Revision and Reflection

Enterprise Cyber Security

1A

1. Tramiel & Rejewski is a new medical practice, specialising in children's health, in a bustling European city. The practice joins an emerging community of medical practices in the city that specialise in different areas, such fertility and geriatrics. The relatively modern medical practice, much like others in the community, stores all patient records digitally.

   a) Tramiel & Rejewski are concerned about the availability of data, especially when patient records are likely to escalate during the winter months. Tramiel & Rejewski are concerned they do not have the budget to heavily invest in new machines and infrastructure to store and access digital medical records. They are also concerned that they may need to invest in 24-hour technical staff to manage new infrastructure, an expensive concern especially if patient registrations slow down. A competing medical practice recommends cloud computing as a solution.

   Describe FOUR advantages of utilising cloud computing in the given context.

   [8]

1B

b) Tramiel & Rejewski have identified the fictional PublicCloud Inc., a public cloud infrastructure offering. However, they have concerns about the confidentiality of medical records on PublicCloud Inc. as well as rules and regulations regarding patient data.

State THREE concerns with the use of a public cloud deployment model and describe an alternative solution in the given context.

[6]

2A

2. OrangeBricks is a web-based estate agent where home and business owners can sell property for low administrative fees. The business has grown from strength to strength, leading to the storage of considerable data. The business is concerned about its business continuity planning.

    a. The management team believes the business can withstand permitted data loss of approximately 10 hours. The management team state the figure has been determined by the IT department, given the current level of infrastructure.

    Argue whether the figure is relevant or not in the given context, explain RPO and state your final position.

    [8]

2B

b. The management team are committed to business continuity planning, but are unsure what should inform decisions.

Describe an initial process with FOUR main stages that would inform business continuity planning.

[8]

2C

c. The management team is considering storing duplicate copies of data on cloud computing infrastructure. The data would include standard bidding letters for properties. Buyers use the standard letter and alter the address and price when submitting sealed bids for properties. The management team has learned the provider uses the process of deduplication and this may present some concerns for the business.

Describe a potential attack that could utilise a potential vulnerability in an implementation of data deduplication in the given context.

[4]

3A

b. EHL Inc. have decided to make a legacy mainframe application, ScanCheck, accessible outside depots via a custom smartphone application. Delivery drivers currently use dedicated barcode scanners directly wired to the mainframe to scan packages before departing the depot. The legacy ScanCheck application rapidly processes the expected input from the barcode scanner. EHL Inc. plan to allow smartphones to act as barcode scanners and send the expected output to the legacy ScanCheck application.

Identify a potential problem in the proposal and outline an appropriate solution.

[4]

3B

c. EHL Inc. have decided to evolve all their legacy systems after concerns that they may expose the organisation to unwanted cyber threats. EHL Inc. want to evolve the legacy systems rapidly, but are concerned as they have limited staff with sufficient experience of the legacy systems.

Describe FOUR approaches to evolve legacy application and argue for the optimal approach.

[10]

4A

c. Spence states that they could offer existing French customers better financial products and interest rates, if the pair stored and processed all data at their Lilliput branch. Spence argues all that would be required is to transfer and store all existing customer data at the Lilliput branch. Bartik argues that since Lilliput is not part of the European Union (EU), no such data transfer can occur. Spence argues this is not a problem as the company's customer data is transited all over the world, effectively passing through various non-EU networks to their back-up systems in various other EU countries.

Appraise different options for the restricted transfer of customer data in the given context and argue whether the different positions adopted by Bartik and Spence are accurate.

(400 word limit)

[8]

5A

2. The Lena Corporation design various Image Processing Units (IPUs) for portable devices, such as smartphones and tablets. The company remains competitive due to a number of valuable trade secrets related to the design of its IPUs. However, many of these trade secrets have now been leaked to the public in a suspected cyber-attack.

   The management team are concerned that attackers have intruded into company systems that were perceived as secure from such threats. The management team have requested Simon, Stallman and Stroustrup to investigate and to determine the anatomy of the suspected cyber-attack as well as suggest appropriate defences.

5A

a. Simon, Stallman and Stroustrup have reviewed the log of security incidents, that have been reported in the past 12 months within the company. The pair have already determined several relevant incidents:

- Two removable media drives (USB memory drives) with the label 'HR department' written on them have been discovered in the toilets in separate site offices. The USB memory drives contain various Microsoft Excel files.

- 36 suspicious emails have been reported within the organisation, specifically in the administration office. Each email has been structured to appear from the immediate superior to the recipient, such as their line manager or team leader.

