INTRODUCTION TO CYBERSECURITY - CCF10403

ASSIGNMENT 1

CHAPTER/TOPIC: INTRODUCTION TO CYBERSECURITY

Administrative Instructions

1. Report MUST contain a maximum of 10 pages.
2. Mode: Individual
3. Submission in the form of a written report.
4. Upload softcopy in (eKlas Teams) & hardcopy during class.
5. Date of Submission: 24/07/2026
6. Cover Page: RED
7. Assessment Weight: 100% Written Report
8. Check plagiarism before submitting.

COURSE LEARNING OUTCOME

- **CLO1:** Explain the key knowledge areas of cybersecurity and the common types of cybersecurity attacks and threats. (C2, PLO1)

ASSIGNMENT INSTRUCTIONS

1. Purpose

This assignment helps students understand how real cybersecurity incidents happen, how attackers operate, and what organisations can do to protect their systems. You will apply your knowledge from Chapters 1 to 3 to analyze a real-world breach.

2. Written Report Task

Choose ONE publicly documented cybersecurity incident. The incident must provide sufficient evidence about the attack vector, affected assets or data, organisational response, and consequences. The selected case must be unique within the class and approved by the lecturer.

Suitable cases include data breaches, ransomware, supply-chain compromise, cloud exposure, insider incidents, denial-of-service attacks, or attacks against critical services.

- **Example cases:** JPMorgan Chase (2014), Equifax (2017), WannaCry/NHS (2017), SolarWinds (2020), Colonial Pipeline (2021), MOVEit Transfer (2023), or any equivalent incident.

The student must not rely on Wikipedia, blogs, or generative AI as principal evidence. Such material may help discovery but does not satisfy the source requirement.

- **Case approval submission:** Incident name, year, affected organisation/sector, and two preliminary credible sources.

3. Report Questions

Prepare a professional, evidence-based case-study report that answers the following questions based on your chosen case:

- **a. Incident Profile and Verified Timeline (15 marks):** What organisation, sector, systems, users, and data were involved? What happened before, during, and after discovery? Present a concise timeline with cited dates. Who was affected, and what verified operational, financial, legal, privacy, or reputational consequences followed?
- **b. Attack, Threat, and Vulnerability Analysis (20 marks):** What threat actor or threat category was reported? If attribution is uncertain, state that clearly. What attack type and attack vector were used? Which technical, administrative, or human vulnerabilities enabled or worsened the incident? Distinguish threat, vulnerability, attack, asset, and impact; do not use these terms interchangeably. Explain the attack sequence using a diagram or flowchart supported by evidence.
- **c. CIA Triad and States of Data (15 marks):** Explain the effect on confidentiality, integrity, and availability. Identify unaffected elements where evidence supports this. Identify whether affected data were at rest, in transit, or in use at relevant stages. Prioritise the CIA impact and justify the ranking using case evidence.
- **d. Organisational Response and Security Roles (15 marks):** How did the organisation detect, contain, eradicate, recover from, and communicate the incident? Which roles were or should have been involved, for example, SOC analyst, incident responder, forensic analyst, security engineer, management, legal/privacy team, communications team, and regulator? What was effective or ineffective in the response? Support the evaluation with evidence.
- **e. Countermeasures and Framework-Based Evaluation (15 marks):** Classify relevant controls as technological, administrative, or human. Apply one suitable

framework at an introductory level, for example NIST CSF functions or ISO/IEC 27001 control areas to identify gaps. For each proposed control, explain which identified vulnerability or impact it addresses.

- **f. Ethical and Legal Considerations (10 marks):** Examine responsible disclosure, timeliness and transparency of notification, privacy, accountability, potential data misuse, and duties to affected parties. Identify applicable law or regulation only where supported by a credible source; do not provide unsupported legal conclusions.
- **g. Lessons Learned and Prioritised Recommendations (10 marks):** What should the organisation have done differently before, during, and after the incident? Provide 3-5 realistic recommendations and for each recommendation, state the action, responsible role, expected security benefit, and implementation consideration.

4. Required Report Outline

- a. Introduction
- b. Incident Profile and Timeline
- c. Threat and Vulnerability Analysis
- d. CIA Triad and States of Data
- e. Incident Response and Security Roles
- f. Controls and Security-Framework Analysis
- g. Ethical and Legal Issues
- h. Lessons Learned and Recommendations
- i. Conclusion and Self-Reflection

RUBRIC ASSESSMENT

Criteria	Beyond Expectation (4)	Meets Expectation (3)	Below Expectation (2)	Needs Improvement (1)	Marks
Introduction	Clearly introduces the selected incident, organisation, purpose, scope and source approach. Provides a focused direction for the report.	Introduces the incident, purpose and scope with minor omissions.	Provides a basic introduction, but the purpose, scope or context is unclear.	Introduction is missing, irrelevant or fails to establish the report context.	/15

