WJEC A2 DIGITAL TECHNOLOGY

A Complete Course Guide for Theory

Unit 3: Connected Systems

Covers the full WJEC A2 Level Digital Technology specification for Unit 3: Connected Systems

by Aiyan Hussain

Definitions are reproduced word-for-word from my own notes, cross-referenced against the WJEC specification.
26/08/2026

Contents

Right-click below and choose "Update field" (Word) or use Insert > Table of contents > Update (Google Docs, after pasting) to populate page numbers.

Introduction

A-Level Digital Technology is (as of the production of this document) still a very new course based on an ever-changing industry. I was disappointed when I realised how few resources there are to support students taking the A-Level. Sure, there are plenty of resources on the Internet that give thorough explanations of the concepts mentioned in the specification, but none of those are specific to the exam. That is what led me to produce this document, specifically tailored to the WJEC A-Level.

All definitions in this document will be in blue, with particularly important parts of the definition being in **bold**. Definitions provided in this document have either been taken directly from WJEC resources, or have been slightly modified for improvement of accuracy. I recommend you try to remember definitions word for word - you can use an SRS-based flashcard algorithm (such as with Anki) to help you remember it all.

If you do intend to use flashcards, I really recommend you physically type up the definitions into your cards rather than copying and pasting it, or using AI to produce a deck. Typing the words yourself gives you a moment to actually understand what you're reading/ typing, and also plants a seed in your brain for when you actually encounter the card while revising. It's better to clarify anything you don't understand before you need to revise the card rather than after.

Disclaimer: This document was produced solely by an undergraduate student and an AI assistant, so there may very well be overlooked errors. Feel free to report mistakes to ***contact@aiyanhussain.com****, or find me through my website aiyanhussain.com.*

Notes on the Exam itself

The exam is 2 hours and 30 minutes long, which – as with any other exam – will fly by.

Since the exam is taken on a computer, **your ability to type fast is your strongest weapon.** Chances are if you're taking this subject you're probably into computers anyway, so you might already have decent typing speed. You should start typing right away, and let your fingers move autonomously while your mind processes the question. There's no time to waste!

The questions asked in the exams aren't exactly orthodox: you can get questions worth 7 marks with strangely specific mark schemes, or very general 10 markers. The structure you want to take differs depending on the question. You don't need a specific explanation for a 'Describe' question, and you only need to list examples for an 'Identify' question. A good general structure may look like this:

Main Point → Example → Explanation → Impact

Example:
Explain **one** ethical constraint with smart devices in the built environment. [4]
"An ethical constraint with smart devices in the built environment can be privacy concerns with people being observed in public *(Main Point).* For example, including public surveillance cameras that are able to identify and store information about people passively, without them realising *(Example).* This means that people, despite potentially being aware that there are cameras, may not necessarily know what kind of data is being captured about them, which can raise privacy concerns for the general public *(Explanation).* This can cause controversy for the organisations using the cameras and handling the data, and may result in a negative perception of the use of smart devices in the built environment."

Always link the answer back to the question, even if it seems obnoxious. See what I did in the very last sentence? I basically name-dropped the question word-for-word. It has to be tailored to the question, or else the examiner might think it's not specific enough and mark you down.

Remember, there's nothing to lose with writing a little extra. They can't take marks from you, they can only give marks to you.

2.3.1 Contemporary Practices Involved in Collecting, Storing, Analysing and Using Data

Every digital technology you have studied so far ultimately exists to do one of four things with data: collect it, store it, analyse it, or use it to help someone (or something) make a decision. This topic pulls all four of those stages together into a single, detailed picture — from the moment a sensor or a form captures a raw fact, through to an artificial intelligence system using millions of those facts to draw a conclusion. It is a large, dense topic, and one of the most heavily examined in Unit 3, so expect to return to this section of the guide often.

(a) Collecting Data

All technologies in this modern, interconnected world have one thing in common: data. Computer systems are designed to store and process data, but data on its own is meaningless — it only becomes useful once it is placed into context. Consider the functionality of a *speed camera*. This device captures the different speeds that drivers are travelling on a road: car 1 – 30, car 2 – 40, car 3 – 35. It is only when we put this data into the context for which it was gathered — to catch any drivers exceeding a 30mph limit — that we can identify drivers 2 and 3 broke the speed limit and a fine can be issued.

> Data is a **set of recorded facts, numbers or events** that have **no initial meaning or structure**. Data itself isn't valuable, but the information that data reveals.
>
> The main purpose of data collection is to **gather information in a measured and systematic manner** to **ensure accuracy and facilitate data analysis**. Since the data collected is meant to provide content for data analysis, it must be high quality to be valuable.

Beyond catching speeding drivers, data can be gathered for a wide range of purposes, including to:

- increase productivity in the workplace;
- perform calculations;
- undertake scientific enquiry;
- gather sales reports;
- carry out decision-making;
- provide warnings when a trigger point occurs;
- benchmark performance;
- identify trends;
- conduct research;
- help organisations to strategically plan.

Methods of Data Collection

The way in which data is gathered varies between different devices and situations. Some devices are autonomous, meaning they have the power to make their own decisions — a robot in a warehouse can decide how to get from one section of the warehouse to another, and this decision would not be possible without the data it collects.

> Autonomous devices are **computer systems that have the power to make their own decisions** without human input, e.g. autonomous warehouse robots.

Overall, the collection and analysis of data has become increasingly important in today's society for two key reasons:

- Enables organisations to make **informed decisions.**
- **Identifies trends** that may have gone unnoticed.

While there are various methods of data collection, each has its own strengths and weaknesses, and it is essential to choose the appropriate method depending on the type of data and the context in which it will be used. You need to be able to define, and weigh up the advantages and disadvantages of, four contrasting methods.

> Active data collection is where the **data you need has been specifically requested**, and a person needs to comply and **actively provide the data requested**, e.g. requesting customer feedback or preferences via surveys.

Advantage:

- Easily learn more detailed information.

Disadvantage:

- People must comply before they provide data.

> Passive data collection is the opposite of active data collection. It works **without a person realising that their data is being gathered**; it is often gathered in the background of their daily activities.

Advantage:

- **Doesn't rely on the person** self-reporting information.

Disadvantage:

- **Users must permit tracking** of the devices/apps they use.

> Manual data collection typically means data is gathered with the use of pen and paper, **based upon observations**, e.g. watching a football match and writing the number of shots on target.

Advantage:

- **Simple & easy** to conduct.

Disadvantage:

- **Mistakes** can be easily made.

> Usage data collection means **collecting information about how a product or service is used** by its customers and users.

Advantage:

- **Easy to gather**, and is in-depth.

Disadvantage:

- **Privacy Concerns**

Ethical and Legal Implications of Collecting Data

Data collection should be carried out with the explicit consent of those from whom the data is collected, from both an ethical and a legal standpoint. This is because once data is transformed into information and

stored in computer systems, it becomes sensitive and must be protected to avoid potential misuse. In the UK, the government has established legislation — the General Data Protection Regulation (GDPR) — that organisations must follow to ensure data is collected, processed, and stored correctly. If organisations fail to comply, legal action may be taken.

Under GDPR, organisations must ensure data is:

- Processed **lawfully, fairly and in a transparent manner**.
- Collected for a **specified, explicit and legitimate purpose**.
- Kept **up-to-date**.
- Kept **no longer than is necessary** for the purpose it is used.
- Processed in a manner which ensures **appropriate security** of personal data.

(b) Storing Data

Binary Data and Storage Units

The storage of data requires a computer system to provide storage space so that data can be stored and processed on a temporary or permanent basis. At the lowest level of computing, data is stored in binary. We use different units to represent different amounts of data, working as a hierarchy in the same way we use hundreds, tens and units in the denary number system.

At the bottom of the hierarchy is a **bit** — a binary value of one or zero, with no other data storable. The next unit is a **nibble** (four bits), useful in hex-to-binary conversions. The next is a **byte** (eight bits stored as a binary number, e.g. 10110110). To make larger amounts of data easier to remember, we use terms including the word 'byte' with a prefix multiplier of 1024, right up to truly enormous quantities of data:

Unit	Symbol	Value
bit	b	1 bit
nibble	—	4 bits
byte	B	8 bits
Kilobyte	KB	1024 bytes
Megabyte	MB	1024 KB
Gigabyte	GB	1024 MB
Terabyte	TB	1024 GB
Petabyte	PB	1024 TB
Exabyte	EB	1024 PB
Zettabyte	ZB	1024 EB
Yottabyte	YB	1024 ZB

Table 1: the hierarchy of binary data storage units.

Representation of Characters

Storing data using characters is relatively simple, as we use a character set, which works by mapping each character in an alphabet system to a unique binary number. This is important because characters can be represented differently by different computer systems, so an agreed convention allows accurate data exchange.

> ASCII (American Standard Code for Information Interchange) is a well-known **7-bit character set** used in early computing, **allowing storage of 128 different characters**.

Each character is stored using seven digits — for example, the character A is stored as *1000001*, while lowercase 'a' is stored as *1100001*. ASCII's biggest constraint is that it only allows 128 characters, a problem given the huge number of languages and symbols used across the world.

