced, cloned, and purchased again, Jim, he is a living, breathing entity and is invaluable to the organization because of the experience and knowledge that he brings with him, as it should always be protected by value to its organization and the most important order, people, data, hardware, software. Compliance. Compliance is a term that's thrown around very often in the IT set community. Compliance represents the laws that are set forth and industry regulations that are example HIPAA, HITECH, PCI, DSS, FISMA. I want to also add with compliance, that compliance is the bare minimum. Compliance does not equal secure security models. What is the CIA triad? It does not stand for the Central Intelligence Agency. The CIA triad is the core model of all information security. The CIA is confidentiality, integrity, and availability.

Confidentiality is only allowing those who are authorized to access the data requested, integrity is keeping the data unaltered by accidental or malicious intent, and availability is the data being ready to access when needed. The next security model we're going to talk about is the Parkerian hexad. Interesting on how to pronounced that. Less or no models is a less or no model that includes the CIA triad and expands on it.

We have confidentiality, integrity, and availability here as well. Possession and control, authenticity and utility are the three additional sections that are added with the Parkerian hexad. Possession and control refers to where the physical disposition of the media in which the data is stored. Authenticity allows us to talk about the proper attribution, as to the owner or creator of the data in question and utility refers to how useful the data is to us. Attacks. When we're talking about different types of attacks, there are four different categories that we generally place attacks in. They are interception, interruption, modification and fabrication, and each one of them effects the CIA triad differently. Interception allows the attacker to intercept our data as it's in process, and it basically deals with an attack against confidentiality. Interruption is when there is a denial of service to our data or system on a temporary or permanent basis that can affect availability and integrity. Modification is the tampering with the asset that could also attack against integrity and availability.

Fabrication attacks involve generating, processing communications or other similar activities within a system that also attacks integrity and availability. Basically added these four types, interception is the only one that deals with confidentiality and interruption, modification and fabrication, all three of these deal with availability and integrity. Risk. Risk is the likelihood that an event will occur, and in order to occur, there have to be two pieces of risk. There are threats, vulnerabilities, and a third, depending on which framework you're using to evaluate risk is called impact. Threats are any events man-made, natural, environmental, that could cause damage to our assets. Vulnerabilities are internal weaknesses that a threat event or a threat agent can take advantage of.

Impact is that last step, and that's just taking into account the asset's cost. When we bring it all together, most people that drive have car insurance. Vulnerabilities are that when we have a car we might have an older car that has bad breaks. That's internal weakness, something that we can't control. A threat is it's been raining heavily. That's something that we can't control. A risk comes when these two are put together, we're out driving and it's been raining heavily, and let's say we run into something and now the car is totaled and we are at a loss of $10,000. This is the whole property of risk we have our vulnerability, weak brakes, we natural threat that it's raining heavy and the risk is when you put the two together. The impact is the $10,000, that is what the car is worth when it's been totaled.

Risk management is the constant process. As assets are used, purchase and retire, they must be assessed. Depending on your organization, it will depend upon how this process usually goes about, but there are generally six steps. You have to identify your assets, most important, and the first step, don't know what to protect if you don't know where it is. You have to identify the threats. Now we have to look at those outside event that could affect our assets.

We have to look at and assess the vulnerabilities, the internal weaknesses of those assets. We put those together, we get our risk and in order to help us mitigate our risk, we put countermeasures in place. These measures that alleviate risk are called controls. Controls are divided up into three categories: physical, logical slash technical, and administrative. How do we protect our assets?

We already discussed that there are controls that we can put in place and I believe the waivers are, I'll say them again, physical, technical, logical and administrative. Physical controls are think of a lock, a fence, a door, guards, dogs, guard dogs. Technical controls are those devices and software that used to protect our assets. Firewall, antivirus, IDS, IPS, DLP, data loss prevention. Administrative controls are policies that organizations create for governance. An example set for use policy and email policies, and I'm also going to throw out there privacy policies as well. Incident response. Incident response is what happens when risk mitigation practices or a risk management practices fail. In incident response have six steps as well.

We have the preparation phase, that is the phase that we're gathering together. Well, this might happen. This is the might phase, but we are planning for an incident to occur and we're preparing for it. Detection and analysis. This is where the action begins. This is where something is occurring. We don't know what it is, so we need to detect it and analyze it to properly put it in the right category. Is it an environmental event or is it an actual attack on our assets?

Containment is containing this issue to a certain area. Eradication is dealing with or removing all effects from our environment. Recovery is putting the environment back to a state prior to the incident, and post incident is post-mortem. This is usually overlooked and it's unfortunate because it's the lessons learned phase where we can go back and take a look at what we did right, what we did wrong, and we can actually build upon this and improve.

Last but not least, this is defense in depth. This happens when we put several of these different controls on top of one another to make it so that it's difficult for those on the outside or inside are trying to get at our assets. Remember our three types of controls, physical, logical, and administrative. We might have a lock on our server cabinets, and we might put several layers of authentication for our users, and we might have an acceptable user use policy, so that if there is an issue, we have these several overlapping layers. Again, I appreciate you stopping by and listening to this audio series on C836, fundamentals of information security, and with this, I would challenge you to contact your course instructors if you're having any issues within the course and apply these concepts to your daily lives and they will flow a lot easier.

Thank you very much, and have a nice day.

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