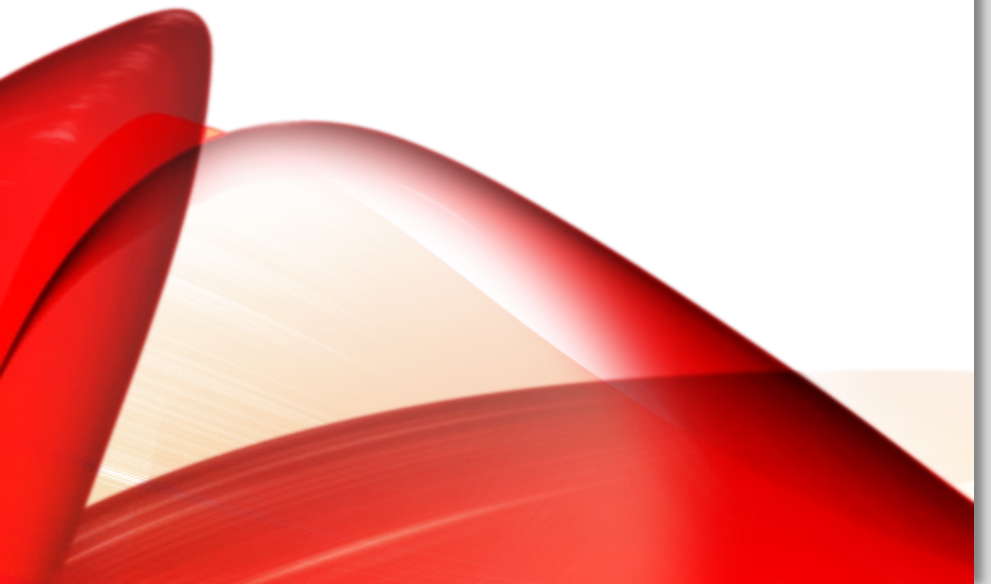
SECURITY PERSONNEL

Data Security

DIFFERENT TYPES OF PERSONNEL



The security personnel will vary depending on the size of the company, its IT infrastructure, employee numbers and type of sector it operates in, as well as the type of data it holds.

CHIEF INFORMATION SECURITY OFFICER (CISO)

This person oversees security and has overall responsibility for ensuring that the security of the physical network and data is maintained.

They will lead a team of experts and must oversee the development of security plans and policy designed to protect against a cyber-attack.

FORENSIC ANALYST

A forensic analysist would have a computing science background, and have specialist skills and knowledge on how data is stored in digital devices.

They can retrieve data that has been lost or damaged.

They would also be able to use forensic tools to help them figure out how a data breach occurred.

EDUCATION SPECIALIST

Specialists in cyber security education would be employed to conduct training workshops.

They would make sure that staff have good cyber hygiene and are aware of good practice when it comes to security.

These sessions would be available to all staff, and would allow staff to ask questions about their company's cyber security policies.

PENETRATION TESTER

Penetration testers, or ‘white hat hackers’, are used to try to break into a system and exploit weaknesses in a company’s security.

They would have the same set of skills as a ‘black hat hacker’ but are employed to help defend against people trying to exploit weaknesses.

They would run various tests and then report back on what they have discovered, and outline the steps needed to protect the network and data.

Penetration testers will also test the physical security of a company.

They will try to gain unauthorised access to buildings and other secure locations of the company.

INFORMATION SYSTEM SECURITY OFFICER (ISSO)

This role involves making sure that all private data belonging to the company, its employees and its customers remains confidential.

The ISSO is also responsible for implementing, testing, and reviewing a company's cyber security.

The ISSO will monitor networks, install software and implement security measures, while informing users about the security measures they must take to avoid or limit an attack.

