FIT1047 Introduction to computer systems, networks and security

Semester 2, 2025

Assignment 4 – Cybersecurity

Purpose	1. Students will analyse and discuss a recent vulnerability or cybersecurity attack. This demonstrates an understanding of related cybersecurity topics and the ability to research information on cybersecurity incidents. 2. Students will write a report on how a specified set of security controls is implemented in a medium-sized enterprise scenario. This report shows the understanding of various security controls in the departments and the ability to evaluate and explain their utilisation. 3. Students will examine the security of two or more apps in the same category on their mobile device, such as Entertainment, Shopping, Education, Messaging, Banking, Games, or Social Networks, showing an understanding of mobile security, privacy and ethical concerns. The assignment relates to Unit Learning Outcomes 5, 6, and 7.
Your tasks	Part 1: Your **weekly reflection** (Weeks 10 - 12) Part 2: Select ONE article from your assigned category. Utilise generative AI (ChatGPT) to analyse and discuss this recent vulnerability or cybersecurity attack. Additionally, provide your judgment to evaluate whether the analysis conducted by the generative AI is accurate and correct, as well as identify any gaps present in the analysis. Submit **presentation slides with video presentation** to present your findings regarding the selected vulnerability incident and the evaluation conducted by the generative AI. The instructions below include steps required in this task. Part 3: Provide **a report** demonstrating how a specific set of security controls is utilised within a medium-sized enterprise scenario. The instructions below include concrete questions that you should answer.

	Part 4: Select two or more mobile apps from the assigned category, analyse and demonstrate the security aspects of access control, data protection, app and system security, and communication. Provide **presentation slides with video presentation** that explain how to secure mobile devices from personal data, including access control, data protection, system security, and communication. The instructions below include steps required in this task. All files have to be submitted through Moodle.
Value	**30**% of your total marks for the unit: **9% for Part 2** **9% for Part 3** **12% for Part 4** The assignment is marked out of 30 marks.
Word Limit	See individual instructions
Due Date	11:55 PM, Monday 3 November 2025

Submission	• Via Moodle Assignment Submission.
	• **DRAFT** upload confirmation email from Turnitin is not a submission. You must click the submit button to accept the terms and conditions in Moodle. Note that **DRAFT submissions will not be assessed**.
	• Once the submission is confirmed, **any requests to revert it to DRAFT** for resubmission will NOT be accepted. Additionally, any submission **containing incorrect, corrupted, empty, or incorrect file type**s will not be assessed. Please review your submission carefully before confirming.
	• Turnitin and MOSS will be used for similarity checking of all submissions.
	• This is an individual assignment (group work is not permitted).
	• In this assessment,
	  ○ **Part 1 (reflection):** you **must not** use any Generative AI tools.
	  ○ **Part 2:** you **must** use **ChatGPT 5 (GPT-5)** (but not any other Generative AI tools). It must be appropriately acknowledged. For details, please refer to the instructions (Acknowledging the use of generative artificial intelligence).
	  ○ **Parts 3 & 4:** using any Generative AI tools is optional. Acknowledge appropriately if you use it.

Assessment Criteria	Please refer to the rubrics at the bottom of Parts 2 - 4 submission pages.

Late Penalties	● A **5% deduction per calendar day** or part thereof, up to a maximum of one week. ● Submissions made **more than 7 calendar days** after the deadline will receive a mark of **zero (0), and no assessment feedback** will be provided. ● The **late penalty is automatically calculated** based on Moodle submission.
Support Resources	See Moodle Assessment page
Feedback	Feedback will be provided on student work via: ● General cohort performance ● Specific student feedback was provided ten working days after submission

INSTRUCTIONS

Read the entire specification carefully FIRST before you start working on the assignment.

Part 1: Reflections (Not marked, but cap on overall mark applies)

Complete your reflection activities for Week 10 to Week 12 in the corresponding Ed Lesson and copy/paste them into a PDF file. Write at least 100 words for each week (relevant and meaningful to the specific week).

