BSBXCS401

Maintain security of digital devices

Assessment 1 of 3

Short Answer Questions

Version 1

Assessment Instructions

Task overview

This assessment task is divided into ten (10) questions. Read each question carefully before typing your response in the space provided.

Additional resources and supporting documents

To complete this assessment, you will need:

- Learning Resources
- CBSA Information Technology Policy & Procedure

Assessment Information

Submission

You are entitled to three (3) attempts to complete this assessment satisfactorily. Incomplete assessments will not be marked and will count as one of your three attempts.

All questions must be responded to correctly to be assessed as satisfactory for this assessment.

Answers must be typed into the space provided and submitted electronically via the LMS. Hand-written assessments will not be accepted unless previously arranged with your assessor.

Reasonable adjustment

Students may request a reasonable adjustment for assessment tasks.

Reasonable adjustment usually involves varying:

- the processes for conducting the assessment (e.g. allowing additional time)
- the evidence gathering techniques (e.g. oral rather than written questioning, use of a scribe, modifications to equipment)

However, the evidence collected must allow the student to demonstrate all requirements of the unit.

Refer to the Student Handbook or contact your Trainer for further information.

Please consider the environment before printing this assessment.

Question 1

Describe five (5) technology-based external party security risks and explain at least one method for mitigating each risk.

Assessor instructions: Students must describe five (5) technology-based external party security risks and explain at least one method for mitigating each risk. Students must include any five of the seven provided in the sample answer below.

Technology-based external party security risks	**Description and Method for mitigating each risk** (Approximate word count: 70 - 150 words/risk)
<<Insert your response here>> *Malware/viruses/Trojan/worm*	<<Insert your response here>> – *Malware (short for malevolent software) is any computer code written with malicious intent – such as stealing data, comprising data, and locking computer systems as is the case in Ransomware.* *A virus is a form of malware, but the virus is designed to replicate from computer to computer and typically is destructive rather than providing a mechanism.* *The term 'trojan' refers to software that masquerades and loads a virus into a computer system.* *A worm is a type of virus that seeks out and finds weaknesses in your computer's security system. It can steal sensitive information, install software or code that allows a user to access files in the future, or it can corrupt files.* – *Mitigation method: All digital devices should be loaded with a reputable anti-malware software package that is regularly updated with the latest library of emerging malware. Importantly, users of these devices need to be trained to:* – *understand how the software works* – *not to interfere or impede the anti-malware software operation* – *and if automatic reporting is not enabled, contact IT support staff if the anti-malware software reports the interception of malware.*
<<Insert your response here>> *Phishing*	<<Insert your response here>> – *Typically received as an email, phishing involves a user being tricked into providing personal details such as banking and login details. This is done by pretending to be a recognised authority, such as a bank, and requesting a user login with a provided URL. The URL will appear to be related to the bank, but in fact, it is a fictitious and fraudulent website. When the user enters their real information, the actors behind the phishing quickly log on to the real bank online to steal. This can be limited by online account users setting low limits for transfers except momentarily as the need to transfer and using two-factor authentication on logins.* – *Mitigation method: Having anti-malware software installed on the device will help intercept the code using email/websites as a*

