Cyber Security

Section A: Activity Booklet

Cyber Security Threats, System Vulnerabilities & Security Protection Methods

Unit 2 | Pearson BTEC Level 3 Information Technology

New College Bradford

About This Booklet

This activity booklet covers all topics from Section A of the Unit 2: Cyber Security and Incident Management specification. It is designed to help you revise and check your understanding of cyber security threats, system vulnerabilities, legal responsibilities, and security protection methods.

How to Use This Booklet

0. Work through the activities in order - they follow the specification sequence.
1. Each activity has a question type icon so you know what is expected:
    - Multiple Choice Questions (MCQ) - select the correct answer(s).
    - Sort/Match - draw lines or reorder items to match pairs.
    - Short Answer - write 2-4 sentences to explain your answer.
    - Long Answer - write a detailed paragraph or essay-style response.
2. Every question includes a helpful website link - use this if you are stuck!
3. You can complete this booklet digitally or print it and write your answers.

Student Details

Name:

Tutor Group:

Date:

Contents

Right-click and select "Update Field" to refresh page numbers

A1: Cyber Security Threats

Activity 1 [Multiple Choice] Specification: A1.1.1 & A1.1.2

1. Which of the following is an example of DELIBERATE employee sabotage?

A. An employee accidentally deletes important files while cleaning their desktop

B. An employee intentionally installs unauthorised software to steal customer data

C. A power failure causes loss of unsaved work

D. An employee spills coffee on a server due to clumsiness

Your answer: _____

2. Which of these would be classed as ACCIDENTAL damage to an organisation's IT systems? (Select all that apply)

A. A fire caused by faulty electrical wiring

B. A flood from a burst water pipe

C. Intentional destruction of equipment by a disgruntled employee

D. Data loss due to an unexpected power outage

Your answer: _____

→ Helpful resource: National Cyber Security Centre - Insider Threats

Activity 2 [Short Answer] Specification: A1.1.3 & A1.1.4

3. Describe TWO examples of weak cyber security measures or unsafe practices that could put an organisation at risk. For each example, explain how it could lead to a security incident.

Write your answer here:

→ Helpful resource: UK Government Security Policy Framework

Activity 3 [Sort/Match] Specification: A1.2.1

4. Match each type of malware to its correct description. Draw a line between each pair.

Virus	Self-replicating program that spreads independently across networks
Worm	Malicious software that attaches itself to legitimate programs/files
Trojan	Software that secretly monitors user activity and steals information
Spyware	Malware disguised as legitimate software to trick users
Ransomware	Encrypts files and demands payment for their release

Write your answer here:

→ Helpful resource: CrowdStrike - Types of Malware

Activity 4 [Multiple Choice] Specification: A1.2.2

5. A hacktivist group launches a DDoS attack against a government website to protest a new policy. What type of hacking is this?

A. Commercial hacking

B. Government espionage

C. Hacktivism - politically motivated hacking

D. Individual identity theft

Your answer: _____

6. State TWO common techniques used by hackers to gain unauthorised access to systems.

Write your answer here:

→ Helpful resource: Motivations of a Hacker - Focus Group

Activity 5 [Long Answer] Specification: A1.2.3

7. Explain the difference between sabotage targeting commercial organisations and sabotage targeting government infrastructure. For each, give ONE example of a potential impact and ONE motive the attacker might have.

Write your answer here:

→ Helpful resource: National Security Bill Factsheet - Sabotage

Activity 6 [Sort/Match] Specification: A1.2.4

8. Match each social engineering technique to the correct description.

Phishing	Fraudulent text messages sent to trick victims
Smishing	Emails pretending to be from trusted sources to steal credentials
Pretexting	Leaving infected USB drives in public places for victims to find
Baiting	Creating a fabricated scenario to gain victim's trust
Tailgating	Following someone into a secure area without authorisation

Write your answer here:

→ Helpful resource: CrowdStrike - Social Engineering Attacks

Activity 7 [Short Answer] Specification: A1.2.5

9. Describe THREE physical security breaches that could compromise an organisation's cyber security. For each, suggest ONE countermeasure.

Write your answer here:

→ Helpful resource: Physical Security & Cybersecurity

Activity 8 [Multiple Choice] Specification: A1.3

10. A hospital suffers a ransomware attack and cannot access patient records for 3 days. What type of loss is this primarily an example of?