Failure to submit all relevant reflections (missing all submissions or incomplete submissions) will result in your Assignment 4 having a maximum mark of 50%. For example, if the overall combined mark is 16/30, it will be scaled to 15/30. If the overall combined mark is 14/30, then it will remain as 14/30.

You may use this template:
https://docs.google.com/document/d/18UIEJQeyarYW1pl8oDEaf--ubCdJ5LDf-9_jSLbGxrE/edit?usp=sharing to write down your reflections.

Submit your **PDF** file through the Moodle **Assignment 4 Part 1** activity.

Part 2 - Analyse cybersecurity vulnerabilities or incidents [7.5 marks]

Details on security issues, weaknesses, and attacks can be found in various sources, including blogs, newsletters, and experts' pages. Your task is to select **one news** item from your assigned group of URLs, read it, and verify the sources it references. Then, **you MUST use the generative AI tool, ChatGPT 5 (GPT-5), but NOT any other Generative AI tools** to analyse and discuss this recent vulnerability or cybersecurity attack, and provide your own assessment to determine whether the AI's analysis is accurate and correct, as well as identify any gaps in the analysis. Create **presentation slides with video presentation** on your findings. **Choosing an incorrect news item for analysis will not be marked.**

Group 0 or 5: Students with student number ending with "0" and "5": Data Breach

1. WhatsApp Zero-Click Spyware Exploit
   Updated: 01/09/2025
   https://nypost.com/2025/09/01/tech/sophisticated-whatsapp-attack-targets-iphone-users/

2. McDonald's AI Hiring Bot (Olivia) Breach
   Updated: 25/08/2025
   https://ctomagazine.com/mcdonalds-ai-hiring-blunder-a-massive-security-breach/

3. Microsoft SharePoint "ToolShell" Exploit
   Updated: 23/07/2025
   https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/

Group 1 or 6: Students with student number ending with "1" and "6": Software Security

4. Android Security Alert: Google Patches 120 Flaws
   Updated: 03/09/2025
   https://thehackernews.com/2025/09/android-security-alert-google-patches.html

5. SAP code injection flaw (ERP suite)
   Updated: 08/09/2025
   https://www.techradar.com/pro/security/sap-users-patch-now-worrying-s-4hana-vulnerability-being-exploited-in-the-wild

6. Cloudflare 1.1.1.1 Hit by 12 Unauthorised Certificates
   Updated: 05/09/2025
   https://securityonline.info/cloudflare-1-1-1-1-hit-by-12-unauthorized-certificates-fina-cas-misissuance-raises-microsoft-trust-concerns/

Group 2 or 7: Students with student number ending with "2" and "7": Network Security

7. Multiple TP-Link Router Flaws Actively Exploited
   Updated: 04/09/2025
   https://cyberinsider.com/multiple-tp-link-router-flaws-actively-exploited-one-zero-day-still-unpatched/

8. Critical Buffer Overflow Vulnerability in Linksys Routers
   Updated: 01/09/2025
   https://www.ameeba.com/blog/cve-2025-9357-critical-buffer-overflow-vulnerability-in-linksys-routers/

9. Widespread npm Supply Chain Attack
   Updated: 08/09/2025
   https://www.paloaltonetworks.com/blog/cloud-security/npm-supply-chain-attack/

Group 3 or 8: Students with student number ending with "3" and "8": Human Behaviour Security

10. Social Engineering at Marks & Spencer
    Updated: 10/06/2025
    https://www.bbc.com/news/articles/c4gqepe5355o

11. Louis Vuitton reveals major data breach impacting Australian customers
    Updated: 22/07/2025
    https://www.news.com.au/lifestyle/fashion/louis-vuitton-reveals-major-data-breach-impacting-australian-customers/news-story/8a964354990305175051 9afd5b67439a

12. Qantas confirms cyber-attack exposed records
    Updated: 11/09/2025
    https://www.qantas.com/au/en/support/information-for-customers-on-cyber-incident.html

