Information Security and Incident Management

Objectives:

At the end of this episode, I will be able to:

Understand what basic information security concepts are and why they are important.

Explain the basic concepts of confidentiality, integrity, availability, authenticity, and non-repudiation.

Identify the reasons why an organization needs to implement and use information security policies.

Define what common information security threats and attack vectors organizations should be aware of.

External Resources:

Information Security Concepts

Information security refers to the protection or safeguarding of information and information systems that use, store, and transmit information from unauthorized accesses, disclosures, alterations, and destruction.

It relies on five major elements: confidentiality, integrity, availability, authenticity, and non-repudiation.

1. Confidentiality - "Keeping good data away from bad actors"

For Confidentiality to be maintained in a network, data must be protected at rest, in use and on the wire.

Violations of Confidentiality can come from ANYWHERE, at ANY TIME... bad decisions on the part of users, administrators and customers can all lead to a violation. Also, remember that security policies that are not implemented properly can lead to potential confidentiality violations.

Possible countermeasures include:

```
a. encryption
b. traffic padding
c. strict access controls / authentication
d. data classification
e. awareness training
```

Confidentiality & Integrity depend on each other. One is not effective without the other.

Additional concepts linked to Confidentiality:

```
1. sensitivity
2. discretion
3. criticality
4. concealment
5. isolation
```

2. Integrity - "Change control for data - no unauthorized modification without knowledge and consent of data owner"

Three ways in which we can understand Integrity:

```
1. Preventing unauthorized subjects from making modifications
2. Preventing authorized subjects from making unauthorized
```

modifications
3. Maintaining consistency of objects so that they are true and accurate

Possible countermeasures include:

```
a. strict access controls / authentication
b. IDS
c. encryption
d. hashing
e. interface restrictions / controls
f. input / function checks (validation)
```

Additional concepts linked to Integrity:

```
1. accuracy
2. authenticity
3. validity
4. nonrepudiation - user cannot deny having performed an action
```

3. Availability - authorized subjects can access objects in a timely manner without interruption

Possible countermeasures include:

```
a. strict access controls / authentication
b. continuous monitoring
c. firewalls & routers to prevent DoS / DDoS attacks
d. redundant system design
e. periodic testing of backup systems
```

Additional concepts linked to Availability:

```
1. usability
2. accessibility
3. timeliness
```

4. Authenticity - the characteristic of a communication, document, or any data that ensures it is genuine.

5. Non-Repudiation - a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Individuals and organizations use digital signatures to ensure non-repudiation.

NOTE: Confidentiality, integrity, and availability are together referred to as the CIA triad.

• Information as a business asset

• Defense in depth

• Information Security Policies -

Define the basic security requirements and rules to be implemented in order to protect and secure an organization’s information systems.

Should help to answer 2 questions:

```
1. WHY are we doing this?
2. WHAT are we doing?
```

Policies are not technology specific and accomplish three things:

▪ They reduce or eliminate legal liability of employees and third parties.

▪ They protect confidential and proprietary information from theft, misuse, unauthorized disclosure, or modification.

▪ They prevent wastage of the company’s resources.

There are 2 types of policies:

```
1. Technical - configuration
2. Administrative - behavior
```

Who is involved in the implementation of the policies?:

▪ Director of Information Security
▪ Chief Security Officer

What are the types of security policies?

```
• Promiscuous Policy - No restrictions on usage of system resources

• Permissive Policy - Policy begins wide open and only known dangerous
services/attacks or behaviors are blocked -- It should be updated regularly to
be effective

• Prudent Policy - It provides maximum security while allowing known but
necessary dangers -- It blocks all services and only safe/ necessary services
are enabled individually; everything is logged

• Paranoid Policy - It forbids everything, no internet connection, or severely
limited internet usage
```

Information Security Threats and Attack Vectors

What makes an attack?

```
Attacks = Motive (Goal) + Method + Vulnerability
```

What are some attack vectors?

```
Cloud computing
Advanced Persistent Threats (APTs)
Viruses & Worms
Ransomware
Insider Attacks
Web Applications
IoT
```

What are the broad information security threat categories?

```
1. Network
2. Host
3. Application
```

Threats and Threat Actors -

```
Threats are “[t]he potential for a person or thing to exercise (accidentally
    trigger or intentionally exploit) a specific vulnerability.”

Threat actors are the bad actors that exploit threats to cause harm.
```

What is the impact of information security attacks?

```
Financial Losses
Loss of C I A
Reputational Damage
Legal and Regulatory concerns
```

Information warfare - Defense vs Offense

What are Information Security Incidents?

Incidents are events that have negative outcomes or consequences in relation
to C I A for one or more assets within the enterprise.

```
Unauthorized Access
Insider Threat
Unauthorized usage of services
```