	vector that is malicious. While the software will be effective, user training is required to: – *inform users of why and how a virus, worm, etc., can be loaded over an email to a receiving digital device* – *train users not to open suspicious emails from untrusted sources* – *visit non-business-related websites with business equipment – in effect, personal web browsing is prohibited.*
<<Insert your response here>> *Man in the Middle attack*	<<Insert your response here>> – *The Man in the Middle [MITM] attack vector uses public Wi-Fi. When a mobile digital device connects to the Wi-Fi, traffic of the digital device is recorded for later exploitation. Often, the actors behind the fraud are the ones offering the free Wi-Fi.* – *Mitigation method: The remedy for this vector requires user discipline to never:* – *use USB charging ports in public spaces for business digital devices* – *use public Wi-Fi and always use 4G/5G connectivity when outside the business network.*
<<Insert your response here>> *Distributed Denial-of-Service [DDoS]*	<<Insert your response here>> – *A Distributed Denial-of-Service [DDoS] attack is a deliberate flooding of a computer network to make legitimate access impossible as the web server cannot process the volume of requests.* – *Mitigation method: A web server is designed to 'listen' on a port for web traffic. In effect, a DDOS attack can always be made. There are 'flavours' of DDOS attacks; some target the webserver passing traffic to back-end systems, and some target the application servers themselves. They, in effect, seek to overwhelm legitimate requests for service. The response to DDOS attacks is two-fold:* – *Deploy a webserver with network monitoring capability to detect unusual traffic, block traffic from that source and continue to process. When very large DDOS attacks are made, the buffer of a web server may simply 'flood' and cause the webserver to fail. Of note, unless a small business has significance to sophisticated Black hats, a massive attack is unlikely. Large businesses and businesses with public profiles should consider placing specialised network devices in front of their webserver to cater for such DDOS attacks.* – *More expensive web hosting from large data centres may offer DDOS protection in their service delivery.* – *In the event of a DDOS attack, intervention to track, trace and report the event to Australian cyber security agencies [such as the ACCC and the Australian Cyber Security Centre].*

<<Insert your response here>> *Zero-day exploit*	<<Insert your response here>> – *It is possible that Blackhats discover breaches before gaps are identified by software developers. A zero-day exploit is an exploit to access a computer network using a method that no patch has yet been developed.* – *Mitigation method: The only effective way to manage the occurrence of a Zero Day exploit on digital devices is to remain current with all software patches and to actively research and network with the software suppliers and the broader cyber-crime community. The role in a business managing cyber security requires detailed and regular research to react quickly to a new exploit as soon as it is identified. Importantly, being one patch behind the current patch is an effective way to:* – *Not fall behind in patches so that in the event of a Zero Day exploit, there will not be considerable change/outages to operations in the business as multiple patches are applied.* – *Not leap at the latest patch as soon as it arrives. New patches have been known to contain bugs as well as new opportunities for exploits.*
<<Insert your response here>> *SQL injection*	<<Insert your response here>> – *SQL stands for Structured Query Language and is the code format for making enquiries – from databases. An SQL injection posts a query to the database directly – rather than through security layers – to copy or reveal sensitive corporate information. It can be performed on the business' website using common SQL URL substitution.* – *Mitigation method: SQL Injection is a common attack method. Software that acts to vet SQL exploits will block SQL injection attempts before any data is stolen. Hackers using this exploit rely on uninformed and/or poor cyber security management to succeed. It may be challenging to prevent the injection of SQL in website code; however, it is possible to build extra layers into the website code called 'SQL parameters'. The parameters are values that are added to an SQL query at the time of execution in a controlled manner. This prevents the program from logging the input in a way that can be exploited. This prevents the application code from being input directly and helps to 'sanitise' inputs while the web administer goes in to remove malicious code*
<<Insert your response here>> *Domain Name System (DNS) tunnelling*	<<Insert your response here>> – *Definition: This is a complex exploit that relies on the nature of computer networks. A DNS tunnel will reroute the user to a malicious web address, and from there, the hacker can input or gather data from the computer at will. In networking, DNS requests must be allowed to pass from one server to the next. The exploit uses DNS data wrapped around malicious commands to 'tunnel' into another network.* – *Mitigation method: A DNS firewall can be placed between a business' firewall and the internet as an additional layer of security. This DNS firewall blocks calls from suspicious web*

	domains to the business' web-facing applications. It is possible to whitelist domains so that only the domains listed can see traffic to and from the business (synchronous). In effect, unless a domain name is in the list, users on the business network cannot access a website looking to DNS tunnel. Importantly, user education to avoid suspicious or non-business-related websites is the primary defence.

Question 2

Describe three (3) physical-based external party security risks and at least one method for mitigating each risk.

Assessor instructions: Students must describe three (3) physical-based external party security risks and at least one method for mitigating each risk. Students must include any three of the four provided in the sample answer below.

