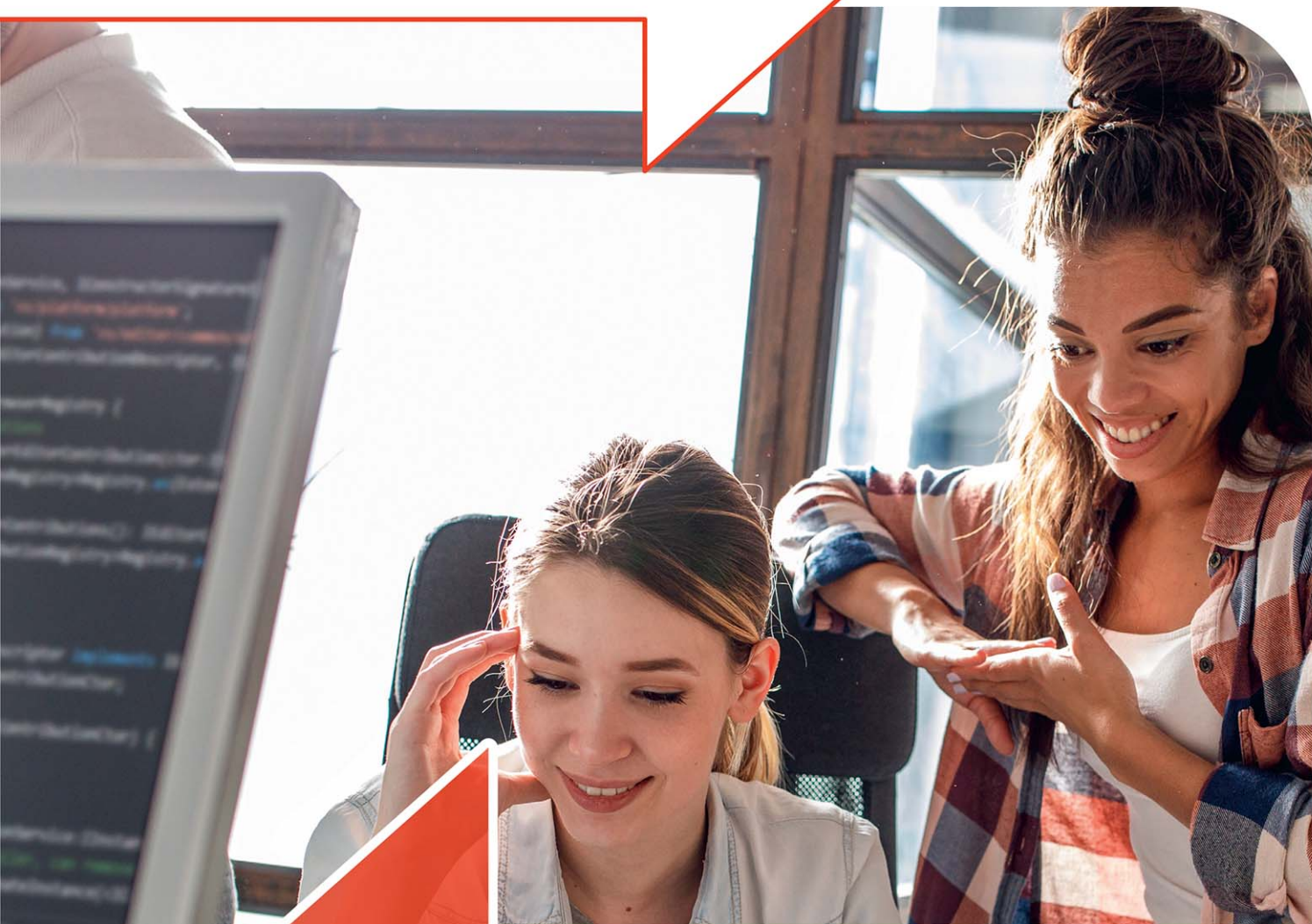


T-LEVELS

THE NEXT LEVEL QUALIFICATION



DIGITAL

Mo Everett
Sonia Stuart

DIGITAL SUPPORT SERVICES: CORE
DIGITAL BUSINESS SERVICES: CORE

NCFE
ENDORSED

Boost

HODDER
EDUCATION
LEARN MORE

Contents

Guide to the book	iv
-------------------------	----

THE CORE

Core element 1	Business context	1
Core element 2	Culture	59
Core element 3	Data	73
Core element 4	Digital analysis	100
Core element 5	Digital environments	112
Core element 6	Diversity and inclusion	153
Core element 7	Learning	166
Core element 8	Legislation	188
Core element 9	Planning	216
Core element 10	Security	236
Core element 11	Testing	270
Core element 12	Tools	279
	Core skills	295
	Assessment	303
	Glossary	317
	Index	325

ONLINE MATERIAL

Pathway Core element 1: Careers within the digital support services sector

Pathway Core element 2: Communication in digital support services

Pathway Core element 3: Fault analysis and problem resolution

Access this content at www.hoddereducation.co.uk/digitalsupportservices/pathwaycore

Guide to the book

The following features can be found in this book.

Learning outcomes

Summaries of the knowledge outcomes that you need to learn in each content area.

Case study

Scenarios that place content into real-world contexts.

Key term

Definitions of key terms.

Test yourself

Short questions designed to test your knowledge and understanding.

Industry tip

Tips and advice to help you in the workplace.

Assessment practice

Knowledge-based practice questions to help you to prepare for the core exams.

Important point

Important points that you need to be aware of.

Project practice

Short scenarios and focused activities reflecting one or more of the tasks that you will need to undertake during completion of the employer set project.


Activity

Short activities that encourage you to apply the knowledge and skills covered in the Student Book.

Research

Research-based activities – either stretch-and-challenge activities, enabling you to go beyond the course, or industry placement-based activities encouraging you to discover more about your placement.

Core element 10: Security



In this core element you will learn about the potential risks and threats to the digital systems used by organisations. You will apply your understanding of the implications of these to digital systems themselves, as well as to organisations and their stakeholders. You will also learn about the relationships between the different aspects of the data and information that an organisation stores and uses, including confidentiality, integrity and availability.

Each of these risks or threats can be mitigated against to limit its impact and to reduce the threat of it happening again. You will learn about a range of measures that can be used to do this. You will learn about several types of security. Cyber security is the most important type in relation to digital systems, data and information. Physical security can also be used to protect digital systems, data and information, including closed-circuit television and access badges.

Learning outcomes

In this core element you will learn about:

- | | |
|---|--|
| 10.1 Types of confidential company, customer and colleague information | 10.5 The potential impacts of threats and vulnerabilities on an organisation |
| 10.2 The importance of maintaining and the consequences of not maintaining confidentiality, integrity and availability | 10.6 Risk mitigation controls to prevent threats to digital systems |
| 10.3 The technical and non-technical threats that may cause damage to an organisation | 10.7 The process and protocols of internet security assurance |
| 10.4 The technical and non-technical vulnerabilities that exist within an organisation | 10.8 The interrelationship of components required for an effective computer security system |

10.1 Types of confidential company, customer and colleague information

Important point

All businesses and organisations will have data and information that need to be kept secure, classified and confidential, which should be covered by the confidentiality, integrity and availability (CIA) triad. What data and information are stored will depend on the function of the organisation and will differ from sector to sector.

Confidentiality relates to data, while privacy relates to the individual. In this context an 'individual' can be a single person, a business or an organisation.

The General Data Protection Regulation is covered in section 8.1, p. 202.