- 14 suspicious attachments, specifically Microsoft Excel files, that appear relevant to the recipient's role and benign, but contain a malicious payload. An example would be a financial analyst receiving a spreadsheet labelled 'Annual Budget'.

- Remote administration tools have been located on various employee systems, that were not present at the previous inspection.

- Several employees report receiving suspicious friend requests and messages on social networking services from profiles masquerading as colleagues.

The trio agree that the identified incidents alone are not sufficient to gain insight into the anatomy of the cyber-attack. The trio propose using an approach to better understand the cyber-attack, but cannot agree on an optimal approach. Simon proposes using Attack Trees, Stallman suggests the Cyber Kill Chain approach, while Stroustrup advocates for the STRIDE approach.

Appraise each of the proposed approaches from Simon, Stallman and Stroustrup in the given context. Argue for the optimal approach and formulate the anatomy of the cyber-attack in the given context.

5B

b. The management team want to ensure that the company is not susceptible to such a cyber-attack in the future.

Argue for THREE distinct defensive steps that could be taken to optimally defend against the attack identified in (a) and at what stage they should be taken.

(450 word limit)

[9]

5C

(b) The fictional country of Freedonia is not a member of the European Union (EU) or the European Economic Area (EEA). The new law firm intends to increase custom from EU and EEA member countries. The expectation is that this will inevitably lead to the firm controlling, transferring and processing data of EU and EEA citizens. Eich & Rassum state they already process and transfer personal data of citizens from EU and EEA member countries. However, while Liskov, Ableson & Sassenrath are keen to increase such custom they are concerned about legality. Eich & Rassum state all the firm needs to ensure is it has adequate data protections in place.

Argue whether or not the position of Eich & Rassum is accurate in the given context.

[6]

6A

3. The management team of Mauchly Hospital have been reviewing the expense in the back-up of medical records associated with patients. The medical records largely comprise of multiple standard forms and letters for each individual patient. Consequently, multiple forms and letters have small changes between them. A typical example is that of an appointment letter where only the address and name are altered for each patient.

6B

(a) Mauchly Hospital require a more efficient approach to storage of back-up medical records for patients. The current back-up solution maintains a complete duplicate for each patient. The management want to make efficient use of infrastructure and avoid storage of redundant data and reduce the flow of data over their internal network.

Devise and describe an appropriate solution that reduces redundant data in the given context.

[8]

6C

(b) The management team are concerned about threats to patient privacy that may arise from changes to internal back-up infrastructure.

Identify a potential attack that may compromise patient privacy for the proposed solution in (a) and argue for an appropriate solution to the attack.

[6]

6D

(c) The management team are concerned that any sophisticated solution to reducing redundant data may hamper the organisation to comply with aspects of data protection and privacy. They are particularly concerned about the right of an individual to have their data deleted.

Outline how the proposed solution in (a) may be perceived as in conflict with the right of data subjects to be forgotten. Argue how the solution would not conflict with the right to be forgotten.

[6]

7A

2. Steve Mann Life (SML) sells life insurance policies to individuals across Europe. The organisation offers monthly discounts on insurance premiums for those that enroll in ActivSystem. The system rewards customers that lead active lifestyles with discounts on monthly premiums. The ActivSystem comprises of a web portal and smartwatch to monitor the activity of customers.

The organisation requires customers to wear a smartwatch and consent via the web portal to the company collecting time and location data as well as activity data, such as footsteps taken. The organisation states the data is not encrypted, stored for five years and will only be used to determine calories burned per day. The entire data collection and processing process has not been documented, but the company is considering performing a risk analysis and reviewing relevant policies. SML customers can observe activity data on the web portal with the company expected to add features such as correcting data, data export and data deletion in time.

7B

(a) Data analysts within SML have determined that time and location data from customer smartwatches can also be used to determine the venues they visit. Consequently, the company has decided that discounts will be reduced for those customers that visit fast food restaurants. The analysts have also determined that the data could be sold to various companies to offset the discounts offered to customers.

The company are yet to appoint a data protection officer and the management team are concerned about some of the design decisions from the perspective of data protection.

Critique the ActivSystem from the perspective of FOUR principles of the General Data Protection Regulations (GDPR).

[12]

7C

(b) The developers of ActivSystem are keen to consider and discuss potential threats to the web portal component with various company stakeholders. SML customers are expected to access the system using their web browser and login with their personal email address and password. SML customers can update address details and can also use the web portal to purchase more sophisticated smartwatches.

Evaluate the web portal using an appropriate framework for thinking, discussing and classifying common threats.

[8]

Revision and Reflection

Enterprise Cyber Security