Technology-based external party security risks	Description and Method for mitigating each risk (Approximate word count: 50 – 70 words/risk)
<<Insert your response here>> *USB plant*	<<Insert your response here>> – *Leaving USB sticks with malware around company carparks is a tool that hackers use to gain access to networks.* – *Mitigation method: Business policy must include that any staff finding USB sticks/portable hard drives or other devices should hand them to the business' IT support personnel. IT staff will make use of a test PC that is unplugged from the internet/business network to examine any device.*
<<Insert your response here>> *Internet cabling accessible to the outside*	<<Insert your response here>> – *The 'plumbing' of a business' internet should be hidden and guarded. Access to cabling allows a hacker to splice a cable to connect directly to a business' network.* – *Mitigation method: Security of server rooms, network racks and switches should be such that only authorised personnel can access the space for authorised work. As should all network cabling into the business be hidden/protected.*
<<Insert your response here>> *Tailgating*	<<Insert your response here>> – *Literally walking into an office with actual employees, hackers have been known to access facilities in order to gain access to networks and introduce malware by plugging in an external drive or working on a computer from within the office itself.* – *Mitigation method: All staff should be made aware of the practice of tailgating and be watchful.*
<<Insert your response here>>	<<Insert your response here>>

Over the shoulder	– *Watching keystrokes as they are entered, passwords can be recorded by hackers to use for later access.* – *Mitigation method: Staff training should include awareness that screens can be read 'over the shoulder' and confidential information should not be read in public places (such as on planes and in cafes).*

Question 3

IT risk assessment and management methodology is the process of identifying and analysing potential threats to your IT systems. Quantitative and qualitative risk analysis are the two prevailing methodologies for assessing and managing IT risk. Research and explain what is meant by Qualitative and Quantitative IT risk assessment and management.

(Approximate word count: 100 – 120 words)

Assessor instructions: Students must research and explain what is meant by Qualitative and Quantitative IT risk assessment and management. Their wording may vary, but their responses must reflect the content in the sample answer provided below.

<<Insert your response here>>

Qualitative IT risk assessment:

- *uses financial amounts and gives anticipated losses linked with a certain risk*
- *based on asset value, frequency of risk incidence*
- *probability of certain loss*
- *replies on solid data around probability and cost estimates on IT-related risk*
- *management includes tracking issues as reported by IT management systems*
- *management requires data collection at periodic intervals.*

Quantitative IT risk assessment:

- *opinion-based*
- *relies on judgment to identify the probability of risk*
- *uses a scale to measure risk: low (unlikely), medium (possible) or high (likely) to occur*
- *management requires scheduling updates, regular feedback from staff (users)*
- *management requires action based on feedback received from surveys or responses from staff.*

Question 4

Scenario

You work for a small company with eight employees. The company utilises patented technologies to deliver services to its clients and relies heavily on its digital assets and devices.

Your boss's friend has recently become the victim of a phishing scam, and as a result, your boss has become more aware and concerned about the cyber security risks to his company. He has come to work today feeling stressed and anxious about the possibility that someone might try to hack and exploit the company. He has asked you to develop a strategy and a company policy that can address some common cybersecurity threats that the company might face.

Describe a best practice strategy relating to the points in the table below that can be included in a company policy.

Assessor instructions: Students must describe a best practice strategy relating to the points in the table below that can be included in a company policy. Their wording may vary, but their responses must reflect the content in the sample answer provided below.