> Unicode is a well-known and widely used character set which has been **developed to replace ASCII**. It enables computer systems to store and process **137,000 different characters**.

Representing Sound

To store sound digitally from its analogue state, it must first be captured and converted into a digital signal. An analogue-to-digital converter records sound waves at regular intervals and converts each sample to its binary equivalent — this process is known as sampling. For example, if the amplitude of a sample is 6, it is stored as 0110.

> The sample rate is **the number of samples recorded over a period of time**, measured in hertz — the higher the sample rate, the closer the recording is to the original sound. CDs, for example, take 44,100 samples per second.
>
> The sample resolution is **the number of bits used to represent each captured sample** — the higher the sample resolution, the higher the quality of the recording.

The higher the sample rate and resolution, the greater the storage space required. This can be calculated with the following formula:

File size = sample rate × sample resolution × length of sound (or equivalently, File size = bit rate × length of sound)

Worked example: a sound file has a sample rate of 8kHz, a sample resolution of 16 bit, and lasts 30 seconds.

Step	Calculation	Result
Multiply sample rate × resolution × length	8000 × 16 × 30	3,840,000 bits
Convert bits to bytes (÷ 8)	3,840,000 ÷ 8	480,000 bytes
Convert bytes to kilobytes (÷ 1024)	480,000 ÷ 1024	468.75 KB

Worked example: calculating the file size of a sampled sound recording.

Representing Images

Images can be stored as raster or vector graphics, and it is essential you can distinguish between the two.

> Vector graphics use **geometrically primitive objects such as points, lines, curves and polygons based on mathematical expressions** to represent images. They can be scaled up without loss of apparent quality, but tend to require large amounts of memory.
>
> Raster graphics are **dot matrix data structures representing a grid of pixels** and cannot be scaled up without loss of quality. A well-known type of raster graphic is a bitmap image.

The storage requirement for a raster image depends on the number of bits used per pixel (bpp), which determines the range of colours available:

Bits per pixel (bpp)	Number of colours available
1	2
2	4
3	8
4	16
5	32
6	64
7	128

8	256
10	1,024
16	65,536
24	16.7 million
32	4.3 billion

The relationship between bits per pixel and number of colours available.

Storage requirement is also dependent on the number of rows and columns making up the image, giving the formula:

Size of an image = rows × columns × bpp

Worked example: an image is 640 rows by 480 columns, using 24 bits per pixel.

Step	Calculation	Result
Multiply rows × columns × bpp	640 × 480 × 24	7,372,800 bits
Convert bits to bytes (÷ 8)	7,372,800 ÷ 8	921,600 bytes
Convert bytes to kilobytes (÷ 1024)	921,600 ÷ 1024	900 KB

Worked example: calculating the file size of a bitmap image.

General Storage Methods and Their Application

Digitally sampled sound, bitmapped graphics, compressed audio and compressed video all vary in terms of storage methods and application.

Digitally sampled sound: digital audio represents sound using digital technology, largely replacing older analogue technology in audio engineering, record production and telecommunications. In a digital audio system, an analogue electrical signal is converted with an analogue-to-digital converter; the digital signal can then be recorded, edited, modified and copied using computers and other digital tools. Unlike analogue audio, which degrades with each copy made, digital audio allows infinite copies to be made without any loss of quality.

Bitmapped graphics: a bitmap (raster) graphic is an image made up of a grid of individual pixels, each with a binary value representing its colour. Bitmaps are stored in file formats such as GIF, PNG, TIFF, XBM, BMP or PCX, which specify how the data is organised and compressed. Bitmap graphics are widely used for photographs and are common in web graphics, digital art and print media; while they offer high detail and colour accuracy, they require more storage than vector graphics and can suffer pixelation when scaled up.

Compressed audio: audio data compression reduces the size of audio files, making them easier to store and transmit, by removing redundancies in the audio signal. Lossy compression sacrifices some quality for higher compression ratios, while lossless compression preserves the original quality. As an indication of just how much smaller compressed audio can be, a digital sound recorder can typically store around 200 hours of clearly intelligible speech in only 640MB.

Compressed video: video compression reduces the amount of data needed to represent a video sequence, achieved through algorithms such as H.264/AVC or H.265/HEVC, which can reduce the amount of raw content data by as much as 1,000 times — allowing far more efficient storage and transmission of video files.

Advanced Storage Techniques

As organisations grow, storing data on a single hard drive quickly becomes impractical — too slow, too fragile, and too limited in capacity. The specification requires you to know six advanced storage techniques used to solve this problem: RAID, NAS, High Availability Storage, SAN, Cloud Storage, and Hosted Storage.

> RAID (Redundant Array of Independent Disks) is a data storage technique that **combines multiple physical hard drives into fewer units** in order to improve performance, reduce redundancy and offer fault tolerance.

There are three broad forms of RAID that you need to know:

> RAID 0 (Striped) **provides improved performance and additional storage, but does not provide any fault tolerance**, so errors on the disk can destroy the RAID. RAID 0 Striped **only works on a single disk**.
>
> RAID 1 (Mirrored): each disk provides the same information, **providing some fault tolerance**. Since data repeats on multiple disks, **read speed increases but write speed decreases**. RAID 1 needs **at least 2 disks and an even number of disks to function**.
>
> RAID 3–6 (Striped Parity) **requires at least 3 disks**, providing fault tolerance, parity checks and error correction. **Parity data is stored on one disk so that other disks can continue to function if one fails**, as the lost data is calculated using the parity data on the single disk. This method means **losing storage space in exchange for fault tolerance via parity data**.
>
> Network Attached Storage (NAS) is a **file-level storage system** connected to a network, allowing **multiple systems to access and share files**. NAS devices are a convenient method of file sharing across multiple computers, and remove the responsibility of file serving from other servers on the network.
>
> High Availability Storage operates continuously, providing an uptime of about 99.999% (about 5.5 minutes of downtime per year). It ensures **data is stored in multiple locations**, allowing data access in the event of a single failure, but **requires significant duplication**.
>
> A Storage Area Network (SAN) is a high-speed network enabling a pool of storage devices to access multiple servers, typically assembled with cabling, host bus adapters and SAN switches.

It is easy to confuse SAN and NAS, but the exam expects you to be precise about the difference: a SAN is **a local network consisting of multiple storage devices**, whereas a NAS is a **single storage device connecting to a local area network**.

> Cloud storage is where a cloud storage provider **allows the storage of an organisation's data on their servers**, rather than at the organisation's own premises. The **data is accessed through an Internet or dedicated network connection**.

Advantages of Cloud Storage:

- **Cloud storage providers are responsible for the security** and integrity of the data, not the clients using the storage.
- **Clients can simply buy more storage** instead of having to invest in further physical storage systems.

> Hosted storage refers to technology services with **infrastructure located outside a recipient's physical location**, e.g. websites, e-mails and backups.
>
> A Content Delivery Network (CDN) speeds up the loading process of webpages for data-heavy applications by using content stored **geographically closest to the user**. CDNs take information from the main server and provide that to their closest users.

Storing and Processing Contrasting Types of Data

Organisations often need to manage, store and process diverse types of data. To optimise storage capabilities, organisations may use four further techniques: hosted instance, virtualisation, clustering and blockchain storage — each providing unique advantages for managing and storing contrasting types of data.

> A hosted instance is a type of virtual machine running on cloud computing infrastructure. It allows users to run an operating system as if running on a physical computer, with the **benefit of remote access**. Users can increase or decrease data capacity as they please.
>
> Virtualisation means **creating a software-based version of hardware without sacrificing functionality**, used to save space, cut costs and improve functionality & security.

The specification identifies four types of virtualisation:

> Virtual Storage: **virtual drives split across physical hard drives** (e.g. a school server storing student files).
>
> Virtual Applications: **applications hosted remotely without local storage** (e.g. database applications).
>
> Virtual Memory: **the memory used by the Virtual Machine**.
>
> Virtual Machine: **an operating system independent of the physical host machine**. A VM's operation won't be affected if something goes wrong with the host hardware.

Virtualisation can also involve virtual desktops (hosted by a third party, lowering costs and simplifying deployment) and, more broadly, three types of virtualised software:

- **Operating system virtualisation:** a thin client connects to a server which emulates the operating system; one server can emulate many different operating systems at once.
- **Application virtualisation:** a technology that encapsulates a computer program within the operating system, allowing an application to run as if it were native.
- **Service virtualisation:** a development team uses virtual servers rather than physical ones, allowing complex applications to go through testing much earlier in the development process; it simulates the behaviour of components in a mixture of component-based applications.

> Clustering uses **multiple computer systems running in parallel together**. These offer a stronger, more efficient output by **combining memory and processing power which improves performance**.
>
> Blockchain works by **using a decentralised network to save data by using unused hard drive space of users across the world**. The goal is to **record and distribute data while remaining unchanged via encryption**, improving privacy & security. However, blockchain is **slow, has high latency, and cannot be scaled greatly**.

Cloud Computing

> Cloud computing refers to **the delivery of computing services over the Internet**, including storage, processing power & software applications. It **allows access of services from anywhere with an Internet connection**.