Group 4 or 9: Students with student number ending with "4" and "9": AI Security

13. Zero-Click AI Vulnerability Exposes Microsoft 365 Copilot Data Without User Interaction
    Updated: 12/06/2025
    https://thehackernews.com/2025/06/zero-click-ai-vulnerability-exposes.html

14. PromptLock: The First AI-Powered Ransomware
    Updated: 22/08/2025
    https://www.itpro.com/security/ransomware/security-researchers-have-just-identified-what-could-be-the-first-ai-powered-ransomware-strain-and-it-uses-openais-gpt-oss-20b-model

15. Microsoft's agentic AI roadmap had a flaw
    Updated: 07/08/2025
    https://www.tomsguide.com/computing/internet/microsofts-agentic-ai-roadmap-had-a-flaw-that-let-hackers-take-over-browsers-heres-what-to-know-and-how-to-stay-safe

Follow the steps below:

1. **Select your article:** Select one of the three news articles in your assigned group above and read it. Read the article and references in the news item.
2. **Use ChatGPT to generate a report:** Use only **ChatGPT 5 (GPT-5)**[1] FREE version (NOT any other generative AI tools or version) to perform an initial analysis on your chosen article, addressing the following items:
    a. Provide a summary of the news item.
    b. Identify which software, hardware or system is affected. The identification should be as precise as possible. Include exact product names, distribution of the product, version numbers, etc.
    c. Describe how the issue was identified and initially published, referencing articles. The problem might have been found by a security firm, hacker, or published in a conference, journal, newspaper, or blog. Was it targeted research, discovery by chance, or were tools used?
    d. Discuss the seriousness of the issue, what's needed to exploit the weakness, and potential consequences, including causes (why it happened?) and outcomes (impacts, implications, affected parties).
    e. Discuss the necessary or proper measures on
        i. a technical level,
        ii. in terms of human behaviour, and
        iii. on a policy level, to prevent or mitigate the attack or vulnerability.
    f. Choose **at least THREE** fundamental "Ethical Principles" and analyse potential and real ethical issues based on your selected case. You must refer to the Week 9 workshop (Ethical material) which can be accessible from this link: https://learning.monash.edu/mod/resource/view.php?id=4807246
3. **Create presentation slides:** Create your own presentation slides (length of slides: maximum **18** pages excluding references, acknowledgement and appendix, if any) to present the following:
    a. The key points (as listed above from 2a. to 2f.) in the ChatGPT-generated report.
    b. Justify the correctness of the information generated from ChatGPT, based on your research information collected from other sources, e.g., researchers at a university, professional security firms, scientific conferences or journal publications, newspapers, and blogs:
        i. If you think ChatGPT is correct and accurate, give the reasons to support your claim, or

[1] Use the Monash student account.

   ii. If you believe ChatGPT has missed something or does not provide an accurate analysis, provide evidence to support your claim.

c. If the slides are more than 18 pages (excluding references, acknowledgement and appendix, if any), the exceeding pages will not be assessed.

4. **Add additional references to your slides:** The last slide(s) should be the reference page, which must include **at least 6 references:** including (i) the original article you chose; and (ii) at least 5 other related sources, like articles or academic papers, for your analysis and justifications. Use APA 7th referencing style.
   - For example, you may use the following statement at the beginning of the slide: "The following slides reference the article cited in (XXX, 2025)," where (XXX, 2025) is put as one of the references (the original article).
5. **Add ChatGPT acknowledgement to your slides:**
   a. Add the acknowledgement of using ChatGPT according to the Monash guideline described here.
   b. You **MUST also include the link to demonstrate your interaction with ChatGPT (Refer to Appendix - Requirements for using ChatGPT). Please read the detailed instructions in the Appendix carefully on how to share the link. Failure to follow the instructions may result in a significant deduction of your marks.**
6. **Record a video presentation:** Record a video (using Panopto, Zoom, Teams, or any software of your choice) to present your slides (length of video: **maximum 8 minutes**, excluding self-introduction):
   a. At the start of the video, please introduce yourself and **turn on your camera, showing your photo ID** (Monash or other). Otherwise, the video presentation (Step 6) and your elaborations in Step 3 will **NOT** be assessed.
   b. During the **entire** presentation, you must turn on your camera and record your whole face. Otherwise, the video presentation (Step 6) and your elaborations in Step 3 will **NOT** be assessed.
   (Note: These two rules are to ensure academic integrity, and therefore, they will be strictly reinforced during marking.)
   c. You must NOT use AI to generate the voice (and face) for your presentation!
   d. The video should be in a standard format (e.g., MP4, AVI, WMV, MOV) that is supported by Windows or macOS players and should be clear and viewable. It must be **NO larger than 500MB**.
   e. If the video is more than 8 minutes, the exceeding portion will not be assessed. Any attempt to speed up the video will **NOT** be assessed.