Point	Best Practice Strategy
Password management [Approximate word count: 80 – 100 words]	<<Insert your response here>> *Enforce a policy of using complex passwords that stops the use of easily guessed words. Further, numbers and escape characters [e.g.! or + etc.] must be included at least once. Password policy should also stop the re-use of passwords for a set time [e.g. 12 months] and require passwords to be changed automatically [e.g. three monthly]. Such a policy can be implemented using security network administration software. On Windows, the group policy editor can create all these conditions. [Note that in business running SSO – Single Sign On – the admin burden on users is reduced as they manage a single password only].*
Use of anti-virus software [Approximate word count: 20 – 30 words]	<<Insert your response here>> *All digital devices should be loaded with a reputable and up-to-date anti-malware software package regularly updated with the latest library of emerging malware.*
Virtual Private Network use on public Wi-Fi [Approximate word count: 30 – 40 words]	<<Insert your response here>> *The policy should ensure that VPN is always used when connecting remotely to the business and, under no circumstances, use computer support that is not provided by the business. All requests by third parties for remote access should be refused.*
Router settings [Approximate word count: 20 – 30 words]	<<Insert your response here>> *Routers should be configured with strong passwords, use Wi-Fi Protected Access (WPA), disable remote administration, enable a firewall and operate on a closed network.*
Two-factor authentication [Approximate word count: 40 – 50 words]	<<Insert your response here>> *All mobile devices should use two-factor identification (2FA). Local Area Network devices are cable-attached and within the firewall. It may be that only stakeholders with access to sensitive information are required to access systems using 2FA or multi-factor authentication (MFA).*
Encryption [Approximate word count: 60 – 70 words]	<<Insert your response here>> *All data coming into and out of the office network system needs to be encrypted so that it cannot be intercepted and exploited. Files and*

	databases should be encrypted to ensure that any breach of the security system doesn't give away the contents of the files, which remain encrypted and illegible. Encrypted files and databases are protected by complex passwords and two-factor authentication methods.
Patching software applications [Approximate word count: 30 – 40 words]	<<Insert your response here>> *Regular and planned patching of digital devices should always be undertaken. For user assets such as phones and laptops, patches should be auto-configured to install outside normal business hours.*
Data in transit [Approximate word count: 50 – 60 words]	<<Insert your response here>> *Any documents sent out of the office network should be encrypted with a password required to open them, and data transfers should use File Transfer Protocol Secure [FTPS] using a service-providing validation. Further, always consider sensitive documents if sending by fax or secure courier is a safer alternative.*
Data in third-party applications [Approximate word count: 40 – 50 words]	<<Insert your response here>> *When dealing with digitally sensitive information within these applications, encryption becomes paramount. All data should be encrypted, and access to it should require a secure and unique password. Additionally, the use of applications that implement robust security protocols, such as end-to-end encryption, should be prioritised.*

Question 5

Given that your company uses several mobile devices for its operations, like mobile phones, tablets and laptops, consider what a mobile device policy might look like. List all of the appropriate actions relating to the use of mobile devices that you understand to be important. At a minimum, you must include actions relating to:

- lost or stolen devices,
- storage of information,
- how and where the device can be used and how to connect to the internet using the device.

[Approximate word count: 120 – 150 words]

Assessor instructions: Students must list all of the appropriate actions relating to the use of mobile devices that they understand to be important. At a minimum, they must include actions relating to lost or stolen devices, storage of information, how and where the device can be used and how to connect to the internet using the device. Their wording may vary, but their responses must refer to the points in the sample answer provided below.

<<Insert your response here>> ▪ *in the event a device is lost, report the loss immediately to the business* ▪ *never store data on the device or use USB/portable data storage* ▪ *restriction on installing applications and other digital tools on the device* ▪ *report any unusual activity on your device to the business* ▪ *always allow the resident anti-malware to operate as it requires*

- *always use the company VPN when logging on outside the network*
- *the device is only to be used for business purposes*
- *ensure you accept all requests to patch the device when they occur*
- *ensure you change your password when requested to do so*
- *only use 4g/5g when outside the business network and never charge the device using public USB charging*
- *protect your screen from third-party viewing when working with business data.*

Question 6

Explain what a gap analysis is in terms of cyber security and how it might help to monitor the performance of cyber security protocol. Indicate the tools and techniques that can be used for gap analysis.

[Approximate word count: 150 – 200 words]

Assessor instructions: Students must explain what a gap analysis is in terms of cyber security and how it might help to monitor the performance of cyber security protocol and indicate the tools and techniques that can be used for gap analysis.

Their wording may vary, but their responses must reflect the content in the sample answer provided below.

