MODULE 1: FOUNDATIONAL CONCEPTS IN SECURITY
WEEK 1

Learning Outcomes:

After completing this course you are expected to demonstrate the following:

1. Define the term Confidentiality, Integrity and Availability.
2. Understand its importance and impact to the society.

A. Engage

Review Topic

In your own opinion, what do you think about the web security of our government nowadays?

B. Explore

Video Titles:

1. **Key Info**
2. **What Is the CIA Triad**

Youtube Links:

1. https://www.youtube.com/watch?v=xtlFO8Q2GDQ
2. https://www.youtube.com/watch?v=cPfRUr9fbWg

Video Module Filenames:

1. **Week 1 - Key Info**
2. **Week 1 - What Is the CIA Triad**

C. Explain

Figure 1.0
Information Assurance and Security

Information Assurance and Security is the management and protection of knowledge, information, and data.

It combines two fields:

1. **Information Assurance**, which focuses on ensuring the availability, integrity, authentication, confidentiality, and non-repudiation of information and systems. These measures may include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

2. **Information Security**, which centers on the protection of information and information systems from unauthorized access, use, disclosure, disruption,

modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Assurance vs. Information Security

Although related, information assurance and information security are two different disciplines. Both disciplines involve a variety of similar issues, including risk management, cyber security, corporate governance, compliance, auditing, business continuity, disaster recovery, forensic science, security engineering, and criminology.

D. Elaborate

CIA (Confidentiality, Integrity, Availability)

The CIA Triad of **confidentiality**, **integrity** and **availability** is considered the core underpinning of information security. Every security controls, and every security vulnerability can be viewed in light of one or more of these key concepts. For a security program to be considered comprehensive and complete, it must adequately address the entire CIA Triad.

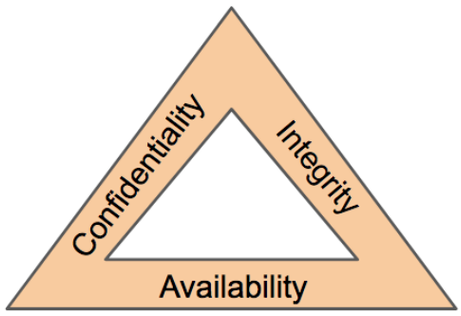

Figure 1.1
The CIA Triad

Confidentiality means that data, objects and resources are protected from unauthorized viewing and other access.

Confidentiality measures protect information from unauthorized access and misuse. Most information systems house information that has some degree of sensitivity. It might be proprietary business information that competitors could use to their advantage, or personal information regarding an organization's employees, customers or clients.

Confidential information often has value and systems are therefore under frequent attack as criminals hunt for vulnerabilities to exploit. Threat vectors include direct attacks such as stealing passwords and capturing network traffic, and more layered attacks such as social engineering and phishing. Not all confidentiality breaches are intentional. A few types of common accidental breaches include emailing sensitive information to the wrong recipient, publishing private data to public web servers, and leaving confidential information displayed on an unattended computer monitor.

Integrity means that data is protected from unauthorized changes to ensure that it is reliable and correct.

Integrity measures protect information from unauthorized alteration. These measures provide assurance in the accuracy and completeness of data. The need to protect

information includes both data that is stored on systems and data that is transmitted between systems such as email. In maintaining integrity, it is not only necessary to control access at the system level, but to further ensure that system users are only able to alter information that they are legitimately authorized to alter.

As with confidentiality protection, the protection of data integrity extends beyond intentional breaches. Effective integrity countermeasures must also protect against unintentional alteration, such as user errors or data loss that is a result of a system malfunction.

Availability means that authorized users have access to the systems and the resources they need.

In order for an information system to be useful it must be available to authorized users. Availability measures protect timely and uninterrupted access to the system. Some of the most fundamental threats to availability are non-malicious in nature and include hardware failures, unscheduled software downtime and network bandwidth issues. Malicious attacks include various forms of sabotage intended to cause harm to an organization by denying users access to the information system.

Concepts of risk, threats, vulnerabilities, and attack vectors

Nowadays, gathering data and protecting the data are consideration for business. Customers want to ensure the security of their data if the company can keep it safe or can't.

In order to have a strong handle on data security issues that may potentially impact your business, it is imperative to understand the relationship between three central components: threat, vulnerability and risk. Though these technical terms are used interchangeably, they are distinct terms with different meanings and implications. Let's take a look.

Figure 1.2
The Relationship between Three Central Components

Threat

A ***threat*** refers to a new or newly discovered incident that has the potential to harm a system or your company overall. There are three main types of threats:

1. **Natural threats**, such as floods, hurricanes, or tornadoes
2. **Unintentional threats**, like an employee mistakenly accessing the wrong information
3. **Intentional threats**, such as spyware, malware, adware companies, or the actions of a disgruntled employee

Worms and viruses are categorized as threats because they could cause harm to your organization through exposure to an automated attack, as opposed to one perpetrated by humans.