The CIA triad is covered in section 10.2, p. 239.

Typically, an organisation will store information about:

- ▶ human resources
- ▶ commercially sensitive information
- ▶ access information.

It is important that this information is kept confidential. Any breaches relating to the information can have a serious impact, leading to the possible loss of clients or business. This in turn can lead to a downturn in the health of the organisation which may, ultimately, lead to the organisation's failure.

Human resources

Human resources (HR) will store and update any data and information held about everyone who works in a business or organisation, irrespective of their job role. The main data and information held include:

- ▶ employee salaries
- ▶ employee perks
- ▶ employment data
- ▶ medical information.

The data held by HR is confidential, personal and should be stored following legislation guidelines related to the storing and processing of data.

Employee salaries and perks

Salaries should only be known by the employee and the HR department. It is important that this information is kept confidential as different employees carrying out the same task may be paid different salaries based on the number of years they have worked for the organisation, their experience and other factors such as qualifications and training courses attended. It is illegal to pay different salaries on the basis of gender as this would contravene the Equality Act. (Protected characteristics are covered in section 6.1, p. 156.) Data held by HR about salaries will also include National Insurance number and tax codes.

Many employers provide perks. Workplace perks can range from retailer discounts to free tea and coffee. Individual employee perks can include extra days holidays for long service or discounts on health insurance. Which employee gets which perk should, as with salaries, only be known by the employee and the HR department.

Employment data and medical information

Employment data will typically include start date, qualifications, contact details and emergency contact details. This data may also include any warnings about a breach of policy and disciplinary action. Medical data will be stored as an employer has a duty of care to provide, where required, adapted equipment and reasonable adaptations to enable their staff to carry out their job role. This is covered under the Equality Act. Staff may also require time off to attend medical appointments related to any medical condition.

Legislation is covered in section 8.1, p. 189.

Commercially sensitive information

Any business or organisation will store information which can be classed as commercially sensitive. This means that if the information was leaked, competitors could use it to gain a commercial advantage.

Commercially sensitive information includes:

- ▶ sales revenue
- ▶ trade secrets
- ▶ profit margins
- ▶ client/customer details
- ▶ stakeholder details
- ▶ contracts
- ▶ intellectual property.

Client and customer details

All organisations interact with people – clients and customers. Client lists and customer information are business-sensitive information that result from these interactions.

Client details may include individuals, but may also include named representatives from different organisations or businesses. Client details include anyone who interacts with the organisation and they should not be accessed by employees unless absolutely necessary. Clients may interact with the organisation by using the services provided. For example, a client may use the services of an organisation that provides cloud-based storage facilities. Many organisations will have a client relationship team that looks after clients so this team will need access to this information.

Customer details usually relate to those who buy goods or services. The information held about customers will typically include personal details such as name and contact details but may also include order history.

If the privacy and confidentiality of client and customer details are not maintained, the organisation could lose clients and customers. People expect that any organisation storing their personal data will keep it safe and secure to limit any breaches. A breach of personal data can impact the organisation and also the people whose data has been leaked.

Activity

Select an online retailer. Define the data that would be held about the customers. What would the impact on the retailer and customers be, including the consideration of relevant legislation (see Core element 8), if there was a data breach leading to the loss of this data?

Create a digital communication detailing your findings. Present your findings to your group.

Stakeholders and sales revenue

Most organisations have **stakeholders**. Depending on the size and type of the organisation these may be shareholders – **external stakeholders**. Employees can also be classed as **internal stakeholders**. Some organisations may have a policy of keeping stakeholders informed about sales numbers as this may have a financial impact. Some organisations provide a financial bonus to employees or a dividend to investors

or shareholders based on the previous year's sales numbers and revenues. Sales numbers can also be used to determine the goods that are bought and sold by the organisation. For example, goods that have low sales numbers may be reduced in price and not stocked again while those goods with high sales numbers will be restocked to continue the sale of them to customers.

Profit margins

The profit margin set on any goods supplied should also be kept confidential. The profit margin is the difference between the price paid for the goods and the selling price. Where the price of the goods is reduced, the profit margin will also reduce.

Contracts

A contract will be in place where goods are bought from a third party. The contract will usually include the delivery time, quantity required and the price to be paid. These details will be negotiated and should be kept confidential between the two parties. Any breach in this could lead to other companies having a stronger negotiating power.

Trade secrets and intellectual property

Where an organisation sells specific goods, these could be classed as a trade secret. Trade secrets often apply to a patent.

The Copyright, Designs and Patents Act is covered in section 8.1, p. 199.

The Intellectual Property Act (IPA) also covers software processes in addition to patents for tangible items. This means that if the function of the organisation is to provide cloud-based services then the software processes used by the organisation could be covered by the IPA.

Key terms

Stakeholders: anyone with an interest in a business or organisation. Stakeholders can be individuals, groups or other organisations, or businesses that are affected by the organisation's activity.

External stakeholders: groups outside an organisation, for example shareholders.

Internal stakeholders: groups within an organisation, for example owners and employees.

Activity

Using the same online retailer as in the previous exercise, define the data that could be held about the goods that are sold. What would the impact on the retailer and stakeholders be if the data was breached?

Create a digital communication detailing your findings. Present your findings to your group.

Access information

It is important that any access information provided to staff, at all levels, is kept confidential. This is to maintain the security of the workplace and the digital devices on which data and information are stored. The access information stored will include:

- ▶ passwords
- ▶ multi-factor authentication
- ▶ email accounts
- ▶ phone numbers
- ▶ access codes.

Passwords, multi-factor authentication and access codes are covered in section 10.6, p. 253.

How a threat can be carried out using email accounts and phone numbers is covered in section 10.3, p. 244 about malicious spam.

Test yourself

- 1 What is meant by privacy?
- 2 What are the two different types of stakeholders?
- 3 How do clients interact with an organisation?
- 4 Who should access employee salaries?
- 5 What is meant by profit margin?

10.2 The importance of maintaining and the consequences of not maintaining confidentiality, integrity and availability

Security, in particular cyber security, aims to protect digital systems, data and information. **Cyber security** attempts to:

- ▶ act as a deterrent against attackers and hackers
- ▶ prevent an attack from happening

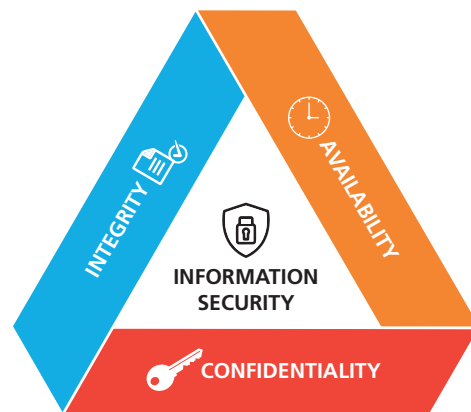
Key terms

Cyber security: the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks.

Confidentiality, integrity and availability (CIA): also known as the CIA triad.

- ▶ detect and warn users of the digital systems that an attack is happening.

The main purpose of cyber security is to maintain the **confidentiality, integrity and availability (CIA)** of digital systems, data and information.



▲ **Figure 10.1** The CIA triad

Figure 10.1 shows the CIA triad, viewed here as a triangle with security in the centre. The CIA triad is a security model developed to define the important parts of cyber security and how they are interlinked.

- ▶ **Confidentiality** means that the digital systems, data and information resources are protected from unauthorised viewing and access (hacking).
- ▶ **Integrity** means that data is protected from unauthorised changes to ensure that it is reliable and correct.
- ▶ **Availability** means that authorised users have access to the digital systems, data and information they require.

