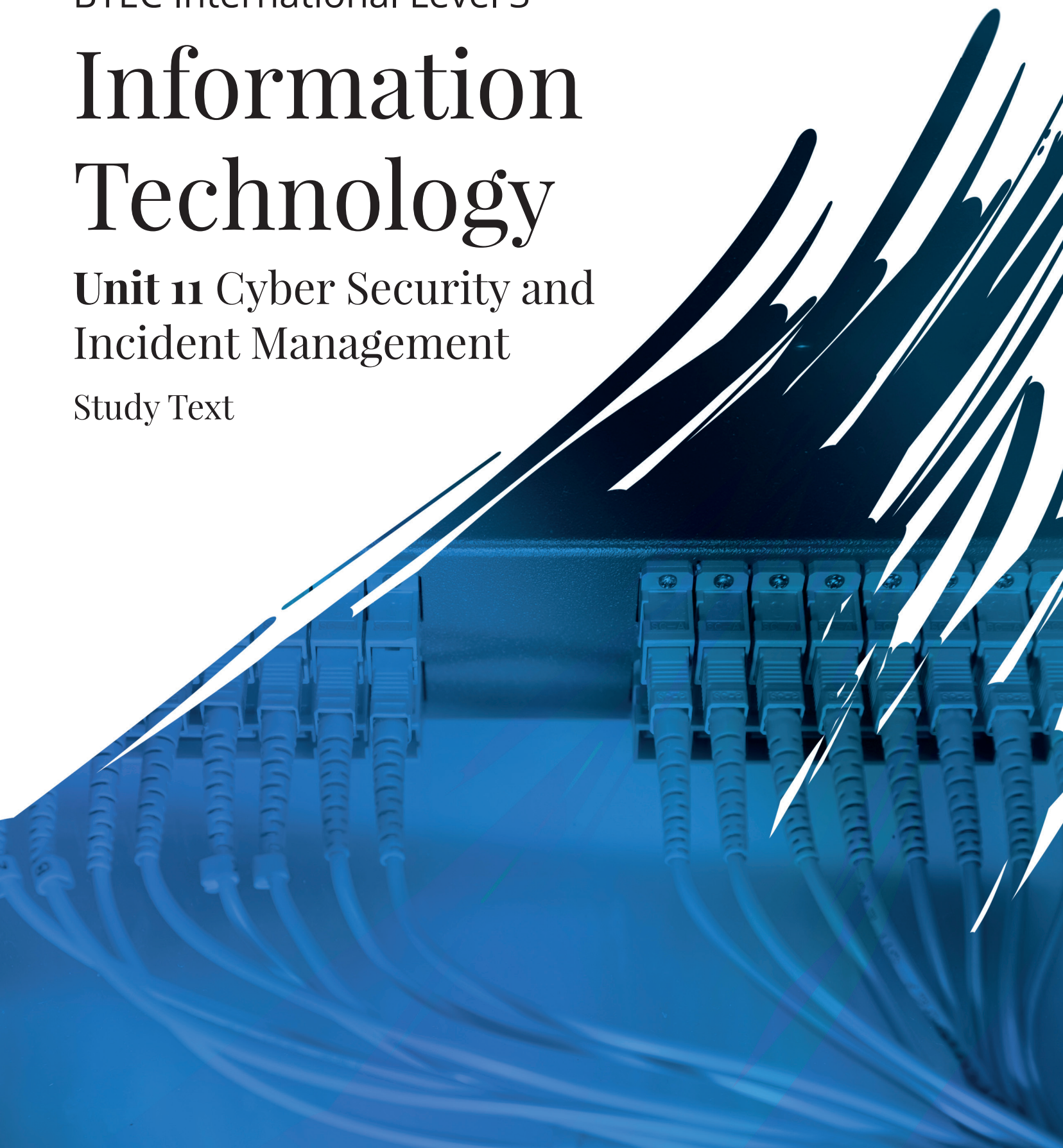
Pearson
BTEC

BTEC International Level 3

Information Technology

Unit 11 Cyber Security and Incident Management

Study Text



Published by Pearson Education Limited, 80 Strand, London, WC2R 0RL.

btecworks.com/level3

Copies of official specifications for all Edexcel qualifications may be found on the website: qualifications.pearson.com

Typeset by Florence Production Ltd, Devon, UK
Produced by Florence Production Ltd, Devon, UK

Illustrated by Florence Production Ltd, Devon, UK
Picture research by SPi Global, Chennai, India
Cover photo © Asharkyu/Shutterstock

First published 2020

23 22 21 20

10 9 8 7 6 5 4 3 2 1

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN 978 1 292 355924

Acknowledgements
Author credit: Alan Jarvis

The author and publisher would like to thank the following individuals and organisations for permission to reproduce the following:

Google LLC: Courtesy of Google LLC 22, **Microsoft**: Screenshot © Microsoft 2020 18, 32, 33 (top), 33 (bottom); **Shutterstock**: underverse 25, AlenD 58.

Websites
Pearson Education Limited is not responsible for the content of any external internet sites. It is essential for tutors to preview each website before using it in class so as to ensure that the URL is still accurate, relevant and appropriate. We suggest that tutors bookmark useful websites and consider enabling students to access them through the school/college intranet.

Note from the publisher
Pearson has robust editorial processes, including answer and fact checks, to ensure the accuracy of the content in this publication, and every effort is made to ensure this publication is free of errors. We are, however, only human, and occasionally errors do occur. Pearson is not liable for any misunderstandings that arise as a result of errors in this publication, but it is our priority to ensure that the content is accurate. If you spot an error, please do contact us at resourcescorrections@pearson.com so we can make sure it is corrected.

Contents

Getting to know your unit

As we rely increasingly on the internet and computer-based systems for many aspects of our lives, these systems have become a target for today's criminals. They are also vulnerable to disruption due to power failures, accidents and natural disasters. Keeping systems secure is a challenge; as security improves, more sophisticated methods of attack are developed.

As an IT professional you must have a good understanding of the current security threats and the methods you must use to keep systems safe and secure. You must also understand how to create a cyber security plan for an organisation. Since no measures of protection can ever be 100 per cent effective, you must also understand the procedures to follow to collect evidence should a security incident occur.

In this unit you will learn about the different cyber security threats that exist and the protection methods that can be used to counter them. You will also investigate the security implications of networked computer systems. You will learn how to develop a cyber security and protection plan for a specific organisation, and you will look at the procedures that should be used to collect forensic evidence in a situation where a security incident has been detected.

How you will be assessed

Assessment

You will be assessed internally using Pearson set assessments.

Throughout this unit, you will find assessment practice activities that will help you work towards your assignments. Completing these activities will not mean that you have achieved a particular grade, but you will have carried out useful research or preparation that will be relevant when it comes to your final assignment.

In order to complete the tasks in your assignment successfully, it is important to check that you have met all of the Pass level grade criteria. You can do this as you work your way through the assignment. If you are aiming for a Merit or Distinction, you should make sure that you present the information in your assignment in the style that is required by the relevant assessment criteria. For example, Merit criteria require you to analyse and discuss and Distinction criteria require you to assess and evaluate.

The final, externally set assignment will consist of research and practical tasks designed to meet the criteria in the assessment criteria table. This will require you to respond to a scenario, detailing a specific organisation. You will need to produce formal reports that contain:

- an exploration of cyber security threats and system vulnerabilities and how an organisation can implement security measures to protect against these
- an assessment of organisation network types and their vulnerabilities
- an implementation plan and evaluation of a cyber security plan for a specified organisation
- an examination of procedures to collect forensic evidence after a security breach.

Assessment criteria

This table shows you what you must do in order to achieve a Pass, Merit or Distinction grade.

Pass	Merit	Distinction
Learning aim **A** Understand cyber security threats, system vulnerabilities and security protection methods		
A.P1 Explain the different cyber security threats that can affect the IT systems of organisations. **Assessment practice 11.1** **A.P2** Explain the system vulnerabilities that can affect the IT systems of organisations. **Assessment practice 11.1** **A.P3** Explain how organisations can use physical, software and hardware security measures to counteract security threats. **Assessment practice 11.1**	**A.M1** Assess the impact that cyber security threats can have on organisations' IT systems while taking account of the legal requirements. **Assessment practice 11.1**	**AB.D1** Evaluate the effectiveness of the measures used to protect organisations from cyber security threats while taking account of the legal requirements. **Assessment practice 11.1** **Assessment practice 11.2**
Learning aim **B** Explore the security implications of networked systems		
B.P4 Explain how different network types and components can be secured. **Assessment practice 11.2** **B.P5** Explain how cyber security impacts networking infrastructure and resources. **Assessment practice 11.2**	**B.M2** Analyse the security implications of different networked systems. **Assessment practice 11.2**	
Learning aim **C** Develop a cyber security protection plan for a specified organisation		
C.P6 Perform a risk assessment of system vulnerabilities. **Assessment practice 11.3** **C.P7** Produce a cyber security plan for an organisation's IT system. **Assessment practice 11.3**	**C.M3** Justify the choice of security measures used to defend the IT systems of an organisation. **Assessment practice 11.3**	**CD.D2** Evaluate the cyber security plan, including its impact on internal policies and external service providers. **Assessment practice 11.3** **Assessment practice 11.4**
Learning aim **D** Examine procedures to collect forensic evidence following a security incident		
D.P8 Explain the forensic procedures for collection of evidence following a security incident. **Assessment practice 11.4**	**D.M4** Analyse how forensic procedures are implemented on a suspect system. **Assessment practice 11.4**	

Getting started

In a small group, discuss cyber security in general terms. Have you ever had any kind of security issue with the computer you have used, such as a virus infection, or have you had an online account hacked? How was it detected and then dealt with? What were the consequences of the security issue? How do you protect yourself against future attacks?

Learning aims

In this unit you will:

A} Understand cyber security threats, system vulnerabilities and security protection methods.

B} Explore the security implications of networked systems.

C} Develop a cyber security protection plan for a specified organisation.

D} Examine procedures to collect forensic evidence following a security incident.

A} Understand cyber security threats, system vulnerabilities and security protection methods

Skills

Cognitive skills/cognitive processes and strategies:

- Analysis
- Interpretation

Key terms

Cyber security – the protection of computer hardware and software (including mobile devices such as smartphones) and the data they store from the threat of damage, disclosure, disruption or loss. It is also known as computer or information technology security.

Unauthorised access – access to computer systems and the data they store by people who are not permitted access to those systems and data.

All computers including digital devices such as phones, laptops and tablets are vulnerable to a wide range of different **cyber security** threats and new threats are emerging all the time. It is essential that computers and digital devices are protected using a variety of methods to keep them as secure as possible.

Cyber security threats

Security threats can come from inside the organisation (internal threats) or from outside the organisation (external threats).

Internal threats

Internal threats normally involve the organisation's staff, who cause a security breach in one of these ways:

- Employees who are unhappy with the company or organisation for some reason may damage or destroy data or physical equipment as a form of revenge. For example, if an employee is dismissed or made redundant, they may delete important information from the company's computer systems.
- Employees may be able to gain **unauthorised access** to data to which they should not have access, such as payroll or financial information. They may do this for personal gain; for example, they may be able to sell confidential company information to others, such as the organisation's competitors. Ineffective management of contractors or partners may also allow them access to data or security procedures that they should not be able to access.
- Weak security measures or unsafe practices may make equipment vulnerable to being lost or stolen. Failing to keep computer rooms secure, for example by locking doors and restricting access, may allow visitors or employees to steal hardware.

Unsecured portable devices which are not password-protected would allow an employee access to confidential data.

- Staff who are not well trained in the use of IT systems may accidentally delete important data. Staff may also disclose company confidential information to people outside the company. For example, in some companies pricing information (such as the cost price of a product, as opposed to its sale price) is confidential. An employee who has not been properly trained may disclose such information by mistake to an external customer or competitor, for example by sending an email with the pricing information attached.
- Staff may inadvertently introduce external security threats to the company by visiting **untrustworthy websites** or opening attachments to emails from untrusted sources.
- Visitors to an organisation can pose a threat. Proper procedures should be in place to check that visitors have a legitimate reason for being in the building and are not left on their own. Organisations such as a bank or doctor's surgery that deal with a lot of customers and confidential information need precautions to prevent accidental disclosure of information. Computer screens in public view must be arranged so only appropriate employees and the customer concerned can see what is on the screen.

Some internal threats may not be caused by staff sabotage or negligence, but by forces that they can't control such as: fire, flood, earthquakes and other natural disasters, or political activity.

Key term

Untrustworthy websites – malicious websites that invite you to download damaging software onto your computer or seek to gain information from you by deception.

External threats

External security threats involve several different methods:

Malicious software (or malware)

These include:

- **Spyware** – this collects information (usually about internet browsing habits) without the user's consent. Information collected is then used to target adverts at the user. Some types of spyware are more dangerous as they include a keylogger which records exactly what the user types on their keyboard and passes this to criminals. Keyloggers can be used to collect usernames and passwords.
- **Adware** – this type of **malware** displays pop-up adverts to the user. Like spyware, it may collect data on internet browsing habits to provide targeted adverts. Usually adware does not have a damaging effect on the user's computer, but it can be irritating for the user.
- **Ransomware** – this can be very damaging and disruptive to a computer system. Typically, ransomware infects a computer via an email attachment and then locks the user's files through **encryption**. It demands a ransom be paid to provide the key to decrypt the files.
- **Viruses** – these types of malware spread across computer systems and networks. The initial infection can enter the system by methods such as email attachments and by a user visiting infected websites. The virus then replicates itself across other computers on the network. Types of virus include the following.
  - Worm: a type of virus that replicates itself across many computers, commonly on a network.
  - Rootkit: this hides in a user's computer and allows hackers to remotely gain access to it.
  - Trojan: software that appears to be legitimate and has a harmless purpose, but hides some form of malware.

Key terms

Malware – software which has a malicious (bad) intention and may cause damage to your computer software or data or collect information about you.

Encryption – a process of encoding data so it cannot be read by anyone but the person it is intended for. Typically, data is encrypted using a key, which is also required to decrypt the data.

Case study

Ransomware

CryptoLocker is a well-known example of ransomware which was active between September 2013 to April 2014. The infection was spread by email attachments and used a Trojan which targeted computers running Microsoft Windows. The infection encrypted computer files and demanded a ransom be paid in bitcoin to provide the key to decrypt the files. It is estimated that about 250 000 desktop computers were infected. In 2017, another ransomware attack called Wannacry occurred. This attack used a vulnerability in Microsoft Windows which had been patched. Users who had not applied the patch, or were running unsupported versions of Windows, such as Windows XP had their computers infected. One of the largest organisations impacted by the attack was the National Health Service (NHS) in the UK where as many as 70 000 computer and associated devices were infected. The source of the ransomware was traced to North Korea.

Check your knowledge

1 What do you think the impact of such an infection was on the computer networks used by the National Health Service?
2 Why do you think they were targeted?

Key term

Hacker – someone who attempts to gain unauthorised access to a computer system using a variety of different methods

Hacking

This is the process where someone (the **hacker**) attempts to gain access to a network computer system. This can be done for a variety of reasons. Some individuals like to attempt to hack into systems just for the challenge. Others intend to steal or destroy data. Hacking may also be done by governments or companies. Hacking for commercial reasons is an attempt to steal data that would give a competitor an advantage, for example new product details, pricing or customer information. Governments may use hacking to try to collect secret information from other countries, such as military or political secrets.

Sabotage

This happens when malware or a hacker does not just access systems or collect data, but actively seek to disable the systems in some way so they can no longer function as intended. This can be done by individuals, for purposes of revenge or blackmail, or by commercial organisations to gain a competitive advantage over rival companies. Government-led cyber warfare can be used to disable systems that are of strategic importance to other countries. Sabotage can also be done for terrorist purposes, causing disruption and potentially even injury or death by disabling important systems.

Case study

Denial of Service attack (DoS)

This is an attack aimed at sabotaging an organisation's website. It involves flooding the site's web server with so many requests that it is overwhelmed and cannot respond to real requests. This effectively takes the site offline. A common version of this type of attack uses large numbers of computers (often ones which are infected with malware in a so-called botnet) to flood the targeted web server. The use of many different computers in the attack makes it difficult for the web server to distinguish between legitimate and malicious traffic. This type of attack is sometimes called a Distributed Denial of Service attack (DDoS). Since many organisations such as Amazon rely heavily on their websites to do business, DoS attacks are a serious threat. There are a number of reasons why people carry out DoS attacks.

Check your knowledge

1 What could the motivation be for a DoS attack?
2 Why do people carry out DoS attacks on larger companies such as Amazon as opposed to small companies?

Case study

Phishing

Phishing is a social engineering threat which is very common and often targets online banking users. Criminals set up a web page which looks like the login page for a legitimate bank's online service. They then email large numbers of people (often using lists of emails harvested from other cyberattacks) telling these users that they need to log in to their online account using the link provided in the email. The link sends the recipient of the email to the fake page, where they enter their online banking login information, which is then collected by the criminals. They can then use the login information to access the real banking site and potentially steal money. This type of phishing has declined in recent years due to awareness of the threat and the methods that banks are starting to use to defend against it.

Check your knowledge

1 Have you ever been subject to a phishing attack?

2 If you were able to detect that it was a phishing attack, how did you know?

Pause point What are the different reasons why people attempt to hack into systems? Do hackers always have a malicious intent? Research the meaning of the term 'white hat hacker' to find out what these are and why this type of hacking is sometimes done.

Hint Financial gain isn't the only motivation for hacking.

Extend Think about the ways social engineering threats differ from other methods of security threat. Why are social engineering threats difficult to defend against?

Social engineering threat

This happens through a combination of external and internal methods. It involves an external attacker attempting to fool an internal employee to reveal company information that should be kept secure. This can be as simple as the attacker telephoning the company, claiming to be from their IT support department and asking for their username and password. This kind of attack relies on people's natural assumption that other people are telling the truth and so can be very effective.

Impact of threats

A threat which successfully gains unauthorised access to a computer system will cause some kind of loss to the organisation involved. The loss suffered by the organisation can be of a number of different types.

Operational loss

When an organisation's systems suffer a **cyberattack** there is very likely to be some disruption, which will make the systems unavailable for some time or reduce their performance. This can range from the minor disruption that a relatively harmless virus may cause, to significant disruption caused by a ransomware attack which locks some or all of the organisation's data. A major catastrophe such as fire or flood could destroy an organisation's computer systems. Most organisations rely heavily on computer systems, so disruption of these is very likely to have an impact on their ability to run their operations. For example, a manufacturing company that relies on computerised manufacturing systems would suffer loss in manufacturing output. A website that is a victim of a DoS attack would suffer a lack of service availability and a website that is attacked by a hacker could suffer a loss of important service data.

Financial loss

An operational loss is likely to have a financial impact. If an organisation is unable to carry out its operations, such as providing a service or distributing products, it can't charge customers for these. Financial loss may be incurred if specialist cyber security experts need to be employed to investigate and resolve security issues and to replace equipment that has been stolen, damaged or destroyed. Depending on the type of attack and its impact, the company may be liable to pay compensation to customers who are inconvenienced by the lack of availability of its products or services. For example, in some countries airlines and train companies are required by law to pay compensation to customers if their service is delayed. Companies may also face significant fines if personal data is lost in an attack due to their legal obligation to keep that data secure.