Cloud computing is a broader term than cloud storage: cloud storage refers specifically to online storage of data for backup, file sharing and collaboration, whereas cloud computing also covers the delivery of processing power and entire software applications. The specification identifies four common examples of cloud computing services:

- Data Storage
- Cloud Email
- Virtualised Software
- Remotely Hosted Applications

Cloud email is a well-known example — services such as Gmail and Outlook see a third-party host run the e-mail server on the user's behalf in a distributed environment, ensuring 24/7 access and maximising uptime. Cloud email can also act as a backup facility, since the provider stores and archives all e-mails.

Cloud computing brings a wide range of benefits to organisations:

- **24/7 access:** services and data can be accessed at any time, from anywhere with an Internet connection — at home, on holiday, or during a commute.
- **Backup & recovery options:** data is backed up and protected, minimising downtime in the event of a disaster, and providing business continuity.
- **Scalable data storage:** businesses can scale their operations and storage up or down quickly, buying more storage instead of investing in further physical infrastructure.
- **Cost savings:** cloud computing reduces the cost of managing and maintaining IT systems, since upgrades are often included in the contract and less need arises for specialist in-house staff.
- **Collaboration:** employees, contractors and third parties can securely share and collaborate on data.
- **Staying up-to-date:** IT requirements are automatically updated by the provider, without the organisation having to manage this itself.

(c) Analysing Data

Once data has been collected and stored, it is of little use sitting untouched — raw data has no meaning until it is processed. UK census data, for example, has no meaning to a computer until data analytic tools extract trends, patterns and correlations from it, turning it into statistics that can inform real decisions (such as opening more GP practices where a population has grown faster than local GP provision).

Data Analytics and Descriptive Analytics

> Data analytics means **analysing data to make conclusions and produce information**. Technology can be used for data analytics via extremely fast automation and algorithms.
>
> Descriptive data analytics is where **the information provided from the data describes the answer to a proposed question** regarding the dataset, e.g. the description of customer preferences obtained from a supply & demand data set.

Descriptive data analytics is useful for three main reasons:

- Can **help decision-making** with real statistics.
- Can **identify trends in data** (e.g. what time a restaurant has the most footfall).
- Uses real obtained statistics, **improving reliability.**

The specification identifies five common examples of data commonly summarised with descriptive data analytics:

- Financial statements
- Surveys
- Website traffic
- Scientific research findings
- Weather reports

Data Visualisation

> Data visualisation means **graphically representing information** and data through visual elements, e.g. line graphs, pie charts, bar graphs.

Data visualisation is useful for two key reasons:

- Different visualisation methods can **give different outlooks.**
- **Easier for humans to understand.**

In practice, a wide range of visualisation formats are used, including pivot tables, line graphs, pie charts, whisker plots, maps and infographics — the choice depends on the type of data and what the audience most needs to understand from it, and is especially valuable when dealing with genuinely large data sets.

Management Information Systems (MIS)

> A Management Information System (MIS) is a collection of systems and procedures that **gather data from multiple sources** and compile them into a **readable format**.

An MIS serves four key uses:

- **Obtains real data** from company operations.
- Able to **simulate hypothetical scenarios.**

- Creates **data-based projections** to help decision making.
- Helps create an **evaluation of data** based on previous decisions.

For example, a specialised MIS used by a national restaurant chain could show restaurant managers revenue, expenses, and popular/unpopular hours and dishes — helping them make decisions such as running a promotional event on a quiet evening, or reducing staff hours at low-footfall times. Its typical features include information from company operations (sales, expenses, investments, workforce data); the capability to run 'what-if' scenarios (showing how variables change when a decision is made, e.g. reduced staff levels or an increased promotion budget); projections to assist decision making (trend analysis, business strategy projections); and implementation and evaluation (determining whether decisions had the desired effect).

Project Management Software (PMS)

> Project Management Software (PMS) is **software used for project planning**, scheduling, resource and change management.

PMS is used to:

- Define a project's **critical pathway.**
- **Identify different tasks.**
- **Outline project schedule** and set milestones.
- **Break down task completion** and task responsibilities.
- **Allocate staff and resources** for each task.

Beyond these core uses, PMS also helps manage and track tasks — from an individual unit level right up to macro (whole-project) level — supports collaboration with team members, suppliers and stakeholders, and can track bugs or issues, archiving resolutions as a reference for future problems.

Data Warehouses

> A data warehouse is a type of digital management system which **acts as a central repository of information**, which can be **analysed to make decisions**.

Data warehouses draw data from four main sources:

- Transactional systems
- Application log files
- Historical data
- Relational databases

There are two main approaches used to build a data warehouse, known as ETL and ELT, which differ in the order in which data is transformed.

> An ETL (Extract, Transform, Load) data warehouse uses **3 layers for its key functions**. The **staging layer** stores **raw extracted data**. The **integration layer transforms the data** into the correct format for the data warehouse. The **access layer allows users to retrieve** the transformed data for analytics.
>
> An ELT (Extract, Load, Transform) data warehouse is where the **raw data is extracted and loaded into the data warehouse first, then transformed** into the correct format before the access layer for

> users. Unlike ETL, ELT does not use a separate transformation tool — the staging area sits inside the warehouse itself.

Data Mining and Large Data Sets

> Data mining is the **extraction of valuable information from available data** to discover patterns & anomalies within data sets. It is an interdisciplinary field, joining together computer science and statistics techniques — but note that data mining is not the extraction of the data itself, only the patterns and information within it.
>
> Large data sets ('big data') are data sets that are **too large or complex to be dealt with by traditional data-processing software**.

Data sets with many fields offer greater statistical power, while higher complexity may lead to higher false discovery rates. Working with large data sets brings a distinct set of challenges, including capturing, storing, analysing, searching, transferring, visualising, querying, updating and protecting the privacy of the information involved.

(d) Using Data

The final stage of the data cycle is putting analysed data to use — and increasingly, this means artificial intelligence. This section covers how AI systems are built and how they draw conclusions, before turning to how organisations identify trends within data and present the results of their analysis to decision-makers.

Artificial Intelligence

> Artificial Intelligence (AI) is the **simulation of intelligent behaviour** by a computer, which enables it to make decisions **without human intervention**.

AI encompasses systems able to perform tasks that in the past normally involved human intelligence — visual perception, speech recognition, decision-making, and translation between languages — using mathematics and logic to simulate the logic people use to learn from new information. AI can be divided into two broad categories: weak AI, designed for one particular job (e.g. self-driving cars, or systems used in hospital operating rooms), and strong AI, designed to perform tasks associated with human intelligence more broadly, and which is considerably more complex and advanced.

The Turing Test

Alan Turing proposed a test in 1950 to determine whether a computer system has the ability to 'think'. The test works as follows:

- Proposed by Alan Turing in 1950.
- A human interrogator must distinguish between a computer and a human respondent based on their responses to the interrogator's questions.
- The interrogator must distinguish between them within a certain timeframe.
- The computer is considered an AI if the interrogator cannot distinguish between the human and computer respondent.

No machine has passed the Turing Test to date, but it paved the way for AI research, and remains a well-known benchmark referenced throughout the field.

Neural Networks

> A neural network is a type of machine learning algorithm that **uses a network of interconnected nodes to recognise relationships in data**. A 'neuron' contains layers of interconnected nodes, each known as a perceptron.

The specification identifies five types of neural network:

- Feed-forward
- Recurrent
- Convolutional
- Deconvolutional
- Modular

> A feed-forward neural network **conveys information in one single direction** through input nodes until it reaches the output node, e.g. used for facial recognition.

> A recurrent neural network **takes the output of a processing node and transmits the information back into the network**, which influences the next output. It is most useful with sequential data, e.g. text or time, and is often used for text-to-speech.
>
> A convolutional neural network has **an input layer, an output layer, and a multitude of hidden convolutional layers** in between. It **extracts features from data** using these layers to create feature maps, e.g. for entity recognition in images.
>
> A deconvolutional neural network is the **reverse of convolution**, aiming to **generate the original data from the extracted features**, e.g. generating an image based on a text description.
>
> A modular neural network contains **several computer networks working independently**, allowing for **more efficient processing**. Each network's goal **contributes to the larger goal at hand**.

Expert Systems

> An expert system is an **application of artificial intelligence** where **the knowledge of a human expert is made available** through a computer package, typically in a **narrow field of knowledge with easily drawable conclusions**, e.g. determining potential illnesses after inputting symptoms and other data.

To create the rules and facts that power an expert system, its development involves a subject expert, a team of programmers, and knowledge engineers — also called technical experts — whose knowledge is programmed in to create a knowledge base of facts and rules. This includes heuristic knowledge captured from a person's experience rather than logic, i.e. ‘rules of thumb’.