The CIA triad shows the clear relationship between these three parts of cyber security. Looking at these in a triangle we can see that they overlap, but they can also work against each other when deciding which types of mitigation to use. Visualising things in this way enables an organisation to plan and prioritise the implementation of new security policies and processes.

A good example of how confidentiality, integrity and availability interact can be found in online banking:

- ▶ **Confidentiality** – it is important to a customer that their financial details are kept confidential between them and the bank. One strategy that can be used to maintain the confidentiality of the financial data is through access-level login. When a customer logs into the bank website their log-in details provide access only to their bank account (and no one else's).
- ▶ **Integrity** – the financial data of the customer must demonstrate integrity. This means that the customer can expect their financial data to be correct. For example, their recent transactions using their debit or credit cards should be true and accurate. The financial data should also be reliable, which is linked to its accuracy.
- ▶ **Availability** – customers should be able to access both the bank website and their financial records when they want and need to. If the website or personal financial data is not available, then this part of the CIA triad has been broken.

The importance of maintaining confidentiality, integrity and availability

It is important that any business or organisation maintains CIA. By maintaining CIA:

- ▶ compliance with legislation and regulations associated with data can be maintained
- ▶ internal and external stakeholders can trust the business or organisation to keep data safe
- ▶ the business or organisation will have a positive brand image which may lead to an increased customer base so leading to more profit
- ▶ security risks and unauthorised access to data can be minimised.

Stakeholders are covered in section 1.1, p. 2.

Legislation is covered in section 8.1, p. 189.

The consequences of not maintaining confidentiality, integrity and availability

If CIA is not maintained, then the business or organisation may suffer consequences. These consequences include:

- ▶ financial
- ▶ legal
- ▶ reputational.

Financial consequences

The financial consequences can have a devastating effect. If data is breached, then fines can be issued under legislation relating to data. For example, the Data

Protection Act 2018 (DPA) and Computer Misuse Act (CMA) both have the provision to fine data holders where a breach has occurred.

In addition to the fine issued under the legislation, compensation will also have to be paid to the customers whose data has been part of the breach. The DPA requires data to be kept secure, usually by following the CIA triad. This means that measures must be put in place to prevent unauthorised or unlawful processing of data. Data must also be protected against accidental loss, destruction or damage. If a breach occurs, then those whose data is involved can make a claim for compensation. Refunds of any extra costs may also need to be paid. For example, if airline tickets need to be changed, then the cost of doing this can be claimed back.

When a data breach occurs, it is possible that the reputation of the business or organisation will be damaged. Customers need to be assured that their data is safe. After a breach it is probable that customers will move away as they feel their data is unsafe. This reduction in customers will cause a decrease in trading, leading to a reduction in revenue or earnings.

Legal consequences

The legal consequences of not maintaining the CIA triad can also have dire consequences. After a data breach, those whose data has been affected can take legal action. This can, as already discussed, have financial consequences in terms of paying compensation and refunds, as well as any legal action taken under the DPA and CMA. Suppliers or customers can also terminate their contacts if a data breach occurs. This will have an operational impact. If suppliers refuse to allow their data, which is often business sensitive, to be stored and processed, then they may withdraw from supplying goods and/or services – terminate their contract. Customers may also terminate contracts as they do not trust the security of their data.

Reputational consequences

The damage to reputation after a data breach can also have dire consequences. The main issue will be that customers/clients may refuse to deal with a business or organisation that cannot maintain the security of their data. This decrease in customers will also have a negative effect on the brand. As data breaches have to be reported to the ICO it is highly likely that, with the increased use of websites including social media, news of the breach will travel very quickly.

Research

Three high profile businesses – Adobe, eBay and British Airways – have been victims of data breaches.

Investigate one of these data breaches for each business. For each breach, explain how the CIA triad was broken. Consider the impact on the customers of, and consequences to, these businesses.

Create a presentation showing the results of your findings. Present your findings to your group.

Test yourself

- 1 What does the I in CIA stand for?
- 2 How is the CIA security model represented graphically?
- 3 Define confidentiality.
- 4 Describe one reason why CIA should be maintained.
- 5 Identify one Act that can be used to issue fines following a data breach.

10.3 The technical and non-technical threats that may cause damage to an organisation

There are many technical and non-technical threats that can have an impact on systems, data and information. It is important that cyber security is considered by everyone who uses a digital system. This covers large multinational organisations, governments and individuals. Digital systems store and use a wide range of data and information, all of which are important and, if lost or stolen, can have far reaching impacts.

Every industry, business, organisation and individual can be the target of technical threats. Every digital system, irrespective of where and why it is used, can also suffer vulnerabilities. The technical threats will vary depending on the nature of the data and information held and the motivation of the attacker.

Technical threats

There are many technical threats that can affect systems, data and information. These include:

- ▶ botnets
- ▶ denial of service (DoS)
- ▶ distributed denial-of-service (DDoS)

- ▶ hacking
- ▶ malware
- ▶ malicious spam.

Bots/botnets

The aim of a bot/botnet is to take control of a digital system. A bot is a type of malware that allows a cyber security attacker to take control of a digital system that has been infected without the user's knowledge. It can result in a botnet which is an interconnected network of infected computer systems.

Denial-of-service

This is an attempt to make a digital or network system unavailable to its users. The result of a DoS attack is that users are unable to access the digital or network system. The attack is usually focused on, for example, email, websites and online accounts (e.g. banking). The DoS attack floods the digital system under attack with network traffic until the digital system can no longer either respond to the requests, or crashes, preventing access for users. A DoS attack uses only one digital system to carry out the attack.

Distributed denial-of-service

This is another type of attempt to make a digital or network system unavailable to its users by flooding it with network traffic. A DDoS attack has the same aim as a DoS attack, but a DDoS attack uses many digital systems to carry out the attack. A DDoS is usually focused on preventing a website or internet service from either functioning efficiently, or at all, either temporarily or indefinitely. DDoS attacks usually target websites or services hosted on high-profile web servers, such as banks, payment websites, for example. Google Pay or PayPal, and mobile phone companies.

Test yourself

- 1 What is a botnet?
- 2 What is the aim of a DoS threat?
- 3 What is the difference between a DoS and a DDoS?
- 4 What type of websites are usually targeted by a DDoS threat?

Hacking

Hacking can take many forms. These include using techniques such as:

- ▶ cross-site scripting (XSS)
- ▶ password-cracking software
- ▶ SQL injection (SQLI).

