Cybr373 2024

Assignment Two - Analysis of Incident Response Case Study

Due Monday 16 September 2024 at 23:59
Weighting 30%

This assignment must be completed and submitted individually. Refer to the Deloitte reports included in the zipfile with this assignment brief (Deloitte Ministry of Social Development Independent Review of Information Systems Security Phase 1 and Phase 2). Refer to the NZ Information Security Manual (NZISM). You will also need to research other material and include what you believe to be appropriate. Provide appropriate citations and referencing using IEEE format. The use of AI in any form must be acknowledged (e.g. brainstorming, editing).

Complete Q1-Q4 as listed below. This assignment is marked out of a possible 100 marks. Word count allocation is specific to each question, not the overall document (e.g. 300 words maximum for Q1, and 400 words maximum for Q4). References are not included in the word count.

Q1 Summary (300 words maximum)

[18 marks] Utilising the 5W and H decision framework, (what, when, where, why, who and how), provide a concise summary of the breach and response, including the points that you believe are most relevant. Technical details and organisational impact are both important aspects to consider when completing the summary.

Q2 Ethics/Disclosure (400 words maximum)

[32 marks] Consider the breach and response scenario from an ethical perspective.

a) Discuss and explain whether you believe Mr Ng acted in an ethical manner when revealing details of the breach, and how he revealed the details. Did the Ministry act ethically toward their customers in terms of their initial actions, and their response when the breach was notified? (possible 16 marks)

b) What is the correct way of disclosing a vulnerability today? Discuss and explain responsible disclosure, including what current procedures and rules are in NZ. Is Ministry of Social Development's responsible disclosure policy in line with general responsible disclosure policy in NZ today? (possible 16 marks)

Q3 Incident response (300 words maximum)

[20 marks] Explain and critique the following, providing 2-3 key points for each aspect by the Ministry in response to the incident. This should include actions taken by all incident handlers on this incident. You should consider both immediate actions and longer-term measures.

(a) the containment strategy (possible 6 marks),

(b) the Incident Response (possible 8 marks), and

(c) Disaster Recovery (DR) actions (possible 6 marks)

Q4 Controls and governance (400 words maximum)
[30 Marks] Referring to the NZ Information Security Manual (NZISM) https://nzism.gcsb.govt.nz/ism-document, consider how vulnerabilities in the physical and logical design and architecture of the kiosk example could be mitigated or minimised by application of physical and technical controls.

Name, and discuss **6** controls, justifying why each would be appropriate, using relevant information that you locate in NZISM. List your results in a table formatted as below in Fig. 1. One basic example is provided to guide you on appropriate format and content. Providing a greater level of detail within your table (within word count limits) will result in a higher grade than providing basic information as shown below. Reference NZISM at the end of the document, using IEEE format. You do not need to cite each entry.

Each of the 6 controls are worth up to 5 marks each, allocated as following per control:
Correctly identifying the control (possible 1 mark)
Providing some concise details on the control (possible 2 marks)
Identifying the chapter, and if directly relevant, the topic (possible 1 mark)
Identifying the relevant objective (possible 1 mark)

You must reference NZISM in your references section, but citations not required for Q4.

Control	Detail	Chapter & topic	Summarised Objective
Example: Physical security	Example: More physical security	Example: 8. Physical Security 8.1. Facilities	Example: 8.1.1. Physical security measures applied to facilities to protect systems and their infrastructure
1.			
2.			
3.			
4.			
5.			
6.			

Fig. 1