An expert system is made up of four core components:

> Knowledge Acquisition System: **where the expert (or knowledge engineer) enters facts and information about the subject.**
>
> Knowledge Base: **where the facts are stored, used as points of reference or ‘heuristics’.**
>
> Inference Engine: **compares given inputs against the knowledge base to draw potential conclusions** (developed by programmers).
>
> User Interface: **where users input information in order to obtain a conclusion from the expert system.**

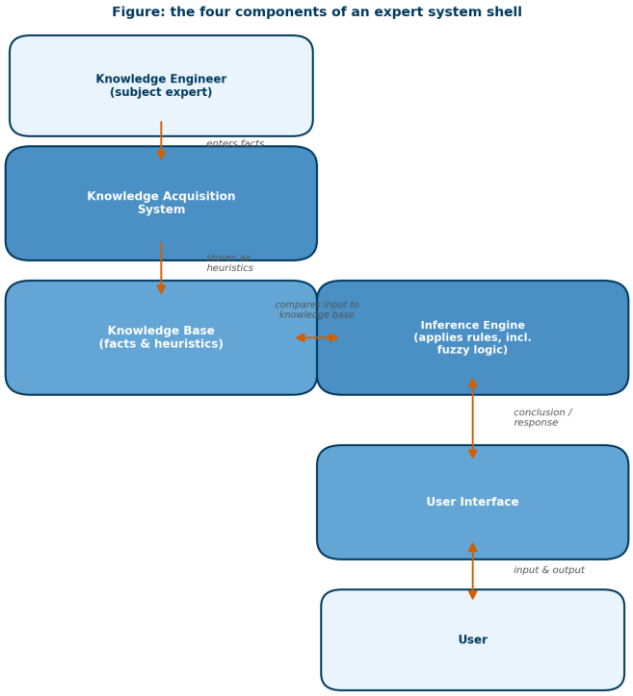

Figure 1: the four components of an expert system shell.

> An expert system shell is **the software framework made of the core components**, including the knowledge base, acquisition system, inference engine and user interface.
>
> Heuristics are **the facts and information obtained from experts**, used as **'rules of thumb'** by the inference engine when drawing conclusions.
>
> A knowledge engineer is a specialised and **experienced practitioner in their subject expertise**, who provides the **facts and information** to the expert system, **creating the knowledge base**, e.g. a GP providing information to a medical diagnostic expert system.

An inference engine interrogates the knowledge base and draws conclusions based on the rules and facts entered, posing questions to a user and using the answers to determine a suitable response — e.g. a cough plus a headache might allow the system to determine a head cold. Not all responses can be given using standard logic, however, so fuzzy logic may be applied instead.

> Fuzzy logic is where **variables can be expressed in linguistic terms** and are assigned **'degrees of truth'** ranging from 0 (False) to 1 (True), e.g. on a 'hotness' range, warm may be 0.6, whereas cold would be 0.

For example, an anti-lock braking expert system could use fuzzy logic to adjust brake pressure if the brake temperature is assessed as 'warm' and the speed as 'not very fast' — variables that could not easily be expressed as simple true/false logic.

Expert systems are used across many industries, including health care, where a knowledge base of medical information can be used to input a patient's symptoms and provide a diagnosis, helping medical professionals make timely, effective decisions about treatment order, urgency and medication. A key strength of an expert system is that it can combine the knowledge of many human experts and share it globally, all through a single system.

Ethical Considerations of AI and Expert Systems

The specification identifies three broad ethical considerations of AI:

- Unemployment
- Privacy Concerns
- Discrimination & Bias

AI cannot currently replicate human emotion, so its decisions are made purely on logic. Consider, for example, an autonomous vehicle whose brakes fail while travelling at high speed towards a group of people: it might decide to deviate slightly in order to hit a smaller group instead — a decision based purely on its expert system's rules, with no human emotion involved. Other ethical questions raised by AI include: is it right if AI becomes more knowledgeable than humans; how many jobs will be lost to AI; how much data does AI gather; does AI take away people's privacy; how can we safeguard AI from discrimination and bias; and who is accountable if a wrong decision is made?

Expert systems specifically raise three further ethical considerations:

- **Accountability** of wrong decisions/conclusions.
- **Privacy concerns** and use of data.
- **Overreliance** can hinder human capabilities.

Natural Language Processing (NLP)

Natural Language Processing (NLP) aims to develop computer systems that understand text or voice data as humans do, using a rule-based model of human language combined with statistical, machine learning and deep learning models. NLP simplifies business operations and increases productivity by translating text, responding to spoken commands, and summarising large amounts of text in real time.

A well-known worked example is Amazon Alexa, which uses NLP as follows:

- Alexa records speech and sends it to Amazon's servers for analysis (interpreting sounds needs heavy computation).
- The speech is broken into individual sounds, and a pronunciation database is consulted to find matching words.
- Keywords are identified to determine the task requested (e.g. the word ‘weather’ opens the weather app).
- Information is sent back to the device, going through the same process in reverse if a spoken reply is needed.

Other everyday NLP systems include voice-operated GPS, chatbots, digital assistants, and speech-to-text dictation software.

Identifying Trends and Patterns: the Four Stages of Data Analysis

The rapid development of AI means organisations now gather, store and process so much data that it can be difficult to understand what it actually shows. Achieving genuine ‘AI utilisation’ requires four distinct types of data analysis, each building on the last:

- Descriptive
- Diagnostic

- Predictive
- Prescriptive

> Descriptive analysis **assesses the gathered data** in an attempt to **identify specific patterns**, presenting the data in a visual format. Descriptive analysis is 'what happened', e.g. data showing an increase in sales over a specific time period.
>
> Diagnostic analysis uses techniques such as *data mining, discovery and correlation identification* to **find further data to support any reasoning for the data**. Diagnostic analysis is 'why it happened', e.g. further data showing which business sectors contributed most to an increase in sales.
>
> Predictive analysis uses techniques such as *forecasting, pattern matching and predictive modelling* in order to **predict what might happen based on historical data**. Predictive analysis is 'what is likely to happen', e.g. using a prediction model to forecast sales in the next few months.
>
> Prescriptive analysis uses techniques such as *graphs, heuristics and neural networks* to help **determine what the best next step** to make is, based on all three previous analysis stages. Prescriptive analysis is 'what should be done', e.g. choosing to manufacture less of a certain product after forecasting decreased sales.

The accuracy of prescriptive analysis is entirely dependent on how well the previous three stages were carried out — AI is far cheaper and faster than hiring human experts to perform this kind of analysis at scale.

Presenting Data and Analysis

Once data has been analysed, it needs to be presented to stakeholders so that decisions can be made or explanations given. How this is presented depends heavily on the target audience — employees may need live Key Performance Indicators (KPIs) shown on a dashboard, while management may instead need a series of graphs presented within a formal report document.

One of the most important ways of representing how data moves through an organisation is the Data Flow Diagram (DFD), which graphically represents how data flows both in and out of a system.

> A logical DFD shows the **flow of data through a system** to perform functionality.
>
> A physical DFD **describes the implementation** of the logical data flow.

A DFD is built from just four symbols:

> Process Box: **describes the process formed** (verb followed by noun, e.g. 'calculate tax').
>
> Data Flow: **arrows indicate the direction of data flow**, labelled with the data element or set being moved, e.g. 'customer ID'.
>
> Data Store: **indicates the data repository** being used, e.g. a product database.
>
> External Entity: **describes an external system that provides or receives data** from the internal data flow, e.g. suppliers.

There are several strict rules that govern how a valid DFD must be drawn:

- A process must have at least one data flow entering and one exiting.
- An external entity cannot provide data to another entity without a process taking place.
- Data cannot move directly from an entity to a data repository without being processed.

- Data cannot move from one repository to another without being processed.
- A data repository must be connected to a process with a data flow.
- A data repository must have at least one input flow and one output flow.
- External entities do not process data.
- An external entity must be connected to a process with a data flow.
- Data flows must not cross.
- Objects cannot be duplicated (e.g. only one customer external entity is allowed).

The Use of AI and Large Data Sets

AI can help handle large data sets by being involved in every process within the data cycle — learning patterns and watching how users interact with an organisation's data flow. (Note that machine learning is itself a subcategory of AI, where computers learn from data using algorithms.) The specification identifies three specific uses of AI in this context:

- **Identifying data types.**
- **Finding connections between data.**
- **Automating data analysis** tasks.

This combination of AI and large data sets raises real social implications, both positive and negative. Questions worth thinking through include: how do we know the information AI is generating is accurate and unmanipulated; is AI gathering too much information about a person, taking away their right to privacy without them realising; and how clever should we allow AI to become? Overall, the specification identifies five key social implications:

- Improvements in **medical diagnosis accuracy.**
- Improves **business efficiency.**
- **Removes ethical factors** in decision-making.
- Can cause **unemployment.**
- **Reduced privacy.**

In summary, AI and large data sets together can disenfranchise minorities and discriminate against people not represented in the data sets used to train a system (e.g. women being under-represented in historical car safety data), while also leading to huge improvements in medical diagnosis accuracy, improved business methods and efficiency, large-scale unemployment in some sectors, and a general reduction in privacy. AI use must therefore be carried out ethically and within carefully set parameters — a theme that will keep recurring throughout the rest of this unit.

2.3.2 Cyber Security

This is the biggest single topic in Unit 3 — and it needs to be, because cyber security touches almost everything else you have studied across the qualification. Every network, every smart device, every piece of AI and every website relies on being kept secure, so this topic pulls together threats, defences and the human side of security into one connected picture. Because of its size, take this topic section by section rather than trying to absorb it all at once: (a) sets out what cyber security actually is; (b) works through the many ways systems and data can be damaged or compromised; (c) covers the professional, technical and organisational controls used to defend against and recover from attacks; and (d) looks specifically at social engineering — attacks that target people rather than machines.

