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

Operations security

- Operations security is known in military and government circles as OPSEC, is, at a high level, a process that we use to protect our information. Although we have discussed certain elements of operations security previously, such as the use of encryption to protect data, such measures are only a small portion of the entire operations security process.
- While OPSEC may be a relatively new term the origins can be found in historical text.
- Sun Tzu was a Chinese military general who lived in the sixth century BC. Among those of a military or strategic bent, Sun Tzu's work *The Art of War* is considered one of the foundational doctrinal texts for conducting such operations.

The Historical Context

- The Art of War second passage is "(when) making tactical dispositions, the highest pitch you can attain is to conceal them; conceal your dispositions, and you will be safe from prying of the subtlest spies, from the machinations of the wisest brains. This is a recommendation to very carefully protect our activities so that they do not leak to those that might oppose our efforts.
- George Washington, the first president of the United States, was well known for being an astute and skilled military commander and is also well known for promoting good operational security practices. He is known in the operations security community for having said, "Even minutiae should have a place in our collection, for things of a seemingly trifling nature, when enjoined with others of a more serious cast, may lead to valuable conclusion" meaning that even small items of information, which are valueless individually, can be of great value in combination.

OPSEC Process

- The operations security process, as laid out by the US government, will look very familiar to anyone who has worked with risk management. In essence, the process is to identify what information we have that needs protection, analyze the threats and vulnerabilities that might impact it, and develop methods of mitigation for those threats and vulnerabilities.
- **Identification of Critical Information**: The initial step, and, arguably, the most important step in the operations security process, is to identify our most critical information assets.
- **Analysis of Threats**: A threat is something that has the potential to cause us harm. With the list of critical information, we can then begin to look at what harm or financial impact might be caused by critical information being exposed, and who might exploit the exposure.
- **Analysis of Vulnerabilities:** Vulnerabilities are weaknesses that can be used to harm us. In the case of analyzing the vulnerabilities in the protections we have put in place for our information assets, we will be looking at how the processes that interact with these assets are normally conducted, and where we might attack in order to compromise them.
- **Assessment of Risks:** Risk occurs when we have a matching threat and vulnerability, and only then. If we found that we had a threat in the vulnerability controls on access and configuration/version management to our source code, and a lack of policy in how exactly it was controlled. These two matching issues could potentially lead to the exposure of our critical information to our competitors or attackers.
- **Application of Countermeasures:** Once we have discovered what risks to our critical information might be present, we would then put measures in place to mitigate them. Such measures are referred to in operations security as countermeasures.

Kurt's Laws of Operations Security

- As a somewhat different, and briefer, viewpoint on the operations security process, we can look at the Laws of OPSEC, developed by Kurt Haase while he was employed at the Nevada Operations Office of the DOE.
- The first law "If you don't know the threat, how do you know what to protect?"
- The second law "If you don't know what to protect, how do you know you are protecting it?"
- The third and last law of operations security is "If you are not protecting it (the information), … THE DRAGON WINS!"
- The case of the "dragon" winning—from the constant appearance of security breaches reported by the news media and on Web sites that track breaches, appears to be unfortunately common.

How to implement OPSEC in our daily lives

- Although we have discussed the use of the operations security process in both business and government throughout this lesson, it can also be of great use in our personal lives.
- What could you do differently to mitigate some risk when dealing with your personally identifiable information?