Cyber Security risk mangment assement Two

John 12345

|  |  |  |  |
| --- | --- | --- | --- |
| Name of Student |  | ID | 1 |

Contents

[Task 1 1](#_Toc194394954)

[Task 2 1](#_Toc194394955)

[Task 3 1](#_Toc194394956)

[Task 5 2](#_Toc194394957)

[Task 6 2](#_Toc194394958)

[Task 7 2](#_Toc194394959)

[Task 8 2](#_Toc194394960)

[Task 10 2](#_Toc194394961)

[Task 11 2](#_Toc194394962)

[Task 12 3](#_Toc194394963)

[Task 13 3](#_Toc194394964)

[Task 14 3](#_Toc194394965)

[Task 15 3](#_Toc194394966)

[Task 16 3](#_Toc194394967)

[Task 18 3](#_Toc194394968)

[Task 19 3](#_Toc194394969)

[Task 20 3](#_Toc194394970)

[Task 22 Fill in the blanks question 4](#_Toc194394971)

**Assessment 2 – Research and Questioning**

***Instructions***

This task is to be completed individually. You need to be able to demonstrate knowledge to complete the tasks outlined in the elements and performance criteria of this cluster.

***Duration:***

Trainer will set the duration of the assessment.

## Task 1

Differentiate between a threat and a vulnerability

## Task 2

Identify and explain the main factors that determine cyber security risk to an organisation, and how are they related to each other?

## Task 3

The engineering team of company X is working on a new high-end mobile phone. The product is announced, and the CEO of X describes it capabilities and fixes its release date. All is going fine until a key member of the design team voluntarily discloses design specifications (for extra money and a better job) and implementationlevel details to the company’s key competitor, company Y. As a result, Y improves the specifications, adds more capability, and, following an Agile go-to-market strategy, it announces an earlier release date. This results in X’s image being downgraded, its share price crashing, investors losing confidence, and a complete panic in the design team.

Using Microsoft’s STRIDE threat classification system, identify the nature of the threat experienced by company X. What controls could company X have put in place to prevent this threat?

## Task 4

Explain what the acronym ISMS stands for, and what it means. How does this term relate to ISO 27001?

## Task 5

When considering cyber security threats, how could an IT auditor use major vulnerabilities of password file protection to test authentication processes?

## Task 6

APRA’s Prudential Practice Guide CPG 234 – Management of Security Risk in Information and Information Technology recommends a ‘Security principles’ to IT security. How would security principles to regulation work in practice?

## Task 7

Why is risk assessment needed in an organisation? What elements comprise the scope of cyber security risk assessment?

## Task 8

You are interested in an emerging technology in the ICT sector. Explain some benefits and drawbacks of using Google Scholar for your research.

## Task 9

Discuss some reasons why risk assessment is an important tool for technology implementation projects.

## Task 10

Explain why the use of cross-functional teams is considered good business practice when implementing new technologies.

## Task 11

Your supervisor has invited you to join a cross-functional team investigating potential new technologies in the ICT sector which may be of interest to the organisation. Each of the team has been asked to research an emerging technology and present their findings to the group. Because of recent data breaches you have been asked to research any emerging technologies which might impact cyber security defences. a) How will you conduct your research?

b) How might current technologies and practices be impacted?

## Task 12

Assuming your report on emerging cyber security methods is accepted by the cross-functional team, what sort of planning methods will be needed before the new technology can be implemented?

## Task 13

Identify some organisational practices that may need to be reviewed and adapted following the implementation of proposed new cyber security technologies.

## Task 14

The ACS Code of Ethics talks about ‘the Primacy of the Public Interest’ for its members. Explain some of the difficulties the ACS may have in enforcing this aspect of their code of ethics.

## Task 15

When a new ICT company develops a privacy policy for the first time, it needs to consider not only legislative compliance but also the principles of access and equity. In the context of an ICT privacy policy, provide an example where access will not be equitable.

## Task 16

Copyright policies often use the term ‘moral rights’ when describing the expected behaviour of those required to comply with the policy. In your own words, explain the concept of moral rights in copyright.

**Task 17**

Provide examples of where organisations are legally required to collect personal information.

## Task 18

Explain the relationship of the Spam Act 2003 (Cwlth) with organisational communication processes and procedures.

## Task 19

Outline some circumstances where customer service could become unethical. How could these behaviours be rectified?

## Task 20

How can the security features of a server operating system help to ensure the integrity and security of stakeholder’s personal or confidential data?

**Task 21**

Outline some of the system security procedures that may be put in place to protect sensitive information.

## Task 22 Fill in the blanks question

1. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a factor in securing the environment against an attack on security?**

1. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ phase of hacking performs actual attack on a network or system?**

1. **The purpose of a Denial of Service attack is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_?**

1. **Some of the most common vulnerabilities that exist in a network or system is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_?**

1. **The first phase of hacking an IT system is compromise of \_\_\_\_\_\_\_\_\_\_\_ foundation of security?**

1. **Phishing is a form of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**

1. **Keyloggers are a form of \_\_\_\_\_\_\_\_\_\_\_\_\_\_.**

1. **\_\_\_\_\_\_\_\_\_\_\_\_ is the best statement for taking advantage of a weakness in the security of an IT system. 9) In terms of cyber-security, resilience refers to the ability of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_?**

1. **'cyber-crime' means any** crime that involves \_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1. **An effective way of securing against cyber threats is the Acceptance that there can be no absolute security, instead \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_\_\_\_\_ in order to reduce threat and increase resilience.**

1. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a practice that hacker locks out users and encrypts their personal computer files and data, holding it hostage until they agree to pay to the attacker.**

1. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ is a common example of a "phishing" attack.**

1. **On the evening news you heard the reporter talking about an Internet threat called a 'Botnet'. Botnet is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**

1. **The best description of a blockchain is\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. **From information below work out the Total Control Cost (TCC) = \_$\_\_\_\_\_\_\_\_\_\_\_\_** 
   * Annual expected savings: $550
   * Combined control effectiveness: 50%
   * Annual covered loss: $950