(a) Introduction to Cyber Security

> Cyber security is a practice that aims to **protect computer systems, networks and electronic devices** from unauthorised access, theft, damage or disruption. It involves software, hardware and human practices to prevent cyber attacks.

Notice how that definition covers three different categories of measure: software (antivirus, firewalls, encryption), hardware (secure devices, physical access controls) and human practices (staff training, strong passwords, safe browsing habits). A very common exam mistake is to only think about the technical side of cyber security and forget that human behaviour is just as often the weak point — you will see this theme come back repeatedly in section (d) on social engineering.

Cyber security also has a second, closely related aim beyond just stopping attacks: safeguarding personal information stored on electronic devices and online from unauthorised access, theft or misuse. This is why cyber security overlaps so heavily with data protection law (such as GDPR) — protecting a system and protecting the personal data that flows through it are, in practice, the same job.

As you work through this topic, it helps to keep three underlying goals in mind — you will see these referred to again later under cryptography, but they apply to cyber security as a whole: **confidentiality** (only authorised people can access data), **integrity** (data has not been tampered with or corrupted) and **availability** (authorised people can access the system and data when they need to). A DDoS attack, for example, is primarily an attack on availability, whereas a data breach is primarily an attack on confidentiality.

(b) Threats and Vulnerabilities

Before you can defend a system, you need to understand precisely what it needs defending from. This section works through the full range of threats the specification expects you to know — starting with damage that happens by accident, moving on to damage that is deliberate and malicious, and finishing with some of the wider risks around data itself.

Accidental Damage

Not every threat to data and systems is malicious. A huge proportion of data loss in the real world happens simply because people, software and hardware are all imperfect. The specification identifies six types of accidental damage:

- Human error
- Accidental data file deletion
- Software corruption
- Hardware malfunction
- Natural disasters
- Power failure

> Human error is where **errors are made by humans in data manipulation through typing, editing, updating and deletions** (processes that are prone to error by users). Human error is the root cause of most data loss problems in businesses.

The day-to-day running of any business involves constant data manipulation — typing, editing, updating and deleting records — and every one of those actions is an opportunity for a mistake. This is precisely why human error sits at the top of the list: humans are, by nature, not perfect, and no amount of technical security can fully eliminate the risk of someone simply clicking the wrong button.

- **Accidental data file deletion:** usually results from user error, where a file or folder is deleted without an available backup. If there is no backup, unintentionally erased files may be permanently lost — this is why setting up proper workflow processes, including routine saving and systematic data backup, is so important.
- **Software corruption:** any program used to access or manipulate data has the potential to crash, leading to data loss or corruption. When updating multiple files, file-editing software can malfunction, causing files to fail to save or update correctly — the same can happen during backups. Common backup issues include the system's inability to make file copies or to halt file deletions automatically; incorrect malware detection by antivirus software can also cause files to be deleted, as can errors during file format conversion.
- **Hardware malfunction:** hardware failure usually results in irretrievable data loss, caused by internal or external factors. Hard drives are vulnerable to physical or mechanical failure caused by misuse, overheating, water and fire damage, power outages, human error and faulty connections; read/write head failure, bad sector corruption and firmware corruption can also cause hardware to malfunction, and devices simply lose effectiveness as they age.
- **Natural disasters:** floods, earthquakes and other natural disasters threaten physical devices such as computers and servers directly, and can also damage the wider infrastructure — bringing down power lines, mobile phone towers and other power sources that systems depend on.

- **Power failure:** if data have not been routinely saved, a disruption to the power supply while a user is working may cause data loss, with only the previously-saved portion recoverable through auto-recovery processes. A sudden loss of power can also damage hardware and the operating system itself, and sudden voltage fluctuations (usually a voltage spike) can cause data loss and hardware damage — computers may experience rebooting issues that make it impossible to retrieve data at all.

Malicious and Deliberate Damage

Malicious or deliberate damage refers to any action intended to cause harm or disruption to computer systems, networks or data. Unlike accidental damage, there is a human attacker behind it, actively trying to cause harm. The specification identifies six types:

- Malware
- Phishing
- DDoS attacks
- SQL injection
- Insider threats
- Ransomware

> Malware is a **piece of software** that can infect and damage computer systems and is used for **malicious purposes** such as stealing information.
>
> Phishing / social engineering involves **using deception and manipulation** to **trick people** into revealing sensitive information or installing malware to their devices.
>
> A DDoS attack aims to **flood the server with requests** so that it **becomes overwhelmed and unavailable**, making it difficult for users to access the server.
>
> SQL injection involves **inserting malicious code** into a web application to **execute code on a server**.
>
> Insider threats occur where **individuals within the organisation** intentionally cause harm to the digital system from the inside.
>
> Ransomware is a type of malware that **encrypts victims' files**, and the **culprit demands a ransom** for the malware to be removed.

It is worth noticing the range covered here: some of these attacks (like malware and ransomware) target a device directly, some (like DDoS) target availability rather than data itself, some (like SQL injection) exploit weaknesses in how software is built, and some (like insider threats and phishing) exploit trust and access that already exists inside an organisation. A strong exam answer identifies which of these categories a given scenario falls into before suggesting a defence.

Risks of Online Marketing Communications

Digital marketing brings its own distinct set of cyber security risks, separate from the threats to a company's own systems:

- **Spam and unwanted email:** unsolicited email marketing can be annoying or harmful, damaging customer trust and reputation.
- **Phishing and scam attempts:** attackers impersonate legitimate organisations to steal login credentials or financial information, which can lead to identity theft and financial loss.

- **Privacy concerns:** organisations collecting and using personal data (such as email addresses or browsing history) must comply with data protection regulations and be transparent about how that data is used.
- **Ad fraud:** bots artificially inflate ad clicks, wasting a company's marketing budget.
- **Brand safety:** adverts appearing on inappropriate or offensive websites can damage a brand's reputation.
- **Misinformation:** spreading false information causes confusion, mistrust or harm.

Organisations mitigate these risks through strong security protocols, strict adherence to privacy regulations, and by verifying sources before sharing information — the same underlying discipline that runs through every part of this topic.

Security and Integrity of Online File Updates

Software regularly needs to update itself over the internet — but the update process itself is a security risk, since it involves downloading and installing new code onto a system. Special security and integrity problems that can arise during online file updates include:

- **Unauthorised access:** an attacker gaining access to the update server can alter or replace the files being updated, compromising their integrity.
- **Man-in-the-middle attacks:** an attacker intercepts and alters update files while they are in transit between the server and the device.
- **Malicious software:** an attacker includes malware or viruses inside update files, compromising the security of every device that installs the update.
- **Incomplete updates:** an attacker causes an update to fail partway through, leaving the system in an insecure, half-updated state.
- **Denial of service:** an attacker overloads the update server, making it unavailable, so systems relying on it become out of date.
- **Rollback attacks:** an attacker forces a system to install an old, less secure version of a file in order to exploit vulnerabilities that have since been fixed.

To mitigate these risks, organisations use secure methods for transmitting and verifying file integrity — secure protocols such as HTTPS or SFTP, digital signatures and hash functions — combined with a robust incident response plan and regular security assessments.

Malicious Software

Malware is not a single thing — it is a whole family of different software types, each designed to cause harm in a slightly different way. The Anki-level definitions below cover four commonly-tested types and three common operations; the fuller table extends this with the complete range you may be asked about.

> Trojan, Ransomware, Adware and Spyware are the four core types of malware:

- **Trojan:** a hidden program that appears legitimate but performs malicious actions once installed.
- **Ransomware:** a type of malware that encrypts a victim's files, with the culprit demanding a ransom for their removal/release.
- **Adware:** malware that displays unwanted advertisements to the user.
- **Spyware:** malware that collects and sends a user's personal information without their knowledge.

The Blended Learning resource extends this list with three further common types of malware:

- **Virus:** a self-replicating program that attaches itself to other files and spreads between devices.
- **Worm:** a self-replicating program that spreads through networks, without needing to attach itself to another file.
- **Rootkit:** malware designed to hide its own presence and give attackers full remote control over an infected device.

Malware also has three core operations you should know — the actual harmful actions it carries out once it has infected a device:

> Data theft, spamming and crypto mining are the three core operations of malware:

- **Data theft:** stealing personal or confidential data from the infected device.
- **Spamming:** using the infected device to send large volumes of unsolicited messages.
- **Crypto mining (cryptojacking):** secretly using the victim's device to mine cryptocurrency for the attacker, without their knowledge or consent.

Two further operations are also worth knowing for a fuller answer: **system disruption** (interfering with the normal operation of the device or network) and **extortion** (demanding payment in exchange for not carrying out a malicious action — distinct from ransomware, which demands payment to reverse damage already done).

MAC Address Spoofing

> A MAC address (Media Access Control address) is a **unique identifier assigned to a network interface controller** for use as a network address in a network segment.
>
> MAC spoofing means **changing the MAC address of a device to impersonate another device** on a network, used to bypass security measures.

