# Transcript: IT Podcast - Ep 110 - C836 Lesson 7 - 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 with WGU. I'm one of the course instructors for C836, Fundamentals of Information Security, and this is Lesson 7. Just as a reminder, this series is there to enhance the learning resources, not meant to replace the learning resources. Let's go ahead and jump into it. Operations security. Operations security is known in the military and government circles as OPSEC. At a high level, it is a process where we protect our information, although we have discussed certain elements of operation security previously such as these are encryption, and such measures only a small portion of the entire operations of the security process. While OPSEC may be relatively new term, the origins can be found in historical texts. Sun Tzu was a Chinese military general who lived in the sixth century BC.

Among those of the military strategy, Sun Tzu's work, The Art of War, is considered to be one of the foundational doctrines for conducting such operations. I have personally read Sun Tzu's Art of War. It is a great book. It's not only for the military or strategic mindset, you can apply the same principles that Sun Tzu was talking about directly into the operation security aspect of your professional workplace or your daily life.

The Art of War second passage. When making tactical dispositions, the highest pitch that you can attain is to conceal them. Conceal your dispositions, and you will be safe from prying of the subtlest of spies from the machinations of the wise's brain. This is a recommendation to very carefully protect our activities so that they do not leak to those that might oppose our efforts.

This was written in the sixth century BC, and it can still be applied to our networks today. Conceal data and keep it away from prying eyes. George Washington, first president of the US, was also well-known for being a student military commander. He also said that even minute should have a place in our collection for these things are of seemingly trifled nature when enjoyed with others of a more serious curse can lead to a valuable conclusion, meaning that small bits of information, whereas they might not seem valuable apart, can become very valuable when combined together. If you think of any tools that do this, the first thing that comes to my mind is a sim.

Whereas you can see the entirety of the network, and then you can slowly piece together small things in order to build a much larger picture of what's going on on your network. The operation security process, the OPSEC process, is laid out by the US government, but is very familiar for anybody who has worked with risk management. Always, and the most important step, is to identify critical information.

Once you have identified your critical information, analyze the threats that could possibly cause damage to that information, then analyze the vulnerabilities, the internal weaknesses that outside threats could exploit to get back at that critical information. Once you have a vulnerability and a threat together, you have a risk. You have to assist the risk, mitigate the vulnerability through the application of countermeasures. Countermeasures can also be labeled as controls. It's any item that can be used to lessen risk to a viable or lower risk appetite to an acceptable level. Kurtz Law of OPSEC.

A somewhat different and briefer viewpoint of the operations security is the laws of OPSEC by Kurt Hassle. Wow, he was employee for the Nevada operations office of the DOE. The first law, if you don't know the threat, how do you know what to protect? Second law, if you don't know what to protect, how do you know that you're protecting it? The third and most important law, if you're not protecting it, information, data, the dragon wins. The dragon, of course, being the consistent appearance of security breaches that we are seeing throughout the media. The dragon is just a metaphor, it can be any other mythological beast or anything that you want to put in the place of the dragon, that means some kind of malicious consequence. I'm going to bring this to a close with more of a question this time for this particular session. Although we have discussed the use of OPSEC in the business and government section, how can we go about also using OPSEC in our personal lives? What can we do different to mitigate some of the risks that we're doing with our personal information? For example, at the time of this recording, I have to say, for those of you that use DoorDash, DoorDash was recently breached. You might want to consider looking at your credit cards and your other instances, a PII. That goes into my example, is how do we go about fixing or better guarding our own data? Maybe not trusting companies the way we should, maybe not so easily volunteering our information online in social media circles.

But I will bring this very brief session to a close and leave you with that question. My name is Arthur Moore, you have a nice day now. Again, I appreciate you stopping by and listening to this audio series on C836, 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.