Reputation loss

An organisation is likely to suffer a loss in reputation if they are unable to protect their service, employee or customer information during a **cyberattack**. A significant cyberattack may be reported widely: the knowledge that a company has suffered a cyberattack will damage the company's reputation. It can make people unwilling to do business with that company as it demonstrates that their computer systems are not adequately protected. For example, a company that sells products online would need customers to enter credit or debit card numbers on their website. Customers may be unwilling to do this if they know the company has been victim of a cyberattack in which data was lost. Potential employees may be unwilling to work for the company if they think their personal information could be at risk.

Intellectual property loss

A company may fall victim to a commercially motivated attack. They could lose designs for new products, confidential pricing or customer information, or trade secrets such as the details of ingredients for food products or paint.

Key terms

Cyberattack – a malicious attempt to disable computers, steal data or use a computer to launch an attack in another way.

Intellectual property – 'property' that is a result of creativity such as inventions, written work (books), artistic work (works of art), musical work, symbols, names and images.

Impact levels

How much a successful attack impacts on an organisation will largely depend on the value of the loss they suffer. This may be a direct financial loss, for example if the attack gained access to the company's bank account and stole money. Or it could be an indirect financial impact, such as lost productivity because staff are unable to carry out tasks while the problems caused by the attack are resolved.

Cyber security threats over time

Cyber security changes all the time and security threats vary. Cyber security organisations keep up to date with the latest threats and fixes. They provide regular updates to their customers.

Pause point

What could be the impact of a cyberattack on you?

What would happen if all the data you have on your laptop or the computer you use at home or at school/college was destroyed?

What if your email account was hacked? Or your social media account (e.g. Facebook)?

Hint Consider the time and effort that might be needed to replace lost data.

Extend What if some of your financial details were stolen in the attack, such as bank or credit card account numbers? Are you aware of your bank's policy on money stolen from you in a cyberattack?

System vulnerabilities

Vulnerabilities can be exploited by hackers and malware to breach the security measures of a computer system. A networked computer system is made up of a variety of hardware and software components, all of which potentially have vulnerabilities.

There are different threats and different vulnerabilities depending on the type of computer or computer system.

Network vulnerabilities

Many external threats, such as hackers, may try to gain access to a computer system through its external connection to the internet. External connections are usually protected by a **firewall**. External storage devices such as Universal Serial Bus (USB) memory sticks provide another way that malware could enter a network system. Using an infected USB memory stick could introduce malware, such as a worm, which could spread throughout the network.

Organisational vulnerabilities

There are several types of vulnerability associated with the way an organisation sets up its networked computer systems:

File and folder permissions

Companies which run a network computer system with a file server will usually restrict access to files using the file and folder permissions systems built into server operating systems such as Windows Server and Linux. With file and folder permissions, groups of users can be given different levels of access to specific folders (such as read-only, read and write, etc.) or no access at all. Setting up groups and folders can be complex and it can be frustrating for users if they need a folder or file that they don't have permission to access.

Privileges

The manager of a network system can control a wide variety of things that the systems users can do. These are known as operating system privileges. Ideally, for the best protection, a user should be restricted from doing anything that poses a security risk. For example, users should not have access to the command prompt, be able to use the run command, or be able to install software. If a system administrator fails to apply these settings correctly, this could pose a security risk.

Password policy

The system manager sets the password policy using the server operating system. This includes setting how long user passwords must be, how often they are changed and how complex the password must be (such as which characters to use, e.g. numbers, upper and lowercase letters and symbols). If the system manager does not apply robust password policies, the system can be vulnerable to attack.

Software vulnerabilities

Legitimate and properly updated software is usually at low risk of cyberattack. Unlicensed or illegal software is a risk. If employees download software from untrustworthy sources there is a danger it may include malware. Criminals may lure users into downloading what appears to be a free version of an expensive software application, but in fact contains malware, which gets installed instead. Other software related vulnerabilities include:

Structured Query Language (SQL) Injection. This is a common method of attacking e-commerce websites. These have a web server which runs database applications to maintain information on products for sales, customers, orders, etc. For example, a visitor

Skills

Cognitive skills/cognitive processes and strategies

- Critical thinking
- Analysis

Link

For more about the operation of a firewall see the section on *Physical security measures* on page 15.

Key terms

System vulnerability – a weakness in an operating system or other software which can be exploited by an attacker.

Firewall – a software or hardware device which filters incoming and outgoing data between a local area network and the internet with the aim of blocking unauthorised or malicious access.

Discussion

Discuss the legal and ethical considerations of unlicensed or illegal software and the risks it can pose.

Key term

Structured Query Language (SQL) – the command language used to extract data from a database.

Case study

Between 2005 and 2007 American hacker Albert Gonzalez, along with several Russian hackers, carried out one of the largest thefts of credit card numbers and other personal details using SQL injection combined with other techniques. In a series of attacks Gonzalez and his accomplices stole over 170 million card numbers and ran a website where stolen details were sold. Gonzalez was arrested in 2008 and was found in possession of $1.6 million in cash. He was sentenced to 20 years in jail.

Check your knowledge

1. How can SQL injection be used to obtain information such as credit card numbers and personal details from a website?
2. What can companies do to protect themselves against such attacks?

to an e-commerce site might search for a product by entering the product description into a search box on the site front page. The entry the user makes is then used to search the product database for matching products. This is done by inserting the search string the user enters into an SQL search command. The SQL injection vulnerability involves an attacker entering an SQL command into the search box on the website. In certain circumstances this can make the database display information which should be kept confidential, such as customer credit card details. SQL commands can cause database tables to be dropped from a site's backend database, which then prevents the search feature from working effectively on the website. Cross Site Scripting (called XSS) is another common form of attack, when a hacker injects a client-side script into a website, usually through an HTML form. The malicious script may display pop-up messages, steal cookies or redirect the browser to another website.

Zero-day exploits. Any known vulnerabilities in an application are fixed by the software developer by security updates. There may be a time lag between when a vulnerability is discovered and when the software developer releases the update that fixes it. This time gap provides an opportunity for a hacker to exploit this so-called 'zero-day' period when there is no protection available.

Operating system vulnerabilities

Security vulnerabilities exist in operating system software, but they are fixed by updates. In the Windows operating system, security updates are switched on by default, though it is possible to turn them off; this might be done by mistake. If a computer has an operating system which has not been updated, or an older version of the operating system which is no longer supported by the system developer, then such vulnerabilities may allow attackers access. For example, Windows XP is used on many computers around the world, but security updates are no longer provided for it by Microsoft®. If a new vulnerability is discovered, computers running Windows XP will not be protected.

Mobile device vulnerabilities

For many organisations, mobile devices provide an opportunity and a challenge. Many employees would like to use their own mobile devices to access company systems. This can allow employees to work flexibly. However, the company may have very little control over these devices, how secure they are, how often they are updated and what happens if they are lost or stolen. Mobile devices are also reliant on updates produced by their Original Equipment Manufacturers (OEMs). The individual user is in control of if or when these updates are applied. In contrast, updates to computers within an organisation's networked computer system are controlled by the system administrator.

Physical security vulnerabilities

Depending on the type of organisation and the location of computers, systems may be vulnerable to theft or loss. This is particularly the case with portable mobile devices and laptop computers, which may contain sensitive company information. As well as computers, USBs and memory sticks also represent a major risk. Due to their size they are also easily lost or stolen. As mentioned earlier, a variety of social engineering methods can be used to collect passwords from unsuspecting users.

User processes vulnerabilities

Users represent a major vulnerability and potential compromise to system security. Login details can easily be leaked either deliberately or by mistake. For example, a user might openly display their username and passwords on a sticky note on their computer monitor which would be visible to other employees and visitors to the office. Sharing login details is not safe. Users may be tempted to do this if a colleague is unable to log in, perhaps because they have forgotten their password or if their accounts lack the permissions to access a particular folder; but they should not.

New technologies vulnerabilities

New technologies provide new opportunities for cybercriminals.

Cloud computing

Many of the vulnerabilities considered so far relate to traditional client server computing, where servers are kept and administered within the organisation. Increasingly organisations are adopting cloud computing models, where file storage and computing is done outside the organisation, run and maintained by an external cloud computing provider. One of the benefits of cloud computing is that the responsibilities for the security of the system is with the cloud computing provider. It is assumed that they have the skills and resources to keep the system secure, but it is important for an organisation to choose a cloud computing provider that can be trusted to maintain the security of their data.

Internet of things (IoT)

With so many devices able to exchange data with each other, the Internet of Things technology provides advantages for homes or offices. For example, video cameras connected to the internet allow individuals to monitor their home or office remotely. If criminals hack into these devices, they can tell when the home or office is unoccupied and might be able to disable any alarms too.

Key term

Internet of Things (IoT) – a general term referring to the technology which allows everyday devices (such as a video camera, heating thermostat or lights) to have computing devices embedded in them allowing them to send and receive data over the internet.

Research

Research the internet to find up-to-date security information for the following major software suppliers.

Microsoft – https://support.microsoft.com

Norton – https://uk.norton.com (Internet security)

McAfee UK Threat Centre – www.mcafee.com (Threat center)

Pause point Research recent IT security issues experienced by large companies. What actually happened? Which types of attack described in this section were used? What was the impact on the company? Did they lose money or were there legal consequences?

Hint News or newspaper websites such as these are excellent places to start your research.

- *New York Times*: www.nytimes.com (Technology)
- *The Australian*: www.theaustralian.com (Technology)
- *Telegraph*: www.telegraph.co.uk (Technology)
- *The Guardian*: www.theguardian.com (UK Technology)
- BBC News: www.bbc.co.uk (News)

Extend Consider how the company could have avoided the security breach. Are there protection methods they could have used? If so, why didn't they use them? How can organisations protect themselves in the future from this kind of security issue?

Skills

Cognitive skills/cognitive processes and strategies

- Critical thinking
- Analysis

Reflect

Why do you think that data protection is important to an individual? Think about your own circumstances. Why is it important for you to have your data protected? Why is it an important issue for a company or organisation? What could be the consequences if a company or organisation breached data protection laws? What are the data protection laws in your country? Do they differ from those listed here?

Research

Find out about the data protection laws that affect you. What are their main principles? What rights do these laws give individuals?

Legal responsibilities

Attack vectors

These are methods by which a hacker can gain access to a system to exploit a vulnerability. This is typically via a network connection. Wireless network access, such as Wi-Fi or Bluetooth, provide an obvious way to access a system due to their broadcast nature. Gaining access through a wired internet connection is more difficult, and gaining access via the internal Local Area Network (LAN) would require an internal attacker.

Data protection

Many countries around the world have laws which protect the data held about living individuals on computer systems. For example, in Europe, the data protection legislation that applies to all the member states of the EU, is known as the General Data Protection Regulations (GDPR). There are six main principles of the GDPR relating to personal data:

- It should be processed lawfully.
- It should be collected only for specific purposes.
- It should be relevant and limited to what is necessary for the purpose.
- It should be kept only for as long as necessary.
- It should be kept secure.

The GDPR give individuals several rights relating to data about them which is stored on computer systems. These include the following:

- The right to be informed about the collection of their data.
- The right to have access to the data stored about them on request.
- The right to be forgotten (individuals can ask to have data recorded about them erased).
- The right to object to their data being used for certain purposes, such as for promotional emails.

Computer misuse

This legislation is used to make hacking and the spreading of viruses and related actions illegal. In the UK the Computer Misuse Act, passed in 1990, defines a number of different actions as illegal. These are:

- unauthorised access to computer data
- unauthorised access with intent to commit other offences
- unauthorised acts with intent to impair a computer system
- unauthorised acts with intent to cause serious damage
- unauthorised modification of computer data
- making, supplying or obtaining articles for use in computer misuse offences.

This policy has been used as a model for similar policies in other countries around the world.

Telecommunications legislation

In the UK, employers are allowed by law to intercept communications sent over their own networks. This comes under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000). For example, a company could lawfully intercept their own employee's emails and record their telephone conversations (if they use the company network). Employees must be aware that their communications may be intercepted, and this would usually be included in their contract of employment.

Case study

In February 2014, a UK citizen with complex medical conditions including Asperger's syndrome was accused of hacking into US computer systems, including the FBI, the US Army and the Missile Defence Agency. He was allegedly trying to find evidence about Unidentified Flying Objects (UFOs). He has indictments in the US for breaching large numbers of computer systems and could face a long jail term. Attempts to extradite him from the UK to the US have been unsuccessful, mainly due to the health issues he faces.

Check your knowledge

Research the internet to find other similar cases. Why do you think hackers are attracted to organisations such as the FBI or the Missile Defence Agency?

Fraud legislation

Cyberattacks which involve obtaining money by deception may be covered under fraud legislation. Fraud is when someone intentionally attempts to achieve some monetary or other benefits by unlawful means. Criminals, for example, may use various methods to gain information (such as an individual's name, address, or bank account number) which they can use to apply for a bank loan in someone else's name.

Health and safety

Most countries have health and safety legislation which protects employers and employees in the workplace. Legislation also places requirements on employees to perform their duties in a way which does not endanger others.

Physical security measures

Physical security measures can be used to help prevent theft and keep data secure.

Site security

Keeping computer equipment secure and controlling who has access to it is an important part of protecting computer systems. Computer rooms, where servers and other sensitive equipment are located, should be kept locked and access controlled, for example through use of a card key entry system when the time and name of the person entering the room is recorded. Cables can be vulnerable to tapping, especially in a shared office space or building. Cabling and other network equipment should be kept in locked cabinets to prevent unauthorised access.

There are several other ways such locations can be kept secure:

- **Biometrics** can be used instead of keys or cards. These rely on a unique human characteristic such as fingerprints or iris scans to identify a person entering a secure area.
- **Closed Circuit Television (CCTV)** allows security staff to monitor large areas of a building and can be recorded for evidence. CCTV can also be linked with facial recognition systems which can then track movement around a building.
- **Security staff** can be used to check visitors on arrival and to carry out patrols in person.
- **Alarms** can detect unauthorised entry to a building. They can be fitted to doors and windows or include motion sensors to detect if someone is in part of a building when they should not be.

Skills

Cognitive skills/cognitive processes and strategies:

- Critical thinking
- Analysis

Data storage

Data is one of the most important resources an organisation has. It is not easily replaced if lost. Data must be protected from loss by regular planned backups run automatically by an organisation's operating system. Some organisations copy backups to external media (such as a USB external hard drive) and store the drive offsite. Offsite storage is important to protect against disasters such as fire or flood. Cloud backup, when files are copied across the internet to a remote location, is increasingly used. Cloud backup has the same security concerns as other cloud-based facilities in that responsibility for the safety and security of the data is passed to a third party (the provider).

Skills

Cognitive skills/cognitive processes and strategies:

- Problem solving
- Critical thinking

Software and hardware security measures

Due to the many ways that systems can be attacked, a range of different hardware and software security measures are needed to keep a system secure.

Anti-virus software

This is used to defend against a range of malware threats. Anti-virus programmes use a number of techniques to try to identify viruses in files.

- **Virus signatures**. Every known virus file has a pattern by which it can be recognised. These patterns are known as virus signatures. An anti-virus programme scans each file on a computer and compares it to the virus signature it has so it can identify if any of the files are viruses. New viruses appear from time to time, so it's important that the list of virus signatures is kept up to date.
- **Heuristics**. Virus signatures will only recognise known viruses. Heuristics looks in files for the types of commands or instructions which would not be found in harmless applications and might indicate that a file is suspicious.
- **Identified threats**. Once a virus or suspicious file is identified an appropriate anti-virus program needs to deal with it. In some cases, the anti-virus program may simply delete the file. In other cases it may place the file in a 'quarantine' folder which severely restricts what the file can do but does not delete it. Some virus infections may be difficult to remove. They may require a computer to be started up in safe mode or the user to use a bootable rescue disk to restart their computer using a different operating system to permanently remove the virus files.

Key terms

Packet – a unit of data made into a small 'package' or 'packet' that travels along a network path.

IP address – a numerical address that uniquely identifies a computer on a network.

Port – in the context of firewalls a network port is a software feature which allows different applications which are communicating on a network to be identified.

Protocol – a network protocol is a set of rules which govern how a particular type of communication is done over a network.

Software and hardware firewalls

One way that external threats can attempt to gain access to an organisation's computer systems is via an external link to the internet. Firewalls analyse the data coming in and out of the organisation's LAN to and from the internet with the aim of blocking suspicious data. Firewalls can be implemented in software and run on individual computers. In an organisation, firewalls are commonly a single hardware device that performs the analysis for all the computers on the LAN. Firewalls use a number of different analysis techniques.

- **Packet filtering and inspection**. This technique involves looking at each **packet** of data as it passes through the firewall. Based on rules set by the firewall or the network administrator, packets are either allowed through the firewall or they are blocked. Rules can include things like sources and destination **IP addresses**, network **port**, **protocol** used or other settings.
- **Application layer awareness**. Working at the application level rather than the packet level, this technique applies rules for each application and rejects any connections that break the rules. For example, you can set up a Firewall to block network applications such as remote terminal.

- **Inbound and outbound rules**. Rules are set to control how the packet and application filtering works. The firewall will have some default rules, but the network manager can adjust and add to these. Rules can be set for both outbound data (from the LAN to the internet) and inbound data (from the internet into the LAN).
- **Network address**. Firewalls hide the real IP addresses of devices on the LAN to prevent hackers outside the LAN from being able to identify addresses of individual devices. This technique is called Network Address Translation (NAT). It works by keeping a table of the multiple internal IP addresses of devices inside the LAN and mapping these to the external public IP address(es) used on the internet.

User authentication

Ensuring that legitimate users can log in to a system and gain access to the correct files and applications is the aim of user authentication. Login procedures should prevent unauthorised people from accessing the system, without causing authorised users excessive inconvenience.

- **User login procedures**. The standard method of user authentication is the username and password combination. The username identifies the user to the system, the secret password is used to protect the account from unauthorised access. In some organisations simple username and password combinations are not considered secure enough, so a range of other methods is used.
- **Strong passwords**. Simple passwords with just alphabetic characters are not considered strong because they are vulnerable to dictionary attacks. This kind of attack tries all words in an online dictionary. Short passwords (fewer than 8 characters) are considered weak as they are too easy to hack. Strong passwords need to be long – the longer the better – and need to be a combination of alphabetic characters, numbers and symbols. The more complex a password is, the more difficult it can be for users to remember it. Passwords should be changed every few months to keep them secure, but that can be inconvenient for users.
- **Text and graphical passwords**. Graphical passwords are a strong alternative to text passwords. These work particularly well on touch screen devices where the user draws a pattern to unlock the device.
- **Biometric authentication**. Biometrics use unique physical attributes to authenticate an individual user, such as fingerprints, iris or retina scans, facial recognition and voice identification. The benefit of biometrics is that the user does not need to remember anything, but they may require additional software and hardware, such as a scanner to read the fingerprints or iris. The latest mobile phones include a fingerprint scanner that can be used to unlock the phone. The system stores the user's biometric data so that it can be compared with the data provided at login. Biometric authentication is generally secure, though if the biometric data is accessed or stolen by a hacker, it could cause major problems, as unlike a password, biometric data cannot be changed.
- **Two-step verification**. Also called two factor authentication (2FA). This is commonly used where more secure authentication than simple username and password (sometimes called single factor authentication) is required. Two-step verification involves the user entering a password and using a second method of authentication such as biometrics or a security token code. Two-step verification provides an extra layer of security.
- **Security tokens**. These are small hardware devices (sometimes like a credit card or key fob) that provides the second step in a two-step verification process. There are several types of token, for example, when the user wants to log in to the system, the token generates a one-time code which they must enter as part of the authentication

Key terms

Near Field Communication (NFC) – a wireless communication method used by services such as Apple Pay and contactless card payments. Two devices (such as a debit card and a card reader) need to be brought very close to each other (within a few centimetres) and are then able to transfer small amounts of data.