Criteria	Beyond Expectation (4)	Meets Expectation (3)	Below Expectation (2)	Needs Improvement (1)	Marks
Incident Profile and Timeline & Threat and Vulnerability Analysis	Presents an accurate, well-contextualised incident profile. The chronology, affected parties, assets, data and consequences are clearly supported by credible evidence. Clearly distinguishes threats, vulnerabilities, attack vectors, assets and impacts. Explains the attack sequence accurately and in substantial depth using case evidence.	Presents a mostly accurate and logically sequenced account with minor omissions or limited context. Correctly explains the main attack type, vector and exploited weaknesses, although some details are underdeveloped.	Provides a basic description, but the timeline, affected assets or consequences lack depth, precision or support. Provides a mainly descriptive or partial analysis. Important concepts are occasionally confused or weakly supported.	Incident profile is incomplete, inaccurate, poorly sequenced or largely unsupported. Analysis is minimal, inaccurate or unsupported. Key cybersecurity concepts are misunderstood.	/10 /15
CIA Triad and States of Data	Provides insightful, evidence-based analysis of confidentiality, integrity, availability and relevant data states. The prioritised CIA impact is convincingly justified.	Correctly maps the main CIA effects and data states with reasonable justification.	Identifies some relevant CIA effects or data states, but the analysis is incomplete, generic or weakly justified.	CIA triad and data-state concepts are missing, materially incorrect or unrelated to the case.	/10
Incident Response and Security Roles	Critically evaluates detection, containment, eradication, recovery and communication. Clearly explains the responsibilities of relevant cybersecurity and organisational roles.	Explains the principal response actions and relevant roles with some evaluation.	Provides a surface-level response summary. Discussion of responsibilities is limited or generic.	Response actions and roles are missing, inaccurate or irrelevant to the incident.	/15

Criteria	Beyond Expectation (4)	Meets Expectation (3)	Below Expectation (2)	Needs Improvement (1)	Marks
Controls and Security-Framework Analysis	Proposes feasible and prioritised technological, administrative and human controls directly linked to case weaknesses. Applies a suitable security framework accurately and meaningfully.	Recommends relevant controls and generally applies an appropriate framework, but some links require greater specificity.	Controls are generic or weakly linked to the identified vulnerabilities. Framework application is limited or partly inaccurate.	Controls are unrealistic or unrelated. No meaningful framework analysis is provided.	/15
Ethical and Legal Issues, Lessons and Recommendations, Conclusion and Individual Self-Reflection	Presents a balanced, evidence-based ethical and legal analysis. Provides three to five prioritised, realistic and case-specific recommendations with clear responsibility and expected benefits. Provides a concise synthesis and thoughtful personal reflection. Clearly explains lessons gained, challenges faced, relevant Chapter 1-2 concepts and areas for future improvement.	Provides an adequate ethical and legal discussion with relevant lessons and useful recommendations. Summarises the report and provides relevant personal reflection with minor gaps.	Ethical or legal analysis is limited or vague. Recommendations are generic, insufficiently prioritised or weakly justified. Provides a general summary with limited personal reflection or weak connection to the course concepts.	Ethical and legal issues are largely overlooked. Lessons and recommendations are absent, unsupported or impractical. Conclusion is missing, introduces unsupported information or contains little meaningful self-reflection.	/10 /10
Evidence, APA Referencing, Presentation and Visuals	Meets the required source mix. Uses consistent claim-level-citations and accurate APA 7 referencing. The report is professional, well organised and supported by clear, cited visuals.	Meets the minimum source requirement with minor APA or formatting issues. Visuals are relevant and generally clear.	Uses weak or insufficient sources, inconsistent citations, limited visual support or several presentation problems.	Uses insufficient or unreliable sources. Referencing is poor or absent, and the report is disorganised or lacks the required visuals.	/10

Criteria	Beyond Expectation (4)	Meets Expectation (3)	Below Expectation (2)	Needs Improvement (1)	Marks
Total					**/100**

Penalties

Late Submission Penalty

Days Late	Marks Deducted
1 Day Late	-3%
2 Days Late	-5%
3 Days Late	-7%
More than 3 Days	-10%

Absenteeism Penalty

If a student is absent for 50% or more without any valid reason:

- -20% marks will be deducted from the final score

MANAGEMENT & SCIENCE UNIVERSITY (MSU)

Introduction to Cybersecurity / CCF10403

ASSIGNMENT 1

- **Received Date:**
- **Submission Date:**
- **Weightage:** 20%
- **Semester:** JULY-2026
- **Prepared for:** Dr. Nur Fasihah binti Mohd Esa

Instruction to students:

> This is a GROUP assignment. EVERY GROUP HAS 2 OR 3 MEMBERS ONLY.
> Complete this cover sheet and attach it to your assignment (first page).

Student Declaration

I declare that:

- This assignment is my own work.
- I understand what is meant by plagiarism.
- My lecturer has the right to deduct my marks in the case of:
  - Late submission
  - Any plagiarism or AI detection found in my assignment
  - Absenteeism rate more than 50%

No.	Student ID	Name	Total Marks
1.			
2.			
3.			

Revision #1
Created 2026-07-28 04:36:05 CEST by kalvin0x1ad
Updated 2026-07-28 04:36:27 CEST by kalvin0x1ad