Type of malware	Why it is used	How it works
Adware	Adware generates revenue for its author.	Adware is also known as advertising-supported software. This is any software package which automatically shows adverts, such as pop-ups. It may also be in the user interface of a software package or on an installation screen. Adware, by itself, is harmless; however, some adware may include spyware such as key loggers.
Key logger	Key loggers can take two forms. They can be legitimately installed to monitor users or can be installed maliciously.	Key loggers collect information and send it back to a third party. Algorithms are used to monitor keyboard use through, for example, pattern recognition. Some key loggers will only collect keyboard strokes into one website or application. Others record every keyboard stroke including any information/data that is cut and pasted.
Remote access Trojan (RAT)	RATs access and infect digital systems, usually through the internet.	RATs are typically installed without user consent and remain hidden to avoid detection, allowing a hacker to control your device remotely. When a RAT is connected to a digital system, the hacker can access and use the files and folders, login and personal details or use the connection to download viruses that could infect other digital systems.
Ransomware	Ransomware holds a digital system captive and demands a ransom, usually money, to release it.	Ransomware can restrict user access to the computer system by encrypting files or locking down the computer system. A message is usually displayed to force the user to pay so that the restrictions can be lifted and the user has access to the data/computer system. It is spread like a worm and can be started by downloading an infected file or by a vulnerability on the computer system.
Spyware	Spyware can collect data from an infected digital system, including personal information like websites visited, user logins and financial information.	Spyware is usually hidden from a user and can be difficult to detect. It is often secretly installed on a user's personal computer without their knowledge. However, some spyware such as key loggers may be installed to intentionally monitor users. Spyware can also install additional software or redirect web browsers to different websites. Some spyware can change computer settings which could lead to slow internet connection speeds or changes in web browser settings.
Trojan	A Trojan is a standalone malicious program designed to give full control of a digital system to another digital system.	Trojans often appear to be something which is wanted or needed by the user of a digital system. They can be hidden in valid programs and software. Trojans can make copies of themselves, steal information or harm their host digital system.
Virus	A virus attempts to make a digital system unreliable.	A computer program that replicates itself and spreads from computer to computer. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by other computers.
Worm	A standalone program that replicates itself so it can spread to other digital systems.	A worm can use a network to spread. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause some harm to a network, even if only by consuming bandwidth.

▲ **Table 10.1** Different types of malware, why they are used and how they work

Test yourself

- 1 What is the purpose of adware?
- 2 What does RAT stand for?
- 3 How does ransomware work?
- 4 Identify one example of how spyware can change settings on a digital system.
- 5 What does a worm do to bandwidth?

Malicious spam

Spam is junk email. But, unlike the physical junk mail that arrives though snail mail, spam can be malicious and attempt to trick users into providing details such as personal or financial information. Malicious spam can take many forms including email, phone calls and text messages.

Table 10.2 shows different types of malicious spam, why they are used and how they work. Many victims of malicious spam are people who are not tech-savvy.

Malicious spam	Why it is used	How it works
Pharming	Pharming is malicious spam that tries to redirect users from a genuine website to a fake one. This is done without the knowledge of the user.	Pharming is very similar to phishing in that both use fraudulent websites. The main difference is that a phishing attack will use fake or hoax emails while pharming attacks very rarely use this type of tactic.
Phishing	Phishing tries to get users to input, for example, their credit or debit card numbers and security details, or log-in details into a fake website.	Phishing uses a fake website which looks identical to the real one. The most common targets for phishing are bank, building society and insurance websites. The attackers send out emails or text message which pretend to be from, for example, your bank. A link is contained in the email which you are asked to click on. This link takes the user to a fake website.
Smishing	Smishing is a form of phishing and is the fraudulent practice of sending text messages.	Smishing is when someone tries to trick you into giving them your private information, such as passwords or credit card numbers, via a text or SMS message which pretends to be from a reputable company.
Spear phishing	Spear phishing is a form of phishing. The emails are sent to specific and well-researched targets alleging to be from someone they know and trust.	An email is sent alleging to be from a trustworthy source and redirects the user to a bogus website full of malware.
Vishing	Vishing is making phone calls or leaving voice messages pretending to be someone they know and trust.	The calls and messages pretend to be from reputable companies to try and trick people into revealing personal information, such as bank details and credit card numbers.

▲ Table 10.2 Different types of spam, why they are used and how they work

Buffer overflow

A **buffer** overflow threat is probably the most common threat to software. The threat occurs when data is being written to a buffer which overruns the buffer capacity. The data then exceeds the buffer boundary and overflows into other buffers. When this happens the data in the other buffers is corrupted or the data is overwritten. The threat can overwrite executable code with malicious code or can selectively overwrite code which can lead to the normal function of the program being changed.

Legacy programming languages, for example C and C++, are more vulnerable to a buffer overflow attack. This is because these languages have no built-in checking or protections. Languages such as Python and Java do have built-in features to minimise the possibility of a buffer overflow but do not totally reduce the possibility of this type of threat.

A buffer overflow threat can lead to a change in the program's execution path and expose data. New code can be inserted into the program code to enable unauthorised access.

Research

The Wannacry ransomware attack used the buffer overflow technique.

Investigate how the Wannacry attack began, how it spread so quickly and how it was stopped.

Discuss your findings with the rest of your teaching group.

Key term

Buffer: contains data stored in random access memory for a short amount of time before it is used.

Research

In 2015 a US health insurance company, Anthem, suffered a data breach. Social engineering was thought to have provided the access codes to the customer database.

Identify the different types of social engineering and describe how each type could have been used to gather the required access codes.

Lightning strikes are another natural disaster that can affect computer systems and devices. A lightning strike can cause a surge or spike in the electricity supply. These surges can affect how hard drives and other storage devices operate.

Research

Investigate the different devices that can be used to protect against power surges. Identify where each device could be used.

Natural disasters

With the increase in the use of digital devices and the cloud, there are external threats, also known as environmental or natural disasters, that can affect data, information and digital systems.

If a natural disaster occurs, for example an earthquake, then it is probable that internet access could be lost. This could mean that any data and information stored in the cloud could be inaccessible. The impact of inaccessible data and information could affect the recovery from a natural disaster.

It would also be possible that digital devices could be destroyed during a natural disaster. If a tsunami or flood happened, the water coming onto the land could destroy or wash away buildings. If digital devices were in these buildings, then they would be destroyed or lost. The cabling infrastructure or any internet service equipment could also be affected. Even if buildings could be made safe, the tremors that can happen with a natural disaster, such as an earthquake, could damage any hard drive surfaces causing the data and information stored on them to be unreadable.

Even if physical backups were available, there is a probability that these would also be affected by the same natural disaster. If the backups were stored in the cloud, then these may also be inaccessible as there may be no internet access.

Power failure is one of the potential after-effects of a natural disaster. As digital systems need electricity to either charge or operate, this will also mean very limited accessibility of data and information, and the digital devices these are stored on. One method that can be used to keep digital systems operating is to use batteries or a power generator as backup power sources. However, the batteries must be kept fully charged and fuel must be available to run the generator.

Test yourself

- 1 What is a turncloak?
- 2 What are the two steps involved in cross site scripting (XSS)?
- 3 Why is phishing used?
- 4 Which type of programming language is most at risk from buffer overload?
- 5 Identify two types of natural disaster (environmental) threat.

10.4 The technical and non-technical vulnerabilities that exist within an organisation

Technical and non-technical vulnerabilities can increase the chances of a threat occurring to an organisation.

You will learn about the ways to mitigate against these vulnerabilities in section 10.6, p. 249.

Technical vulnerabilities

Weak or outdated encryption

There are two different types of encryption and a stronger method of encrypting data called hashing. What is important is that, whether encryption or hashing is used to secure data, the software used is updated to the latest versions as released by the vendor. Checking for updates to encryption software should form part of scheduled, routine maintenance tasks.

Out-of-date software, hardware and firmware

All the components of a digital system will, eventually, become out of date. Vendors and manufacturers will

Non-technical vulnerabilities

Employees

As already discussed, people are the weakest link in any security procedure or process.

All businesses and organisations will have policies and procedures which must be followed to maintain a high level of security. It is important that employees read, understand and act on the policies and procedures. Training and continuing professional development should be carried out on a regular basis to maintain awareness of the contents of the security policies and procedures and to increase the competency of staff. If staff are not competent then they may be unable to follow the contents of policies and procedures because they do not have the necessary skills. When staff are being recruited, questions about the skills and competencies of the applicant may need to be included on the application document. This information could be verified through the use of practical assessments prior to an offer of employment. This is called recruitment screening.