7. **Submit to Moodle:** Submit the following files to Moodle:
    a. Presentation slides, in PPT (.pptx/.ppt) or PDF (.pdf) format; and
    b. Video recording file, in any standard video format.

Remark: You do not need to submit the ChatGPT report generated in Step 2 (that is, no need to copy and paste the report into your presentation slides, or put it as the appendix of your slides, or as an independent pdf). Instead, **you must include the share link** of your ChatGPT report into the slides. You cannot just copy the URL of your ChatGPT report as the link, as it does not work for other people's login. Instead, you must follow the instructions given in the appendix (the last page) of this specification to share the correct link.

Part 3 - Security Controls in an IT Network of a Medium-Sized Company with Automated Vacuum Cleaner Production [7.5 marks]

In this task, you assume the role of a security architect (as defined in the NIST NICE workforce framework[2]). You are responsible for redesigning a company network (using best practices, as outlined in the NSA Network Infrastructure Security Guide), including placing security controls in the appropriate locations within the network. As security always incurs costs, prepare **a report** that explains to company management why each security control is required at a particular part of the company network.

Functional requirements of the company network:

- Production uses automated machines controlled by network-connected PCs. The system runs 24/7, and outages would be costly for the company. The company is very modern, allowing customers to design their own colour combinations and specifications for their vacuum cleaner. Therefore, data needs to be transferred frequently (every 6 hours) to the PCs controlling the machines.
- Outward-facing servers, including a web server used for marketing and online sales, as well as the company's mail server.
- Administration involves PCs and laptops, a server running administration software and databases, wireless printers, and Wi-Fi for meeting rooms and general office areas. Employees also travel with their laptops and need access to the administrative network, but not the production area.

Entities to be connected:

[2] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

- PCs to control production machines
- Production machines themselves
- Employee PCs and laptops for administration
- Server for administration and internal databases
- Wireless printer and scanner for administration use
- Authentication server
- DNS server
- Webserver
- Mail server
- WIFI access points
- Routers
- Switches

Security controls and appliances (applicable in multiple locations)

- Firewalls specify port numbers to allow outside traffic.
- VPN gateway
- VPN clients
- TLS (provide information on which computers TLS is used)
- Authentication server
- Secure the storage of passwords using seed values
- Disk encryption
- WPA3 encryption
- Air gaps
- Intrusion detection system
- Intrusion prevention system

The company has various departments. Based on the **final digit of your student ID**, you are assigned to **ONE department** with a **designated IP subnet**.