Digital Certificate – a secure website (using the HTTPS protocol) must apply for a digital certificate from a certificate authority to prove it is a genuine site.

Certificate Authority – a certificate authority (CA) is an organisation which issues digital certificates

Discussion

Discuss the advantages and disadvantages of using biometric authentication to access a website.

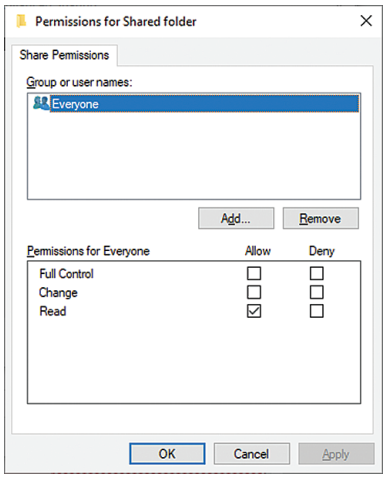


Figure 11.1 Shared folder permissions

process. Some types of token plug into a computer's USB socket. Other types of token use **Near Field Communication (NFC)** where the token is a card or tag that only needs to be brought close to the NFC reader attached to the computer.

- **Knowledge-based authentication**. This is commonly used as part of a multi-part verification process (such as that required when logging onto a bank website), or for forgotten password retrieval which requires the correct answer to be given to a question. Typically, when setting up an account the user will provide an answer to some pre-set questions (such as 'what town were you born in', 'what's the name of your first pet' or similar). When the user needs to log on (or recover their password) they need to provide the same answer to the question.
- **Kerberos authentication**. This is the standard user authentication protocol used in Windows client server systems. Versions also exist for Linux and other operating systems. It ensures passwords are never sent over the network without being encrypted first. With Microsoft Windows, user accounts are created on a server and stored in a database called Active Directory (AD). AD works as a Kerberos Key Distribution Centre (KDC). User accounts have a password which is stored (in encrypted form) on the KDC. When the user logs onto a client machine and enters their password, it is encrypted using the same method as when the account was created on the KDC. If the two encrypted keys match, then the user has entered the correct password.
- **Certificate-based authentication**. This method is used by websites which need to ensure secure and trusted communications, for example when making an online purchase, or logging onto a banking website. The digital certificate is used within the HTTPS secure protocol which ensures data sent between the end-user and the website is encrypted. Websites that want to use this type of authentication must have a **Digital Certificate**, which is provided by a **Certificate Authority**. The process depends on the public key encryption process which is described in the next section.

Access controls

Network operating systems such as Microsoft Windows and Linux provide access controls. These access controls can be used to regulate which users have access to different files and folders, and what type of access they have – full control, write- or read-only access. Windows file permissions is a fairly complex topic with slightly different permissions used for files held locally and on the servers (called NFTS file permissions), and folders shared over the network (called shared folder permissions). The Linux operating system provides similar facilities which are known as Linux file permissions, or sometimes Linux octal file permissions, because there are 8 levels ranging from 0 (no access) to 8 (read/write and execute permission).

You can easily share a folder on a Windows computer by accessing the folder properties and choosing to share the folder. You can control what access other users have to the shared folder by adjusting the permissions. Figure 11.1 shows the Permissions dialog box for a folder called 'Shared folder'. In this case all users (the 'everyone' group) only has Read access to the folder, so they cannot change any files in the folder.

Trusted computing

This is a general term which refers to attempts to resolve security problems through hardware and associated software developments. A cooperative venture known as the Trusted Computing Group has been set up by a number of hardware manufacturers (including HP, IBM and Microsoft). The Trusted Platform Module (TPM) is a chip which can be included on a device, such as a computer motherboard. The TPM chip is used to support whole disk encryption.

Purpose and uses of encryption

The purpose of encryption is to hide data so that only the intended user or recipient can read it. There are many different techniques to encrypt data and they are used for different applications, some of which are listed below. Most encryption techniques use a key, which is a binary number, to encrypt and decrypt the data.

Password storage

Server computers commonly need to store the passwords of authorised users. If hackers gain access to a database of user passwords the consequences could be severe. Therefore, stored passwords should always be encrypted to keep them secure even if a hacker gains access to the system.

Digital rights management (DRM)

With computer-based systems, digital media such as software, films, games and music can be easily copied from one computer to another. Digital rights management is a general name for technologies used to protect copyrighted works. Some types of DRM use encryption. One of the simplest forms of DRM is the product key which is required to install software applications such as Microsoft Windows or FairPlay, which is used to access online music and film services such as Spotify and Apple® iTunes.

File, folder and disk encryption

Operating systems like Microsoft Windows allow users to encrypt files or folders (known as encrypted file system or EFS). The encryption key (needed to decrypt the files) is encrypted using the user's password. When the user is logged in the encryption key is available so files can be accessed; other users cannot access the key so cannot decrypt the folder or files. Generally, on a networked computer system files and folders are protected from different groups of users using the permissions feature. If a laptop computer is stolen and the hard disk removed and attached to another computer, then it is possible to bypass the permissions system and access the files (called an **offline attack**). This would also apply to hard drives stolen from desktop and server computers. Using file or folder encryption safeguards data from this kind of theft because the files can only be decrypted by the user who encrypted them. If the user forgets their password and has to have it reset, then their encrypted files will no longer be accessible.

A better solution, especially for laptop computers (which are prone to loss or theft), is to encrypt the whole hard disk drive. With Microsoft Windows this can be done using a feature called BitLocker, which is available with the Enterprise or Pro versions of Windows, but not with the Home editions. BitLocker works in conjunction with the TPM chip in the computer motherboard. To encrypt the hard drive on a computer you must enter a password which will be required every time you start up the machine, before you get to the Windows login screen. You can use a typed password or USB memory stick as a key. If you forget your password, you will lose access to your computer, so a recovery key is also created. You can save the recovery key in several different places and print it if you wish. Once the drive is encrypted you can only gain access to it by entering the key when the machine starts up.

Communication encryption

When transmitting data over networks it is vulnerable to interception by others. This is especially the case with the internet where data may pass through many types of intermediate communications equipment on its route from sender to receiver. Therefore, when sensitive data (such as personal or financial data) is sent, it should be encrypted. The following are examples of communication encryption.

Key term

Offline attack – when an attacker steals a computer or hard drive and either attaches the hard drive to a different computer or boots the computer from a different operating system (e.g. Linux on a USB memory stick). These methods bypass the normal Windows security features.

Key terms

Open source – a type of computer software in which the source code is available for users to view and modify if they wish. This contrasts with software where the source code is not available, which is called proprietary software.

Tunnelling protocol – a network protocol that creates a private network within the internet by encapsulating the data to be sent and encrypting it, before inserting it in standard data packets. The protocol also authenticates the users of the connection and negotiates the encryption keys to be used to encrypt and decrypt the data sent.

- **Built into devices**. Mobile phone conversations are transmitted using encrypted digital data. GSM (Global System for Mobile communication) mobile phone conversations are encrypted using the A5/1 stream cypher. The A5/1 stream cypher is no longer secure; it has been shown that it is possible to crack the encryption and decrypt mobile phone data, allowing conversations to be eavesdropped on in real time.
- **The Onion Router (Tor)**. This is a free, **open source** tool which is designed to protect users' privacy when using the internet. It hides the users' locations and usage (including which websites they visit, online posts made and instant messaging) from anyone carrying out network surveillance or traffic analysis.

Virtual private networks (VPNs). In general, private networks which are only accessible by an individual or organisation exist within a building or site, commonly called a LAN, while the internet is a Wide Area Network (WAN) open to the public. Therefore, if an organisation has two geographically separate offices or sites each with their own LAN they can be connected via the internet. But the traffic between them travels over a public, not private network, so can be vulnerable to interception. A VPN allows an organisation to make the connections over the public internet private using encryption. Organisations often allow remote workers to connect securely to their organisation's network when working from home or another remote location. They use VPNs to ensure their communication is secure. VPNs use **tunnelling protocols** to create virtual point-to-point connections over the internet.

Hypertext Transfer Protocol Secure (HTTPS). This is the secure version of the HTTP protocol which is used to request and serve web pages on the internet. The HTTPS protocol uses digital certificates to ensure a web page you are visiting is secure. It encrypts the data transferred between you and the web page so others cannot intercept it using the **public/private key** method.

Public/private key. This technique is used for secure transactions over the internet using the HTTPS protocol. It involves the creation of a pair of mathematically related keys, the public key and the private key. This is called asymmetric key encryption because

Case study

The San Bernardino attack

In December 2015, fourteen people were killed in a terrorist attack in San Bernardino, California, USA. An Apple iPhone 5C belonging to one of the terrorists was recovered, and the FBI wanted to unlock the phone to see if other people had been involved in the attack. (The two terrorists who carried out the attack were shot dead by police.)

However, in 2014 it had been revealed that the FBI and the British security services had ways of accessing all information on Apple and other smartphones. In response to this Apple had improved its encryption in iOS version 8, and this prevented the FBI gaining access to the terrorist's phone. The FBI therefore asked Apple to unlock the phone. Apple refused, stating that it was company policy not to undermine the security features of its products as to do so would not be in the interests of its customers. The FBI issued a court order compelling Apple to unlock the phone. However, before the case was due to go to court the FBI dropped the case because they stated that a third party (said to be the company Cellebrite) had enabled them to access all the data on the phone.

The case raised many technical and ethical questions about whether technology companies should build a 'backdoor' into their encryption products for the purpose of allowing government agencies to access them in cases such as the San Bernardino shooting, and if it is in their customers' interests to protect their encryption methods at all costs.

Check your knowledge

1. Do you think it was right for the FBI to want access to the information on the terrorist's phone?
2. Should the government have access to our data? If you are doing nothing illegal, what is there to hide?
3. Why would Apple want to protect its encryption methods? Do you think they were right to withhold the information?

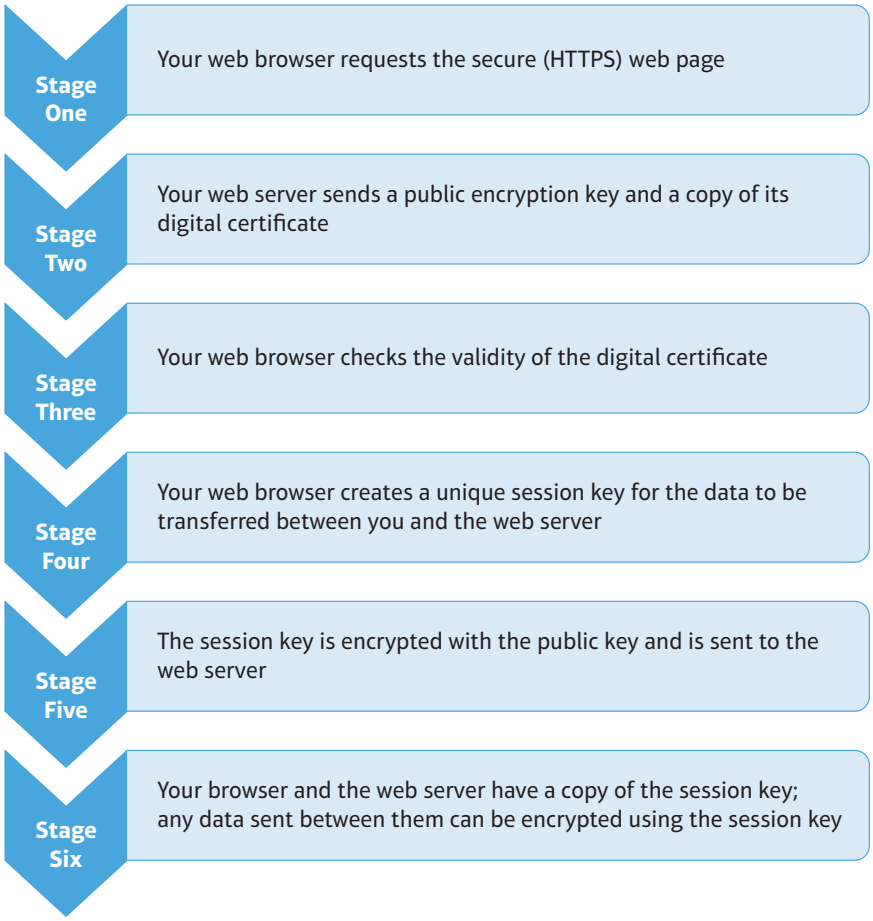


Figure 11.2 Process when accessing a website using the HTTPS protocol

different keys are used to encrypt and decrypt the data. The public key is available to anyone, but the private key is kept secret on the web server. Data encrypted with the public key can only be decrypted with the private key.

When a user wants to access a website using the HTTPS protocol the process is as shown in Figure 11.2.

It is not efficient to encrypt large amounts of data using asymmetric key encryption. It is only used to transfer the session key between the client and the server. The rest of the session data is encrypted and decrypted using the session key.

Pause point Encryption predates the computer era and has been used for many different purposes where information needs to be kept secret.

- How does encryption keep data secure?
- The public/private key system uses asymmetric keys where the different keys are used for encrypting and decrypting data. What is symmetric key encryption and how does it differ?

Hint You can research these terms on the internet.

Extend As computers become more powerful, methods of encryption which use only short key length become easier to crack. Why is this?

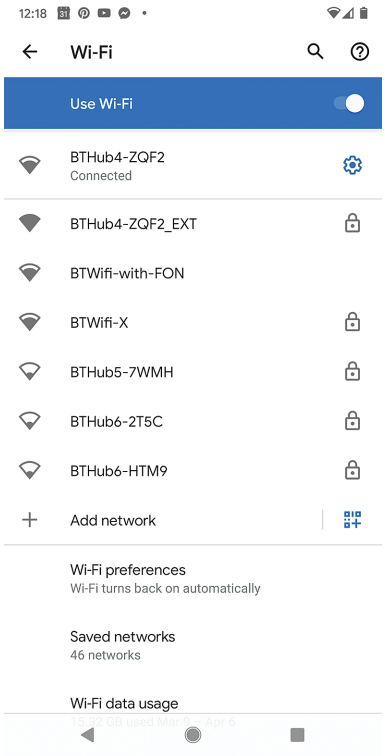


Figure 11.3 SSIDs listed on a device

Wireless Local Area Network protection

Wireless Local Area Networks (WLAN), commonly known as Wi-Fi networks, are particularly prone to interception of data because, unlike in a wired network, the data is broadcast on a radio-based network so anyone in range can intercept the messages. There are various techniques used to help protect Wi-Fi networks.

Service set identifier (SSID) hiding

Each WLAN has one or more wireless access points which provide a link between the radio-based wireless network and the wired LAN and internet. In a home network these are often called broadband routers. The SSID is the name of the Wi-Fi network. When a user looks for available Wi-Fi networks to connect to on their device, SSIDs of the networks in range are shown. You can set your access point so it does not broadcast the SSID; anyone who needs to use the network would need to be told what the SSID is. This provides a very basic level of security since an attacker with the right tools would be able to locate the network SSID easily even if it is not being broadcast.

MAC address filtering

Every network device has a unique hardware address called a Media Access Control (MAC) address. This is built into the device and cannot be easily changed. To improve the security of a WLAN, you can configure it to accept connections from certain devices based on their MAC address. While this increases the security of the WLAN, as only approved devices can connect, it can be inconvenient since any new device which wants to join the network must have its MAC address identified and entered into the access points list of allowed devices. MAC address filtering will not stop a determined and knowledgeable attacker. With the right tools it is not difficult to identify which MAC addresses are allowed on the system and then fake this on a device to gain access to the network.

Wireless encryption

The primary method of protecting data transmitted over a WLAN is to encrypt the data. This uses a Wi-Fi password to encrypt all the data sent over the WLAN. Various standards have been developed over time for Wi-Fi encryption.

- **WEP** (Wired Equivalent Policy) was the original encryption standard for Wi-Fi networks. But it can be cracked within minutes with commonly available tools, as WEP uses relative short keys (64 or 128-bit) and the same key is used for each packet of data.
- **WPA** (Wi-Fi Protected Access) was introduced around 2003 to address the weaknesses in WEP. It used 256-bit keys and different keys for each packet. Due, in part, to the fact that WPA was designed to allow WEP devices to be upgraded to WPA, it was also shown to be fairly easy to crack.
- **WPA2** (Wi-Fi Protected Access 2) dealt with the weaknesses in WPA and became an official standard in 2006. It uses the powerful Advanced Encryption Standard (AES) system and is the most secure wireless security standard currently available, and the one all home and organisational Wi-Fi networks should be using.
- **WPS** (Wi-Fi Protected Setup) is not an encryption standard but a method that was developed to allow home users to easily add devices to a Wi-Fi network. Typically, this allows users to press a button on their Wi-Fi router and on the device they wish to connect. Alternatively the user enters an 8-digit PIN to join the network. While WPS is convenient it has a security vulnerability. The PIN can be cracked using **brute force attacks** in as little as four hours. It is recommended that this feature is disabled on routers that support WPS.

Key term

Brute force attack – an attack in which an attacker submits all possible passwords or PINs until the correct one is found. The longer the password or PIN, the longer a brute force attack is likely to take.

Another consideration with Wi-Fi security is the location of the Wi-Fi router. Most home-based routers have the Wi-Fi key printed on a sticker on the back of the router. If the router is easily accessible, anyone (workmen, cleaners, etc) can easily get the password for the WLAN.

Security issues need to be considered at the design stage of a large Wi-Fi installation to ensure it is built in from the development stage. Some examples of things that might be considered are:

- Will the WLAN just be for the company's employees or will visitors be allowed access?
- If visitors are allowed Wi-Fi access, will they share the same WLAN as the employees?
- Will the WLAN use a fixed password or will it use individual passwords for each user?
- Who will monitor the devices attached at any one time?

Pause point Public Wi-Fi 'hotspots' are sometimes 'open' and do not use any encryption.

- How can you tell if a Wi-Fi hotspot uses encryption or not?
- What kind of activities should you not engage in while using an open Wi-Fi hotspot?

Hint When you join a Wi-Fi hotspot your device will provide information about the connection.

Extend How is Wi-Fi different from a 4G mobile data connection?

Assessment practice 11.1 A.P.1, A.P2, A.P3, A.M1, AB.D1

A company has employed you to provide support and guidance in the area of IT security. You need to write a guide for all IT users which provides an explanation of:

- The various cyber security threats which could affect the company's systems.
- The system vulnerabilities which could affect the company's systems.
- The security measures (including physical, software and hardware) that can be taken to protect the organisation systems from the security threats.

Plan

- Make a plan to complete the assignment, listing all the things you need to do and when you will do them.

Do

- Make sure you have covered all the different types of security threats.

Review

- Read through what you have written to make sure it is clear and makes sense.

B Explore the security implications of networked systems

The use of networked computer systems by individuals and within organisations is widespread and new network technologies continue to be developed. Networks have security implications and an understanding of the nature of networks and security issues helps in the selection of networks for different purposes and the technique needed to protect them.