Poor data/cyber hygiene

It is important that the data and information stored continue to be useful and up to date. This is also one of the requirements of the Data Protection Act. A vulnerability could occur if an employee has left, but their account and log-in credentials are still 'live'. This means if the employee was disgruntled about the termination of their employment, they could still access the digital systems and the stored data. Ex-employees who hold a grudge are also susceptible to social engineering attacks. To close this vulnerability, data about clients, customers and suppliers should be reviewed and cleaned on a regular basis but data related to employees who have left should be archived as soon as they leave employment.

Malicious employees and turncloaks are covered in section 10.3, p. 245.

The Data Protection Act is covered in section 8.1, p. 202

User access, policies and procedures, and user access restrictions, are covered in section 10.6, p. 253.

Physical access controls

While it is important that data is kept secure with authenticated and authorised users having access, the physical environment should also be protected. While physical access controls can be implemented, it is how they are used that could cause the vulnerabilities.

Many physical environments have door access codes which must be input before access to the room is granted. Like many other security procedures, these codes should be regularly changed, with only staff who need access to those rooms being provided with the updated codes.

It is not good practice to reuse access codes. The practice of using the same code for multiple doors and using weak, or easily guessed, codes, for example 1234, can also cause a vulnerability. For example, if an intruder manages to crack one access code, then they will have access to all other areas with that code. This will increase the potential damage that could be caused.

Limiting knowledge of access codes can ensure that only staff who need access to secure areas, for example server rooms, can gain access. It can, however, be difficult to monitor who has access to areas if simple key code locks are used. Access codes could be shared by staff which would lead to an increase in people who know the codes.

Security procedures should be put in place and reviewed at regular intervals. If security procedures are not adequate enough or are outdated, then the chance of an attack on the physical environment will increase.

Test yourself

- 1 What is backward compatibility?
- 2 Give an example of a weak password.
- 3 What is a fail-open software lock?
- 4 Why should users be authenticated and authorised?
- 5 What is a zero-day bug?

10.5 The potential impacts of threats and vulnerabilities on an organisation

Threats and vulnerabilities can have an impact on an organisation. Many of these impacts have already been covered in this core element when the threats and vulnerabilities have been described.

As a recap, the most common potential impacts are:

- ▶ loss of sensitive information
- ▶ unauthorised access to the system or service
- ▶ overload of the system to affect a service
- ▶ corruption of a system or data
- ▶ damage to system operations
- ▶ disclosure of private information and credentials

- ▶ unauthorised access to restricted physical environment
- ▶ essential security updates not installed.

10.6 Risk mitigation controls to prevent threats to digital systems

Digital systems and the data and information stored on them are very valuable assets, not only to the businesses and organisations that collect, store, process and use them, but also to each individual.

Data and information such as customer shopping records, financial data, and health data and information, are used for a variety of purposes. What is important is that all data and information are kept secure and protected from the large range of threats that could occur.

Activity

Find and watch the video called 'What is penetration testing' at www.cisco.com.

What are the main points related to the importance of cyber security raised in the video?

Make notes about your findings.

National Cyber Security Centre Cyber Essentials

The UK-based National Cyber Security Centre (NCSC) has developed guidance for businesses, organisations and individuals about cyber security. Cyber Essentials is a UK Government-backed scheme to help people learn about how to protect themselves against an attack.

Some of the guidance relates to:

- ▶ using a firewall to secure an internet connection
- ▶ selecting, and using, the most secure settings for hardware devices and software
- ▶ how to protect against viruses and malware
- ▶ how to control access to software and hardware devices
- ▶ how to keep hardware devices and software up to date.

Activity

Find the NCSC website. Investigate the guidelines and advice provided.

Select one area and create a digital communication to provide these details to the owner of a business.

Anti-virus and anti-malware

Anti-virus and anti-malware programs are security software designed to prevent, detect and remove viruses and other malware, including adware, Trojans and worms. It is essential that any digital system connected to the internet has some form of security protection. If security software is not installed then it is possible that within minutes of connection to the internet the system will be infected.

Security software performs several tasks including:

- ▶ scanning files or directories for any viruses, malware or known malicious patterns
- ▶ automatic real-time scanning
- ▶ performing a manual scan of a digital device
- ▶ removing any malicious code detected – sometimes you will be notified of an infection and asked if you want to clean the file; other programs will automatically do this behind the scenes
- ▶ blocking unsafe websites or alerting a user about infected emails.

When security software finds a malicious program on a digital system, the user is usually offered two options:

- ▶ to quarantine it so the software cannot infect the digital system – this option gives the vendor the opportunity to analyse the program so that they can offer an update to users
- ▶ to delete it – this option clears the digital system of the infection.

Automatic versus manual updates

Some security and application software updates automatically. This process is usually completed in real time. This means that when the computer system is connected to the internet the software will automatically be checking all the time for new updates. If an update is found, then the security software will automatically update it. This happens because new viruses and other security threats are being released all the time. These updates are known as **patches**.

Key term

Patch: software code that can be downloaded and installed, after the software program is originally installed, to correct an issue with that program.

This means that the user does not have to remember to manually check for updates and so the digital system is always protected from any threats.

If a business uses automatic updates of software then they do not have to remember to manually check for updates and can be sure that their digital system is as up to date as possible. This also means that any vulnerabilities identified by the vendor are solved before an attack can take place.

Manually updating security software can be dangerous to the digital system and the data and information held on it. Employees can forget to carry out manual updates and this can leave the digital system vulnerable to threats.

A manual update for security software could be completed on an ad hoc basis or can be set to check at a specified time (scheduled) by a user.

One of the problems with manual updating of security software is the time it can take to download the patch. There may also be a time delay between the patch being released by the software vendor and the time when the manual update takes place.

Another problem with manually scheduling an update is that the digital system must be switched on and connected to the internet for the update to be downloaded. If the manual update has been scheduled for a time when the business system is switched off, then the business will never get updates or download patches. This can leave the digital system open to attacks and threats and could result in data being lost or stolen.

Some users, however, may prefer to update their software manually because they want to look at the updates to decide whether or not to download them. Some users may consider the updates to be intrusive or not appropriate.

Activity

Choose any two of the different providers of anti-virus software – look on the internet to see the different providers available.

Copy and complete this table to show the features which are available (two features have been given for you). You may need to add more rows to the table.

Feature	Provider 1	Provider 2
Internet links scanner		
Live support		

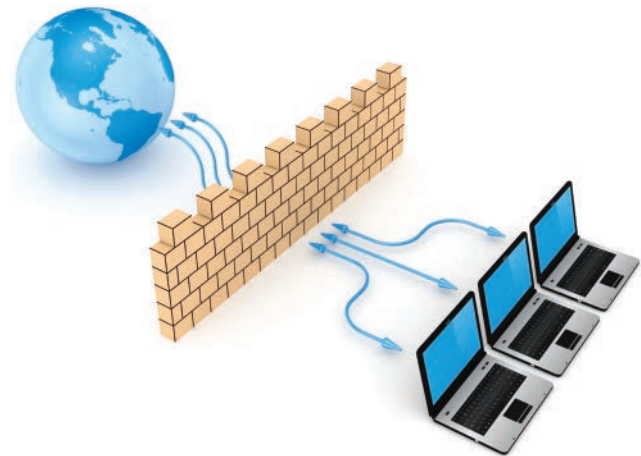
Test yourself

- 1 Identify two tasks carried out by security software.
- 2 Manual updating can be carried out. Identify the other method of updating.
- 3 Describe one disadvantage of manual updating.

