# Transcript: IT Podcast - Ep 107 - C836 Lesson 4 - 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.

Hello, this is Arthur with WGU. I'm one of the course instructors for C8 36 fundamentals of information security. This is Lesson 4, so let's go on ahead and jump into it. Just as a reminder, this series is meant to enhance the learning resources and not meant to replace them. It's highly recommended that you don't schedule the first assessment until all materials are covered. Take the pre-assessment review lessons 1 through 12.

Paying close attention to Chapters 1 through 6, you certify will read to you there is an invisible playback button on the left of the beginning of each section. Complete lessons 1 through 12 flashcards at a 100 percent. Again, paying close attention to Chapters 1 through 6 and complete all lessons 1 through 12. And test mode and Laura mode scoring 100 percent. Paying close attention to Chapters 1-6. Accountability.

Accountability provides us with the means to trace our activities within our environment back to the source. In addition, it provides us with a number of capabilities when properly implemented, which can be of great use in conducting the daily business of security information technologies of our organization. In particular organizations need to carefully maintain accountability in order to ensure that they are in compliance with any laws, regulations associated with the types of data that they handle or the industry that they operate in. Accountability depends on identification, authentication, access control being present. That way, we can know when a given transaction is associated, and what permissions were allowed to carry out this transaction. Repudiation, that turns an admissibility of records. Non-repudiation refers to a situation in which sufficient evidence exists that to prevent an individual from successfully denying that he or she made a statement or taken an action. Basically, what that means is you cannot deny it was you, user, Jim Bob that was sitting at the computer at 12:53 logged on, which are your unique credentials? Jim Bob, 1, 2, 3, 4. This email must have come from you if you were logged on at this time.

That is non-repudiation. The exact opposite of non-repudiation is repudiation, where basically you can have a username that is used by multiple people. You can't pin down who logged in at what time since it's shared across several different users. With that being said, this is why every organization needs to implement unique identifiers for each user.

Because if you have a user that can say, well, that wasn't me. Where's the accountability? How are the record showing that it was this user at that time? Deterrence. Accountability can also provide a great deal of deterrence against misbehavior in the environments. If we're monitoring the environment correctly and it's communicated to the users of the rules, they might think twice before it's straying away from set rules, which is true.

If you are know that you're being watched, you will always act accordingly. People are little different when you get them on camera. Miscibility or records. When we seek to include records in legal settings, it's often much easier to do so than having them accepted when they are produced from a regulated and consistent tracking system. Basically, what this is saying is, when you're trying to get records submitted in the court of law as evidence, it needs to be part of a daily cycle, regular day-to-day business operations. It can't be, we thought he was doing this, so we just decided to record him. Well, that's not going to work in the court of law. You have to have where the user has signed over their Fourth Amendment rights to the company stating that they have no privacy and they agree to not having any privacy by logging in and clicking on and submitting and going.

Because if that comes up in court where there wasn't a privacy policy in place, the evidence can be ruled is inadmissible. Which means they will basically be thrown out and not be considered along with the greater case.

Intrusion detection and intrusion prevention. Intrusion detection is where we monitor our networks, our facilities. We're looking for unusual activities in our day-to-day environments, both physical and biological. The difference between the two is that intrusion detection systems are those that just monitor and alert personnel when there is any event or some change has happened in our environment. Whereas intrusion prevention systems actually take action against the change.

For example, there is a lot of traffic coming from this IP address space out of Thailand. It hit a certain threshold for the amount of bandwidth that it's supposed to exceed being a new IP address. That's not normally done business with. So the IP, the intrusion prevention system says, ''we're going to shut down this particular IP address until somebody can take a look at this, we're going to deny all traffic coming to and from this IP address.'' Remember, Intrusion Detection Systems just notify and alert personnel that it takes no action. Intrusion prevention systems take action against the issue.

Auditing. One of the primary ways that we can ensure accountability through technical terms is by auditing records. When we perform our audit, there are a number of items that we can examine primarily focused on compliance with regulatory laws and industry environments. We can focus on the information security that we tend to look at on axis from our systems as a primary focus, but often extend to other fields such as physical activity.

For example, you might want to audit the amount of master keys for your physical environment. Who has master keys? How many are there? How long has that master key been held and actually go to that person and ask and say, do you still have this master key? This is a type of audit that we can do to make sure that we're keeping our physical environment safe. Technical audit would be along the terms of patching.

Do we have all our machines? Are they patched and up to date? Do we have the latest firmware on our devices? Things of this nature. Logging and monitoring. Logging and gives us a history of the activities that took place in the environment. Without this evidence, audits and investigations are not practical. It is the key to any organization to determine the correct level of logging to support its needs. You might not need to log everything.

You might just need to log particular items for high value datasets. Monitoring is a subset of auditing and tends to be observing all in information. Where else logging is more past hints and what's already happened. Monitoring is real-time and looking for those failures that are there. It's more reactive than actually going through the data.

Now, based off of this, we have assessments. Assessments are audit set, take a more active route depending on your laws, compliance, and regulations for it. There are really two types of assessments that we're going to discuss in this particular course. They're used interchangeably but that's not correct. We have vulnerability assessments, which are scanning tools such as nurses in map that actually go and probe that network and look for open ports and compare them against vulnerabilities with the particular protocols that have these open pores. Whereas a penetration test takes the vulnerability assessment one step further and starts to actually poke and prod at the weaknesses and see if we can actually turn the vulnerabilities against ourselves. Using them as if a bad actor would use though. This brings us to the end of this lesson. Have a nice day.

I appreciate you stopping by and listening to this audio series on C8 36, Fundamentals of Information Security. 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 U.