This page has been intentionally left blank

89/100

Question 1

Ransomware attacks are becoming more common nowadays. In 2017, a ransomware, known as SamSam, attacked a hospital in the United States. The attack exploited three vulnerabilities: 1) poor password security practices (such as not changing the default password of some IT equipment or using weak passwords); 2) a vulnerability in a Java-based application server; and 3) the availability of remote desktop protocol (RDP) on many Windows machines in the organisation. Once Samsam got into the hospital's IT system, it encrypted data on more than 6,000 computers of the centre, making staff and clinicians unable to access email, electronic health records, and important websites. It took over two weeks for the system to be restored and costed the organisation over $10 million.

- Which security goal (Availability/Integrity/Confidentiality) was compromised in this ransomware attack? Explain your reasoning. Your argument must be based on the information within the question.
- Describe one (1) action that should have been taken by the hospital to prevent this ransomware attack. Briefly explain how it would address such a threat.

7

[8 Marks]

Answer:

- Security goal compromised: Accessability ✓ - (Main) & Integrity
- Reasons: • Accessability is the main goal compromised because the system's user did not have access to system default information ? and the system did not perform as expected.
  • Integrity was also compromised because the data must have been modified to effect the changes seen in the system
- Suggested action

Back Effective back up of the system would have made the system recovery much quicker and less expensive

Regular installation of software patches on the server and education and training of staff to update default passwords would have helped To prevent the attack.

Question 2

A company is developing an online platform that allows registered users to post jobs and registered professional tradies (painters, plumbers, electricians, etc.) to bid for the job. The platform is designed to work on both desktop computers and mobile devices. Describe three (3) requirements of the online platform that address the security goal Integrity. Your answer must be specific to this context.

12

[12 Marks]

Answer:

- Requirement 1: Access control
  - Good Authentication so that only specific identities can modify the information about the jobs they do (cost rates etc per tradie) - cannot change the rates of another tradie ✓
- Requirement 2: Some form of certificate system to verify the Tradies are properly qualified to complete the jobs - This could be an initial account verification process to verify professional certificates and other forms of ID. ✓
- Requirement 3: Users could then use a photo of the tradie on their mobile device to ensure they are the designated person by facial recognition.

Logging and Auditing of the Tradie & user databases by system admin ✓ - This would allow for the removal of fake accounts that are reported by users or detected using automated protocols.

Question 3

The figure below shows the impact of key factors on the average total cost of a data breach according to a recent study (IBM Data Breach Report 2020). Describe your intepretation of this finding and how you would advise organisations on their security expenditure to reduce the data breach total cost.