Skills

Cognitive skills/cognitive processes and strategies:

- Analysis
- Interpretation

Network types

Applications and features of networks

There are several different types of network. They differ in their geographical extent:

- **Local Area Network (LAN)**. This type of network has a limited geographical extent, usually within a single building or a small group of buildings on the same site. Usually a LAN is private in that it is only used by one organisation. Traditionally, connections to LANs are wired with copper or fibre-optic based cables. Since a LAN is usually internal and used only by a single organisation it is less vulnerable to external threats, although security precautions are needed to protect the LAN's connections to the internet.
- **Wide Area Network (WAN)**. This type of network has a wide geographic extent and the most common WAN is the internet, which is open to the public. Connections to WANs are wired. Since it is open to the public the internet is the main source of external security threats.
- **Wireless Local Area Network (WLAN)**. This is a Wi-Fi based network commonly used by home users and organisations. There also are public WLANs. These are provided in many public spaces such as shops, cafes, railway stations, airports. These allow members of the public to access the internet from mobile devices. Due to the broadcast nature of a WLAN, precautions must be taken to avoid data being intercepted by people for whom it is not intended.
- **Storage Area Network (SAN)**. This is a specialised high-speed network for storage devices. They are typically connected via fibre-optic cables or high speed **ethernet** cables but do not normally share traffic with a LAN. A SAN allows multiple servers to access the same storage devices (typically disks). SANs tend to be used by large organisations who need to store and have access to very large amounts of data.
- **Personal Area Network (PAN)**. This is a network which interconnects devices in a user's personal workspace. For example, they are connected using the Bluetooth standard. This is a short range, low power consumption wireless connection method which is used to connect devices such as mobile phones to audio headsets, keyboard and mice to computers and other devices.

Key term

Ethernet – a set of technology standards developed in the 1980s that define a way for computers to talk to each other both in wired and wireless networks.

Network classification

Networks using internet technology can be classified in terms of who can access them.

- **Intranet**. This is an organisation's internal private network that uses internet technology. By using internet browsers users can access an organisation's specific information and interact with the organisation's systems.
- **Extranet**. This is an intranet which is shared by the organisation with selected partners such as customers, suppliers, etc. This allows the organisation's partners to access some of the organisation's systems. However, precautions must be taken to ensure external organisations cannot access systems which are for internal use only.

- **Internet**. The word describes any public network which can be accessed by anyone.
- **Cloud**. Cloud technology involves the use of internet-based systems to provide facilities which were previously provided locally. A common use for cloud technology is file storage. Traditionally organisations would keep their files on a file server computer located in the organisation's offices. The cloud-based alternative is for files to be stored by a cloud storage provider (e.g. Dropbox) somewhere on the internet.

Wired and wireless integration

Both home and organisation users need to integrate wired and wireless networks. Home users are provided with a device, usually called a wireless router, which performs a number of functions. It provides a wired link using the internet via a telephone cable or cable TV connection. It also includes a wireless access point so users can connect wirelessly to the internet, and it usually includes a number of wired LAN connections so a fixed device such as a desktop computer can have a wired connection to the internet.

Organisations commonly provide wired connections to desktop computers on employees' desks within their offices. They may also provide a wireless network for the connection of mobile devices such as laptops and mobile phones.

Figure 11.4 The back of a wireless router

Applications and features of network topologies

A network topology is the way the network is laid out and connected. Topologies can be defined as physical topologies or logical topologies.

Physical topologies

These describe how cables are connected to various devices. There are variety of commonly used physical network topologies:

- **Star** is used for simple wired LAN configurations. Here, all devices are connected to a central switch. See Figure 11.5.

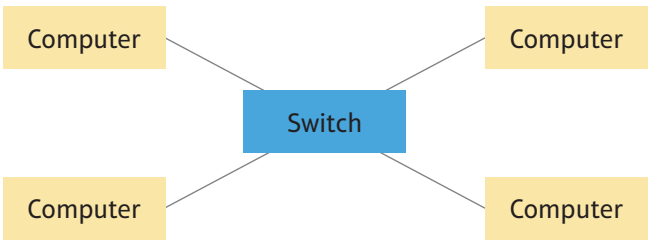


Figure 11.5 Star topology

- **Extended star** uses the same concept as the star topology but is extended by additional switches to provide more available device connections. See Figure 11.6.

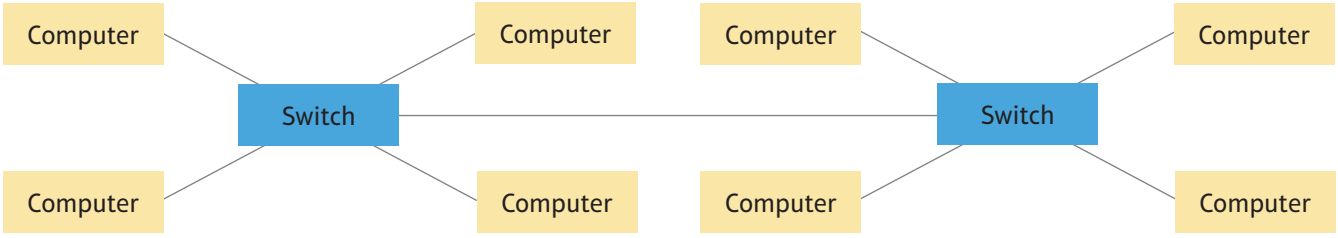


Figure 11.6 Extended star topology

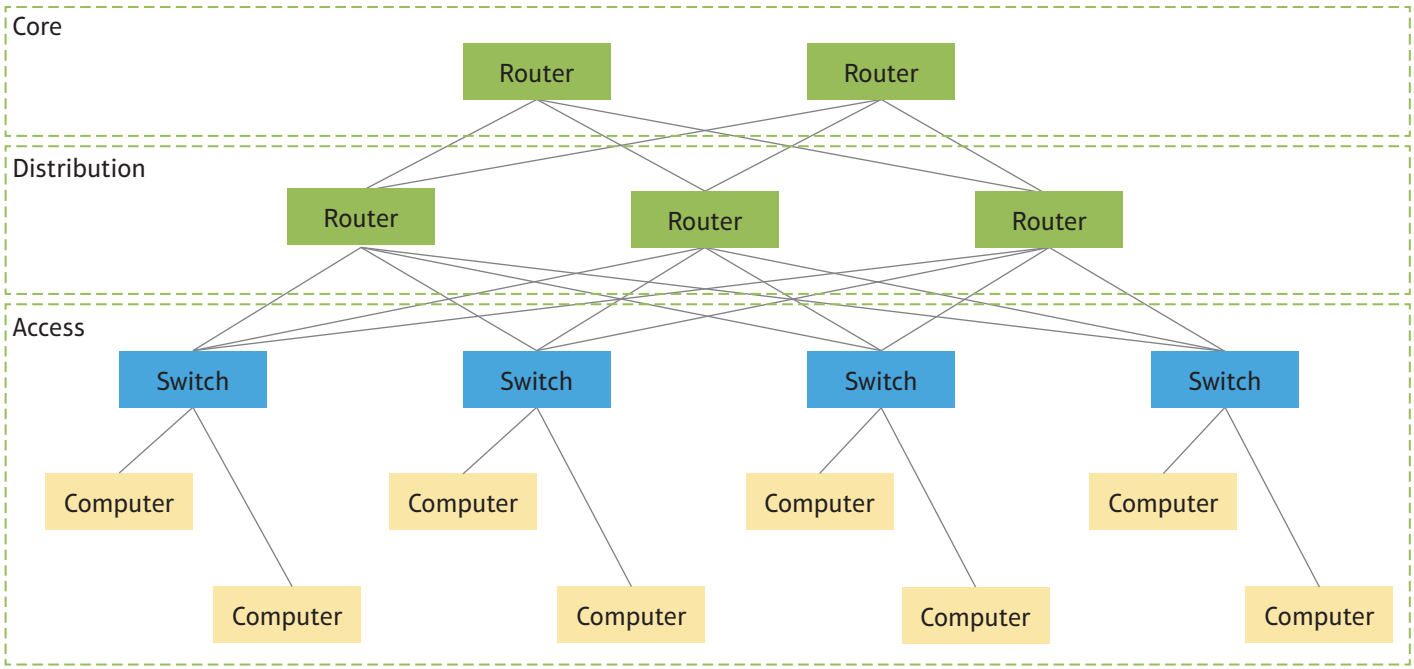


Figure 11.7 Hierarchical network topology

- **Hierarchical** is where a large network needs to be created. It divides the network into three different layers. The access layer provides individual device access to the network, the distribution layer controls the links between the access and the core layers and the core layer provides links between the distribution routers. See Figure 11.7.
- **Wireless mesh**. This wireless topology is used to cover larger areas than can be covered by a single wireless access point. Wireless mesh networks have a number of wireless nodes which provide coverage over areas such as an office or warehouse. Only one of the nodes needs a wired connection to the internet, as each node shares its connection with the next nearest node.
- **Ad hoc.** This type of network uses a combination of wired and wireless networks. This can be found in offices and buildings where some workers have access to the wired desktop computers but others use their own devices (smartphones, tablets, etc.). When employees access a company WLAN using their own devices this is known as Bring Your Own Device (BYOD). See the next section for more details.

Logical topologies

These describe how devices communicate on a given topology. Wired Local Area networks transmit data using ethernet technology. Modern Ethernet LANs use unshielded twisted pair cables (UTP) and connect to devices (computers and switches) using RJ45 connectors. Data transmission speeds are very high (up to 400 Gbits per second, depending on the type of UTP cable used). Network switches which connect the computers on an Ethernet LAN are intelligent devices, so they inspect incoming data packets for their network address and only transmit the packet to port(s) where it is intended to go rather than to all the ports. Ethernet cable runs have a theoretical maximum length of 100 metres although this can depend on the type of UTP cable used and the speed of the link. Ethernet is an international standard known as IEEE802.3.

Wireless networks use a connection standard known as IEEE802.11 which has some similarities to the ethernet wired standard in terms of access control. Various versions of the IEEE802.11 standard have been developed over the years with increasing data transmission speeds and other improvements. The original widely used standard

was 802.11b which had a data rate of 11Mbit per second. Many current devices support the 802.11n standard which has a data rate of up to 600Mbit per second. Other faster versions are currently in development.

Applications and features of network architecture

- **Peer-to-peer networks**. These are unstructured and do not have a centralised server computer that controls the network. Users log on to individual computers and can share files and resources such as printers. Peer-to-peer networks are ideal for home users or small offices which have a limited number of users. They are easy to set up and manage and don't require additional hardware. However, with larger networks peer-to peer networks become difficult to manage. With no centralised control each computer has to be managed separately and individual users can only log on to computers for which they have an account.
- **Client server networks**. These have a central server computer. Users log on to the network rather than an individual computer so if they have a network account they can log on at any computer. Management of all the computers in the network is done centrally on the server. This means that updates, account creation, security restrictions, file and folder permission, backups and many other things can all be managed centrally on the server.
- **Thin client**. Traditionally the end user device (the client end in client server computing) is powerful enough to run applications locally and has the storage capacity to also store files locally. However, with recent advances in high-speed networks and cloud-based facilities, lower specification hardware devices, known as thin clients, can be used. These run web-based applications (such as the Google® Office application suite) and store files on the cloud. With lower hardware specs these devices are cheaper than traditional laptop or desktop computers. The 'Chromebook' range of laptop computers is an example of this type of technology.

Modern trends

Computing technology tends to progress at a very rapid rate. Some of the current emerging technologies include:

- **Virtualisation**. Traditionally a large company or organisation would have a number of different server computers, each of which carries out a specific task. However, it is common today for a powerful server computer to use virtualisation software to run several **virtual computers** to carry out specific tasks. Creating multiple servers on a single physical computer makes managing workloads easier and improves scalability. It also makes more efficient use of hardware.
- **Cloud computing**. Cloud computing has already been mentioned in the context of cloud storage, but there are several other ways cloud technology can be used:
  - **Cloud applications**: these are software applications that, rather than running on the user's local machine, run on a server in the cloud and are accessed through web browser software. An example of this type of application is Google Docs. This type of cloud service is sometimes called Software as a Service (SaaS).
  - **Cloud development platform**: this is a service provided to software developers where a cloud service provider creates a development environment, including program development, database and web service tools. This is sometimes known as a Platform as a Service (PaaS).

Cloud computing has security concerns for organisations as the responsibility for protecting the organisations data is passed to the cloud service provider. These include:

- **Bring your own device (BYOD)**. Letting employees use their own mobile devices (such as smartphones) has advantages for both employers and employees. It allows a

Key term

Virtual computer – a software emulation of the hardware of a computer which allows a separate copy of an operating system and associated applications to be hosted on an existing physical computer hardware. This would allow a single physical computer to host a number of different virtual computers potentially running different operating systems and applications.

Theory into practice

Some network topology diagrams were shown earlier and there is another example in Figure 11.8.

Create a simple network topology diagram of the network in your school or college using the Microsoft Word Drawing tools or other drawing software such as Visio or take one of the diagrams and add an internet link, server computer and Wi-Fi link.

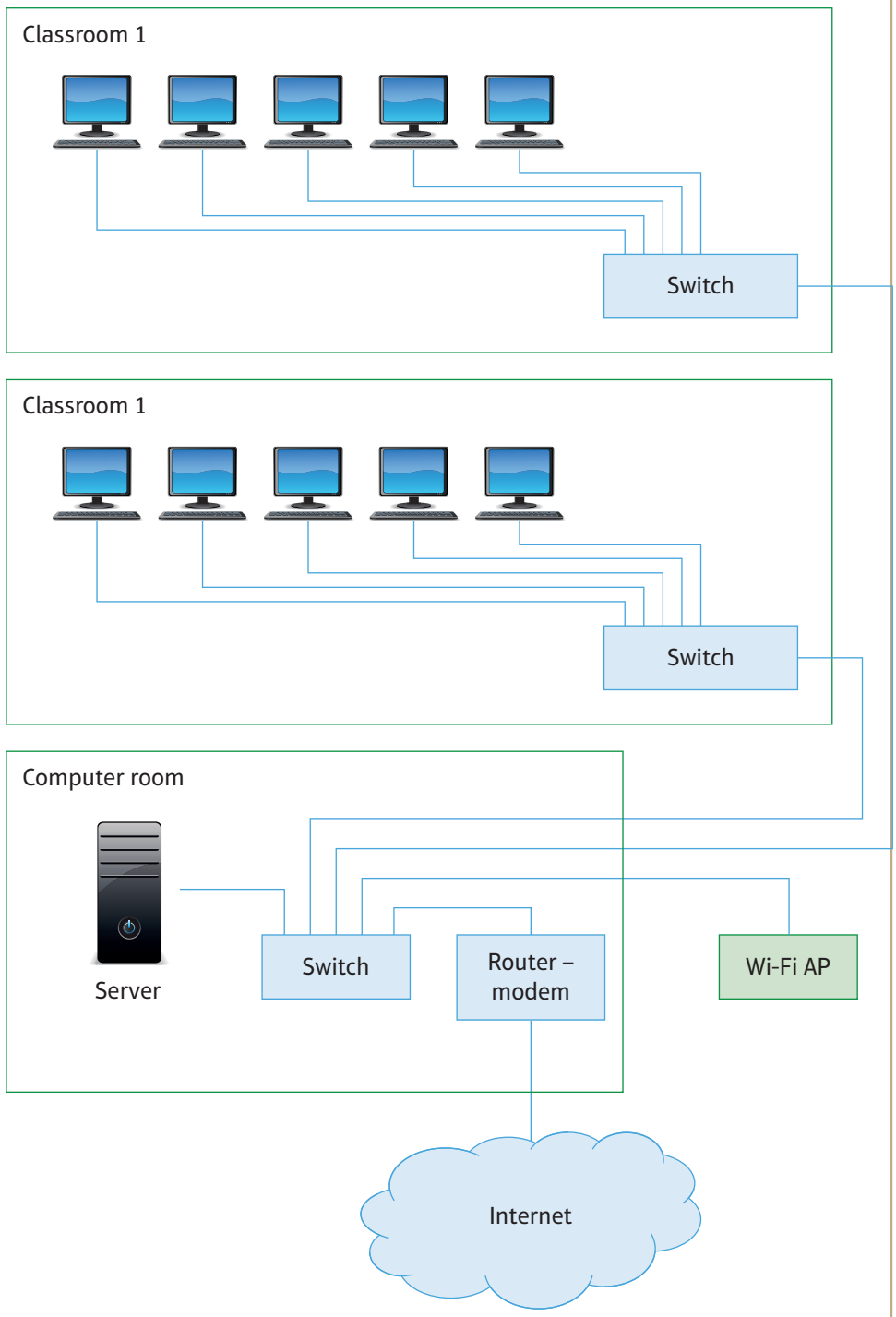


Figure 11.8 Example of a network topology

greater degree of working flexibility and employees often feel more comfortable using their own devices. However, allowing these devices to access company systems is a major security issue. They are not fully under the control of the company and may not have sufficiently strong security settings.

- **Software defined networking (SDN)**. This is a more flexible approach to networking than the traditional network architectures. It provides cloud-like facilities within an internal company network. SDN networks have controllers which provide network managers with a method to manage and configure the network. The SDN also has connections to the networking hardware devices and applications.
- **Storage defined networks**. This is a method of connecting storage devices directly to a network so they are available for all network users to access. They are generally used in large organisations where users may benefit from easy access to large amounts of data.
- **Internet of things (IoT)**. This is the concept of connecting any electronic device (so long as it can be turned on and off) to the internet and other electronic devices.

Pause point

Computing technology develops at a rapid pace and new features and facilities become available all the time. However, with each new technology comes security issues and opportunities for criminals to exploit possible weaknesses.

What are the security implications of the internet of things?

Why are organisations concerned about the impact of BYOD? What could be the security issues?

Other current trends include Artificial Intelligence and Robotics. Find out what you can about the security implications of these technologies.

Hint Since technology and security issues develop and change all the time, the best place to research into these topics is the internet.

Extend What other or more recent trends or developments in IT are there? Find out about them and their security implications.

Network components

Networks are made up of a variety of different devices, each of which have different functions.

Skills

Cognitive skills/cognitive processes and strategies:

- Analysis
- Problem solving

Hardware components

- **End user devices**. These are the devices which provide an interface to human users and include desktop and laptop computers and mobile devices such as tablets and smartphones.
- **Connectivity devices**:
  - **Switches**: are used within a wired LAN to connect devices. Switches direct data to the end device to which they are addressed.
  - **Routers**: act like a road junction sending packets of data off to different networks or network segments depending on their destination IP address.
  - **Access points**: provide a link between wired LAN and a wireless network.
  - **USB hubs**: devices which allow multiple USB devices (such as printers, external hard disks, etc.) to be connected to a computer.
  - **Modems**: are used to connect a LAN to the internet. There are two types of modem widely used. An ADSL modem connects to the internet via a traditional telephone line while a cable modem connects via cable TV where available.

- **Multifunctional devices**: most home users are provided with a multifunctional device which combines modem, router, wireless access point and wired switch by their internet service provider (ISP).

- **Connection media**:
  - **Cables**: the most common cable used for LANs is known as Unshielded Twisted Pair (UTP), which has four pairs of copper cables twisted together to reduce interference. There are a range of 'categories' of UTP cable, the lowest category of UTP cable suitable for computer networks is Category 5, commonly called Cat 5. The different UTP categories and their features are shown in Table 11.1 below.