Because MAC addresses are often used as a simple way of identifying and controlling which devices are allowed onto a network, spoofing one creates several distinct problems:

- **Network security risks:** spoofing can bypass systems that identify and control network access, such as MAC-based access control lists.
- **Privacy concerns:** MAC addresses can normally be used to track a device's location and activity, so spoofing can be used to conceal a device's true identity and activity.
- **Network performance issues:** spoofing can confuse network devices, causing data to be sent to the wrong device — leading to lost or duplicated packets.

Mitigation involves strong general network security measures (encryption, firewalls, access controls), regular monitoring of network traffic for suspicious activity, and technologies such as MAC authentication, which require a device to present a valid, verified MAC address before it is allowed onto the network.

Cryptocurrencies and Cyber Security

Blockchain is a decentralised, digital ledger that records transactions across a network of computers, using cryptography to secure and validate transactions and ensure the ledger is tamper-proof. *Cryptocurrency* is blockchain's most well-known application, but blockchain technology has a number of other uses within cyber security specifically:

- **Decentralised identity management:** storing and managing digital identities securely, reducing the risk of identity theft.

- **Secure record keeping:** the immutable, transparent nature of blockchain makes it suitable for storing sensitive financial or medical records.
- **Supply chain security:** tracking goods and ensuring product authenticity, reducing the risk of counterfeit goods.
- **Cyber threat intelligence sharing:** a decentralised network for sharing and analysing threat data between organisations.
- **Data privacy:** implementing privacy-focused technologies, such as zero-knowledge proofs, which prove a fact without revealing the underlying data.
- **Cyber insurance:** streamlining the process of purchasing and managing cyber insurance.

Data Mining and the Individual

Data mining involves collecting and analysing large amounts of personal data — often to spot patterns useful for marketing, risk assessment or research. But this practice poses significant privacy threats to the individuals whose data is being mined:

- **Data breaches:** sensitive personal information is illegally obtained, potentially leading to identity theft, financial fraud and abuse.
- **Unauthorised data sharing:** companies sharing personal data with third parties without the individual's consent.
- **Discrimination:** data mining algorithms unfairly discriminating against groups of people, e.g. based on a medical condition or geographic location.
- **Profiling:** creating detailed profiles of individuals for targeted advertising, which can be misused for discriminatory decision-making.
- **Lack of control:** individuals having limited control over how their information is collected, used and shared.
- **Inaccurate data:** algorithms producing inaccurate results, leading to false conclusions that negatively affect a person's life.

To mitigate these threats, organisations should implement strong data protection policies and technologies, while individuals should be cautious about the information they share online and should review the privacy policies and settings of the services they use.

The Importance of Large Data Sets to Health, Finance and Retail

It's easy to think of large data sets purely as a security risk — but they are also hugely valuable to organisations, which is exactly why protecting them matters so much. The specification highlights three sectors in particular:

- **Health:** large data sets such as electronic health records (EHRs), patient data and clinical trial data are used to improve patient care, support medical research and streamline operations. EHRs give healthcare providers a comprehensive view of a patient's medical history, enabling informed decisions and better care.
- **Finance:** financial institutions use large data sets — transaction data, credit history and market data — to make informed investment decisions, identify fraud and improve risk management. Credit card companies, for example, use transaction data to detect fraudulent activity.

- **Retail:** retail organisations use large data sets — customer data, sales data and supply chain data — to improve marketing and sales efforts, optimise supply chain operations and provide personalised customer experiences.

This is a useful point to remember for exam questions that ask you to evaluate cyber security measures: the reason organisations invest so heavily in protecting large data sets is not just to avoid fines, but because the data itself is a genuinely valuable business asset.

(c) Resilience Controls

Having covered the threats, this section turns to defence — the professional responsibilities, technical measures and organisational controls that together make up an organisation's cyber security strategy. This is the longest section of the topic, so it is broken into distinct H3 sub-sections you can revise individually: legal duties, identifying and preventing threats, the main categories of security measure, cryptography in depth, biometrics, ethical hacking, diagnostic tools, and finally cyber resilience and recovery.

Legal and Professional Responsibilities

Legal and professional responsibilities encompass preventing and mitigating the damage caused by malicious or deliberate attacks. Attackers can be motivated by financial gain, political beliefs, or simply the desire to cause disruption — and the resulting damage can range from a minor inconvenience to complete system failure and permanent data loss.

Countering such attacks requires a multi-layered approach: security awareness training, regular security updates, penetration testing and incident response planning all working together, rather than relying on any single measure. As the UK's Information Commissioner, John Edwards, put it:

"The biggest cyber risk is complacency, not hackers."

This is a genuinely useful quote to remember for exam essays: it captures the idea that most breaches succeed not because attackers are unstoppable, but because an organisation failed to keep up its own basic defences. The Interserve Group Ltd case is a real example of the serious consequences that can follow from failing to keep data secure — the UK's Information Commissioner's Office fined the construction company £4.4 million in 2022 after a phishing email led to the personal data of up to 113,000 current and former employees being compromised, precisely because of avoidable security failings rather than a sophisticated attack.

Alongside general duty of care, organisations must comply with specific legal and professional frameworks:

- **GDPR and the Network and Information Systems Regulations (NISR):** these outline specific requirements for ensuring the security and resilience of personal data, critical infrastructure and systems.
- **ISO 27001:** an international standard setting out best practice for information security management.
- **The Cyber Essentials scheme:** a UK government-backed baseline standard for cyber security, which many organisations must hold to bid for public sector contracts.

Together, these give organisations a responsibility for the protection of personal data (implementing appropriate security measures to prevent unauthorised access, use, disclosure and destruction), a duty of care to ensure continuity of critical business functions (through business continuity planning and disaster recovery strategies — see 'Cyber Resilience' below), and a duty to ensure the security and confidentiality of sensitive information such as financial data and intellectual property.

Identifying and Preventing Threats

Attacking vulnerabilities refers to identifying and exploiting weaknesses in a system or network to gain unauthorised access, steal data or cause damage. You should be able to name the following attack techniques:

- **Brute force attacks:** trying all possible combinations of passwords or encryption keys until the correct one is found.
- **SQL injection:** inserting malicious SQL code into a database query.
- **Cross-Site Scripting (XSS):** injecting malicious scripts into web pages that are then viewed by other users.
- **Cross-Site Request Forgery (CSRF):** making malicious requests on a logged-in user's behalf, without their consent.
- **Buffer overflow:** overwriting memory locations with malicious data, beyond what the program intended to allow.
- **Remote Code Execution (RCE):** executing arbitrary code on a remote system.
- **Directory traversal:** accessing restricted files or directories on a server that should not be publicly accessible.
- **Man-in-the-middle (MitM) attacks:** intercepting and manipulating network communications between two parties.
- **Denial of Service (DoS) / Distributed Denial of Service (DDoS):** overwhelming a system with traffic so it becomes unavailable.
- **Social engineering:** manipulating individuals into divulging confidential information (covered in full in section (d)).

Defending against these threats involves measures to prevent, detect and respond to attacks:

- **Firewalls:** controlling incoming and outgoing traffic based on defined rules.
- **Encryption:** transforming data into a secret code to protect confidentiality and integrity.
- **Access control:** restricting access based on predefined rules and policies.
- **Antivirus software:** detecting and preventing malware.
- **Patches and updates:** regularly fixing known vulnerabilities.
- **Backups:** protecting against data loss or corruption.
- **User education and awareness training:** teaching safe computing practices.
- **Network segmentation:** dividing a network into smaller, isolated segments to reduce the impact of any single breach.
- **Intrusion detection and prevention systems:** detecting and preventing unauthorised access.
- **Virtual Private Network (VPN) technology:** establishing secure, encrypted connections over public networks.

The next several sub-sections take some of the most exam-significant of these measures — encryption, firewalls, antivirus software, hierarchical access levels, cryptography and biometrics — and cover each in the depth the specification requires.

Security Measures: Encryption

Encryption is a security measure that uses mathematical algorithms to convert *plaintext* (readable data) into *ciphertext* (unreadable data) in order to protect it from unauthorised access. Converting plaintext to ciphertext is called **encryption**; the reverse process of converting ciphertext back to plaintext is called **decryption**.

Encryption is the backbone of confidentiality: even if an attacker manages to intercept or steal encrypted data, it should be unreadable and therefore useless to them without the correct key. The full detail of how

encryption actually works — the different techniques and algorithms — is covered under 'Cryptography' and 'Symmetric and Asymmetric Encryption' below.

Security Measures: Firewalls

A firewall regulates incoming and outgoing network traffic based on a set of rules and policies, acting as a barrier between a trusted internal network and an untrusted external network such as the internet. Firewalls can be hardware-based or software-based, and typically combine several technologies to control network traffic:

- **Packet-filtering:** examines the header of each network packet to determine its source, destination and whether it should be allowed through — typically based on IP address and port number.
- **Stateful inspection:** more advanced than simple packet-filtering; it examines the packet header but also tracks the entire 'state' of a connection, allowing far more informed decisions about whether traffic should be allowed.
- **Application-level gateways (proxy servers):** inspect data at the application layer of the OSI model, understanding the specific application-level protocol (e.g. HTTP or FTP) in order to make more precise filtering decisions.

