Assessment 1: Security Knowledge Test

Started: Oct 8 at 11:40

Quiz Instructions

Assessment Information

Attached Files: **Assessment 1 Brief.pdf (https://mylearn.torrens.edu.au/courses/19771/files/7321962/preview)**

Please refer to the assessment brief attached above for details on how to complete this assessment.

Click on the link below to submit your assessment

- **Quiz Duration:** 60 Minutes
- **Number of Questions:** 13 Short Answer and 3 Multiple Choice Questions
- **Quiz Weight:** 25%
- **Attempts Allowed:** 1 Attempt

TECHNICAL INSTRUCTION

We strongly recommend that you complete the quiz in its entirety once you start. You may exit the browser and return to complete the quiz later; however, please note that the countdown timer will continue to run even with the browser closed. Once you submit your answers, they will be locked, and you will not be able to make any changes.

ACADEMIC INTEGRITY and MISCONDUCT

By attempting this assessment task, you agree to adhere to the policies and procedures on Academic Integrity before, during, and following this assessment task. The Academic Integrity policy and procedure can be **viewed online (http://www.torrens.edu.au/policies-and-forms)** .

We are committed to fostering integrity in the pursuit of knowledge and to produce graduates with a strong sense of professional ethics. As a student, you have an obligation to work independently and apply scholarly academic conventions in your assessment tasks. Any form of cheating, plagiarism, collusion, or other forms of dishonesty carries serious consequences as they are addressed seriously and thoroughly according to the **Academic Integrity Policy (https://www.torrens.edu.au/policies-forms)** . We encourage you to familiarize yourself with this policy and the different types

Declaration

By attempting this quiz you agree to adhere to the full policies and procedures on Academic Integrity prior to, during and following this assessment.

I have read and am aware of Torrens University Australia Academic Integrity Policy and Procedure viewable online at **http://www.torrens.edu.au/policies-and-forms (http://www.torrens.edu.au/policies-and-forms)**

Please note, all quizzes are closed book assessments and no learning materials are to be used in the completion of the quiz

Question 1 7 pts

What comprises cyber security?

Edit View Insert Format Tools Table

12pt Paragraph

Cyber security combines people with processes with technology to protect systems, networks and of course, data, from digital attacks, theft or damage!

p 22 words

Question 2 7 pts

Does everyone (from C-level to users) always have the same understanding of cyber security? Please explain your answer.

Edit View Insert Format Tools Table

12pt Paragraph

No! I'd say that normally:

- Executives see it as a business risk.

- IT teams normally see it as technical controls

- Users think of it as passwords and emails.

Everyone views it through their own role on the process.

p 38 words

Question 3 7 pts

Why is a successful cyber-security attack bad for a company?

Edit View Insert Format Tools Table

12pt Paragraph

Because it damages trust, reputation and finances.

One single breach can leak customer data, cause downtime and even trigger legal penalties. Especially now that we have laws like GDPR or LGPD (specific for Brazil).

p 34 words

Question 4 7 pts

Why is it important to develop and use secure software?

Edit View Insert Format Tools Table

12pt Paragraph

Because most attacks will try to exploit software vulnerabilities or bugs.

Secure coding reduces risks early, saving time and costs later, helping protect users and the company's data

company's data.

p 28 words

Question 5 7 pts

Should you rely solely on technical methods to create cyber security? Please explain your answer and provide at least two examples.

Edit View Insert Format Tools Table

12pt Paragraph

No! As we discussed on the classes, we need both technical and organizational controls. Firewalls and encryption will help but training team members and clear policies to stop phishing and insider risks.

Technology alone will not be able to fix human mistakes on this case!

p 45 words

Question 6 7 pts

Can cyber-security methods be too strict? Please explain your answer.

Edit View Insert Format Tools Table

12pt Paragraph

Yes, methods that are too restrictive will likely block users or make them find workarounds, like writing passwords on paper

writing passwords on paper.

The security approach should balance the protection with usability/experience.

p 30 words

Question 7 3 pts

Which of the following is NOT a good technical solution:

- Firewalls
- Virus scanners
- User training
- Password rules
- Screensavers with timeouts

Question 8 7 pts

Do unknown devices in a network create a security threat? Please explain your answer.

Edit View Insert Format Tools Table

12pt Paragraph

Yes, because they could be an infected system!

In that case, they would bypass monitoring and be able to access the system's back door for malicious actors to infiltrate and move freely within the network environment.

p 36 words

Question 9 7 pts

Does a very strict password rule (e.g., a password of more than 10 characters with three non-characters, and two numbers) create a secure environment? Please explain your answer.

Edit View Insert Format Tools Table

12pt Paragraph

Not necessarily, because if the rules are too complex, users could reuse their passwords or even write passwords down, creating new risks.

My understanding is that to use MFA and password managers are the best scenario.

p 36 words

Question 10 3 pts

Please select all the tasks that you think are required for secure operations.

- [x] Creating sufficient rules and policies.
- [x] Doing as much as possible within technical and monetary constraints to secure your systems.
- [x] Performing continuous risk assessments.
- [x] Using an information security management system.
- [ ] Documenting as little as possible, as documentation creates risks.

- [x] Constantly checking the applicability and feasibility of the methods used.
- [ ] Not informing users of changes.
- [ ] Applying patches or security upgrades to the systems as soon as they appear and without changing the management processes.
- [ ] Minimising consultations with the business side of the enterprise.

Question 11 7 pts

Does a secure system design need to involve the user?

Edit View Insert Format Tools Table

12pt Paragraph

Yes, it is always important to validate and map usage cases.

If we ignore their input, they'll bypass controls or even use unsafe shortcuts.

The secure designs needs to be usable and supported by natural human behaviour.

p 37 words

Question 12 7 pts

Provide at least two reasons why technical security systems need to change over time.

Edit View Insert Format Tools Table

12pt Paragraph

I understand that this is a never ending field! Threats evolve, new vulnerabilities appear and technology gets old.

Updating tools and processes keep the defense relevant and effective.

p 28 words

Question 13 3 pts

Which of the following statements are true about secure software development?

- [x] It helps to create less vulnerable applications.
- [ ] It creates unnecessary overheads.
- [ ] It can be achieved without proper guidelines.
- [x] It cannot be achieved by untrained coders.
- [x] Some development environments are safer than others.

Question 14 7 pts

Is secure software development faster than just programming without any guidelines? If not, explain why.

Edit View Insert Format Tools Table

12pt Paragraph

No, it will definitely take longer upfront for writing tests, assessing risks, involving users on the stages... but it will become faster long-term because it will avoid expensive fixes, downtime and patching!

p 32 words

Question 15 7 pts

Provide two reasons why secure software design is often overlooked?

Edit View Insert Format Tools Table

12pt Paragraph

1) Pressure to deliver fast - short deadlines will make security seen as a slowing down factor!

2) Lack of awareness or training among developers

p 24 words

Question 16 7 pts

Are some computer languages more secure than others? If so, why.

Edit View Insert Format Tools Table

12pt Paragraph

Yes! Languages with memory management and strong typing (Java, Python, Rust, Typescript) are safer!

While low-level ones like C/C++ that allow buffer overflows, if not coded carefully, can be dangerously unsecure!

It is also important to mention recent cases of these No-Code platforms like lovable, replit, base44 and bolt AI vulnerability cases by exposing secure credentials that users 'sent' with them on conversations to build their 'vibe coded' projects.

p

72 words

Saved at 12:03 Submit Quiz

TORRENS UNIVERSITY AUSTRALIA