A. Financial loss only

B. Operational loss - disruption to normal business operations

C. Reputational loss only

D. Intellectual property loss

Your answer: _____

11. After a data breach, a company loses customers and their share price drops. This is primarily an example of:

A. Operational loss

B. Financial loss

C. Reputational loss

D. All of the above

Your answer: _____

→ Helpful resource: Colonial Pipeline Ransomware Case Study

Activity 9 [Long Answer] Specification: A1.3

12. A small online retailer experiences a data breach where 50,000 customer records are stolen. Describe FOUR different types of loss the company could experience as a result of this incident, giving specific examples for each.

Write your answer here:

→ Helpful resource: WEF - Financial Impact of Cyber Threats

Activity 10 [Sort/Match] Specification: A1.4

13. Match each organisation to its correct description and country.

NCSC	UK government organisation providing cyber security guidance	United Kingdom
NIST	Develops standards including the Cybersecurity Framework	United States
OWASP	Community project focused on web application security	International

Write your answer here:

14. What is the OWASP Top 10 and why is it important for developers and security professionals?

Write your answer here:

→ Helpful resource: NCSC UK

→ Helpful resource: NIST Cybersecurity Framework

→ Helpful resource: OWASP Top 10

A2: System Vulnerabilities

Activity 11 [Short Answer] Specification: A2.1.1

15. Explain what is meant by a 'network vulnerability'. Give TWO specific examples of network vulnerabilities and explain how each could be exploited by an attacker.

Write your answer here:

→ Helpful resource: Heimdal Security - Common Network Vulnerabilities

Activity 12 [Multiple Choice] Specification: A2.1.2

16. Which of the following is an example of an organisational vulnerability?

A. Outdated firewall firmware

B. Weak password policies and insufficient staff training

C. Unpatched operating system

D. Open network ports

Your answer: _____

17. Explain why poor security culture within an organisation is a significant vulnerability.

Write your answer here:

→ Helpful resource: CISA - Weak Security Controls Advisory

Activity 13 [Short Answer] Specification: A2.1.3

18. What is a 'zero-day exploit'? Explain how it differs from a vulnerability for which a patch is already available.

Write your answer here:

19. Describe TWO risks associated with using unpatched or outdated software.

Write your answer here:

→ Helpful resource: Splashtop - Risks of Unpatched Software

Activity 14 [Multiple Choice] Specification: A2.1.4

20. Why might an outdated operating system pose a security risk?

A. It may no longer receive security patches from the vendor

B. It runs too slowly for modern applications

C. It uses too much disk space

D. It cannot connect to the internet

Your answer: _____

21. Give ONE vulnerability associated with using the Command Line Interface (CLI) compared to a Graphical User Interface (GUI).

Write your answer here:

→ Helpful resource: Sternum - OS Vulnerabilities

Activity 15 [Long Answer] Specification: A2.1.5

22. Many mobile devices rely on Original Equipment Manufacturers (OEMs) to provide system software updates. Discuss the security risks this creates, including what happens when a device reaches 'end-of-life' support. Suggest TWO ways organisations can manage these risks.

Write your answer here:

→ Helpful resource: Android Authority - Phone Update Policies

Activity 16 [Short Answer] Specification: A2.1.6

23. Identify THREE physical vulnerabilities that could expose an organisation's IT systems to security risks. For each, suggest a practical countermeasure.

Write your answer here:

→ Helpful resource: Charter Global - Physical Security Threats

Activity 17 [Multiple Choice] Specification: A2.1.7

24. Which of the following user behaviours creates a system vulnerability? (Select all that apply)

A. Sharing passwords with colleagues

B. Leaving a workstation unlocked when away

C. Clicking on links in unexpected emails

D. Regularly updating passwords every 90 days

Your answer: _____

25. Explain the importance of security awareness training in reducing vulnerabilities caused by human behaviour.

Write your answer here:

→ Helpful resource: APMG - Security Awareness in 5 Minutes

Activity 18 [Long Answer] Specification: A2.1.8

26. Discuss the security implications of cloud computing and Internet of Things (IoT) devices for organisations. Your answer should include: TWO risks associated with cloud computing, TWO risks associated with IoT devices, and TWO strategies to mitigate these risks.

Write your answer here:

→ Helpful resource: Fortinet - IoT Device Vulnerabilities

Activity 19 [Short Answer] Specification: A2.2

27. Name TWO reliable sources where IT professionals can find up-to-date information about known hardware and software vulnerabilities. For each source, explain what type of information it provides.