Firewalls can be located in several different places within a network — at the perimeter of a network (facing the internet), between internal network segments, or on individual devices — to monitor and control traffic at each of those points.

Security Measures: Antivirus Software

Antivirus (AV) software is designed to detect, prevent and remove malware such as viruses, worms, trojan horses and other malicious software. It relies on three main detection methods:

- **Signature-based detection:** comparing file or program code against a database of known malware signatures.
- **Heuristic-based detection:** looking for patterns or behaviour typical of malware, to identify new or previously-unknown threats.
- **Behavioural-based detection:** monitoring the behaviour of a running program or process to identify malicious activity as it happens.

Once malware is detected, AV software will typically do one of three things: quarantine it (isolating it from the rest of the system so it cannot cause further harm), delete it (removing it entirely), or repair it (attempting to reverse any damage it has already caused). AV software is typically installed on individual devices and runs constantly in the background as a service, monitoring for suspicious activity.

Hierarchical Access Levels

Hierarchical access levels divide access to a system or network into different tiers, each with its own privileges and restrictions — limiting the scope of damage that an unauthorised user, or even a malicious insider, could cause. The most common example is user accounts and permissions:

- **System administrators / superusers:** have the highest level of access, able to change system configuration and manage the access of other users.
- **Managers / power users:** have access to more resources and functionality than regular users, but less than administrators.

- **Regular users:** have the least access, able to perform only a limited set of tasks or access a limited set of resources.

Hierarchical access can also apply at the network level — for example, a DMZ (demilitarised zone) network segment is deliberately given less access and privilege than the internal network, so that anything exposed to the internet in the DMZ cannot directly reach an organisation's most sensitive internal systems. This approach allows fine-grained control over access to resources, and helps limit the impact of any single security breach.

Cryptography

> Cryptography is **the practice of securing communication and data through mathematical algorithms**.

The need for cryptography arises because information transmitted over networks, or stored electronically, is constantly vulnerable to interception, alteration and unauthorised access. Cryptography exists to protect three properties in particular: confidentiality (encrypting data so it can only be read by authorised parties with the proper decryption key), integrity (creating a digital signature or message authentication code to detect unauthorised changes) and authenticity (verifying the sender's identity, via digital certificates or public key infrastructure). It is also used for non-repudiation (ensuring a sender cannot later deny having sent some data), key exchange (securely exchanging keys between parties) and random number generation (used across many security applications).

The Anki notes identify four core types of cryptography that you should be able to name and describe:

- Symmetric Key (Private Key)
- Asymmetric Key (Public Key)
- Steganography
- Random Number Generation

> Steganography is the process of **concealing data within another file** in order to hide its existence and transfer data discretely.

It is worth being precise about the difference between steganography and encryption for the exam: encryption makes data unreadable but obvious (an attacker can see that a secret message exists, even if they cannot read it), whereas steganography hides the very existence of the data — for example, by concealing a message inside the pixel data of an image file, so that an observer would not even suspect a hidden message was there at all. In practice, the two are often combined: a message may be encrypted first and then hidden using steganography, for two layers of protection.

Beyond the four Anki-listed types, the Blended Learning resource identifies two further cryptography techniques worth knowing for a fuller answer:

- **Hash functions:** create a unique digital fingerprint of a file or message to verify its integrity (algorithms such as SHA-256 and SHA-512 are widely used).
- **Digital signatures:** ensure the authenticity of a message's sender. The sender creates a digital signature using their private key, and the recipient verifies it using the sender's public key.
- **Quantum cryptography:** uses the principles of quantum mechanics to secure communication, and is considered more secure than traditional cryptographic methods.

In practice, real systems rarely rely on just one of these techniques — multiple methods are usually combined for a more robust level of security, as you will see in the next section on symmetric and asymmetric encryption.

Symmetric and Asymmetric Encryption

This is one of the most frequently examined pairs of concepts in the whole cyber security topic, so make sure you can clearly explain both — and, crucially, the difference between them.

> Symmetric encryption uses the **same secret key** for both encryption and decryption. Fast and efficient, but the key must be exchanged securely.
>
> Asymmetric encryption uses **2 keys**, one for encryption and one for decryption. The keys are **not identical** and are often referred to as public and private keys. The encryption key is public, but the decryption key is private.

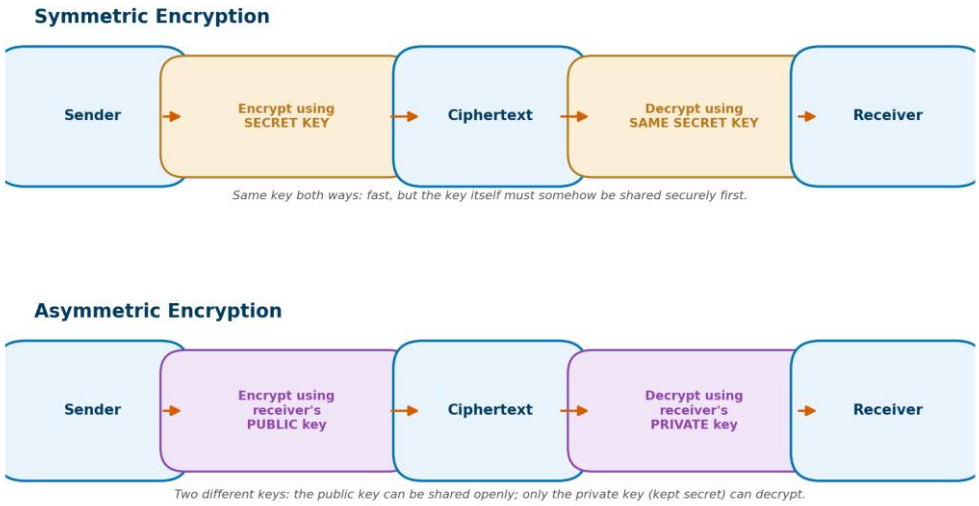

Figure: symmetric encryption (one shared key) compared with asymmetric encryption (a public/private key pair).

Symmetric encryption is fast and efficient because the encryption and decryption process uses only one key — but this creates a genuine practical problem, known as the key exchange problem: the key itself must be shared securely between sender and receiver before communication can take place, and if that key is intercepted in transit, the entire system is compromised. Common examples include AES, DES and Blowfish.

Asymmetric encryption (also called public key cryptography) solves the key exchange problem directly: the encryption key is made public and can be freely shared, while only the decryption key is kept private by its owner. Anyone can use the public key to encrypt a message intended for that owner, but only the owner — holding the matching private key — can decrypt it. The most widely used asymmetric algorithm is RSA.

In practice, both approaches are usually combined rather than used alone: a fast symmetric key algorithm is used to encrypt the actual data, while a slower asymmetric key algorithm is used only to securely exchange that symmetric key between sender and receiver. This gets the best of both worlds — the speed of symmetric encryption for bulk data, and the secure key exchange of asymmetric encryption. Asymmetric encryption is generally considered more secure than symmetric encryption, since it removes the need to

share a secret key at all — but it is computationally more expensive and typically slower, which is exactly why it tends to be used only for the key exchange itself rather than for encrypting large amounts of data.

Contemporary Biometric Technologies

Biometrics is the use of unique physiological or behavioural characteristics to identify individuals, providing a reliable means of identification and authentication that is difficult to forge or imitate. You should be able to describe the following techniques:

- **Fingerprint recognition:** uses unique fingerprint patterns; widely used in mobile devices and laptops.
- **Facial recognition:** uses unique facial characteristics; increasingly used in surveillance and smartphone unlocking.
- **Iris recognition:** uses unique iris patterns; considered one of the most accurate and secure techniques, used in border control and ATM banking.
- **Voice recognition:** uses unique voice characteristics; used in phone-based authentication such as call centres and voice assistants.
- **Signature recognition:** uses unique signature characteristics; used in financial and legal transactions.
- **Behavioural biometrics:** uses unique behavioural characteristics such as typing rhythm or mouse movements; increasingly used as an additional layer of security in online banking.

Biometric authentication provides a high level of both security and convenience, since it does not require users to remember passwords or carry identification cards — this is why its use is increasing across government, healthcare, finance, transportation and consumer devices.

However, capturing, storing and processing biometric data raises real complexities:

- **Data collection:** can be challenging, especially for traits such as iris recognition or vein patterns.
- **Data privacy:** biometric data is personal and sensitive, and could be misused if it fell into the wrong hands.
- **Data security:** biometric data is vulnerable to theft, hacking or other cyber-attack — and unlike a password, you cannot simply 'reset' your fingerprint if it is stolen.
- **Data storage:** requires significant storage space and computational resources, leading to higher costs.
- **Data integration:** integrating biometric systems with existing systems can be complex, requiring specialised expertise and investment.
- **Data accuracy:** can be challenging to process accurately, especially with low-quality or inconsistent data.
- **Data management:** involves complying with privacy regulations such as GDPR, and ensuring data remains up-to-date and accurate.