<<Insert your response here>>

Gap analysis looks at benchmark data before any protocols are implemented. It helps to assess the performance level and threats to the system at regular intervals. Gap analysis provides a baseline to measure how well the recommended and/or implemented protocols are performing against cyber security threats. This provides the basis to monitor the cyber security of the organisation/company. Since cyber security threats are ongoing, it is useful to monitor the systems in place to ensure that as threats evolve, so does the response.

Tools and techniques must include the following:

- *adoption of information security standards [ISO or NIST, for example]*
- *evaluation of how people use their devices*
- *what processes are in place for password protection, two-factor authentication and encryption*
- *gather data from servers, networks, anti-malware software or any other source of data in the system to understand network traffic, storage of information, security breaches and possible threats*
- *look at all the cyber security protocols in place and assess each one against the industry standard*
- *there are external tools available that can help organise this information and assess cyber security in real-time, therefore giving greater insight into gap analysis.*

Question 7

Referring to the **CBSA Information Technology Policy & Procedure**, briefly describe in your own words what the policy says about stored data. Then, explain why the company has included this as part of its information technology policy and procedure.

[Approximate word count: 80 – 100 words]

Assessor instructions: Students must describe in their own words what the CBSA Information Technology Policy & Procedures says about stored data. Then, explain why the company has included this as part of its information technology policy and procedure.

Their wording may vary, but their responses must reflect the content in the sample answer provided below.

<<Insert your response here>>

As per CBSA Information Technology policy and procedure, all information must be stored using the company's cloud-based file management system. Files cannot be stored on local or portable drives. The reasons for this may include:

- *Cloud storage is encrypted and protected at a high level.*
- *Could storage servers act as a reliable backup in case a physical device is lost, stolen or corrupted.*
- *If a device is stolen or hacked into, sensitive data that is stored in the cloud will be inaccessible to the hacker.*

Question 8

List two (2) sources on the internet that can be used to monitor the latest developments in digital security.

For each, indicate the type of information that you can gather from the website you've chosen.

[Approximate word count: 70 – 90 words]

Assessor instructions: Students must list two sources on the internet that can be used to monitor the latest developments in digital security. For each, they must indicate the type of information that you can gather from the website you've chosen.

Students must choose two of the three options provided in the sample answer provided below.

<<Insert your response here>>

- *FireEye gives us information of country and industry-specific information:*
  - *indicates the source of cyber security attacks*
  - *indicates where the attacks are aimed (destinations)*
  - *indicates the number of attacks in real-time.*

  https://www.fireeye.com/cyber-map/threat-map.html
- *Real-time global penetration statistics:*

  Kaspersky

  https://cybermap.kaspersky.com/
  - *provides data on cyber security attacks worldwide and country-specific*
  - *provides a list of the latest malware detected*
  - *provides real-time statistics on cyber security threats.*

- *Data analysis of distributed denial-of-service (DDoS) attacks:*

  Akamai

  https://www.akamai.com/internet-station

  - *provides details on total internet traffic*
  - *indicates internet traffic and cause of outages*
  - *identifies trends in internet traffic and offers predictions on where threats originate and the type of threat.*

Question 9

Review the following bandwidth data for the last week as recorded on a company web server and answer the questions below. All numbers are in megabytes:

	12 a.m. – 6 a.m.	6 a.m. – 9 a.m.	9 a.m. – 12 p.m.	12 p.m. – 3 p.m.	3 p.m. – 6 p.m.	6 p.m. – 12 a.m.
M	100	80	400	525	530	120
T	90	100	450	400	500	110
W	110	90	500	400	600	80
T	80	70	1600	200	500	90
F	95	90	375	550	600	70
S	80	90	1800	No data recorded	80	120
S	80	65	50	70	60	80

The student's responses must match the numbers provided in the sample answers below:

a) Calculate the average bandwidth for each day:

- Monday: *<<Insert your response here>> 292.5*
- Tuesday: <<Insert your response here>> *275*
- Wednesday: <<Insert your response here>> *296.67*
- Thursday: <<Insert your response here>> *423.34*
- Friday*:* *<<Insert your response here>>296.67*
- Saturday: <<Insert your response here>> *361.67*
- Sunday: <<Insert your response here>> *67.5*

b) Calculate the average bandwidth for workdays between 9 a.m. and 6 p.m.:

