Cyber Security Case Study Coursework

Topic Selection Deadline	SEE MYPLACE
Final Deadline	SEE MYPLACE
Weighting	70% of final course mark
Estimated Hours	30 hours
Individual or Group	Individual
Feedback Type	Written ☒ Oral e.g. in class, pre-recorded video or zoom call ☐ Both ☐
Individual Feedback Format	Rubric criteria selected at performance level, plus per submission written feedback
Class wide Feedback Format	Written summary of most common limitations and guidance for improvement
Feedback Return	Mid-January 2024
Marking Criteria	See marking criteria section. **Note that any non-compliance with the instructions provided is subject to a 10% penalty.**
Relevant University Policies	It is your responsibility to familiarise yourself with the university policies below. The University policies on late submission of coursework and extension requests can be found here: Late Coursework Submission Policy Coursework Extension Policy The University take plagiarism (including self-plagiarism) seriously, please see the University guidelines on this here: Plagiarism Student Booklet **Use of generative AI is explicitly prohibited for this assessment**, suspected use of generative AI tools such as chat GPT will be dealt with through the academic misconduct procedure.

Overview

In recent years there have been many information security incidents. In this assignment you must choose **one** of the incidents provided on myplace and write a 1500-word (+-10%) executive summary (12 point, single spacing, Aptos or equivalent San serif font, A4 with 1 inch margins- i.e. the default for Word) on the incident covering the following aspects:

1. What happened and what was the impact?
2. What security failure or failures which led to the incident? For example, did the organisation make any decisions which led to the compromise? If a technical aspect was involved, you should explain how this works e.g., if a privilege escalation attack was performed, describe how this works, relating it to the specific incident as far as possible.
3. Explain what (if anything) could have prevented or mitigated the incident, highlighting why you believe it would mitigate such incidents in this context, how you think it would achieve this and providing details of any technical or non-technical solutions.

It is expected that you will research beyond the content presented in the module. Note that in some instances there may be limited information which impacts your ability to say with certainty what happened. In such instances, you should evaluate what evidence you have and propose possible issues which may have contributed to the successful attack.

Case Study Incidents Selection

On MyPlace in the Assessment Section there will be an activity called 'Real World Case Study Options Choice' which allows students to select one incident from five choices. Your choice is final, and you can only select one topic. If you do not select a topic by the deadline provided on myplace, you will be allocated one at random. Should you wish to complete your study on a different incident, please email the lecturer with the details at least 3 working weeks prior to the deadline to gain authorisation to proceed. **Should you submit a case study on a topic to which you were not allocated then your work will not be marked, and you will be asked to submit a report on your assigned topic within 5 days – the usual late penalties will apply for each day the report is late.**

Referencing, Plagiarism and Academic Integrity

In your report, you should include sources for the information. References should be formatted using the ACM reference guide.

Note that the page limit is exclusive of references which should be included under a heading 'References' at the end of the report. Roughly 10 references should be adequate but note that these should be high calibre. Guidance on evaluating reference quality can be found in this guide . The University provides learner development services should you require support with your writing quality.

The plagiarism detection software Turnitin will be used in the MyPlace submission slot for the assignment. You can upload your report as many times as you wish until the due date at which stage your last submission will be the final submission. The Turnitin software will check your work for indications of plagiarism and present a report to the lecturer. The easiest way to avoid plagiarism is to write the case study yourself, quote where appropriate, and include references where ideas have been taken from other sources. Use of GenAI is not permitted for this assessment. Suspected use of generative AI tools such as chat GPT will be dealt with through the academic misconduct procedure.

Marking Criteria

Submissions will be graded according to the following criteria.

Criteria	0 Points	1 Point	2 Points	3 Points	4 Points	5 Points
Problem Recognition and Understanding	No significant attempt	Minimal recognition and understanding of the problem.	Weak understanding of the problem given the context of the case study. Minimal identification of concerns and impact.	Identification of problem and related understanding is good, there are likely 1 or 2 significant areas for improvement.	Very good identification of the problem given the context. Very good understanding of the problem, likely one or two small areas for improvement.	Excellent identification of the problem given the context of the case study. Strong understanding of the problem given the context of the case study. Excellent understanding of the key concerns and impact.
Understanding Mitigation Techniques	No significant attempt	Minimal recognition and understanding of appropriate mitigation techniques. There are likely to be multiple significant problems with understanding as applied to the context.	Understanding of mitigation techniques is adequate. There are likely to be multiple problems with understanding as applied to the context.	Understanding of mitigation techniques is good. There are likely to be two or three problems with understanding as applied to the context.	Understanding of mitigation techniques is very good. There may be one or two minor problems with understanding as applied to the context.	Clearly appropriate mitigation techniques are identified and explained in a way which demonstrates deep understanding as applied to the context.
Critical Analysis	No significant attempt	Minimal evidence of critical and independent thought as applied to the case study.	Adequate demonstration of critical and independent analysis.	Good demonstration of critical and independent analysis, but it is likely limited to one or two aspects.	Very good demonstration of critical and independent analysis. Could be improved slightly in one or two small areas.	Excellent demonstration of critical and independent thought, no room for improvement in the given context.
Clarity of Communication	No significant attempt	Poorly structured report, predominantly incoherent. There are likely to be little or no relevant references.	Adequately structured, mostly logical, and somewhat coherent. Use of some relevant references.	Moderately well-structured and mostly coherent.	Very well structured, only one or two instances where coherence or structure could be improved.	A highly coherent and well-structured case study which is clearly coherent.

In addition to the above, the following prompts can be used to reflect on your work before final submission. Note that these align with the marking criteria defined above.

1. Depth of Problem Recognition and Understanding – *are you demonstrating deep understanding of the technical and (potentially) non-technical aspects of security which led to the incident? Do you demonstrate critical thought as applied to any security failures?*

2. Depth of Understanding of the possible solutions and/or attack mitigation techniques which would help prevent such an attack – *do you demonstrate deep understanding of the technical security measures which could be used to avoid or mitigate the impact of the attack? Do you demonstrate critical thought as applied to the possible solutions?*
3. Critical Analysis – *Do you research beyond what is presented in class? Are you comparing options and reasoning why a particular option is better than the other? Are you analysing resources to determine if what they report is correct and appropriate? Are you evidencing your argument appropriately?*
4. Clarity of Communication –*Do you present a well-reasoned, coherent and well-structured report? Note that if the writing is poor in terms of coherence and grammar it could be very difficult to convey your understanding of the first points. Do you include a sufficient range of quality sources which indicates a range of reading around the area which contribute to a convincing summary of the incident and argument for fixing it? Does the author use a consistent referencing style and reference appropriate statements?*

It is advisable for all students to get others to read your work, even an uninformed reader – their feedback will help you identify where any issues might be. If you find yourself saying 'I meant this..' then it means you may not have written it clearly enough.

Submission

Students are required to submit a pdf of their report.

Do not include your name or student number in the submission. The assessment is marked 'blind' as recommended by the University, this means myplace hides your identity while marking. If you include your identifying information this results in non-blind marking.

Include a word count. Note the word count is exclusive of references and the note of final wordcount, and it should be 1500 words (+-10%).