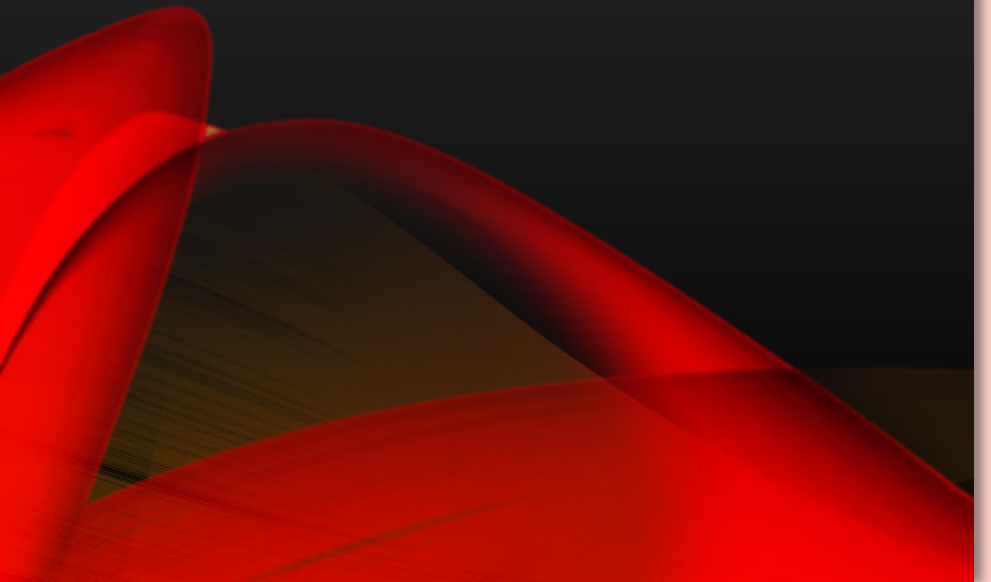
SECURITY ANALYST

The security analyst is responsible for analysing the current security measures in place, and determines how effective these are.

They will create documentation to help the company deal with a data breach or a cyber-attack, and will make recommendations on how to improve overall network security.

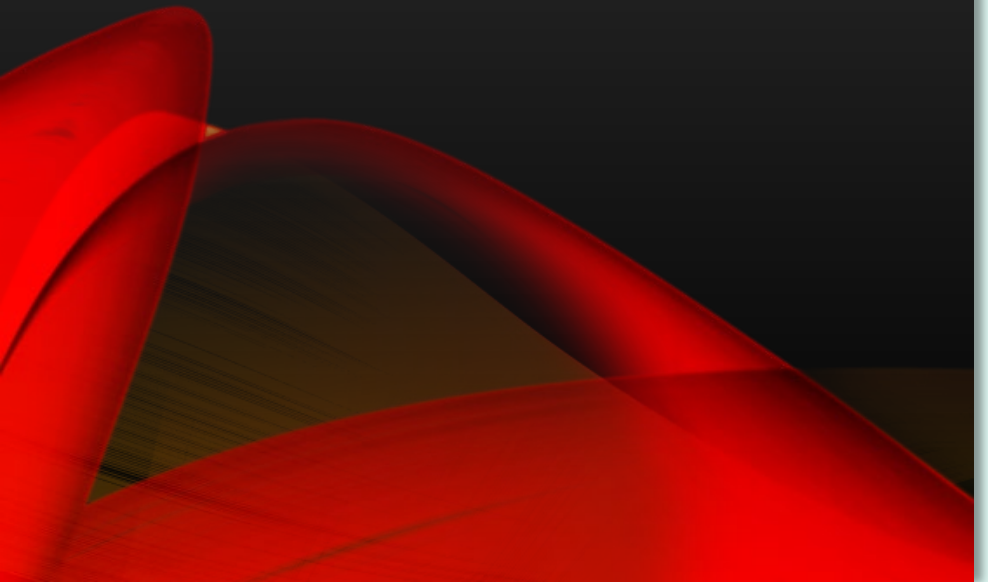
They also have a responsibility to maintain data integrity within the company.

OUTSOURCING



Depending on how much money the company turns over, they may employ an external agency to look after the security of the network and cyber defences.

ONE-MAN TEAMS



Due to the size of the company and the amount of money they turn over, they may only have one person responsible for everything.

They would be responsible for network security and cyber training of staff.

NETWORK MANAGER

Responsible for a team of network engineers who will maintain the computer networks, update software to latest versions, install antivirus and antimalware, and carry out the maintenance of hardware throughout the company.

The network manager will give users access rights to different parts of the network, depending on their position within the company.

Different users will have different access rights to the network.

They also have a disaster recovery plan in case the network goes down, and they are responsible for having a backup strategy for data.

Depending on how much money the company turns over, they may employ an external agency to look after the security of the network and cyber defences.

Now do Task 13

TASK