- Monday: <<Insert your response here>> *485*
- Tuesday: <<Insert your response here>> *450*
- Wednesday: <<Insert your response here>> *500*

- Thursday: <<Insert your response here>> *766.67*
- Friday*: <<Insert your response here>> 508.33*

c) Calculate average bandwidth for times outside of office hours (weekends, before 9 a.m. and after 6 p.m.):

- Monday: <<Insert your response here>> *100*
- Tuesday: <<Insert your response here>> *100*
- Wednesday: <<Insert your response here>> *93.33*
- Thursday: <<Insert your response here>> *80*
- Friday*: <<Insert your response here>> 101.67*

d) Compare the data and answer the following questions:

1. Are there standout bandwidth variations over the last week? If so, calculate the percentage increase over that day when compared to the average during the same time period.

<<Insert your response here>>

The student's response must include:

Standout bandwidth usage is on Thursday during work hours. Average for the period = 542. Percentage difference is 41.452%

2. What does this tell you about a potential breach in the server systems?

<<Insert your response here>>

The student's response must include the following:

This is a fairly large increase in bandwidth, and it indicates that a breach has happened due to analysis of the bandwidth for the days and times. The server is most vulnerable during work hours, probably because this is when there is high traffic anyway, and the attacker would have hoped to disguise their efforts in normal workday traffic on the servers.

Question 10

List and explain three (3) fundamental aspects of two-factor authentication in the space provided below.

(Approximate word count: 200 -300 words)

Assessor instructions: Students must list and explain the fundamentals of two-factor authentication in the space provided below. Students' responses can include any three of the five provided in the sample answer provided below.

Two–Factor Authentication
Two-factor authentication ensures that, aside from a username and password, a user must enter a code sent to a trusted second device. This is typically a mobile phone. An application can be configured to require 2FA when accepting a login. For additional security, multifactor authentication (MFA) requires two or more additional security checks aside from a username and password. Fundamental aspects of Two-Factor Authentication (2FA) with explanations: 1. Something You Know (Knowledge Factor):

- This is typically a password or a Personal Identification Number (PIN). It's the foundational factor in many authentication systems. The idea is that only the authorised user should know this information. However, passwords alone are vulnerable to various attacks, such as brute force, phishing, or credential stuffing. 2FA adds an extra layer of security by requiring a second factor.

2. Something You Have (Possession Factor):
    - This involves a physical item that the user possesses, such as a smartphone, security token, or smart card. The possession factor adds an extra layer of security because even if someone knows your password, they would also need to have the physical device to complete the authentication process. One common implementation is the generation of one-time codes on a device.
3. Something You Are (Inherence Factor - Biometrics):
    - Biometric authentication involves using unique physical or behavioral characteristics for identity verification. Common biometric factors include fingerprints, retina scans, voice recognition, facial recognition, or even behavioral patterns like typing speed. Biometrics provide a high level of security because they are difficult to forge or replicate, adding an additional layer of certainty to the authentication process.
4. Multi-Channel Authentication:
    - This involves using different communication channels for the two authentication factors. For example, a user might enter their password online (something they know) and receive a one-time code via text message on their smartphone (something they have). This approach enhances security by mitigating risks associated with attacks that might compromise a single communication channel.
5. Time-Based Authentication:
    - Many 2FA systems use time-based codes, where the one-time code generated by the possession factor (like a smartphone app or security token) changes at regular intervals. These codes are valid only for a short period (usually 30 seconds to a few minutes). This time-based aspect adds an additional layer of security because even if someone intercepts a code, it quickly becomes invalid, reducing the window of opportunity for unauthorized access.

Assessment checklist:

Students must have completed all questions within this assessment before submitting. This includes:

1	Ten (10) short answer questions to be completed in the spaces provided.	□

✓

Congratulations you have reached the end of Assessment 1!