    Table 11.1 UTP categories and their features

UTP cable category	Max speed	Segment length
5	100Mbits/sec	100m
5e	1Gbits/sec	100m
6	10Gbits/sec	55m
7	10Gbits/sec	100m

    In situations where there is a lot of electrical interference (such as in a warehouse or factory) shielded twisted pair (STP) cable can be used. This has an aluminium foil shield around the twisted pair cables.
  - **Fibre-optic cable**: where high speed links are required, fibre-optic cable may be used. These cables use light to transmit data rather than electrical signals. Fibre-optic cable can be run over much greater distances than UTP, which means it can be used for WAN connections rather than just for LANs. Telephone and broadband internet companies use fibre-optic as an alternative to traditional copper telephone cable to provide higher speed internet connections than can be provided over telephone cables. Traditionally fibre-optic cables were considered to have faster data transfer rates than UTP but the latest versions of UTP (Cat 7) are as fast as fibre. Fibre-optic cables are considered more secure than UTP because none of the signal radiates outside the cable and it is very difficult to tap into a fibre cable without causing light leaks.
  - **Wireless media** such as Wi-Fi uses radio waves rather than any type of cable. This is both their main advantage and disadvantage. You do not need to install cables to connect devices, which is a big benefit for both home and organisation users as they have flexibility in location of devices and there is no cost or disruption in installing cables. However, because the signal is broadcast to everyone it is very easy to eavesdrop on a wireless network and the signal may well radiate some distance outside the house or office where is it intended to be used. Where security is an important issue care must be taken to ensure the network only uses encrypted data and is set up correctly. Wireless networks can suffer from dead spots where no signal is available, especially in a house or office where there are internal walls and floors. Without use of repeaters or wireless mesh systems range is limited.
  - **Bluetooth and Infrared**: bluetooth is a short-range wireless system with low power consumption which is typically used to connect small devices (such as audio headsets and keyboards/mice) to computers or mobile devices. Infrared is a wireless communication method which uses electromagnetic radiation with a wavelength slightly longer than red light (but shorter than radio waves). Infrared communication is short-range and line of sight only (there can be no obstructions between the sender and receiver). The most common use of Infrared is in TV remote controls.

- **Li-Fi** is a technology similar to Wi-Fi but it uses light rather than radio waves. It has the potential to provide higher bandwidth and faster transmission speeds. It can also be used in areas where Wi-Fi cannot be used because of electromagnetic interference, such as in aircraft cabins. The technology is currently under development.

Table 11.2 Comparison of different media types

	UTP	Fibre optic	Wireless
Distance	Medium (LAN only)	Long	Short
Speed	High (depending on cable type)	High	Low/Medium (depends on version)
Ease of installation	Difficult	Difficult	Easy
Security	Can be intercepted	Difficult to intercept	Easy to intercept
Cost	Medium	High	Low

- **External media and storage**. Until cloud storage became popular the use of external media for offline storage and transfer of data files was popular. These included
  - **USB flash drives** (also known as pen drives or memory sticks): these small devices plug into the USB port of a computer and store files with a capacity of up to about 64 GB. They are useful to transfer files between computers which would be too large to send as an email attachment. However, they are a major security concern as they can easily be lost and can be used to spread virus infections from one computer to another. For this reason, many organisations ban their use. In most situations cloud based storage provides a better option except where there is no internet connection. USB flash drives can also provide a simple method for home users to back up their files.
  - **Optical media**: CDs and DVD were also once widely used, especially for software distribution. However almost all software applications are now downloaded over the internet rather than distributed on CD or DVD.

Pause point What kind of network does your school or college have?

- What topology does it use?
- What kind of cabling or Wi-Fi does it use?
- What connectivity devices does it use?
- What cyber security protection methods does it have in place?

Hint Your teacher or IT manager may be able to help you with this.

Extend How could the network and its protection be upgraded?

Operating systems

Every computing hardware device needs some kind of operating system to control the hardware and provide a user interface. Operating systems can be divided into those that support single devices and network operating systems which support a networked system.

- **Mobile operating systems**. These are device operating systems which work on mobile phones and tablet computers. They are designed to support a single user per device. Examples include Android and Apple iOS.

- **Desktop computer and laptop operating systems**. These are end user operating systems with a full range of functions designed to work on large screen devices. Examples include Microsoft Windows and MacOS. These operating systems support multiple user accounts on a single machine, but with only one user actually using the computer at a time. Microsoft Windows comes in two versions, the 'Home' version aimed at home use and designed to work in a peer-to-peer network, and a 'Enterprise' version (sometimes called 'Professional') which can work with both peer-to-peer and client-server networks.
- **Server operating systems**. These include features which are not focussed on end users but instead provide tools to allow a system manager to support a client server network. Server operating systems are designed to allow multiple remote users to simultaneously access the services it provides. Examples of server operating systems are Microsoft Windows Server and Linux.

Network tools

Network tools are provided to allow system managers to set up, administer and troubleshoot the network. They can also be used to protect the system and investigate security issues. There are a number of network tools available.

- **Network monitoring**. System managers use this software to check the network is operating and to see if any connections are down.

Theory into practice

Network management tools

Windows Firewall creates a log. If you open the Firewall management application and choose the Monitoring link on the right, you should see a link to the logging section, see Figure 11.10. You need to check that logging is recording dropped (blocked) packets otherwise there will be nothing in the log file.

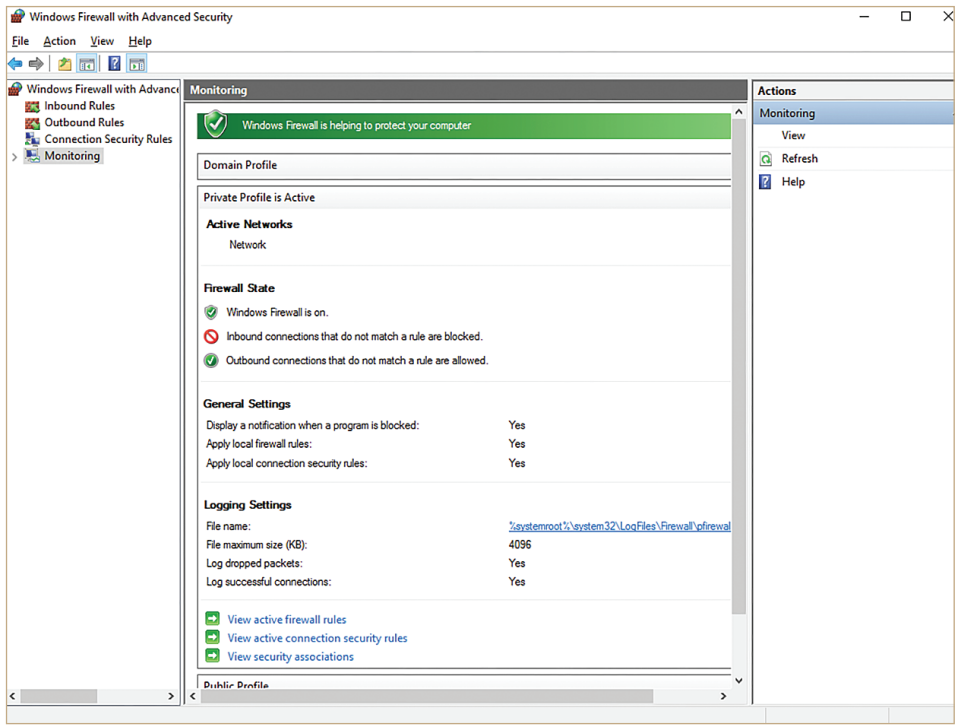


Figure 11.9 The monitoring view of the Windows Firewall

Theory into practice *continued*

Clicking on the link will open the log. An example is shown in Figure 11.10.

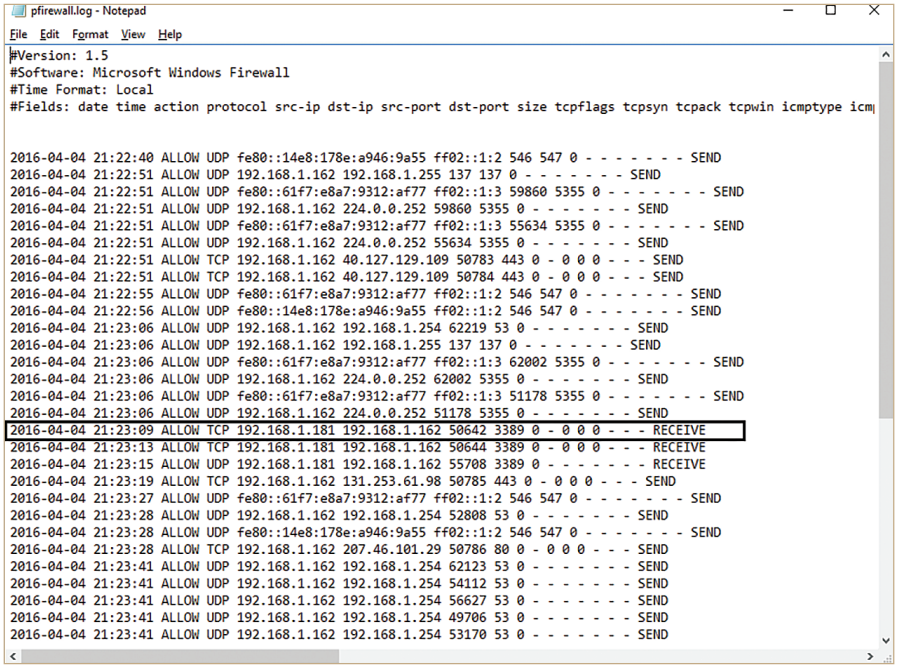


Figure 11.10 Firewall log

Viewing the log may help a system manager identify an attempt by a hacker to gain access to the system.

This is one of the simplest but most widely used troubleshooting tools in the 'ping' program. Ping can be run from the Windows command prompt and allows you to check that your device can get a response over the LAN and/or internet from a remote device, using either its IP address or URL. This is a useful low-level check that connectivity exists. Figure 11.11 shows ping being used to test the link to a local device by IP address (192.168.1.236) and a remote server by URL (www.google.com).

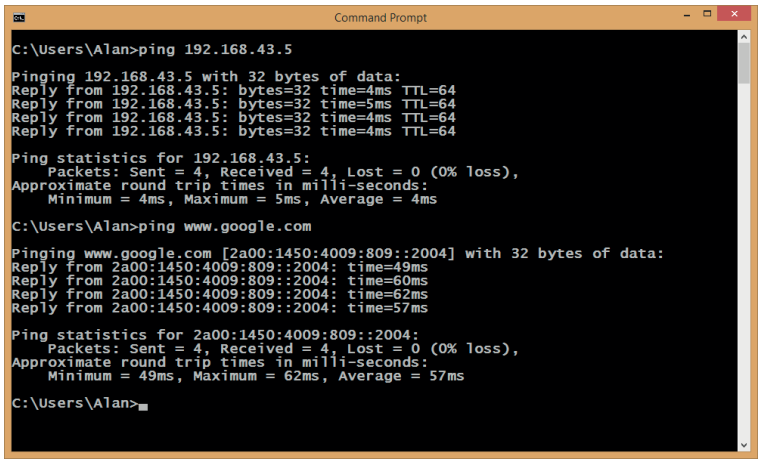


Figure 11.11 Using Ping

Note that some devices will not respond to ping requests as it is considered a security risk. Think about why responding to ping requests might be considered a security risk.

- **Management and troubleshooting**. These tools are used to check network performance, for example:
  - **Performance monitor**: to identify any links which have poor performance and may need further investigation.
  - **Events and logs viewer**: many software and hardware components (such as a firewall) in a large network create logs which list events (such as a network link going up or down) and viewing these logs can help a system manager identify problems.
  - **Vulnerability scanners**: these can scan all the computers on a network. They look for potential vulnerabilities (such as a computer with an operating system which does not have the latest updates applied).
  - **Packet sniffers**: these allow the contents of individual network packets to be viewed. This can be useful for troubleshooting and security investigations. However, packet sniffer software can also be used by hackers to attempt to obtain information which might help them (such as MAC or IP addresses).

Network applications

- **Database systems**. These are one of the most widely used network applications. Sophisticated high-performance database products such as Oracle, Microsoft SQL Server and MySQL allow multiple users to search for, edit and insert data records on large relational databases. These application support systems allow multiple users to access the same data while ensuring the integrity of the data (for example by ensuring no two users can update the same data record at the same time). Because database systems often store large amounts of sensitive information (such as users' names, addresses, credit card details, etc.) they are often the target of cyber security attacks using SQL injection and other techniques.
- **Document management**. Many organisations deal with large quantities of documents, for example insurance companies and banks deal with very large numbers of customer agreements and contracts. Document management allows multiple users to manage, search and access large amounts of documents.

Theory into practice

Here is a simple example of how an SQL injection attack might work. Think of the product search box that appears on websites such as Amazon or eBay. When you type something into the search box (such as 'Nike Trainers') that value is used in an SQL query which searches the Amazon or eBay database for matching values. Typically, the sort of SQL statement that might be used is as follows:

```
SELECT * FROM Products WHERE description = 'Nike trainers'
```

An attacker with a knowledge of SQL can use the fact that the SQL uses a semicolon to indicate the end of a statement. So, suppose an attacker entered the following into the product search box:

```
'Nike trainers';SELECT * FROM customers;
```

When this statement is read by the web application it is turned into two statements (because the semi-colon indicates the end of the first one). The first one is the same as before, the second one is:

```
SELECT * FROM customers
```

This could potentially provide a list of all the records on the customer table, including names, addresses, credit card numbers, etc.

- **Network discovery** is a tool which searches a large network for available services, including software application services and hardware such as networked printers. The available services are presented to users, often in a graphical format, and allows them to see what is available. On a particular device, network discovery can be turned off so it does not appear on the list of available network services that other users can see.

Carry out some research into what a website needs to do to protect itself from SQL injection attacks.

Networking infrastructure services and resources

The network services allow networks to be built and support the functionality required by the applications which use those networks.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Network software is complex and therefore it is split into layers. At the lowest layer you have the hardware components and electrical signals, at the highest layer you have the user applications such as a web browser. The four layers of the TCP/IP model are shown in Figure 11.12.

Application
Transport
Internet
Network access

Figure 11.12 The layers of the TCP/IP model

At the transport layer the TCP protocol is used and at the internet layer the IP protocol is used. These are the main protocols used at these layers. Other protocols are also used for particular purposes.

Ports and the transport layer

The purpose of the transport layer is to keep track of individual connections and to divide up the data to be sent into segments (and reassemble them when received). Unless data is split up like this some applications which need to send large amounts of data (e.g. video streaming) would prevent other applications from sending or receiving data for long periods of time. Because an individual device may well have several applications communicating over the network at the same time, the transport layer must identify which application is which. To do this it assigns a **port number** to each application. Port numbers for commonly used applications are fixed (using so called 'well known port numbers') and some of these are shown in the table below.

Table 11.3 Some of the well-known port numbers

Application	Port number
File transfer protocol (FTP)	20
Simple Mail transfer protocol	25
Hypertext transfer protocol (HTTP)	80
Post Office protocol (POP)	110
Secure HTTP (HTTPS)	443

Skills

Cognitive skills/cognitive processes and strategies:

- Analysis
- Interpretation

Key term

Port number – a communication end point.

The TCP protocol segments data into what are called Datagrams. These contain segments of the data to be sent and additional information including the source and destination port and a sequence number (datagrams may not arrive at their destination in the order in which they are sent so when received TCP must be able to put them back in the correct order).

Packets and the internet layer

When sending data, the internet layer receives segments (or TCP datagrams) of data from the transport layer, and its job is to provide addressing information. It does this by adding IP source and destination addresses to the segment in what is known as an IP header. The process of adding this additional information to the segment is called encapsulation. With the addressing information added to the segment it is now called a packet.

IP network addressing

IP addresses are the method used on the internet to uniquely identify where a packet should be sent. IP addressing is based on the concept of hosts and networks. Hosts are individual devices, while networks are groups of devices in one geographical location (such as a house or office).

IPv4 addressing. This addressing scheme was defined in the 1980s and consists of a 32-bit number which is usually shown in decimal format, with 4 x 8-bit groups (sometimes called octets) of decimal numbers in the range 0 to 255, so for example 192.168.10.5. The first part of the address identifies the network and is used by internet routers to send the packet to the correct house or building. The last part of the address is the individual device address and is used inside the network to send the packet to the correct device. How many of the 32 bits are allocated to the network and device portions of the IP address can be defined in a number of different ways. The simplest method is to use IP address classes. Classes A, B and C are used for device addressing. The class of an IP address is defined by the first octet as shown in the table below.

Table 11.4 Classes of IP addresses

	First octet range	Network address	Host address	Possible number of networks	Possible number of devices (hosts)
Class A	1 to 127	First octet	Second, third and fourth octet	126	16 million (approx.)
Class B	128 to 191	First and second octet	Third and fourth octet	16,384	65,534
Class C	192 to 223	First, second and third octet	Fourth octet	2,097,159	254

For example 129.10.30.16 is a class B address, the network address is 129.10 and the device address is 30.16. 200.20.15.68 is a class C address, the network address is 200.20.15 and the device address is 68. The original idea behind this addressing scheme was that class A addresses would be suitable for very large organisations of which there are a fairly small number (a maximum of 126) but each organisation has a very large number of devices they need to connect. Class B addresses would suit medium sized companies and class C addresses would suit small companies with lots of network addresses but each network only having a small number of devices (maximum of 254).

The classes are no longer used in the way originally intended and it is more common today to indicate where the division lies between the network and the host section of the address by adding the number of network bits preceded by a slash, so a class A address is shown as:

88.100.35.8/8

A class B address would be shown like this:

129.10.30.16/16

A class C address would be shown like this:

200.20.15.68/24

Using this method, you can create the divide between the network and host address anywhere you like using a process called subnetting (subdividing an IP address range).

The addressing scheme was designed long before the growth of the internet and ran out of unique addresses many years ago, so this has been superseded by IPv6 addressing. However, IPv4 is still extensively used for addressing, especially in LANs.

Private IP addresses. While every computer directly connected to the internet must have a unique IP address those devices within a LAN (or WLAN) only need an address that is unique within the LAN. This means that addresses can be reused in each LAN. IP addresses are specifically identified for this use and are called private IP addresses. These addresses are never used on the public internet WAN. Private IP addresses are as shown in the table below.

Table 11.5 Private IP address ranges

	Starting Private IP Address	Ending IP address
/8 block	10.0.0.0	10.255.255.255
/12 block	172.16.0.0	172.31.255.255
/16 block	192.168.0.0	192.168.255.255

The conversion between the unique public IP address used to connect a network to the internet and the private IP addresses used within a LAN is done by the internet router using a process called Network Address Translation (NAT). Private IP addresses are defined by RFC1918 standard. The diagram in Figure 11.13 shows how public and private IP addresses can be used in a home or office network installation. Note that the public internet IP address is provided by the ISP while the end user addresses are normally provided to the devices by the DHCP, which in a home installation runs on the modem/router.

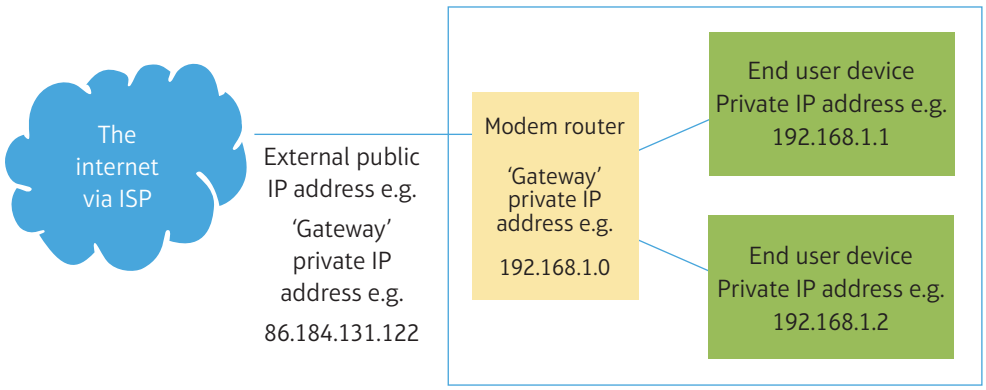


Figure 11.13 Public and private IP addresses

Key term

Hexadecimal – a base 16 number system. It is represented by the numbers 0 to 9 and the letters A to F.