Group 0 or 5: Students with student number ending with "0" and "5":

- IT & Supports (ERP, Inventory, Backup, Cloud Edge)
- Subnet: 10.50.0.0/20
- Capacity: ~300 devices

Group 1 or 6: Students with student number ending with "1" and "6":

- Corporate Office Network (Admin, HR, Finance, Marketing)
- Subnet: 10.10.0.0/22
- Capacity: ~200 devices

Group 2 or 7: Students with student number ending with "2" and "7":

- R&D / Engineering
- Subnet: 10.20.0.0/21
- Capacity: ~200 devices

Group 3 or 8: Students with student number ending with "3" and 8":

- Sales & Marketing
- Subnet: 172.16.50.0/22
- Capacity: ~500 devices

Group 4 or 9: Students with student number ending with "4" and "9":

- Production & IoT Devices
- Subnet: 192.168.100.0/23
- Capacity: ~300 devices

In your report,

1. Provide a suitable title
2. Provide a brief overview of your assigned scenario (less than 100 words).
3. Identify, with justifications, which software, hardware, or system (entities) is used by your assigned department. The identification should be as accurate as possible. For each security control, explain its purpose and justify its necessity within your assigned scenario (around 150 words).
4. Create TWO diagrams of the designed network, including all entities mentioned in 3., using a diagram tool. (i.e., LucidChart).
    - 1 x diagram without security control
    - 1 x diagram with security control

    (scan of hand-written diagrams will not be accepted).
5. For your assigned department, you must include the allocation of IP addresses to devices, which can be included in the diagram or a separate table. Justify your allocation (around 150 words).
6. Provide a Conclusion (around 50 words).
7. Include a reference list to acknowledge the sources.
8. (Optional) Acknowledge the use of Generative AI (if you have used Generative AI in this part). You must follow the Monash guideline described here.

Word limit: Your report should be less than **500 words**, including title and all sub-headers, but excluding references, acknowledgement and the words inside the diagrams or table.

Submit your report as a single PDF file to Moodle.

Part 4 - Mobile App Security & Privacy Analysis [15 marks]

Select two or more mobile apps from the assigned category. Analyse and demonstrate the security aspects related to access control, data protection, application and system security, and communication protocols. Provide

presentation slides with video presentation to address security and ethical concerns, and offer concrete suggestions with practical methods for securing mobile devices and personal data.

Group 0 or 5: Students with student number ending with "0" and "5"

- **Social Networking:**
  - Instagram
  - TikTok
  - Pinterest
  - Twitter
  - Others

Group 1 or 6: Students with student number ending with "1" and "6"

- **Entertainment:**
  - Netflix
  - Spotify
  - YouTube
  - Others

Group 2 or 7: Students with student number ending with "2" and "7"

- **Shopping:**
  - Amazon
  - eBay
  - AliExpress
  - Temu
  - Others

Group 3 or 8: Students with student number ending with "3" and 8"

- **Messaging:**
  - Snapchat
  - Discord
  - WhatsApp
  - Signal
  - Messenger
  - Others

Group 4 or 9: Students with student number ending with "4" and "9"

- **Games:**
  - Fortnite
  - Minecraft

- Roblox
- Candy Crush
- Others

Follow the steps below:

1. **Select apps:** Select TWO or more apps from your allocated group above.
2. **Analyse the chosen apps:** Analyse your selected apps, addressing the following points:
    a. **Permissions:** What permissions does the app request (camera, location, contacts, storage)? Does the app's purpose justify them?
    b. **Authentication & Access Control:** Does the app support multi-factor authentication (MFA), strong passwords, and biometrics?
    c. **Data Security:** Is data encrypted during transmission (HTTPS/TLS/SSL) and when stored?
    d. **Privacy Controls:** Does the app allow users to manage the visibility, tracking, and/or sharing of their personal information?
    e. **Transparency:** How clear is the privacy policy? Is it easy for non-technical users to understand?
    f. **Risks:** What are the potential risks if the app is misused, compromised, or leaks data?
    g. **Ethical Principles:** Discuss the fundamental "Ethical Principles" by choosing **at least THREE principles** based on your selection of apps. You must refer to the Week 9 workshop (Ethical material) which can be accessible from this link: https://learning.monash.edu/mod/resource/view.php?id=4807246
3. **Create presentation slides:** Create your own presentation slides (length of slides: **maximum 18 pages** excluding references, acknowledgement and appendix, if any) to include the followings:
    a. A summary of the TWO apps (ONE slide).
    b. The key points listed above from 2a. to 2g.
    c. Screenshots/embedded recorded video where relevant (i.e., permission requests, security settings).