Firewalls

A firewall is a security device that mitigates against threats by examining **data packets**. A firewall can be either hardware or software or both, but hardware and software firewalls work in the same way.

The purpose of a firewall is to establish a barrier between a digital device and/or a network and incoming traffic from external sources (such as the internet). Firewalls monitor the traffic that flows into a digital device and/or a network through an internet connection. The firewall blocks malicious traffic, like viruses and hackers, based on security rules.



▲ **Figure 10.3** A firewall acts as a barrier against threats to a system's security

There are two formats of firewall:

- ▶ A **software** firewall is a program that monitors traffic through port numbers and applications.
- ▶ A **physical** firewall is a piece of hardware installed between the network and the gateway.

Key term

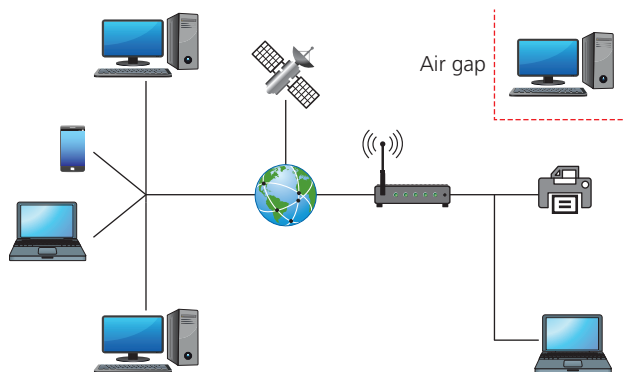
Data packets: small units of data which are sent and received when accessing the internet or any other type of network.

Activity

Invite a member of the IT Department to talk to your group about the routine maintenance carried out in your centre or workplace. Ask about the tasks carried out, the schedule, how maintenance is documented, what the procedures are for emergency maintenance, and how users are advised about any system downtime.

Air gaps/gapping

Air gapping is creating a digital system that is physically isolated from potentially dangerous networks, such as the internet. Air gapping is having a digital system that works offline.



▲ **Figure 10.11** An air-gapped digital system

As shown in Figure 10.11, an air-gapped digital system is one that is not connected, either physically or wirelessly, to other systems or networks. It is usually a standalone system or a network of digital systems that has no external links to any other system.

The name air gap refers to the concept that there is air between the digital system and any other system or network, including the internet. This means that the air-gapped system cannot be the victim of a threat or attack through another network. To carry out an attack on an air-gapped system would require the attacker to be physically sitting at the system.

There are still threats to an air-gapped system. The main threat is the use of removable storage devices. For example, a user downloads an infected file from a network onto a USB memory stick. This memory stick is then used to upload the infected file to the air-gapped

system. This means that the air-gapped system is now infected and has been the victim of a threat.

However, to some businesses and organisations, using the air-gapping technique to mitigate against threats is not always feasible. The reason digital systems are used in business is because users can share information and data, and access these data and information, from a centralised storage area.

But air gapping, if done properly, can provide complete protection to the air-gapped digital system. The other main advantage to using an air-gapped digital system is that, once the air gapping has been carried out, there are no ongoing, recurring costs.

Research

Investigate the types of industries, businesses and organisations that use air-gapped networks and the reasons why.

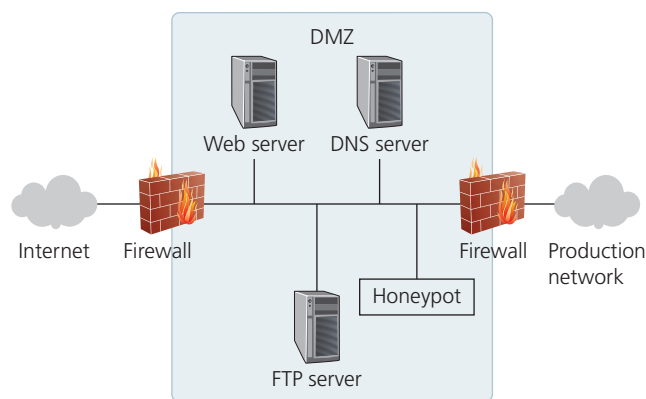
Test yourself

- 1 What is meant by an air-gapped digital device?
- 2 Describe one method of preparing an air-gapped digital device.
- 3 Describe how an air-gapped digital device could be compromised.
- 4 Identify one advantage of using air gapping as a way to mitigate against threats.

Honeypot

A honeypot is a digital system intended to behave like and copy a possible target including applications and data. It can be used to detect or deter attacks from a legitimate target. By using a honeypot it is also possible to gather intelligence about how attacks occur on digital systems.

By monitoring traffic to a honeypot system it is possible to identify which security procedures are strong and those which are weak. The weak procedures are those which will be exploited by attackers. By identifying the weak procedures it will be possible to improve security on the real digital systems that are being copied by the honeypot.



▲ **Figure 10.12** Where a honeypot sits in the network

The honeypot will appear to be part of a network – but it is isolated and closely monitored. Any interaction with the honeypot will be as a result of a possible threat as no authorised users will have access to it.

Research

There are three types of honeypot: pure, high interaction or low interaction.

Research each type, including examples of where they could be used.

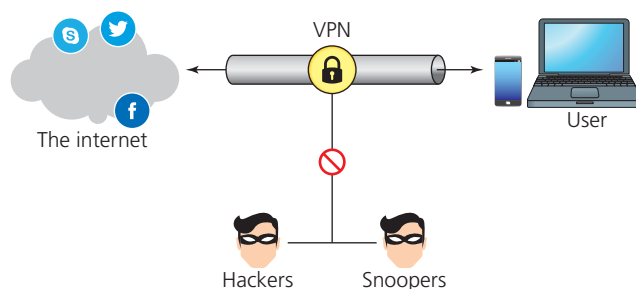
Discuss your findings with the rest of your teaching group.

Virtual private networks

Virtual private networks (VPNs) mitigate against threats by creating a secure connection to another network over the internet. This makes it possible to establish a private, safer and more secure network from a public internet connection.

VPNs were created as a method of connecting business networks together securely over the internet or to allow employees to access a business network remotely. VPNs also mask the **Internet Protocol (IP)** address, which means that online actions are virtually untraceable.

When a digital device is connected to a VPN the device appears to be in the same local network as the VPN. For example, if the VPN is based in Australia then it will appear that the connection is coming from Australia.



▲ **Figure 10.13** A VPN works to protect a user from threats by creating a secure connection to another network over the internet

Figure 10.13 shows how a VPN connection works. All traffic is sent from the digital device over a secure connection to the VPN private server. So, when the internet is browsed the digital device the website requested is contacted through the VPN. The VPN hides the device IP address, protecting the identity of both the device and the user. The VPN forwards the request and sends the response from the website back through the VPN secure connection to the device. A VPN creates a private tunnel from a device to the internet and hides data through encryption. It is also possible to set access controls on a VPN if it is being used by a business or organisation. By doing this, access to data stored on, for example, the cloud, can be limited to those who need access for their job role.

As can be seen in Figure 10.13, using a VPN makes it more difficult for attackers to access the information and data being transmitted. This is because if the data is intercepted then it will be unreadable until the final destination is reached.

Activity

Investigate available VPN providers.

Produce a presentation, including speaker notes, comparing the features they offer. Your presentation should help a business to compare different providers before selecting which one to use.

