THE UNIVERSITY OF SYDNEY

INFO5301 Tutorial 2

Information Security Management

*You will be working in a group. Each group is given **three** questions from the following set of questions.*

1 Single-choice Questions

Exercise 1:

Match the following terms with their meaning:

Terms:

1. Confidentiality
2. Data Integrity
3. System Integrity
4. Availability
5. Assurance

Meaning:

- A. Level of confidence that controls work
- B. System will work as intended
- C. Operation are accessible when needed
- D. Data can be trusted
- E. Data available to authorised users only

Answer:

1-E: Confidentiality is that data is available to authorized users only.

2-D: Data can be trusted, that we know that the data is accurate and complete, that it's trustworthy.

3-B: System integrity is that the system will work as intended; we know that the system will perform in the way that we expect.

4-C: Availability, is that the systems will be operating and accessible when needed.

5-A: Assurance is the level of confidence that the controls work. So, this is where we're going to be doing various testing and audit; it's how we know that what we've put in place is actually working to protect our organizations and our environments.

NOTE: Availability just says that the system is operating and accessible to authorized users, it doesn't mention how it is working. System integrity is a commentary on how the system will work; that it will work as intended.

Duration: 5 min

Exercise 2:

Which of the following terms is used to denote a potential cause of an unwanted incident, which may result in harm to a system or organization?

1. Vulnerability
2. Exploit
3. Threat
4. Attacker

Answer:

Threat.

The question provides the definition of a threat in ISO/IEC 27000.

The term attacker (in option 4) could be used to describe a threat agent that is, in turn, a threat, but use of this term is much more restrictive.

Vulnerability (in option 1) is defined as "weakness of an asset or control that can be exploited by one or more threats".

Duration: 5 min

Exercise 3:

Which group causes the most risk of fraud and computer compromises? Explain?

1. Employees
2. Hackers
3. Attackers

4. Contractors

Answer:

A

It is commonly stated that internal threats comprise 70% – 80% of the overall threat to a company. The reason is employees already have privileged access to a wide range of company assets. In contrast, people from outside who want to cause damage must obtain this level of access before they can carry out the type of damage internal personnel could dish out. A lot of the damages caused by internal employees are brought about by mistakes and system misconfigurations.

Duration: 5 min

Exercise 4:

To perform and review the risk analysis, the team members must come from different departments of the organizations. Which of the following is true? Explain why?

1. To make sure the process is fair and that no one is left out.
2. Because people in different departments understand the risks of their department. Thus, it ensures the data going into the analysis is as close to reality as possible.
3. Because the people in the different departments are the ones causing the risks, so they should be the ones held accountable.
4. It is not true. It should be a small group brought in from outside the organization because otherwise the analysis is biased and unusable.

Answer:

(2) is true.

An analysis is only as good as the data that goes into it. Data pertaining to risks the company faces should be extracted from the people who understand best the business functions and environment of the company. Each department understands its own threats and resources, and may have possible solutions to specific threats that affect its part of the company.

For instance, the team members may be part of management, application programmers, IT staff, systems integrators, and operational managers, any key personnel from key areas of the organization.

Duration: 5 min

Exercise 5:

Many types of threat agents can take advantage of several types of vulnerabilities. Match the following threat agents to vulnerabilities that they can exploit.

Threat Agents:

1. Malware
2. User
3. Employee
4. Attacker

Vulnerabilities:

- A. Mis-configured parameters in the operating system
- B. Lack of training or standards enforcement
- C. Lack of antivirus software
- D. Poorly written application. Lack of stringent firewall settings

Answer:

1-C: Malicious software needs to be detected by using antivirus software. This might lead to virus infection.

2-A: If the operating system is misconfigured, users can gain access to some restricted area of the system.

3-B: If the company does not provide training program to employees, there is vulnerability of employees' mistakes. Employees might alter data inputs and outputs from the data processing application

4-D: Attacker can abuse the poorly implemented application to conduct a buffer overflow. They can also try to conduct denial-of-services attack.

Duration: 5 min

2 Discussion Questions

Exercise 6:

For Internet of Things (IoT), what other aspects of security besides CIA should be considered? Explain why?

Answer:

Human safety: First, as the Internet of Things (IoT) evolves, an increasingly important aspect of security will be human safety. Information security is rapidly including personal security and safety. Computer-controlled medical devices, self-driving cars, home automation and security, robotic surgery, and other innovations are taking information security far beyond

information security to include the security of us. *Ref: Miller, Lawrence C; Gregory, Peter H. CISSP For Dummies 2018, 6th edition, Chapter 3: Security and Risk Management*

Authentication is also important that supports the CIA in IoT. Each device needs to reliably identify itself and prove that it can securely communicate with other devices in the system. This can be achieved using a combination of digital certificates and hardware-based anchor of trust. Strong user authentication should also be used to control user access.

Non-repudiation: This serves as irrefutable proof of the validity and origin of all data transmitted. Digitally signed documents and transactions using hardware security device can provide strong non-repudiation for the date and origin of transaction

Duration: 15 min

Exercise 7:

Company A provides cloud computing services to their customers. To maintain the Confidentiality, Integrity and Availability, what practices that the company should leverage to maintain these measures?

Answer:

Confidentiality: To keep the cloud computing confidential, the company must use encryption scheme to protect data "at rest" and "in transit". Identity Access Management, and Multi-Factor Authentication; network firewalls

Data Integrity: to protect data from unauthorized modification or deletion. There must be a system of permissions and logs that can demonstrate that there is no inappropriate access to customer data. Multi-Factor Authentication, Version Control are also used when users trying to delete things in the Cloud.

Data Availability: ensure that data continues to be available, at a required level of performance, in situations ranging from normal to disastrous. Load balancing is also important. For example, strategies used by Amazon Web Service (AWS) including Auto-scaling, Multiple Availability Zones, using Route 53 with health checks, to detect the failure and automatic failover (switching to a redundant or standby computer server, system).

Duration: 15 min

Exercise 8:

A server called Server1 is running Windows Server 2016. On Server1, a folder called Data is created and shared on the C drive. Within the Data folder, subfolders are created with each user's name within the organization. Each person's electronic paycheck is placed in each user's folder. Later, you find out that John was able to go in and change some of the electronic paycheck amounts, while also deleting some of the electronic paychecks. Explain which one (or more) of the CIA components was not followed.

Answer: All three CIA components were not followed properly.

Confidentiality: because data is stored in a server which is accessible by all users. Furthermore, data is not encrypted. This violate the requirement of *confidentiality* that only authorised user can access the data.

Integrity: because anyone who can access the subfolders can see the data in clear and make change to it. The user can also delete the paychecks in each subfolder. This violate the requirement of *integrity* that data needs to be accurate and complete.

Availability: as some paychecks were deleted, they become unavailable when needed. Thus the availability requirement is not satisfied.

Duration: 15 min

Exercise 9:

In banking industry, a range of online services are now available to assist customers with business banking needs. Discuss the potential security risks of online banking services?

Answer:

The following items are potential risks that a bank must be aware of:

- Loss of data: Online theft of customer's Access Code/User ID/Username, PIN/Password
- Human interaction: Customers accidentally access their Online Banking accounts through hyperlinks in e-mails, pop-up windows, or search engines.
- Inside and outside attacks: Virus attacks, hacking, unauthorized access and fraudulent transactions
- Misuse of data: Sharing customer's information with third parties;

Duration: 15 min