Fundamentals of Information Security Series

C836

Instructor: Arthur Moore

Event time: Every Thursday at 6:00PM MST

WESTERN GOVERNORS UNIVERSITY

ONLINE. ACCELERATED. AFFORDABLE. ACCREDITED.

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

What is information security?

- What is information security? Is it a state of data? Action that an organization needs to take. Or is it information industry best practices against unknown and unnamed threats. The answer is all the above. No device is ever truly 100% secure. The only security device is completely off unused and locked away in a vault. The device at this point is secure but has no value because it can’t be used.
- 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, and people. I know that Jim down the hall can be difficult and hard to get along with but, he is worth more than your security data. Jim has experience and knowledge that makes him an asset. Data can be cloned and copied but not Jim. People will always be more important than data, software, and, hardware.

- Assets should always be protected by value to the organization in this order most important people, data least important hardware/software.

Compliance

- Compliance is a term that is used very often in the ITSEC community.
- Compliance is the requirements that are set forth by laws and industry regulations some examples are listed below.
- HIPPA/HITECH: Healthcare Industry
- PCI-DSS: Payment Card Industry
- FISMA: Federal Government Agencies

Security Models

- What is CIA? It’s not the Central Intelligence Agency.
- The CIA is the core model of all of information security.
- CIA is Confidential Integrity and Availability.
- Confidential is allowing only those authorized to access the data requested.
- Integrity is keeping data unaltered by Accidental or Malicious intent.
- Availability is the ability to access data when needed.

Security Models continued

- The is a Parkerian hexad lesser-known model that includes the CIA triad and expands on it.
- Confidentiality: is allowing only those authorized to access the data requested.
- Integrity: is keeping data unaltered by Accidental or Malicious intent.
- Availability is the ability to access data when needed.
- Possession/Control refers to the physical disposition of the media on 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.
- Utility refers to how useful the data is to us.

Attacks

- When we look at the types of attacks we might face, we can generally place them into one of four categories: interception, interruption, modification, and fabrication. Each type of attack effects one or more sides of the CIA triad.
- Interception: attacks allow unauthorized users to access our data, applications, or environments, and are primarily an attack against confidentiality.
- Interruption: attacks cause our assets to become unusable or unavailable for our use, on a temporary or permanent basis. Interruption attacks often affect availability but can be an attack on integrity as well.
- Modification: attacks involve tampering with our asset. Such attacks might primarily be considered an integrity attack but could also represent an availability attack.
- Fabrication: attacks involve generating data, processes, communications, or other similar activities with a system. Fabrication attacks primarily affect integrity but could be considered an availability attack as well.

Risk

- Risk is the likelihood that an event will occur. To have risk there must be a threat and vulnerability.
- Threats are any events being man-made, natural or environmental that could cause damage to assets.
- Vulnerabilities are a weakness that a threat event or the threat agent can take advantage of.
- Impact is an additional step that is taking into account the asset's cost.
- Let's bring it all together. If you own a vehicle you can relate. Vulnerability: We have a car that has bad breaks Threat: It's been raining heavily. Risk: the breaks on the car might give out while driving. Impact: the is worth 10000 is now totaled.

How do you protect assets?

- Controls are the ways we protect assets.
- Controls come in 3 different flavors physical, technical/logical, and administrative.
- Physical: controls are physical items that protect assets think locks, doors, guards, and, fences.
- Technical/Logical: controls are devices and software that protect assets think firewalls, AV, IDS, and IPS.
- Administrative: controls are the policies that organizations create for governance an example acceptable use and email use policies.

Risk Management

- Risk management is a constant process. As assets are purchased, used, and retired they must constantly be assessed. The steps will vary based on organization policies and procedures. The general steps are below.
- Identify assets: One of the first and, arguably, one of the most important parts of the risk management process is identifying and categorizing the assets that we are protecting.
- Identify threats: Once we have enumerated our critical assets, we can then begin to identify the threats that might affect them.
- Assess vulnerabilities: When we look at assess vulnerabilities, we need to do so in the context of potential threats. Any given asset may have thousands or millions of threats that could impact it, but only a small fraction of these will actually be relevant.
- Assess risks: Once we have identified the threats and vulnerabilities for a given asset, we can assess the overall risk.
- Mitigating risks: In order to help us mitigate risk, we can put measures in place to help ensure that a given type of threat is accounted for.
- Measures used to alleviate risk are call controls. Controls are divided into three categories: physical, logical, and administrative.

Incident Response

- Incident response is the response to when risk management practices have failed and have caused an inconvenience to a disastrous event. There are 6 steps in Incident response cycle
- Preparation: The preparation phase of incident response consists of all of the activities that we can perform, in advance of the incident itself, in order to better enable us to handle it.
- Detection and analysis: The detection and analysis phase is where the action begins to happen in our incident response process. In this phase, we will detect the occurrence of an issue and decide whether or not it is actually an incident so that we can respond to it appropriately.
- Containment: Containment involves taking steps to ensure that the situation does not cause any more damage than it already has, or to at least lessen any ongoing harm.
- Eradication: During eradication, we will attempt to remove the effects of the issue from our environment.
- Recovery: Lastly, we need to recover to a better state that were in which we were prior to the incident, or perhaps prior to the issue started if we did not detect the problem immediately.
- Post incident activity: Post incident activity, as with preparation, is a phase we can easily overlook, but should ensure that we do not. In the post incident activity phase, often referred to as a postmortem (latin for after death), we attempt to determine specifically what happened, why it happened, and what we can do to keep it from happening again.

Defense in Depth

- Defense in depth is an ancient concept that is being applied to the modern information systems.
- Defense in depth is layering multiple controls on top on one another.
- For example: Using the 3 control types in multiple overlapping protections. Locks on hardware server cabinets, multilayers of authentication and policies that control visitors in the building.