Write your answer here:

→ Helpful resource: NIST National Vulnerability Database

→ Helpful resource: CVE - Common Vulnerabilities and Exposures

Activity 20 [Sort/Match] Specification: A2.3

28. Match each attack vector to its correct description.

Wireless eavesdropping	Intercepting data transmitted over Wi-Fi or Bluetooth
Evil Twin attack	Setting up a fake Wi-Fi access point to steal credentials
Packet sniffing	Capturing and analysing data packets on a network connection
Router misconfiguration	Exploiting default or weak settings on network equipment

Write your answer here:

29. Explain why an internal network access device (such as a router or switch) can be a significant attack vector if not properly secured.

Write your answer here:

→ Helpful resource: Codecademy - Wireless Attacks

Activity 21 [Multiple Choice] Specification: A2.4

30. Which tool would be most appropriate for identifying open ports on a network?

A. Antivirus software

B. Port scanner

C. Firewall

D. VPN

Your answer: _____

31. What is the purpose of a network mapper tool?

A. To encrypt network traffic

B. To discover devices and create a visual map of the network topology

C. To block unauthorised access

D. To update software automatically

Your answer: _____

→ Helpful resource: Brightsec - Vulnerability Assessment Tools

Activity 22 [Short Answer] Specification: A2.5

32. Explain why organisations should use independent third-party reviews of their system and network designs before implementation. Include the concept of 'due diligence' in your answer.

Write your answer here:

→ Helpful resource: Pivot Point Security - Network Architecture Review

Activity 23 [Long Answer] Specification: A2.6

33. Explain what penetration testing is and how it differs from vulnerability scanning. Describe how penetration testing can be used to identify threats listed in the OWASP Top 10, giving at least TWO specific examples of tests that could be performed.

Write your answer here:

→ Helpful resource: StationX - OWASP Top 10 Penetration Testing

Activity 24 [Sort/Match] Specification: A2.7

34. Match each passive risk management strategy to its correct description.

Risk transfer	Deciding not to engage in a risky activity
Risk avoidance	Purchasing insurance to cover potential losses

Risk acceptance	Acknowledging a risk exists but taking no action to mitigate it
Risk mitigation	Taking active steps to reduce the likelihood or impact of a risk

Write your answer here:

35. Give ONE example of when an organisation might choose to ACCEPT a risk rather than transfer or avoid it.

Write your answer here:

→ Helpful resource: TWProject - Risk Response Strategies

A3: Legal Responsibilities

Activity 25 [Long Answer] Specification: A3.1, A3.2 & A3.3.1

36. The General Data Protection Regulation (GDPR) and the Computer Misuse Act 1990 are two key pieces of legislation affecting cyber security in the UK.

(a) Describe the main purpose of the GDPR.

Write your answer here:

(b) State TWO principles of the GDPR.

Write your answer here:

(c) Describe what the Computer Misuse Act 1990 makes illegal. Give TWO examples of offences under this Act.

Write your answer here:

(d) Explain why it is important for ALL organisations (not just large ones) to comply with GDPR.

Write your answer here:

→ Helpful resource: CMS Expert Guide - UK Data Protection Laws

→ Helpful resource: ICO - GDPR Guidance

Activity 26 [Multiple Choice] Specification: A3

37. Under GDPR, individuals have the right to:

A. Access their personal data held by an organisation

B. Request deletion of their personal data

C. Both A and B

D. Neither A nor B

Your answer: _____

38. Which of the following would be an offence under the Computer Misuse Act 1990?

A. Accidentally clicking on a phishing link

B. Gaining unauthorised access to a computer system

C. Using strong passwords on your own devices

D. Installing antivirus software on a work computer

Your answer: _____

→ Helpful resource: ICO - Data Protection Self Assessment

A4: Software and Hardware Security Measures

Activity 27 [Multiple Choice] Specification: A4.1.1

39. Which of the following is a biometric security measure?

A. Password protection

B. Fingerprint scanner

C. Security badge swipe

D. Locked doors

Your answer: _____

40. Name TWO other physical security measures (not biometric) that an organisation could use to protect its premises and equipment.

Write your answer here:

→ Helpful resource: HID Global - Physical Security Measures

Activity 28 [Short Answer] Specification: A4.1.2

41. Explain the difference between full, incremental, and differential backups. Include in your answer when each type would be most appropriate to use.