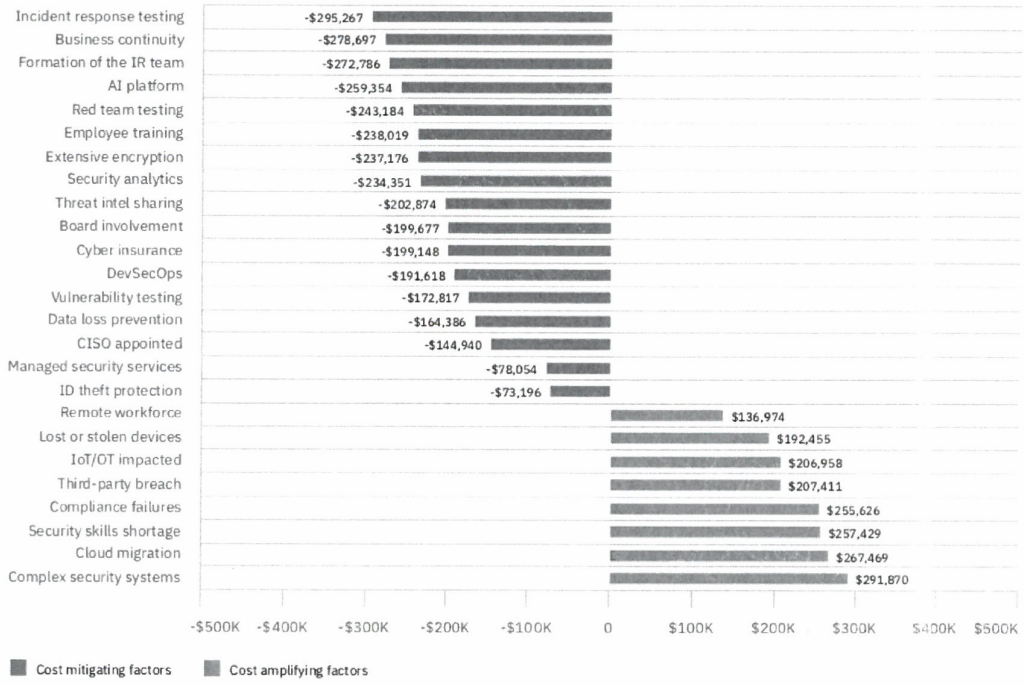

Figure 1: Impact of key factors on the average total cost of a data breach.

not clearly separate interpretation vs advice

[8 Marks]

Answer: The key message is to be well prepared. Having a BCP and testing the responses to incidents will save the most money in the event of an incident. Training is also very beneficial to reducing costs.

Conversely, increasing expenditure on a complex security system ~~will not~~ may not save much money in the event of a breach. Possibly because human factors can circumvent the security system. Care should be taken with IOT, cloud & third party initiatives

Question 4

After study security models, a data security student concluded that the "no read-down rule" of the Biba model does not help address integrity because it is only about reading data and not modifying data. Discuss whether or not you agree with this student's finding and give one example to support your argument.

[8 Marks]

Answer: I do not agree with the student's response. ✓

The no read down rule is designed to preserve the integrity of higher security levels from possibly dirty data at lower levels. ✓ For example a ~~newspaper~~ news organisation may re-publish information from a government website, as this can be considered at the same integrity level as the organisation. However, it could not republish information from a social media news site as this may not be accurate, and would lower the integrity of the news organisation's data. ✓

Question 5

Consider the following case study:
A software development company has just produced a new software package that incorporates the new tax laws and figures taxes for both individuals and small businesses. The president of the company knows that the program has a number of bugs. He also believes the first firm to put this kind of software on the market is likely to capture the largest market share. The company widely advertises the program. When the company actually ships a CD, it includes a disclaimer of responsibility for errors resulting from the use of the program. The company expects it will receive a number of complaints, queries, and suggestions for modification. The company plans to use these to make changes and eventually issue updated, improved, and debugged versions. The president argues that this is general industry policy and that anyone who buys version 1.0 of a program knows this and will take proper precautions. Because of bugs, a number of users filed incorrect tax returns and were penalised by the ATO.

Identify three (3) relevant core ethical values of the ACS Professional Code of Conduct for this case study. For each core ethical value, *briefly* explain the particular ethical issue in this case study. A copy of the ACS Professional of Conduct is reproduced below.

ACS Professional Code of Conduct

1. The Primacy of the Public Interest: You will place the interests of the public above those of personal, business or sectional interests.
2. The Enhancement of Quality of Life: You will strive to enhance the quality of life of those affected by your work.
3. Honesty: You will be honest in your representation of skills, knowledge, services and products.
4. Competence: You will work competently and diligently for your stakeholders.
5. Professional Development: You will enhance your own professional development, and that of your staff.
6. Professionalism: You will enhance the integrity of the ACS and the respect of its members for each other.

[12 Marks]

Answer: 1: 1.2.1 a - The company hees identified those potentially affected by the bugs, but hasint explicitly considered their interests above the comp anies own interests.

PTO

This page has been intentionally left blank

2. 1.2.2 d.

The company hasn't attempted to increase the feelings of personal satisfaction, competence and control of those affected by their work - the affected users may have ongoing issues (regular audits etc) because they have now submitted an erroneous tax return. ✓

3. 1.2.4 a.)

The company has not endeavored to provide a product that matches the financial needs of its customers - The software was known to have bugs that would prevent customers addressing those needs. ✓