IPv6. As the growth of the internet means that there are no longer any free IPv4 addresses, IPv6 was developed. IPV6 uses 128-bit addresses rather than the 32bits of IPv4 which provides a huge 2^{128} addresses. The first 64 bits are used as the network address (called the routing prefix in IPV6) and the last 64 bits are the device address. IPv6 addresses are shown as 8 groups of four **hexadecimal** digits such as:

FE80:0000:B6F7:A1FF:FEA4:E211

When there are groups of zeros these can be omitted so the address above becomes:

FE80::B6F7:A1FF:FEA4:E211

- Find out what the IP address of your computer or phone is when connected to different networks (e.g. Wi-Fi and mobile networks).
- You can find the LAN IP address of a Windows computer from the command prompt screen using the IPCONFIG command (use of the command prompt may be restricted in your school or college due to security reasons).
- The external public IP address used for the internet connection of the network you are using can be found by typing 'what's my IP address' into a search engine such as Google.
- What class of IP address is the device connected to on different networks?

Theory into practice

Figure 11.14 shows the network setting page of an Android mobile phone connected to a public Wi-Fi hotspot network.

It lists the hardware MAC address and the IPv4 address. In this case the public Wi-Fi hotspot uses an address from the /8 private IP address range of 10.0.0.158. The default gateway, which provides the link to the internet, has an address of 10.0.0.1. Typically, the default gateway address is the first (or sometimes the last) IP address in the network range. These addresses are provided by a DHCP server which is probably incorporated in the Wi-Fi access point.

Figure 11.15 shows the same device (note the MAC address is the same) attached to a home Wi-Fi network. This network also uses a private address range but this time in the /16 block, with the device having an address of 192.168.1.141. The default gateway in this network is the last address in that range, 192.168.1.254.

The subnet mask shown in both the screenshots identifies which part of the device IP address is the network part and which is the host (individual device part). In both cases this is set to 255.255.255.0. This indicates that only the last octet of the IP address is used to uniquely identify individual devices. The DNS address (the IP address where DNS requests should be directed) in both cases is set to the default gateway address.

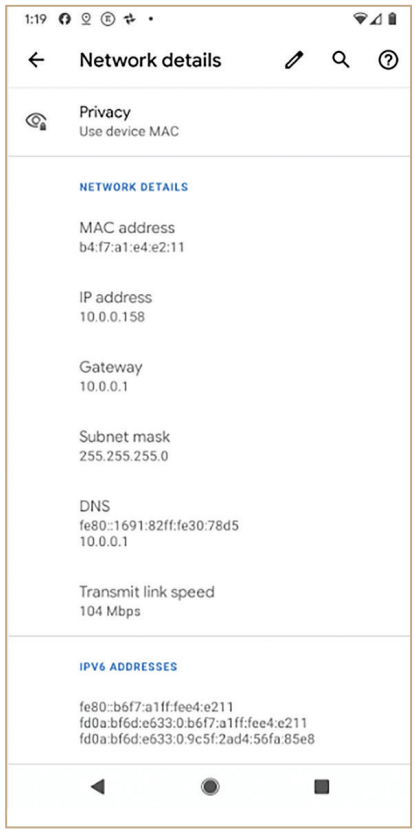


Figure 11.14 Example of IP addresses when connected to a public hotspot

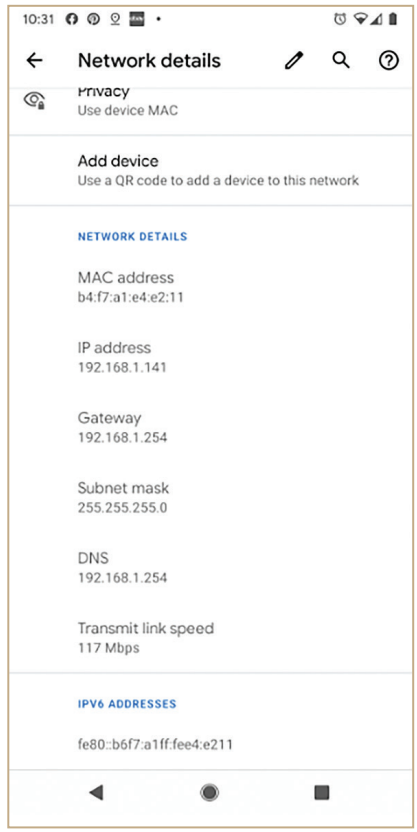


Figure 11.15 Example of IP addresses when connected to a home network

Network operating systems

Network operating systems such as Windows Server are typically divided into Windows domains. These are a collection of users and computers (and peripherals such as printers) that typically would include all the authorised users in a single organisation. Details of the users and devices are stored in the Windows directory service, Active Directory, and the authorisation of users and enforcement of security policies is controlled by Active Directory. A sub domain (also called a child domain) can be created in a Windows network which is part of the main domain and might be used for example if an organisation has a branch office with a separate network from the head office.

Using network devices to configure and segment networks

Large LANS are often segmented into smaller networks in order to reduce network traffic across the whole network. This is the technique used with the hierarchical topology described earlier.

Networks are segmented using routers. Routers are always connected to at least two different networks. When packets arrive at a router, the device examines the destination IP address and then, using the configuration information (called routing tables) it then sends the packet off to the correct destination.

The diagram shown in Figure 11.16 shows a LAN which is segmented into two different networks, 192.168.1.0 and 192.168.2.0. The router connecting the network has three interfaces. For example, packets sent to the router from the 192.168.1.0 network will be inspected. If their destination address is in the 192.168.2.0 network then they will be routed through to the interface connected to that network. If not, they will be routed to the interface assigned as the default gateway which is connected to the external internet.

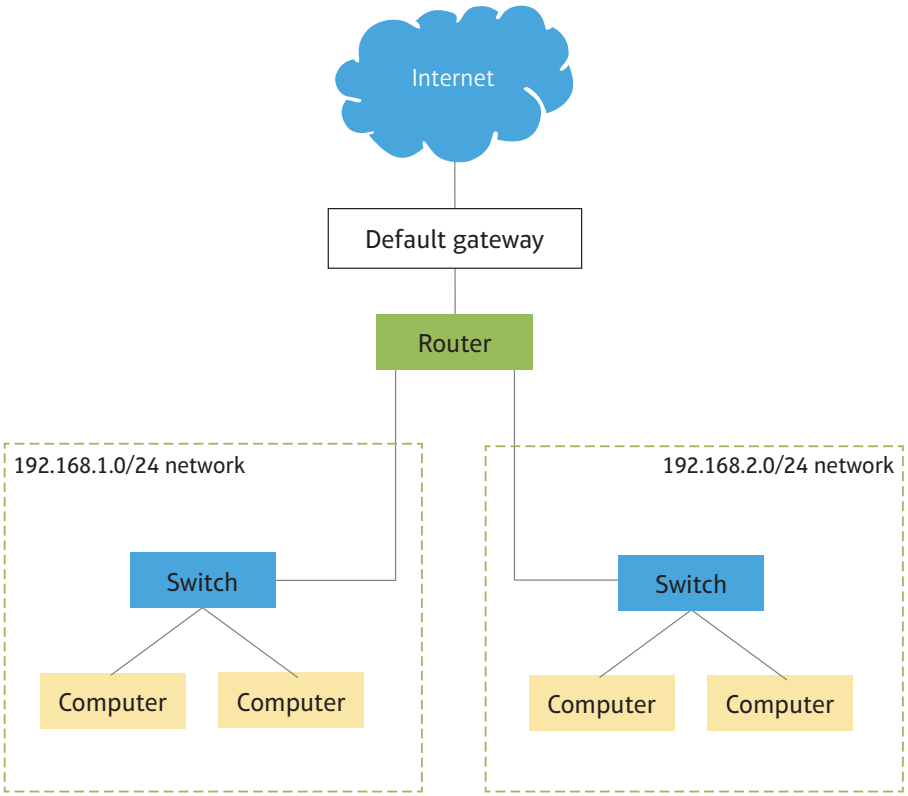


Figure 11.16 A LAN segmented into 2 networks

Link

Topologies were discussed in more detail previously in this unit, see pages 25–26.

Functions and application of network infrastructure

There are a number of network services, which usually run on a server computer within a network. These support network functionality and make networks easier to use.

Domain Name Services (DNS)

Websites are provided by web servers and the web server is identified by its unique IP address. However, IP addresses are difficult to remember. Imagine if you had to navigate to Amazon using a number. Luckily, we access websites using their domain name, such as www.facebook.com or www.amazon.ae. DNS provides the conversion between the domain name and the IP address of the website. DNS name resolution works like this:

- You type a domain name (e.g. dutchnews.nl) into your internet browser on your computer and your browser sends a query over the internet asking to match the domain name with its server's IP address. The query reaches a recursive resolver which is probably operated by your internet services provider (ISP).
- The recursive resolver communicates with a root server, these servers know about the top level domains (such as .org and .jp).
- The root server communicates with a top level domain (TLD) server. These servers store information about the second level domains (nytimes.com). The TLD server provides the IP address of the name server for the domain.
- Having found the name server of the domain the recursive resolver sends a request to the name server which returns the IP address of the domain server.
- If the recursive resolver knows the IP address of the domain server it returns that information to the browser.
- The browser can now contact the domain server using the IP address it has been given and requests it to send its home page using the HTTP protocol.

Directory services

Directory services are used to identify and store details of the different resources on a network such as users, computer systems, services and applications. They map network addresses to network names to make it easier for users to find resources without having to know their IP address. A directory service is provided by a directory server on a network. The industry standard application protocol for accessing and maintaining directory services is Lightweight Directory Access Protocol (LDAP). DNS, as described above, is a type of directory service for website addresses. The directory service used by Microsoft Windows servers which keeps track of all users and computers in a Windows domain is called Active Directory. Apple produce an LDAP directory service for MacOS Server called Open Directory. There is also a free open source LDAP implementation which runs on a wide range of operating systems (including Windows, Linux, MacOS and Android) called open LDAP.

Authentication services

These are used to authenticate users within a network. Within a Windows network, users are authenticated by a server which has been set up as the domain controller. It uses Active Directory and the Kerberos authentication method described earlier.

Dynamic Host Configuration Protocol (DHCP)

Within a LAN, each device needs to have its own unique IP address from the IPv4 private IP address ranges. This address can be individually set by a network administrator, but this would require a record to be kept of which device has which IP address. It would cause complications in the situation where, for example, guest devices joined a WLAN and needed an IP address allocated. A much better solution is for IP addresses to be

dynamically allocated to devices as required. This is the purpose of DHCP, which allocates IP addresses to devices as required. Devices which issue IP addresses are called DHCP servers and can be a server computer or a device such as a broadband router. When a device is switched on, it broadcasts a DHCP message requesting an IP address. The request is received by the DHCP server and it responds with an IP address that the device can use. This IP address is selected from the DHCP server's list of available IP addresses, along with other information including the IP address of the default gateway and the correct subnet mask.

Routing

Routers use routing tables which are configured by the system manager to decide where to send each packet of data. In a very large network, such as the internet, there are many routers connected to each other and packets of data may pass through multiple routers (known as hops) on their journey from source IP to destination IP.

Remote access services

In some situations, it is useful to be able to remotely access the desktop of another computer. This is particularly useful with IT support services where a remote IT technician can use remote access to view and interact with a users' Windows, Mac or Linux desktop to investigate and correct a problem or make a configuration change for them. The Microsoft Windows feature that supports this functionality is called Remote Desktop. There are also third-party versions such as GoToMyPC which add additional features such as the ability to access Windows or Mac desktops from other systems such as iOS and Android.

Applications network services

- **File and print services**. Two of the most commonly shared resources on a network are files and printers. Using Microsoft Windows, folders containing files can be shared with network users from any computer (not necessarily a server). Access to shared folders can be controlled with shared folder permissions. Printers can also be shared so they are accessible to anyone on the network with the correct permissions.
- **Web, mail and communication services**. Large organisations often run their own web and e-mail servers. Internal web servers can provide an intranet.

Link

For more detail about shared folder permissions see page 18.

For more detail on internal web servers and intranets see page 24.

Assessment practice 11.2 BP.4, B.P5, B.M2, AB.D1

You work for an IT company and they wish to set up an 'IT Academy' to train staff and others in IT and networking. You have been asked to produce presentation slides with accompanying speakers' notes to cover the following topics:

- An explanation of different network types and components and how they can be secured.
- An explanation of how network infrastructure and resources can be impacted by cyber security.

An analysis of the security implications of different networked systems.

Plan

- Are you clear about what you need to do? Where will you get the information you need?

Do

- When explaining topics, make sure you include sufficient detail which goes beyond a basic description of the topic. With your analysis you need to think about both positive and negative aspects of security implications.

Review

- Check you have covered all the different network types and components listed in the specification.

C} Develop a cyber security protection plan for a specified organisation

Having looked at the many different cyber security threats that an organisation can face, and the protection methods it can use, you will next look at how a cyber security protection plan can be developed to meet the needs of a specific organisation.

Skills

Cognitive skills/cognitive processes and strategies:

- Analysis
- Critical thinking

Assessment of computer system vulnerabilities

There are a number of different tools and methods that can be used to assess the vulnerabilities in a company or organisation's computer systems.

Types of tools

Port scanner

Network ports allow a computer's various applications to communicate over a network. If a port is not required (i.e. the application using it is not installed) then the port should be closed, and this is normally managed by a firewall. However, a port scanner can check to see which ports are open and which are closed. There are a number of port scanner applications available on the internet. These allow you to scan a network either using its external IP address or scanning individual computers inside a LAN.

Registry checker

The Microsoft Windows registry is a database used by every installation of Windows to record all the many settings used by the operating system and applications. Some types of malware use the registry. Registry scanner or cleaner software can be used to test the integrity of the registry and correct any inconsistencies.

Website vulnerability scanners

These types of scanner software are used to check that the server hosting a website is properly protected. They can check for SQL injection and many other known website vulnerabilities. Many free website vulnerability scanners can be found online, although registration may be required.

Vulnerability detection and management software

This is a sophisticated type of security software that monitors a company or organisation's computer network and looks for vulnerabilities and attacks. Data collected by the software is analysed in a number of ways to attempt to identify threats and alert the systems managers to them. They also suggest appropriate actions. The software typically looks for misconfigurations across the network which could allow attackers to exploit vulnerabilities. An example of this type of software is Microsoft Defender Advanced Threat Protection (ATP).

Assessing user vulnerabilities

Users can be the cause of potential vulnerabilities. They need regular training to remind them of potential dangers, and checks (audits) may need to be done to check compliance. There are a range of ways that users can be vulnerable. Economic vulnerabilities could include blackmail or offers of money to provide information, such as passwords. Physical vulnerabilities could include noting down a password on paper or losing an ID card. Social vulnerabilities include providing security sensitive information to friends.

Third-party review

As in many disciplines it can be difficult to spot faults in a system or network you have designed or created yourself. A more effective approach is to ask an external third-party

expert to review the design of a system or network and comment on how well it is protected from security threats. This should ideally be done before the system is implemented, or goes live, so any issues identified can be resolved before this point.

Discussion

What kind of attacks can users be particularly vulnerable to?

Penetration testing

For this method of testing a system for security vulnerabilities, security experts attempt to compromise the system using a range of common attack methods. Penetration testing is sometimes called ethical hacking, since the tester uses the same techniques as a malicious hacker would use but with the intention of finding issues so they can be resolved. Penetration testing is normally carried out by third-party IT security experts who first plan out their tests in conjunction with the organisation before carrying them out. Tests are sometimes scenario-based, such as connecting an unauthorised device to the network. Tests are done to see if attacks are identified and what action is taken if they are. Once the testing is complete a detailed report is completed. Since threats change all the time it is important than a penetration test uses the attack method most common at the time of the test. The Open Web Application Security Project (OWASP) maintains an updated list of the current top ten web-based security risks based on actual attacks. The most common attack in the 2017 OWASP Top 10 report was injection type attacks like SQL-injection.

Pause point Check the OWASP web site and find out what is the most recent top ten list of attacks.

Hint Use a search engine to search for 'OWASP top ten'.

Extend For each attack type listed in the top ten, identify the kind of methods that an organisation would have to use to protect themselves from the attack.

Assessment of the risk severity for each threat

Risk is an important concept when considering a cyber security plan and you need to assess how severe each risk is. A threat by itself may or may not be something to worry about. As Figure 11.17 shows, risk severity can be seen as a combination of the likelihood of the threat occurring combined with the expected impact if it does occur (or the value of the loss in financial terms). This can be used to create a risk matrix based on the likelihood of the threat occurring.

Skills

Cognitive skills/cognitive processes and strategies:

- Analysis
- Critical thinking
- Problem solving

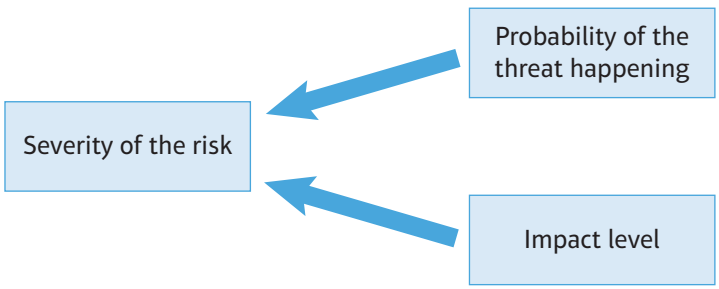


Figure 11.17 Assessing the severity of risk

Likelihood of the threat occurring

This is an approximate assessment of how likely the threat is to occur, divided into Very Likely, Likely and Unlikely. The likelihood of the attack can be assessed by considering two main factors:

The person or group carrying out the attack

What skill level is needed for the attack? What is the motive for the reward? What is the financial gain? What resources are needed? How large is this group? If the threat can be exploited only by developers or system administrators inside the company, the group is small. If, however, the threat can be exploited by anyone on the internet, then the group is large. For example, if a threat does not require a great deal of skill, the motive is financial reward, no special equipment is required and it can be carried out by any authenticated user on the system (a medium-size group) then the likelihood is Very Likely. On the other hand, if the threat requires a high degree of skill, there is no financial gain, it requires a complex setup or resources and can only be exploited by system administrators then it is Unlikely.

The threat itself

How easy is it to exploit? How well known is it? How likely is it to be detected? For example, some security vulnerabilities have automated hacker tools available online, making them easy to exploit. This makes them Very Likely to occur.

The impact of the threat occurring

There are two types of impact to consider, the technical impact and the business impact. They are related to each other.

- **Technical impact** including how much confidential data is lost, corrupted or destroyed. Has availability of the service been impacted?
- **Business impact** such as the amount of financial loss, likely reputation damage and how much personal data is lost.

Table 11.6 shows an example of a risk matrix.

Table 11.6 An example of a risk matrix

Probability of occurrence	The impact of the threat		
	Minor	Moderate	Major
Very likely	Medium	High	Extreme
Likely	Low	Medium	High
Unlikely	Low	Low	Medium

This risk matrix can be used to help you assess the risks in a given system.