Key term

Internet Protocol (IP): the string of numbers an internet service provider assigns a device, for example 192.158.1.38.

Test yourself

- 1 What is the purpose of a honeypot?
- 2 Identify the three different types of honeypot.
- 3 How does a VPN mitigate against threats?
- 4 What do VPNs aim to mask?
- 5 Why is it difficult for attackers to access data that is being transmitted?

10.7 The process and protocols of internet security assurance

The security of digital systems, software and the physical environment have already been covered in this core element. However, most businesses and organisations have an internet presence. So, it is important that internet security is considered.

There are processes and protocols that can be used and utilised in internet security assurance.

Processes of internet security assurance

Installation and configuration of firewalls

The initial task to be completed when installing a firewall is to secure the firewall itself. There are four configuration changes that need to be completed to ensure the firewall is secure:

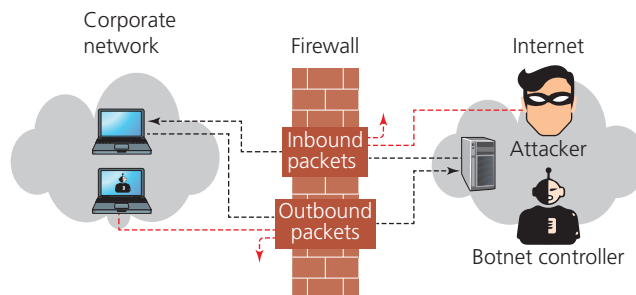
- 1 Update the firmware for the firewall to the latest vendor updates.
- 2 Delete, disable or rename any default user accounts changing all default passwords. Passwords should be changed to complex passwords or passphrases.
- 3 Each person who will manage the firewall should have their own user account. The privileges set on the account should be based on the responsibility. For example, the lead IT technician will have more privileges for the firewall than a trainee technician. Shared accounts should not be created as these will not provide a full and complete audit log detailing who made changes and why.
- 4 Define where changes can be made from. For example, changes can only be made internal to the network.

Firewalls are covered earlier in this core element, in section 10.6, p. 250.

Weak/default passwords are covered earlier in this core element, in section 10.4, p. 247.

Passphrases are covered earlier in this core element, in section 10.6, p. 255.

Inbound and outbound rules



▲ **Figure 10.14** Differences between an inbound and an outbound firewall

Firewalls can be set to monitor **inbound** or **outbound traffic** or both. The inbound and/or outbound rules the firewall will work to will need to be set. The rules will be used to inspect the data packets and determine if they should be blocked or allowed to continue on their journey. There are three rules that will need to be set:

- ▶ traffic type
- ▶ application
- ▶ destination and source.

Research

Research the different rules that need to be set up on a firewall.

Create a digital communication to explain these rules to a business owner.

Key terms

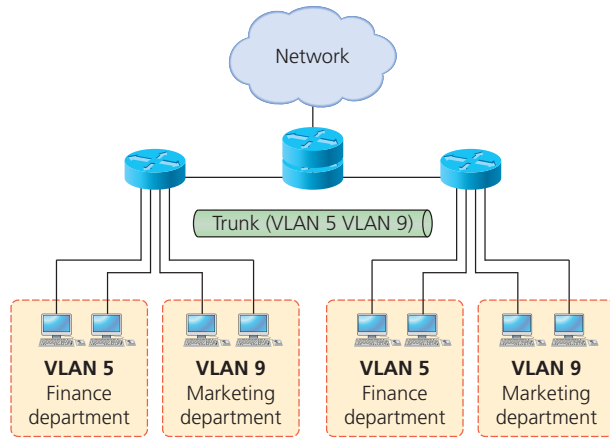
Inbound traffic: comes from outside the network through the firewall into the network.

Outbound traffic: comes from inside the network through the firewall out of the network.

Network segregation

Network **segregation**, also known as network **segmentation**, ensures that if an attack happens then not all of the network will be compromised.

Virtual local area network



▲ **Figure 10.15** A virtual local area network (VLAN)

A virtual local area network (VLAN) is the method used to logically separate out networks. Imagine a LAN for a business with multiple departments or even multiple geographical areas. A VLAN is used to separate each department's area on the network into a virtual network. It helps to increase the efficiency of what would be a very large LAN and saves on network resources. It also helps to reduce the time taken for the transmission of data packets (this is more commonly referred to as latency).

Advantages

- ▶ Provides more security control as each VLAN is a simulated/virtual separate network within a larger overall network. Therefore, sensitive information is not accessible by areas of the larger LAN/WAN.
- ▶ Latency is decreased (the data packets are transmitted around a smaller network area).
- ▶ Easier to scale upwards or downwards as each area can be addressed in isolation and not impact other areas on the main network
- ▶ It is easier to troubleshoot problems on a smaller network than a larger one.

Key term

Segregation/segmentation: dividing a computer network into smaller parts.

Disadvantages

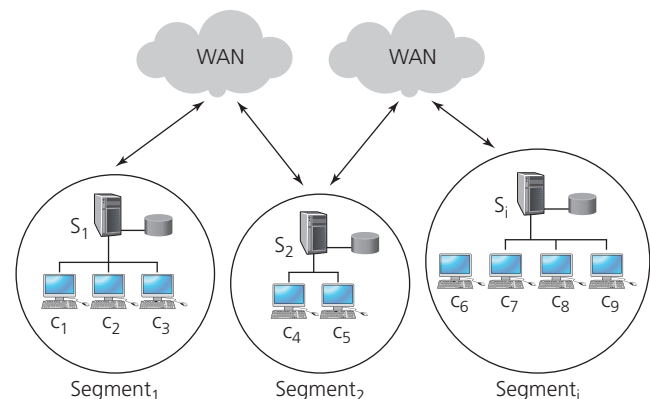
- ▶ It can be more expensive to implement as additional routers may be required to control the traffic of a very large network.
- ▶ Maintenance, including the addition of extra equipment, needs to be carried out using a logical and structured process to maintain existing VLAN segmentation.
- ▶ This means that implementation planning can take longer than other, simpler set-ups.

Physical network separation, or segmentation

This is when a large network is broken down into smaller physical components. Extra hardware may be needed like switches, routers and access points.

Switches, routers and access points are covered in section 5.2, p. 120.

One disadvantage of using physical segmentation is that it is financially expensive as extra hardware may need to be bought and installed, and there are the ongoing maintenance costs. Conflicts between the hardware can also occur. For example if two Wi-Fi access points (WAPs) are located in the same area then each will broadcast a different SSID.



▲ **Figure 10.16** Physical network separation

Research

Investigate the advantages and disadvantages (in addition to those given above) of physically separating (segmenting) a network.

Discuss your findings with the rest of your teaching group.

Offline networks

An offline network is one that is not connected to the internet. An air-gapped system is an example of an offline network.

Air-gapped systems are covered in section 10.6, p. 260.

Network monitoring

Network monitoring is running a system that constantly monitors a network to check performance. The system can detect slow or failing components and provide detailed feedback to the network management team.

Network monitoring is very similar to an intrusion detection system (IDS) in that the monitoring is constant and happens, once installed and set up, automatically. An IDS monitors threats and problems from traffic coming into the network, while network monitoring is working within the network.

Intrusion detection systems, intrusion prevention systems and network-based intrusion detection systems are covered in section 10.6, p. 251.

Problems caused by overloaded or crashed servers and network connections can be identified by network monitoring.