Write your answer here:

42. Describe the 3-2-1 backup rule and explain why it is considered best practice for data protection.

Write your answer here:

→ Helpful resource: Acronis - Backup Types Comparison

Activity 29 [Sort/Match] Specification: A4.1.3

43. Match each antivirus detection technique to its correct description.

Signature-based detection	Analyses behaviour patterns to identify suspicious activity
Heuristic analysis	Compares files against a database of known malware signatures
File integrity checking	Monitors files for unauthorised changes by comparing hash values
Sandboxing	Executes suspicious code in an isolated environment to observe behaviour

Write your answer here:

→ Helpful resource: Comodo - How Antivirus Works

Activity 30 [Multiple Choice] Specification: A4.1.4

44. What is the main difference between a hardware firewall and a software firewall?

A. Hardware firewalls are free; software firewalls cost money

B. Hardware firewalls protect an entire network; software firewalls protect individual devices

C. Software firewalls are more secure than hardware firewalls

D. There is no difference between them

Your answer: _____

45. Which firewall filtering technique examines the state of active connections?

A. Packet filtering

B. Stateful inspection

C. Application layer filtering

D. MAC filtering

Your answer: _____

→ Helpful resource: Palo Alto - Types of Firewalls

Activity 31 [Short Answer] Specification: A4.1.5

46. Explain the THREE factors of authentication (something you know, have, and are). For each factor, give a practical example.

Write your answer here:

47. Why is Multi-Factor Authentication (MFA) more secure than using just a password? Explain with an example.

Write your answer here:

→ Helpful resource: NCSC - Authentication Methods

Activity 32 [Sort/Match] Specification: A4.1.6

48. Match each access control model to its correct description.

Discretionary Access Control (DAC)	Access based on user roles within the organisation
Role-Based Access Control (RBAC)	Owner of the resource decides who can access it
Mandatory Access Control (MAC)	Access controlled by system-wide security policies set by administrators
Rule-Based Access Control	Access determined by predefined rules and conditions

Write your answer here:

→ Helpful resource: Twingate - Access Control Models

Activity 33 [Multiple Choice] Specification: A4.1.7

49. What is the purpose of a Trusted Platform Module (TPM)?

A. To increase internet connection speed

B. To securely store cryptographic keys and authentication credentials

C. To display the desktop wallpaper

D. To manage printer connections

Your answer: _____

50. Give ONE benefit and ONE potential drawback of trusted computing.

Write your answer here:

→ Helpful resource: Trusted Computing Group - TPM Summary

Activity 34 [Short Answer] Specification: A4.1.8

51. Describe TWO technologies or methods that can help locate or secure lost or stolen devices. For each, explain how it works.

Write your answer here:

→ Helpful resource: Apple - Find My Device

Activity 35 [Multiple Choice] Specification: A4.1.9

52. Which of the following is a device-based security feature?

A. Screen timeout / auto-lock

B. Network firewall

C. Cloud backup

D. Email encryption

Your answer: _____

53. Explain why a memory wipe after multiple failed login attempts is an important security feature.

Write your answer here:

→ Helpful resource: Microsoft - Device Security Features

Activity 36 [Sort/Match] Specification: A4.2

54. Match each encryption type to its correct description and example.

Storage encryption	Protects data at rest on devices	Full-disk encryption (e.g., BitLocker)

Communications encryption	Protects data in transit between systems	TLS/SSL for web browsing (HTTPS)
End-to-end encryption	Only sender and recipient can read messages	WhatsApp, Signal messaging

Write your answer here:

→ Helpful resource: OWASP - Cryptographic Storage Cheat Sheet

→ Helpful resource: Cloudflare - End-to-End Encryption

Activity 37 [Short Answer] Specification: A4.3.1

55. Explain what MAC address filtering is and how it is used to secure wireless networks. Also explain why it should NOT be relied upon as the only security measure.

Write your answer here:

→ Helpful resource: Smallstep - MAC Filtering Won't Protect Wi-Fi

Activity 38 [Multiple Choice] Specification: A4.3.2

56. Which wireless encryption protocol is currently considered the most secure?

A. WEP

B. WPA

C. WPA2

D. WPA3

Your answer: _____

57. Why should Wi-Fi Protected Setup (WPS) be disabled on routers?

Write your answer here:

→ Helpful resource: Kaspersky - WEP vs WPA vs WPA2 vs WPA3

Activity 39 [Long Answer] Specification: A4.4

58. Explain the importance of building security into network and system design from the outset. Your answer should include:

- The principle of 'expecting attacks to happen and planning for them'
- Why systems should be designed to run with the fewest privileges necessary
- The risks of relying on 'security through obscurity'
- How following security standards (such as ISO 27000) helps

Write your answer here:

→ Helpful resource: Codecademy - Notable Breaches Case Studies

Well Done!

You have completed all Section A activities.

Check your answers using the resource links provided.