



Oxford Cambridge and RSA

**Monday 18 January 2021 – Morning**

**Level 3 Cambridge Technical in IT**

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

**INSERT**



**INSTRUCTIONS**

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

**INFORMATION**

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

## Stevenson Research

### Introduction

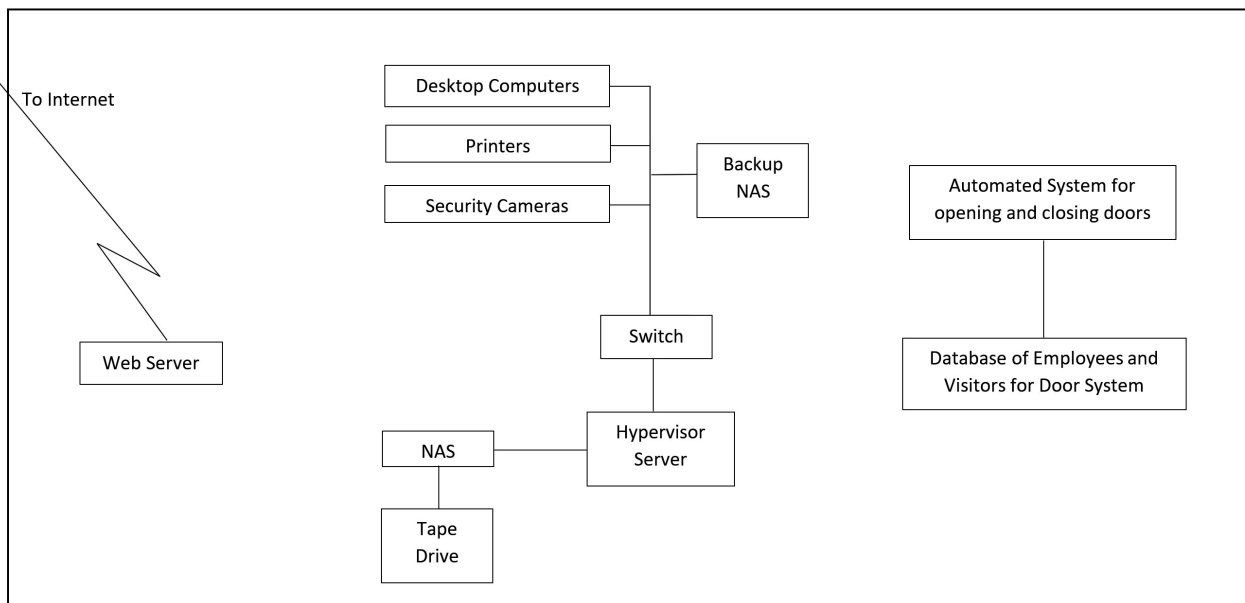
Stevenson Research is a research company, who specialise in the areas of artificial intelligence and robotics. They work on both private and government contracts.

### Network Setup

The network contains three different components:

- Main network
- The company website
- Door management system.

The end users have access to desktop computers and printers – all of which are hard wired. There are security cameras throughout the building.



### Notes:

- The web server has connections to the internal network.
- The door management system is a standalone system with employee and visitor details manually entered into the database.
- Employees and visitors are given ID cards which will automatically open the doors to the areas they have authorised access to.
- The hypervisor server contains file server, mail server, print server and applications server.
- An incremental tape backup is completed every week and stored in an off-site fireproof safe.
- Mobile phones and laptops are not allowed in the building and there are no Wi-Fi connections available.

## **Director of Cyber Security**

Stevenson Research has recently appointed a Director of Cyber Security.

The responsibilities of the Director of Cyber Security include:

- Production of policies and procedures
- Day-to-day management of cyber security
- Risk management
- Identification of different threats to the network and how to mitigate these threats
- Implementation of different measures to identify vulnerabilities in the network.

## **Further Research**

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

- The different types of data stored by Stevenson Research and their importance.
- Different types of cyber security threats that Stevenson Research may be subjected to.
- Different types of attacker, their characteristics and motivations for attacking Stevenson Research.
- The impact of a cyber security incident on Stevenson Research.
- Justification for the different methods of mitigating risk.
- The use of different types of detection systems.



Oxford Cambridge and RSA

**Copyright Information:**

OCR is committed to seeking permission to reproduce all third-party content that it uses in its assessment materials. OCR has attempted to identify and contact all copyright holders whose work is used in this paper. To avoid the issue of disclosure of answer-related information to candidates, all copyright acknowledgements are reproduced in the OCR Copyright Acknowledgements Booklet. This is produced for each series of examinations and is freely available to download from our public website ([www.ocr.org.uk](http://www.ocr.org.uk)) after the live examination series.

If OCR has unwittingly failed to correctly acknowledge or clear any third-party content in this assessment material OCR will be happy to correct its mistake at the earliest possible opportunity.

For queries or further information please contact the Copyright Team, OCR (Oxford Cambridge and RSA Examinations), The Triangle Building, Shaftesbury Road, Cambridge CB2 8EA.

OCR is part of the Cambridge Assessment Group. Cambridge Assessment is the brand name of University of Cambridge Local Examinations Syndicate (UCLES), which is itself a department of the University of Cambridge.