Another monitoring tool is a ping test. A ping test checks the response time of any request to a host on an Internet Protocol (IP) network. A ping test measures the time taken for the round trip of a message from a host to a destination system and back again. A ping test works by sending an **ICMP** echo request packet to the target host and waiting for the ICMP echo reply.

The results of a ping test show any errors, if packets were lost and a summary of the results which include:

- ▶ minimum round trip time
- ▶ maximum round trip time
- ▶ mean round trip time
- ▶ standard deviation of the mean round trip time.

Research

Investigate the ping tests used at your centre or workplace. Talk to the technicians about the results expected from the network. Investigate the results of ping tests carried out on the network.

What are considered good, acceptable and poor ping test results?

Key term

ICMP: Internet Control Message Protocol.

To maintain security of a network, monitoring of websites visited, or attempted to be visited, by users should be carried out. For example, many network managers have put social media websites on a blocked list as well as, in some cases, shopping websites.

One reason for this is that many social media websites allow users to download files, which could have viruses or other malware attached. Network technicians will also monitor, in real time, all website requests which originate from inside the network. This will enable them to pre-empt a possible attack as they will be aware of all traffic on the network.

Removable media controls

Removable media includes portable devices such as USB sticks, SD cards and external hard drives. Typically these enable people to copy and transfer data, take it off site and work away from the physical environment.

As the use of these devices has increased, so have the threats. Because the devices are portable and removable and can be connected to a range of digital systems, the risk of network security breaches has increased.

If the use of removable devices is not controlled, then there may be:

- ▶ **loss of data and information** – removable devices can easily be lost resulting in the compromise of large volumes of sensitive information
- ▶ **introduction of malware** – if removable devices are connected to home or public devices they can become infected and transport the malware to the company's network
- ▶ **reputational damage** – if sensitive data is lost then the reputation of the business or organisation can decrease
- ▶ **financial loss** – if sensitive information is lost or compromised the business or organisation could incur financial penalties as legislation relating to the storage and processing of data will have been broken.

Legislation relating to data and information is covered in section 8.1, p. 189.

Research

Using the BBC News and other websites, investigate cases where removable digital devices have been found by members of the public.

Many businesses, organisations, schools and colleges have implemented a 'no removable device' policy. There are, however, some occasions when removable media need to be used. To make sure these devices are used in the most security conscious way possible, guidelines should be created for staff to follow. One guideline may be:

All removable devices should be password protected. The passwords should be strong as this will increase the security of the data and information stored on the device.

Activity

Create an infographic aimed at 16–18-year-old students showing guidelines for the use of removable storage devices.

Anti-virus software is covered in section 10.6, p. 249.

Managing user privileges

User access restrictions/privileges are covered in section 10.6, p. 253.

What privileges are given to users should be carefully considered. Giving all users full privileges means that there is an increased security risk of a user's account being hacked or attacked. The privileges given to users should be based on their job role and what they need to do with the data.

By providing appropriate user privileges, risks can be reduced. Risks can include:

- ▶ misuse of privileges – this could be accidental or deliberate and can lead to a user gaining access to data and information which should be kept secure
- ▶ increased vulnerability – user accounts need to be deleted as soon as they are no longer required. Attackers can use old accounts to carry out an attack as the account will still have the privileges attached to it. If these privileges were linked to sensitive data, for example financial, then this access can be exploited.

Research

Investigate the user privileges set at your school or workplace. Are the privileges appropriate to job roles?

Discuss your findings with the rest of your teaching group.

Key term

Ethical hacking: an alternative term for penetration testing.

Penetration/vulnerability testing

All businesses and organisations that use digital systems should carry out security testing on a regular basis. By doing this, they can identify vulnerabilities and rectify them before an attacker exploits them.

Penetration testing (also known as **ethical hacking**) can be carried out by white or grey hat hackers. The NCSC defines penetration testing as:

'A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might.'

There are many different types of penetration testing that can be carried out.

Network penetration testing

This can be carried out to look for internet and/or external openings to identify how vulnerabilities could be exploited by internal and/or external attackers.

A network attack is the most common type of penetration test. Network attack tests may include analysing network traffic, testing routers, and identifying legacy devices and third-party appliances where updates have not been implemented.

Social engineering penetration testing

This can be carried out to look for human vulnerability. These tests try to convince employees to part with, for example, log-in details/credentials or sensitive data and information. This type of test evaluates the success or failure of the security policies, procedures and processes which have been implemented to protect against a social engineering attack. This type of test can uncover any weaknesses in employees' understanding of the security policies and procedures and may act as a catalyst for staff training.

Physical penetration testing

This attempts to test the physical security in place. This type of penetration testing aims to test access to rooms or buildings (in an attempt to steal and/or remove digital devices, hard drives or recycling containers) to assess the effectiveness of the current physical security measures. As with social engineering, this type of test



Digital T Level: Digital Support Services and Digital Business Services (Core): Boost eBook

Boost eBooks are interactive, accessible and flexible. They use the latest research and technology to provide the very best experience for students and teachers.

- **Personalise.** Easily navigate the eBook with search, zoom and an image gallery. Make it your own with notes, bookmarks and highlights.
- **Revise.** Select key facts and definitions in the text and save them as flash cards for revision.
- **Listen.** Use text-to-speech to make the content more accessible to students and to improve comprehension and pronunciation.
- **Switch.** Seamlessly move between the printed view for front-of-class teaching and the interactive view for independent study.
- **Download.** Access the eBook offline on any device – in college, at home or on the move – with the Boost eBooks app (available on Android and iOS).

To subscribe or register for a free trial, visit
www.hoddereducation.co.uk/t-levels-digital

The Digital Support Services and Digital Business Services route core elements are covered in this Student Textbook. We have released the Digital Support Services pathway core elements online, for free.
Visit www.hoddereducation.co.uk/digitalsupportservices/pathwaycore to learn more.

‘T-LEVELS’ is a registered trade mark of the Department for Education.
‘T Level’ is a registered trade mark of the Institute for Apprenticeships and Technical Education

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education.

Copyright: Sample material

DIGITAL

DIGITAL SUPPORT SERVICES: CORE DIGITAL BUSINESS SERVICES: CORE

Tackle the core elements of your Digital Support Services or Digital Business Services T Level with this comprehensive resource, endorsed by NCFE.

Written by highly respected authors, Mo Everett and Sonia Stuart, this clear, accessible and thorough textbook will guide you through the key principles, concepts and terminology, as well as providing the inside track into what it takes to kick-start a career in the Digital world.

- ➔ Simplify complex topics with summary tables, diagrams, key term definitions and a glossary.
- ➔ Track and strengthen knowledge by using learning outcomes at the beginning of every unit and 'Test Yourself' questions.
- ➔ Apply your knowledge and understanding across 100s of engaging activities and research tasks.
- ➔ Prepare for your exams and the employer-set project using practice questions and project practice exercises.
- ➔ Get ready for the workplace with industry tips and real-world examples.
- ➔ Be guided through your course by expert authors Mo Everett and Sonia Stuart, who draw on their extensive industry and teaching experience.

This Student Textbook covers the T Levels' 12 route core elements. The Digital Support Services pathway core elements are covered online and available for free on the Hodder Education website. Find out more by turning to the inside back cover.



This title is also available
as an **eBook** with **learning
support**.

Visit hoddereducation.co.uk/boost
to find out more.

HODDER EDUCATION

t: 01235 827827

e: education@hachette.co.uk

w: hoddereducation.co.uk

Schools have a **Licence to Copy**
one chapter or 5% for teaching



Copyright
Licensing Agency

ISBN 978-1-3983-4679-6

