OCR
Oxford Cambridge and RSA

Wednesday 15 January 2025 – Morning

Level 3 Cambridge Technical in IT

05839/05840/05841/05842/05877 Unit 3: Cyber security

INSERT

C387/2501

INSTRUCTIONS

- Do **not** send this Insert for marking. Keep it in the centre or recycle it.

INFORMATION

- This Insert contains the pre-release material that you have already seen.
- This document has **4** pages.

Cyber Security Course

Triangle Widgets has recently sent an employee on a cyber security course. The employee has returned enthusiastic and with lots of ideas. Some of the ideas will be implemented.

The first idea that was recommended on the course was that a review takes place of the existing cyber security measures and controls. The review should include the identification of all assets, procedures and policies and vulnerabilities.

Once the review is complete, the next step recommended on the course was to prepare a list of improvements and implement them.

The cyber security course also covered the basics of dealing with an incident and included:

- how to respond
- categories of incidents and the response required for different categories
- containing, eradicating and recovering from the incident
- dealing with those affected by the incident
- engaging organisations outside of the company.

The course ended with a discussion of how cyber security is not just based on an individual or company but that everyone needs to play their part as a data breach in a company in a different country can have an impact throughout the globe.

Table Top Exercises

One important element in cyber security, which was raised on the course, is to run through scenarios before they happen so that the company is prepared. These are known as table top exercises.

A table top exercise enables procedures to be tested and employees to become familiar with the creation of the Cyber Security Incident Report (CISR). The results of the table top exercise can allow improvements to policies and procedures to be identified.

Triangle Widgets decides to run a table top exercise based around a data breach where a manager's password is compromised. As a result of this, a hacker manages to gain access to:

- emails
- customer information
- employee information
- organisational data.

Further Research

To prepare for the exam, you should research the following themes:

- How the company can analyse risk and identify vulnerable assets
- Measures and controls the company can use to improve its cyber security and the operational considerations required when introducing them
- How the company can use procedures as part of cyber security controls
- How the impact of cyber security incidents can be reduced
- Responses needed to different categories of cyber security incidents
- The impact of cyber security incidents beyond the company.