When should risk assessments be carried out?

Risk assessment should initially be done during the design or planning stage of the system. This is because the review process allows you to check that the system is built in a way that provides sufficient protection, particularly from those risks which have higher severity ratings. Once the system is running, the risk assessment should be done again at regular intervals (for example, yearly) as a form of **audit**. This is needed because threats change and new threats are developed all the time. Also the system itself may develop and change, for example with the introduction of new software or new versions of existing software.

Risk assessment method

The steps for carrying out a risk assessment are shown in Figure 11.18.

The end result should be a list of threats, each with a severity rating. This provides a prioritised list of issues to deal with. Protection methods for the threats with extreme

Research

Risk rating is very often done using the method described by the Open Web Application Security Project (OWASP). Research what the methodology involves, starting here: https://owasp.org (Risk rating methodology)

Key term

Audit – a periodical assessment of finances, resources or efficiency of a system.

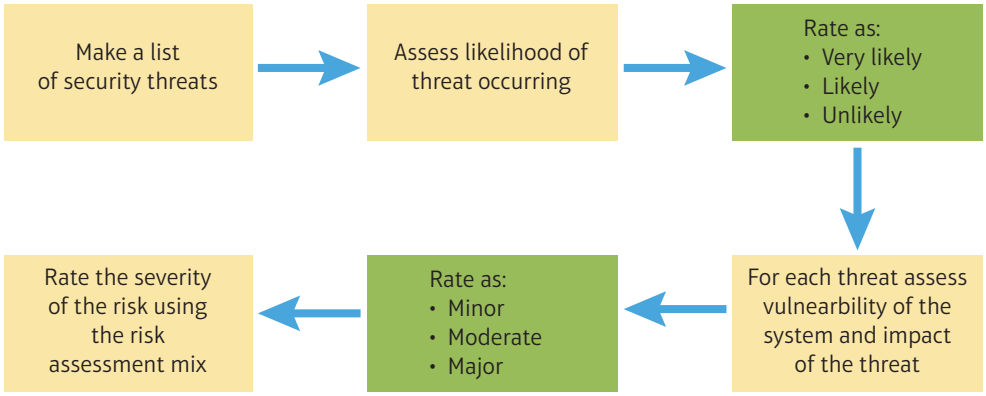


Figure 11.18 Steps in a risk assessment

severity need to be addressed first and any cost associated with the protection methods can be justified in terms of the severity.

A cyber security plan for a system

Having completed a cyber security risk rating to help you prioritise protection methods, the next step is to develop a detailed plan to implement the protection. It may be that the plan has to be approved by the organisation's management. Since it is likely to cost money, they need to know that the expense involved is justified.

The plan needs to list the protection methods that will be applied for all the risks in the extreme, high and medium severity categories. Protection methods would include:

- **hardware** – such as firewalls, routers and wireless access points
- **software** – such as anti-malware, firewall, port scanning, access rights and information availability
- **physical** – such as locks, CCTV, alarms, data storage and backups.

Alternative risk management strategies

Rather than protecting against a threat, another option is to transfer the risk to someone else, for example, a third-party contractor acting as a service provider. This is what happens when an organisation uses cloud services. The responsibility for the risks associated with the services is passed on to the cloud service provider. Other possibilities include:

- stopping some activities because it is considered too risky (for example banning the use of USB memory sticks) or the cost of protection methods is too high
- accepting the risk as might be done with low severity risks.

Justification of protection methods

Each planned method of protection should include a justification of why the method is required and how it will protect the system. This should not be highly technical as the main audience for the plan is likely to be senior managers who may not be technical experts. The important thing is that for each protection method proposed, its use is justified in terms of the threat or threats that it protects against.

Constraints

Each protection method should have its technical and financial constraints listed. Technical constraints include any impact on the configuration and efficiency of the existing hardware and software systems. They also include any limitations of the

Theory into practice

Carry out a basic risk assessment on a computer you use or own such as a laptop. List four or five security threats to the laptop (such as it being lost or stolen, a ransomware attack, etc.) then for each threat make an estimate of how likely it is (for example the theft or loss of a laptop is very likely using the criteria described above). Think about the impact of that threat on you (for example if your laptop was stolen you might lose all your school/college work) and come up with a risk severity for each threat you have listed.

Skills

Cognitive skills/cognitive processes and strategies:

- Decision making
- Critical thinking
- Analysis

Link

For more on legal responsibilities see **Unit 2: Creating Systems to Manage Information**.

protection methods such as types of attack that it might not protect against or updates that are needed to maintain the protection level over time. Financial constraints include an estimate of the cost of implementing the protection method.

Legal responsibilities

This part of the plan should point out the organisation's legal responsibilities under data protection legislation.

Usability

Some types of protection methods can have a negative impact on the usability of the system. For example, very strict password policies with requirements for long complex passwords which must be changed often, while very secure, can be very difficult for users. Also, they may encourage unsafe practices such as writing passwords down. A strict password policy also increases IT support costs by increasing the number of calls to the support department due to forgotten passwords. These usability issues may be used as a justification for spending more money to implement the protection policy. However, it is easier to use authentication methods such as two-factor authentication.

Case study

Typically, standard authentication systems use a single factor, a password. This is something the user knows but no one else does. Two-factor authentication (2FA) requires the user to enter two authentication factors. This provides a higher level of security because a password alone is not sufficient to access the system. The second factor can be a number of different things. For example:

Something the user knows – such as a PIN.

Something the user has in their possession – such as an ID card, a mobile phone or a security token.

Something personal – known as a biometric factor such as a fingerprint, facial or voice recognition (sometimes called the inherence factor).

Withdrawing money from your bank account using an ATM is an example of two-factor authentication, as you must know the PIN and have the bank card in your possession.

Another example commonly used by banks to authenticate certain types of transactions is to send a code in an SMS text message to a registered mobile number. The bank account holder must register their mobile number before this method can be used.

Some organisations issue employees with security tokens or use a mobile app which generates single use passwords (sometimes called one-time passwords (OTP)) which can only be used once and are entered along with the user's password to log on to the organisation's systems.

Check your knowledge

1 Why isn't 2FA used more widely when logging into online accounts?
2 What sort of hacking methods are 2FA vulnerable to?

Cost-benefit

The manager to whom the plan will be presented will want to know what they will get for the money that will need to be spent. The costs should be fairly clear from the hardware and software required but the benefits may be difficult to quantify as they mainly relate to risk reduction. Reference will need to be made to the impact assessment of the various risks.

Test plan

Included in the security plan should be a test plan. This will define how each protection method will be tested to ensure it is working properly. A test plan is normally presented as a table, as shown below. Some of the tests have already been included in the plan.

Table 11.7 An example of a test plan

Test scenario: Testing password policy settings when creating a new password				
Test no.	**Test description**	**Expected result**	**Actual result**	**Actions**
1	Password = "welcome"	Rejected (short)		
2	Password = "mypassword"	Rejected (not complex)		
3	Password = "Gfh12nB?"	Accepted		
4				

Note that the actual result and the actions are only completed when the testing is actually done.

Once the plan is approved and the agreed protection methods implemented the test plan is used to carry out actual tests on the protected system.

Internal policies

Most organisations, especially larger ones, have a number of written policies and procedures which define what the company and employees can and can't do, and how various tasks should be done. Policies and procedures relating to cyber security should be included to make sure employees are aware of their responsibilities in this area.

Requirements for a cyber security policy

The International Standards Organization (ISO) has created a standard for information security management systems known as ISO 27001. This includes the requirement that an organisation should have an information security policy. ISO 27001 requires that the policy is subject to a method of continuous improvement such as the **Plan-Do-Check-Act (PDCA) loop**. The steps in a PDCA approach are:

- **Plan** – before you make any changes, you need to identify what you are trying to improve and how you will measure the improvement. For example, you might want to change the password policy rules. Any improvement will be measured in a reduction in the number of passwords related calls to the IT department.
- **Do** – implement the change.
- **Check** – use the metric defined at the plan stage to check to see if the expected improvement has occurred.
- **Act** – if the outcome of the checking stage is that the change is successful, and you have seen the improvement you defined at the planning stage then the change becomes permanent.

PDCA is a continuous loop, so once the act stage is reached further improvements to the policy should be in the stage of plan.

In many organisations there may be several different policies which relate to cyber security. These can include the following:

- **Internet usage policy**. This policy defines what employees may use the internet for while connected to the company LAN. It will also list various types of inappropriate site employees must not visit. It may also define rules for downloading files.

Skills

Cognitive processes and strategies:

- Analysis
- Interpretation

Key term

Plan-Do-Check-Act (PDCA) loop – a repetitive four-stage model used for continuous improvements in a process or system.

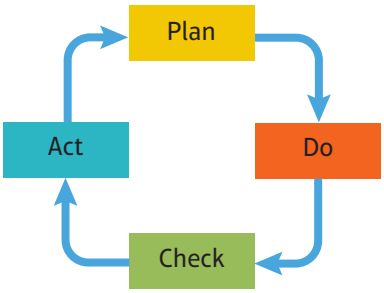


Figure 11.19 A PDCA loop

Discussion

Why is it important to a business that staff are given training about the company's email and internet policies? What is the best way to deliver this training? Are you aware of these policies in your school or college? Did you receive any training about them, perhaps at the start of the course?

- **Email usage policy**. This policy states rules for email etiquette when using the company email such as content should be professional, polite and respectful. It also outlines rules for the use of company email for personal messages. Finally, it covers guidance about dealing with email attachments, links and spotting phishing emails.
- **Password and security procedures policy**. This policy defines the password requirements, including length, complexity, how often they should be changed, etc. It also includes rules about keeping passwords safe such as not sharing them and not writing them down, and may also include other security procedures such as use of biometric or two-factor authentication. This or other policies may also define rules for various physical security measures that are in use.
- **Staff training**. It is important staff are made aware of the content of the company IT security policies. This would usually start with a training session as part of their induction or onboarding when they start with the company. Training should be updated regularly, probably annually or whenever there is a change in security procedures, new issues are identified or there is a security breach.
- **Audits**. One issue with written policies and procedures is that they can easily be filed away and forgotten. To ensure continued compliance over time audits are needed. Some polices such as a password policy can be enforced by the operating system but other polices may need manually checking from time to time.

Pause point What are your school/college's internet usage policy and email policy? Does your school or college have a password policy? Are there any other security procedures you are required to follow such as wearing student ID badges? These should have been explained to you at your course induction.

Hint These policies should be on your school or college website or in your student handbook.

Extend Take a close look at one of the policies and discuss with a fellow student what the rules are for. Could anything be added or explained in more detail?

Key terms

Full backup – a complete backup of all files on a hard drive.

Incremental backup – a backup of all changed files since the last full backup.

- **Data protection policy**. This is required to ensure the organisation complies with data protection legislation. The procedures listed in the policy for dealing with personal data must align with the requirements in the relevant legislation.
- **Backup policy**. Backup is an essential part of an organisation's defence against data loss and therefore a clear policy is needed to define the data for backup and the method for backup. A **full backup** includes all the organisation's data. Although a full backup must be done sometimes, since a large proportion of data does not change very often, a full backup is wasteful and so regular incremental backups are usually done. An **incremental backup** just backs up the data that has changed since the last backup, and so can be done more quickly than a full backup as shown in Figure 11.20. Typically, an organisation might do a full backup on a weekend and an incremental backup each weekday. The only issue with this approach is, for example, a situation where a failure occurs on a Thursday. To restore all of the data, the weekend's full backup needs to be restored and then all the daily incremental backups from Monday through to Wednesday.

How often an organisation needs to back up its data will depend on how much data it can afford to lose. With the daily backup regime described above the organisation must be willing to lose at most one day's worth of data. In some organisations, such as a bank, this would not be acceptable. Finally, the policy needs to describe where the backups will be stored. As mentioned earlier, storing backups at the same site as the data is not acceptable as, in the case of a serious event such as a fire, both the original data and the backup could be lost.

Day	Weekend	Monday	Tuesday	Wednesday	Thursday	Friday
Amount of data backed up						
Description	Full back up of all files	Back up just files changed on Monday	Back up just files changed on Tuesday	Back up just files changed on Wednesday	Back up just files changed on Thursday	

Should a failure occur on Friday, then all the backups since the weekend need to be restored to recover all the data.

Figure 11.20 Incremental backup

Incident response policy

When a cyber security incident occurs in an organisation there is naturally a degree of anxiety and urgent action Is required. Having a response policy in place before the incident occurs helps to ensure that correct procedures can be carried out in a prompt and efficient manner to prevent further damage to the systems and preserve evidence of what happened. The incident policy should include the following:

- **The response team**. When an incident is identified, a Computer Security Incident Response Team (CSIRT) is immediately assembled to deal with the incident. Within the team there are different roles:
  - Team leader: a senior member of staff who can liaise with the company directors and keep them updated on the incident.
  - Incident lead or manager: takes the lead on the detailed technical response and investigation, usually a member of the company IT staff, often the IT manager.
  - Associate members: members of the company IT team with the required technical skills.
- **Reporting procedures**. This section of the policy should define what type of incidents should be regarded as computer security related and how staff should report an incident if they discover one. This section also defines who they should report it to.
- **Initial assessment**. This defines the actions taken immediately after the incident is reported. The first step is to check if the report is a genuine security incident or if it is a '**false positive**'.

Once a genuine incident has been confirmed then the type of attack and its severity (for example, how many systems are affected, in what way they are affected, etc.) is identified.

Communicating the incident

Following confirmation of the incident, the fact that it has occurred needs to be communicated to the CSIRT who need to start work on their response. The company directors should also be notified that the incident has occurred.

Key term

False positive – occurs when a system reports an issue incorrectly, such as anti-virus software reporting suspicious activity which is in fact harmless.

CSIRT procedures

The policy should outline the procedures the CSIRT need to follow for various types of incident, including theft of equipment, theft of company data, malware infection, unauthorised access to company systems, and damage or loss to systems by physical incidents such as fire or flood. Procedures are likely to include the following:

- **Protecting people's safety**. In the case of fire or flood the company evacuation procedures should be followed. If the systems involved are safety critical such as hospital medical systems or air traffic control, then the safety of patients or passengers is a major consideration. However, safety critical systems are often protected by different, more complex arrangements than business systems.
- **Containing damage and minimising further risk**. Depending on the type of incident, systems may need to be shut down, network access disabled, user accounts disabled and passwords changed.
- **Protecting data**. The policy should define the procedures to be followed for protecting data, for example by taking disk drives offline, including priority in terms of ensuring the most sensitive and valuable data is protected first.
- **Protecting hardware and software**. If a physical incident occurs and it is safe to do so, computer hardware and the software on it can be protected by disconnecting it and moving it to a safe location.
- **Minimising disruption**. Once the affected systems have been identified and isolated, other systems may not have been affected but may have had the services they provide interrupted. As a precaution, they should be brought back online to minimise disruption to the company.
- **Identifying the incident**. Although the nature of the incident will have been identified early on, further detailed investigation will be required to identify the precise nature of an attack, what the intention of the attack was (for example, theft of data for financial gain, encryption of data for ransom, etc.) the origin of the attack (for example, if it was internal or external), how it gained access to the systems and which files have been compromised.
- **Protecting evidence**. To support the forensic investigation of the incident, all relevant data should be preserved, which may include creating disk image backups of entire disks including data and operating systems to preserve configuration settings and any files that might have been used in the incident.
- **Notifying external agencies**. Depending on the type of incident there are a variety of external agencies that might need to be contacted. If equipment or data has been stolen, then contacting the law enforcement agency (police) may be appropriate. If personal data has been lost the organisation themselves may face prosecution under data protection legislation. This means that legal representation and advice may be needed. If there is a complex security issue or malware infection the company may need to enlist the help of external security and malware experts.
- **Recovery of systems**. Once the incident has been fully dealt with and all the required evidence has been collected and preserved, the affected systems need to be restored, using backups if necessary.

Following the incident

Once the urgent actions of protecting and restoring the systems have been completed, there are some other important tasks which need to be completed and should be included in the policy document.

Incident documentation

Reports should be written up on the incident in a much detail as possible. The documentation should include details of the incident, what the CSIRT did, and all the

actions taken to identify and resolve the incident. Details of the incident are particularly important as they may be needed to prosecute the people who carried out the attack, so it is important it is accurate, detailed and backed up by evidence such as files, logs, etc.

Evidence collection

Evidence should be collected in case it is needed for legal reasons.

Review outcomes

Another very important part of the incident policy is that it requires a review after the incident. This can help ensure that another similar incident does not occur again and that lessons are learnt. The review should make recommendations for preventing further incidents such as changing security procedures, added additional security and improving staff training.

Disaster recovery plan

A disaster recovery plan shares some features with a security incident policy. However, its purpose is slightly different in that it is created in preparation for a physical disaster which destroys or disables an organisation's computer systems, such as a fire or flood.

The disaster recovery plan should identify critical systems. Not all the systems in a company are critical to its everyday operation. Critical systems are likely to be server computers that are used to run the company business. Just how critical they are to the business can be defined by deciding on how quickly you would need systems to be up and running again after a disaster.

- **Recovery time objective (RTO)** is a term used in disaster recovery to define the amount of time a business can be without a service following a disaster.
- **Recovery point objective (RPO)** is the amount of data (usually in terms of transactions) that can be lost if a disaster occurs. This is the amount of time since the last backup. All new transaction records created between the last backup and the disaster are lost.

Figure 11.21 shows recovery objectives.

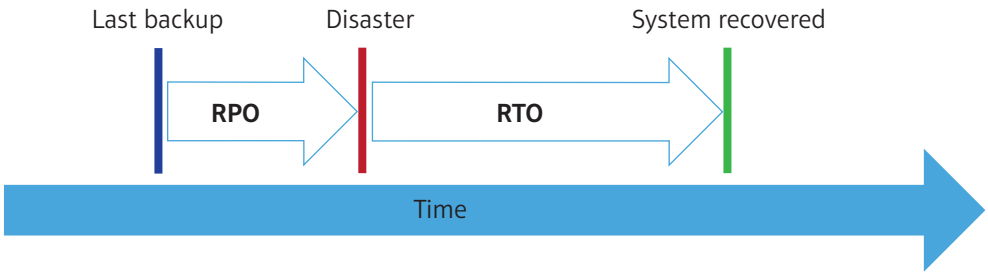


Figure 11.21 Recovery time objective (RTO) and recovery point objective (RPO)

The disaster recovery plan should also include prevention, response, and recovery strategies. For each critical system the disaster recovery plan will need to state the following:

- Who is responsible for managing and implementing the recovery of the system.
- How the recovery will be achieved. Typically, disaster recovery involves setting up a duplicate system to the one that has been destroyed in a different location. There are a number of companies which offer disaster recovery service and for a fee a company can set up their software on the systems they have in their datacentres should a disaster occur. Very large companies may have an alternative site available within the company that can be used in the case of a disaster.

- Where backups will be stored and in what format (for example, tapes, external hard drives, online backup). As well as data backups, full backups of the latest system will be needed with all the applications and associated software installed so the complete system can be installed at the alternative site.
- How the network will be connected to the alternate systems. This will usually be via the internet and disaster recovery companies will have higher speed internet connections available for use.
- Where any necessary additional equipment will be obtained (purchased or rented), how additional people such as contractors to help set the system up, and where they will be sourced from.

Each critical system will need to have detailed procedures which describe how the recovery will be done.

Research

Carry out some research into ISO 27031 to find out more about it and what should be included in an IT security plan.