    Ensure your work shows critical thinking rather than just description.
    Presentation slides MUST be in PPT or PDF format.
    If the slides are more than 18 pages (excluding references, acknowledgement and appendix, if any), the exceeding pages will not be assessed.
4. **Add additional references:** The last slide(s) should be the reference page, which must include **at least 6 references,** such as articles or official websites, to support your analysis and justifications. Use APA 7th referencing style.
5. **(Optional) Add Generative AI acknowledgement:**
    a. If you have used any Generative AI in this part, add the acknowledgement of using Generative AI according to the Monash guideline described here.

6. **Record a video presentation:** Record a video (using Panopto, Zoom, Teams, or any other software of your choice) to present your slides (length of video: **maximum 8 minutes**, excluding self-introduction)
    a. At the start of the video, introduce yourself and **turn on your camera**, **showing your photo ID** (Monash or other). Otherwise, Otherwise, the video presentation (Step 6) and your elaborations in Step 3 will **NOT** be assessed.
    b. During the **entire** presentation, you must turn on your camera and record your whole face. Otherwise, the video presentation (Step 6) and your elaborations in Step 3 will **NOT** be assessed.
    (Note: These two rules are to ensure academic integrity, and therefore, they will be strictly reinforced during marking.)
    c. You must **NOT** use AI to generate the voice (and face) for your presentation!
    d. The video should be in a standard format (e.g., MP4, AVI, WMV, MOV) that is supported by Windows or macOS players and should be clear and viewable. It must be **NO larger than 500MB**.
    e. If the video is more than 8 minutes, the exceeding portion will not be assessed. Any attempt to speed up the video will **NOT** be assessed.
7. **Submit to Moodle:** Submit the following files to Moodle:
    a. Presentation slides, in PPT (.pptx/.ppt) or PDF (.pdf) format; and
    b. Video recording file, in any standard video format.

Remark: You do not need to submit a report for your Step 2. Instead, you should present your findings from Step 2 in your presentation slides (Step 3) and video (Step 6).

Submission Checklist
[3]

Overall, you should submit the following files:

Part 1: Reflections
- 1 x PDF file

Part 2: Recent vulnerability or cybersecurity attack
- 1 x Presentation slides
  - PPT/PPTX/PDF format
  - Max 18 slides
- 1 x Presentation video
  - MP4, AVI, WMV and MOV (or any other standard video format)
  - Max 8 minutes
  - Max file size 500 MB

Part 3: Security controls are used in a medium-sized enterprise scenario
- 1 x PDF
  - Words limit: No more than 500
  - 1 x Diagram without security controls
  - 1 x Diagram with security controls

Part 4: Mobile apps analysis
- 1 x Presentation slides
  - PPT/PPTX/PDF format
  - Max 18 slides
- 1 x Presentation video
  - MP4, AVI, WMV and MOV (or any other standard video format)
  - Max 8 minutes
  - Max file size 500 MB

Please check CAREFULLY before confirming your submissions on Moodle.

[3] Penalty applies for submitting any incorrect file type in each part.

Appendix - Requirements for using ChatGPT for Part 2

When using generative AI in Part 2, you **MUST** adhere to the requirements below:

1. Only ChatGPT 5 is allowed. You only need to use the FREE version (i.e., GPT-5) for this assignment. Sign up (if you do not have an account yet) or log in (if you already have an account).
2. Use ChatGPT to **refine or re-generate the answer** if you are not satisfied with the response, in an interactive manner, until you are happy with it.
3. **Generate the link for your interaction with ChatGPT** (click the button in the top right corner) and **paste it into the last slide,** below the list of references. You MUST use the "Share" button on the top right corner (**the green one in the figure**) to generate the share link for you. **You CANNOT simply copy the URL of the chat as a link, as it cannot be opened by anyone else except you. (the red one in the figure)** These two links (the red one and the green one) are different!