These threats may be uncontrollable and often difficult or impossible to identify in advance. Still, certain measures help you assess threats regularly, so you can be better prepared when a situation does happen. Here are some ways to do so:

1. **Ensure your team members are staying informed** of current trends in cyber security so they can quickly identify new threats.
2. **Perform regular threat assessments** to determine the best approaches to protecting a system against a specific threat, along with assessing different types of threats.
3. **Conduct penetration testing** by modelling real-world threats in order to discover vulnerabilities.

Vulnerability

Vulnerability refers to a known weakness of an asset (resource) that can be exploited by one or more attackers. In other words, it is a known issue that allows an attack to succeed.

Testing for vulnerabilities is critical to ensuring the continued security of your systems. By identifying weak points, you can develop a strategy for quick response. Here are some questions to ask when determining your security vulnerabilities:

1. Is your data backed up and stored in a secure off-site location?
2. Is your data stored in the cloud? If yes, how exactly is it being protected from cloud vulnerabilities?
3. What kind of network security do you have to determine who can access, modify, or delete information from within your organization?
4. What kind of antivirus protection is in use? Are the licenses current? Is it running as often as needed?
5. Do you have a data recovery plan in the event of a vulnerability being exploited?

Understanding your vulnerabilities is the first step to managing your risk.

Risk is defined as the potential for loss or damage when a threat exploits vulnerability. Examples of risk include financial losses, loss of privacy, reputational damage, legal implications, and even loss of life.

Risk can also be defined as follows:

Risk = Threat X Vulnerability

Reduce your potential for risk by creating and implementing a risk management plan. Here are the key aspects to consider when developing your risk management strategy:

1. **Assess risk and determine needs.** When it comes to designing and implementing a risk assessment framework, it is critical to prioritize the most important breaches that need to be addressed. Although frequency may differ in each organization, this level of assessment must be done on a regular, recurring basis.
2. **Include a total stakeholder perspective.** Stakeholders include the business owners as well as employees, customers, and even vendors. All of these players have the

potential to negatively impact the organization (potential threats) but at the same time they can be assets in helping to mitigate risk.

3. **Designate a central group of employees** who are responsible for risk management and determine the appropriate funding level for this activity.
4. **Implement appropriate policies and related controls** and ensure that the appropriate end users are informed of any and all changes.
5. **Monitor and evaluate policy and control effectiveness**. The sources of risk are ever-changing, which means your team must be prepared to make any necessary adjustments to the framework. This can also involve incorporating new monitoring tools and techniques.

Attack Vectors

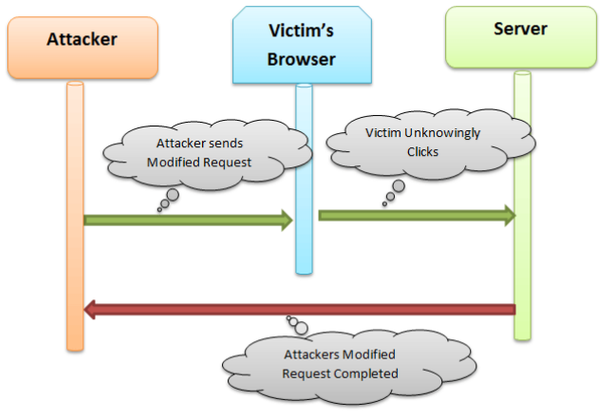

Figure 1.3
Attack vector

An ***attack vector*** is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

Attack vectors include viruses, e-mail attachments, Web pages, pop-up windows, instant messages, chat rooms, and deception. All of these methods involve programming (or, in a few cases, hardware), except deception, in which a human operator is fooled into removing or weakening system defences.

To some extent, ***firewalls*** and ***anti-virus*** software can block attack vectors. But no protection method is totally attack-proof. A defence method that is effective today may not remain so for long, because hackers are constantly updating attack vectors, and seeking new ones, in their quest to gain unauthorized access to computers and servers.

The most common malicious payloads are ***viruses*** (which can function as their own attack vectors), ***Trojan horses***, ***worms***, and ***spywares***. If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.

E. Evaluate

ASSESSMENT:
Instructions: You may write your answer on the Answer Sheet (AS) provided in this module.

CONTENT FOR ASSESSMENT:

1. It includes viruses, e-mail attachments, Web pages, pop-up windows, instant messages, chat rooms, and deception.
2. Means that data, objects and resources are protected from unauthorized viewing and other access.
3. Refers to a new or newly discovered incident that has the potential to harm a system or your company overall.
4. Means that authorized users have access to the systems and the resources they need.
5. Defined as the potential for loss or damage when a threat exploits a vulnerability.

References:

1. *https://www.vectorstock.com/royalty-free-vector/word-cloud-information-assurance-vector-6260049(image)*
2. *https://finosec.com/the-essential-roles-of-an-information-security-officer/(image)*
3. *https://www.capella.edu/blogs/cublog/what-is-information-assurance-and-security.*
4. *https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad*
5. *https://www.bmc.com/blogs/security-vulnerability-vs-threat-vs-risk-whats-difference/*
6. *https://eforensicsmag.com/attack-vector/(image)*
7. *https://searchsecurity.techtarget.com/definition/attack-vector*

Facilitated By:		
Name	:	
MS Teams Account (email)	:	
Smart Phone Number	:	