The International Standards Organization (ISO) have a standard for IT security, known as ISO 27031 (the previous standard was ISO 24762), which includes a section on disaster recovery planning. The sections included within the plan:

- **Introduction** – the objectives of the plan.
- **Roles and responsibilities** – who does what when a disaster strikes. The plan should include an organisation chart and job descriptions of each of the members of the disaster plan team.
- **Incident response procedures** – listing all the hardware, software and network facilities included in the disaster plan.
- **How to activate the plan** – procedures for initiating the processes defined within the plan.
- **Procedures** – recovery strategies for each critical system.

Link

For more on PDCA see page 47.

ISO encourage a PDCA approach to the disaster plan.

Skills

Cognitive skills/cognitive processes and strategies:

- Analysis

External service providers

As discussed previously, one option to avoid some of the issues associated with cyber security and disaster recovery is to use an external agency (called an External Service Provider (ESP)) to provide an organisation's computing service. However, using an external agency is not without its issues. An agreement would need to be drawn up with the provider to ensure the organisation's interests are protected. The agreement between the organisation and the ESP will cover:

- **cloud services** – such as cloud backup and storage
- **hardware** – services such as Amazon Web Services and Microsoft Azure provide cloud-based hardware that organisations can run their applications on
- **software** – ESPs generally provide software to support the running of the organisation's applications. For example, a web hosting company will typically provide Apache web service, MySQL database and PHP programming language along with other software services.

Implications of ESP agreements

There are various implications of ESP agreements.

Legal ownership and jurisdiction

Firstly, you need to consider who owns the data on the ESP's computers. As the data may reside in a different country than the organisation operates in, it is important which country's laws apply. Data Protection legislation, for example, states that data should not be transferred to a country which does not have appropriate data protection legislation. There also needs to be agreement on what procedures should be followed when the

agreement ends. For example, will all the organisation's data be returned and deleted off the ESP's systems?

Security protection

The organisation needs to be sure the ESP is aware of its responsibility to keep their data secure and private using appropriate methods including encryption. The agreement between the ESP and the organisation needs to make it clear who is responsible for any data breaches and the legal liability that the ESP will have for loss or damage to data, whether it is deliberate or accidental. For example, will the EPS compensate the organisation if data is lost?

Dispute resolution

The agreement needs to include a way for disputes between the ESP and the organisation to be resolved. This must include legal (statutory) requirements and any problems that occur due to the data residing in the jurisdiction of several different countries.

Under data protection legislation in the EU, an organisation who uses cloud storage for personal data is defined as the 'data controller', in other words they are responsible for how the data is handled even if they don't have full control over it because it is stored on the cloud by the ESP. Therefore, the organisation must ensure that the ESP takes their data protection responsibilities seriously and a written agreement is in place with the ESP to keep the data secure.

Discussion

Discuss the benefits and drawbacks of using an ESP for an organisation.

Assessment practice 11.3 C.P6, C.P7, C.M3, CD.D2

Select an organisation you know fairly well. It can be a college or school you attend or have attended or a local business.

- Carry out a risk assessment of the threats and vulnerabilities that can impact on the organisation.
- Based on the risk assessment, write a cyber security plan for the organisation, including the proposed protection methods for all the extreme, high and medium severity risks.
- For each protection method you have chosen for the organisations systems, justify its choice in terms of its ability to defend the systems.
- Write an evaluation of the cyber security plan you have produced for the organisation, and include in your evaluation how the plan would impact on the organisation's internal security-related polices and also how it would impact on any external service providers the organisation uses.

Plan

- Which organisation will you select to carry out the risk assessment?
- How will you collect information about the organisation you have selected?
- Make a time plan listing all the tasks you need to do in order to complete the assignment and include how long each task will take. Make sure you will complete the assignment by the deadline date.

Do

- When justifying your protection methods make sure you say why you chose the method, not just what the method is or how it works. You need to explain **how** it will protect the system.
- When writing the evaluation, you need to discuss the benefits and drawbacks of your plan and draw some conclusions about how it might be improved or developed further.

Review

- Did you stick to your time plan? If not, which tasks took longer than you planned? How will you create a more accurate time plan next time?
- Have you proofread your assignment to correct any errors, such as typing mistakes, spelling or grammar errors?

D Examine procedures to collect forensic evidence following a security incident

As already discussed, when a security incident occurs it is important that evidence of what happened is collected properly.

Skills

Cognitive skills/cognitive processes and strategies:

- Analysis
- Problem solving
- Decision making

Forensic collection of evidence

Evidence of a security incident is required for two main reasons. Firstly, it might be needed to support the prosecution of those involved. Secondly, fully understanding exactly what happened will help to make it less likely that it will happen again.

Desktop forensics

This involves collecting evidence from the files that exist on a computer that has suffered a security breach. The computer would first be isolated and removed, or in the case of an individual laptop computer, confiscated from the individual. Several techniques can then be applied:

- **Taking an image** – this is a low-level copy of the entire disk. This is known as a forensic duplicate. The original disk is placed in secure storage. This is done to provide proof that the investigation process has not changed anything on the disk.
- **Analysis of the data** – this can be done using a number of tools, which can, among other things, recover deleted files. Searches may also be done across all the files on the disk for a particular relevant phrase or to filter out certain file types which are not relevant. For example, if the computer is believed to have been involved in a SQL injection attack, a search could be done for various relevant SQL commands.
- **Files and settings** – investigation is done into the configuration settings on the computer. For example, checks might be done on when the most recent operating system updates were installed and when anti-virus software was last updated. Checks could also be done on what files have been downloaded and emails, including attachments that have been received and opened.
- **System logs** – operating system logs keep a lot of information about events on a computer. The Windows event logs keep time-stamped details of users, when they logged on and when unsuccessful login attempts occurred. System log analysis tools are also available.
- **User activity** – individual user activity can be traced in a number of ways. The time the user logged on and off can be identified from the system logs. Files they have created and deleted can be identified, including files downloaded from the internet. Their email and web browsing history can also be viewed.
- **Malware analysis** – anti-virus programs keep logs on when the user carried out scans for malware and when the latest virus definition files were downloaded.

Pause point You are investigating a security incident which involved unauthorised access to a system. When looking in the event log at user logins, what sort of information would you be looking for? What could a lot of unsuccessful login attempts tell you?

Hint Event entries in the log are time-stamped.

Extend Apart from logon events what other evidence might you look for in a situation where unauthorised access to the system may have happened?

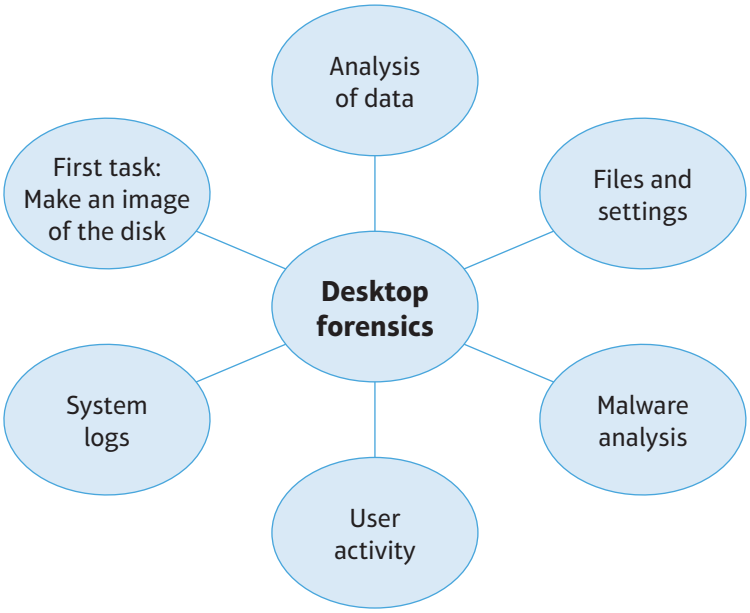


Figure 11.22 The stages of desktop forensics

Live forensics

Live forensics is the process of gathering information on a running computer. This may be necessary because once a computer is shut down the contents of the RAM memory are lost. For example, malware which is running in the computer's memory and which may contain important evidence (such as an IP address it is communicating with) can be lost if the computer is shut down. Also, many applications create temporary files while they are running (for example, Microsoft Word) which are deleted when the application closes. Many other important pieces of information such as encryption keys, chat messages, clipboard contents and open network connections are all lost from RAM when the computer is shut down. Live RAM capture software can be used to record the content of RAM for later analysis.

With a computer that has the disk drive encrypted using tools like BitLocker, data cannot be read (because it is encrypted) unless an authorised user is logged on.

Network forensics

The organisation's network is a likely source of a security breach, with hackers finding a way into the LAN network from the internet. To investigate how the attack was achieved the network needs to be tested to identify the precise technique used. Before any testing takes place the network testing methodology to be used should be agreed with the forensic team supervising and investigating the incident to ensure it is appropriate and permission has been granted to carry out the tests. This is important because the tests are likely to simulate an attack. It is also important that the test does not disrupt a live system. For example, testing a live system by simulating a DoS attack is not a good idea as it may prevent the live system from working. Data about the testing can be collected using both passive tools (collecting evidence by observing what happens) and active tools (actively making changes and collecting the results).

The various infrastructure devices on the network can also be investigated and analysed. Firewalls are commonly configured to create logs of the connections they accept and reject, and routers may also collect logs of activity. The settings on devices such as switches and wireless access points can also be reviewed and the logs of anti-malware

Discussion

What kind of information might you find in a firewall or router log and how might it help you find out more about a security incident?

applications will show any suspicious files that were identified. Some wireless access points will keep a log of devices attached and will also have a list of allowed MAC addresses if MAC address filtering is enabled.

Skills

Cognitive skills/cognitive processes and strategies:

- Analysis
- Problem solving
- Interpretation

Systematic forensic analysis of a suspect system

To be able to use forensic evidence in the prosecution of people involved in an attack, the evidence must be collected in a careful systematic way with every step recorded in a detailed report.

Details of the incident should be noted down as soon as possible after they occur, to avoid the possibility that things are forgotten. The CSIRT team need to take lots of notes (which can be written or audio recorded) on everything they do to be written up in their report at a later date.

As much evidence in terms of system snapshots, such as screengrabs, copies of logs and files should be collected as possible. Again, this should be done as soon as possible and retained for later analysis.

If the investigations into the incident have caused any changes to the system, either intentionally as part of the investigation process or accidentally, this should also be carefully noted.

Depending on the nature of the incident, visual evidence such as photographs and videos can be created.

It is important to check that the evidence does relate to the actual incident that has occurred and is not a false positive. This can be done in a number of ways, for example checking timings to see if the evidence is related to when the attack took place. In the initial stages of the investigation you might collect evidence which you are not sure relates to the incident, but it is best to collect it and then carry out a detailed analysis later to check if it relates or not.

Evidence evaluation

Once all the evidence has been collected, each item should be evaluated.

- Does it actually provide evidence of the crime or incident?
- Does it show how the system has been compromised from outside (external) or inside the organisation (internal)?
- Does it show that the attack was done in one particular way rather than other possibilities?

As part of the evaluation of the evidence, the report needs to explain what it shows and provide a detailed step-by-step description of how the attack was carried out.

Pause point Someone has broken into the server room and one of the removable disk drives from a server computer has been stolen. What kind of evidence would you collect of this incident?

Hint What kind of physical security measures might be relevant in this kind of incident?

Extend What does the organisation need to do to recover the system in a situation like this?

Recommendations

As mentioned earlier it is important that the report on the incident makes recommendations to help avoid similar issues in the future. These can include:

- **changes to policies and procedures** such as the internet usage policy and also, agreements with external organisations such as cloud service providers might need to be changed

- **staff training** to ensure they understand and are adhering to the requirement of the company policies which relate to IT security
- **additional protection methods** including physical, software and hardware protection methods.

Assessment practice 11.4 D.P8, D.M4, CD.D2

You are working in the IT department of an organisation and have been asked to prepare a guide to forensic procedures in case there is a security incident. Your guide needs to include:

- An explanation of the forensic procedures that can be used to collect evidence following a security incident.
- An analysis of how all the different forensic procedures listed above can be implemented on a system which is suspected of being attacked in a security incident.

Plan

- Make a checklist of all the forensic procedures you will cover.
- Carry out research to find out as much as you can about each procedure.

Do

- When writing your explanation of the forensic procedures be sure to include as much detail as you can.
- Remember you cannot copy and paste directly from books or websites, you need to rewrite the information in your own words.
- When writing your analysis of how the procedures can be implemented remember to include advantages and any possible disadvantages and also to consider different types of security incident.

Review

- How have your assignment writing skills (research, planning, writing, reviewing, time management, etc.) improved? What areas still need work?
- How could you have improved the work you did on this assignment?
- How will you approach your live assessment differently?

Further reading and resources

Books

Dulaney, E and Easttom, C. *CompTIA Security+ Study Guide: Exam SY0-501*, 7th Edition, Sybex (2017).

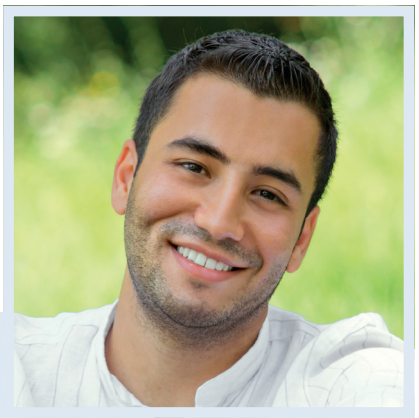
Scott, R. *Computer Networking Beginners Guide*, independently published (2019).

Cisco Networking Academy. *Introduction to Networks V6*, Cisco Press (2016).

Websites

- https://owasp.org
- https://uk.norton.com (Internet security)
- www.mcafee.com (Threat center)

THINK FUTURE



Imran Hussain
IT technician

After school Imran managed to obtain an apprenticeship in a medium-size business working in the IT support department. Although he was aware that security is a big issue, he was quite surprised at the amount of helpdesk requests that he received that were related to security. Security issues create a lot of headaches for users in all sorts of ways. The IT support department have to do a lot of password resets because users have forgotten their passwords which is frustrating for both the technicians and users, but the company policy is that users must change passwords every three months. Some users feel like the IT staff are making life difficult for them but the important thing for the IT support department is protecting sensitive data and the company systems. After six months Imran moved off first line support which means no more password resets, but he then had to deal with much more complex and technical issues. One thing that he feels that he has learnt is that many security issues such as firewall configuration and setting folder permissions are very complex and unless you know what you are doing you can cause a lot of problems. He has learnt a lot but there is still a lot more to learn. The management at the business Imran works for are very concerned about IT security issues and regularly remind the IT staff that new, more sophisticated threats are likely to appear in the future as the situation is only going to get worse and the IT staff need to be constantly on their guard.

Focusing your skills

Planning to work in IT

Security is likely to be an issue in whatever IT role you have in mind for the future. If you are planning to work in technical roles such as programming or web development, or as an IT technician, then your understanding of IT security needs to go beyond the 'user' aspects of security, such as strong passwords and anti-malware measures. If you are working in web or software development security, then it is a particularly important issue because you need to understand how to build security into the products that you are developing.

- As IT security is such a dynamic area, you need to keep up to date with the latest security issues. Following technology blogs is one way of doing this. There are many different technology blogs – some of the best known are Techdirt, Guardian Technology, Techworld and Krebs on Security.
- Do your own research into security issues and aim to develop an in-depth technical understanding of how some of the common threats, such as SQL injection, work. There is plenty of information on all the common threats available on the internet.
- If you are able to obtain it, work experience (or shadowing) has many benefits and will provide very useful experience that is difficult to obtain in any other way. It will help you to understand security issues from both the user's and the technician's perspective. As Imran has found in his work as an apprentice IT technician, users can often find security issues very frustrating, so you need to develop the interpersonal skills required to deal with users who may be upset and angry.

Glossary of key terms

Audit – a periodical assessment of finances, resources or efficiency of a system.

Brute force attack – an attack in which an attacker submits all possible passwords or PINs until the correct one is found. The longer the password or PIN, the longer a brute force attack is likely to take.

Certificate Authority – a certificate authority (CA) is an organisation which issues digital certificates

Cyberattack – a malicious attempt to disable computers, steal data or use a computer to launch an attack in another way.

Cyber security – the protection of computer hardware and software (including mobile devices such as smartphones) and the data they store from the threat of damage, disclosure, disruption or loss. It is also known as computer or information technology security.

Digital Certificate – a secure website (using the HTTPS protocol) must apply for a digital certificate from a certificate authority to prove it is a genuine site.

Encryption – a process of encoding data so it cannot be read by anyone but the person it is intended for. Typically, data is encrypted using a key, which is also required to decrypt the data.

Ethernet – a set of technology standards developed in the 1980s that define a way for computers to talk to each other both in wired and wireless networks.

False positive – occurs when a system reports an issue incorrectly, such as anti-virus software reporting suspicious activity which is in fact harmless.

Firewall – a software or hardware device which filters incoming and outgoing data between a local area network and the internet with the aim of blocking unauthorised or malicious access.

Full backup – a complete backup of all files on a hard drive.

Hacker – someone who attempts to gain unauthorised access to a computer system using a variety of different methods

Hexadecimal – a base 16 number system. It is represented by the numbers 0 to 9 and the letters A to F.

Incremental backup – a backup of all changed files since the last full backup.

Intellectual property – 'property' that is a result of creativity such as inventions, written work (books), artistic work (works of art), musical work, symbols, names and images.

Internet of Things (IoT) – a general term referring to the technology which allows everyday devices (such as a video camera, heating thermostat or lights) to have computing devices embedded in them allowing them to send and receive data over the internet.

IP address – a numerical address that uniquely identifies a computer on a network.

Malware – software which has a malicious (bad) intention and may cause damage to your computer software or data or collect information about you.

Near Field Communication (NFC) – a wireless communication method used by services such as Apple Pay and contactless card payments. Two devices (such as a debit card and a card reader) need to be brought very close to each other (within a few centimetres) and are then able to transfer small amounts of data.

Offline attack – when an attacker steals a computer or hard drive and either attaches the hard drive to a different computer or boots the computer from a different operating system (e.g. Linux on a USB memory stick). These methods bypass the normal Windows security features.

Open source – a type of computer software in which the source code is available for users to view and modify if they wish. This contrasts with software where the source code is not available, which is called proprietary software.

Packet – a unit of data made into a small 'package' or 'packet' that travels along a network path.

Plan-Do-Check-Act (PDCA) loop – a repetitive four-stage model used for continuous improvements in a process or system.

Port – in the context of firewalls a network port is a software feature which allows different applications which are communicating on a network to be identified.

Port number – a communication end point.

Protocol – a network protocol is a set of rules which govern how a particular type of communication is done over a network.

Structured Query Language (SQL) – the command language used to extract data from a database.

System vulnerability – a weakness in an operating system or other software which can be exploited by an attacker.

Tunnelling protocol – a network protocol that creates a private network within the internet by encapsulating the data to be sent and encrypting it, before inserting it in standard data packets. The protocol also authenticates the users of the connection and negotiates the encryption keys to be used to encrypt and decrypt the data sent.

Unauthorised access – access to computer systems and the data they store by people who are not permitted access to those systems and data.

Untrustworthy websites –malicious websites that invite you to download damaging software onto your computer or seek to gain information from you by deception.

Virtual computer – a software emulation of the hardware of a computer which allows a separate copy of an operating system and associated applications to be hosted on an existing physical computer hardware. This would allow a single physical computer to host a number of different virtual computers potentially running different operating systems and applications.