These technical complexities are matched by real legal and ethical considerations:

- **Data protection laws:** in the UK and EU, GDPR sets strict requirements for biometric data protection and privacy.
- **Consent:** collection requires informed consent — organisations must ensure individuals understand how their data will be used and who has access to it.
- **Data retention:** organisations must comply with laws limiting how long biometric data can be stored.
- **Data sharing:** sharing biometric data between organisations raises further privacy and security concerns.

- **Bias and discrimination:** biometric data and algorithms could perpetuate or exacerbate existing biases, leading to discrimination based on race, gender and other factors.
- **Human rights:** raises ethical concerns around the right to privacy and protection from discrimination.

Advantages of biometric technologies:

- **Increased security:** more secure than traditional passwords or PINs, which can be guessed, stolen or shared.
- **Convenience:** simplifies and streamlines authentication — faster and more user-friendly than typing a password.
- **Reduced fraud:** harder for fraudsters to impersonate someone, reducing fraud and identity theft.
- **Increased accuracy:** more accurate than traditional identification methods, reducing errors.

Disadvantages of biometric technologies:

- **Privacy concerns:** biometric data is personal and sensitive, and can be misused.
- **Technical limitations:** not fool-proof — subject to false rejection errors (a genuine user is wrongly rejected) and false acceptance errors (an impostor is wrongly accepted).
- **Cost:** implementing and maintaining biometric technology can be expensive, especially for smaller organisations.
- **Bias and discrimination:** can perpetuate or exacerbate existing biases in who the system correctly recognises.
- **Dependence on technology:** relying solely on biometrics for authentication can lead to loss of access if there is a technical failure or system breakdown.

Black Hat Hacking, White Hat Hacking and Penetration Testing

> Black hat hacking refers to using technology to **gain unauthorised access** to computers, networks or data with **malicious intent**, often for financial gain.

Black hat hacking is illegal and unethical, typically motivated by financial gain or a desire to cause harm, and involves activities such as stealing sensitive information, spreading malware, and disrupting websites and computer systems.

White hat hacking (also called *ethical hacking*) is the practice of using technology and hacking techniques for the purpose of **improving** security. White hat hackers are security professionals who identify vulnerabilities and weaknesses in a system and report them to the relevant organisation so they can be fixed — helping organisations prevent cyber-attacks from black hat hackers before they happen. Unlike black hat hacking, it is legal and widely accepted as an important tool for improving security; organisations hire white hat hackers to perform security assessments and penetration testing.

Penetration testing (or *pen testing*) is a security testing technique used to evaluate the security of a computer system, network or web application by **simulating an attack**, with the goal of identifying security vulnerabilities and weaknesses and providing recommendations for improvement. It is performed by security experts — penetration testers, or ethical hackers — using a combination of automated tools and manual techniques to test a system's defences, deliberately mimicking real-world attacker methods so an organisation can assess the true effectiveness of its security measures and identify areas for improvement. Penetration testing is an important part of an overall security strategy: it provides valuable insight into an organisation's actual security posture, rather than its assumed one, and helps prioritise where improvements are most needed.

Exam tip: it is easy to confuse white hat hacking with penetration testing, since the two overlap so heavily in practice. Think of white hat hacking as the broad ethical role or philosophy (using hacking skills for good), while penetration testing is one specific, structured activity that white hat hackers carry out — a deliberate, authorised, simulated attack against a named target.

Diagnostic and Tracing Tools

Alongside preventative measures, security professionals rely on a set of diagnostic tools that help them investigate networks, trace the source of problems, and verify who is really behind a connection or a domain.

Tracert (traceroute) is a network diagnostic tool used to **track the path taken by data packets** from a source computer to a destination computer, determining the network route, the number of hops, and the time taken for packets to travel. It works by sending a series of packets with incrementing Time-to-Live (TTL) values to the destination, and measuring the time taken for each packet to reach its destination or be returned as undeliverable. This is useful for troubleshooting network connectivity issues, identifying bottlenecks or failures along a route, and verifying network device configuration.

Whois is a protocol and database system that stores information about **registered domain names** and the associated organisations and individuals — including the domain owner's name and contact information, technical and administrative contacts, and creation/expiration dates. It is used to retrieve information about a domain's owner and to verify the accuracy of registration information, which is useful for resolving domain disputes, verifying authenticity, and determining ownership for security purposes.

IP address masking refers to **hiding or changing a device or network's real IP address** to appear as if it originates from a different location or device, done for privacy and security purposes, or to bypass geographical restrictions. **Impersonating an IP address** means pretending to be another device or network using a false IP address, which can be done for malicious purposes — such as accessing restricted resources, launching cyber-attacks, or other criminal activities. Both IP masking and impersonation can be illegal in many jurisdictions and carry serious consequences, so it is important not to confuse the two: masking your own IP for privacy is broadly legitimate, while impersonating someone else's IP to disguise an attack is not.

Cyber Resilience

> Cyber resilience refers to **the ability of an organisation to withstand and quickly recover** from cyber-attacks, system failures or other security incidents.

This involves having the necessary processes, technologies and people in place to prepare for and respond to cyber threats, minimise the impact of a security breach, and ensure the continued availability of critical systems and data. Note the shift in emphasis from the earlier sections of this topic: prevention is about stopping an attack happening at all, whereas resilience assumes an attack may still succeed despite your best efforts, and asks how quickly and completely the organisation can bounce back.

Consequences of a Cyber-Attack

A successful cyber-attack can affect a company in several distinct ways:

- **Financial loss:** the cost of the attack itself, lost revenue, legal fees, and compensation paid to affected customers.

- **Reputational damage:** loss of trust and credibility with customers, partners and stakeholders, leading to a decline in business and brand value.
- **Legal liability:** legal action or fines for failing to comply with regulations such as data protection and privacy laws.
- **Intellectual property theft:** hackers stealing trade secrets, confidential information or other valuable IP.
- **System downtime:** significant disruption to operations and loss of productivity.
- **Long-term damage:** consequences that can be long-lasting, impacting a company for many years after the attack itself.

Temporary loss of data refers to a temporary loss of access to information due to technical issues such as power outages or system crashes, which can usually be resolved and restored from backups. **Permanent loss of data** refers to the complete and permanent destruction of information that cannot be restored, which can occur due to physical damage to storage devices, deliberate destruction of data, or the permanent failure of a storage device.

Mitigating permanent loss of data involves implementing proper backup and disaster recovery procedures, regularly updating software and systems to prevent cyber-attacks, physically securing storage devices, creating regular backups stored in a secure location, testing the ability to actually restore data from those backups, and implementing access controls and monitoring systems to prevent unauthorised access and destruction of data in the first place.

The impact of damaged or corrupted software can be just as significant as data loss: it can lead to system crashes (the software stops functioning properly), loss of data (the software becomes unable to save or retrieve data), security vulnerabilities (exploitable by malicious actors to gain unauthorised access), inefficient performance (reduced productivity and user frustration), and compatibility issues with other software or hardware. This can, in turn, result in financial loss, reputational damage and legal liability — which is why regular software updates and maintenance, access controls and data backups are considered crucial preventative measures.

A website becoming unavailable — whether through a DDoS attack, technical failure, or any other cause — carries its own distinct set of consequences:

- **Loss of reputation:** a poor user experience leads to frustration and loss of trust; lost business opportunities as users cannot access the site; a damaged brand image perceived as untrustworthy or unprofessional; and decreased search engine rankings from being frequently down.
- **Loss of competitive advantage:** lost market share as users are directed to competitors instead; missed sales and business opportunities; decreased visibility and traffic; and damaged reputation.
- **Legal and social implications:** legal liabilities under UK consumer protection laws if unavailability causes financial loss or harm; breach of contractual obligations; negative press coverage; loss of trust; and a high volume of customer complaints.
- **Financial loss:** lost revenue from inaccessible sales or information; increased costs from fixing technical issues and compensating customers; decreased advertising revenue; decreased search rankings reducing future traffic and revenue; and lost customers turning to competitors.

Resilience Controls to Prevent an Attack

The specification identifies six main categories of resilience control aimed at preventing a cyber-attack from succeeding in the first place:

- **Boundary firewalls and internet gateways:** a boundary firewall monitors and controls incoming/outgoing traffic based on predetermined security rules, acting as a barrier between a trusted internal network and an untrusted external network — helping prevent unauthorised access and protect against malware infections, data theft and hacking attempts. An internet gateway allows the exchange of traffic between an internal network and the internet; using it to prevent cyber-attacks involves implementing firewalls, intrusion detection/prevention systems and VPNs, alongside regular software updates, network segmentation and access control.
- **Secure system configuration:** secure admin accounts, audit trails, account management and regular backups provide multiple layers of protection, reducing the attack surface and increasing visibility — making it more difficult for attackers to succeed, and minimising damage if an attack does occur.
- **Access control:** limiting the number of individuals with access to sensitive data and systems reduces the attack surface, and can be combined with logging and monitoring to detect suspicious behaviour.
- **Malware protection:** detecting and blocking malicious software from infecting a computer or network, via antimalware software, firewalls and other security measures.
- **Patch management:** the process of identifying, acquiring, testing and installing updates to software and operating systems — closing known security vulnerabilities, protecting against new threats as they emerge, and maintaining regulatory compliance.
- **Staff training:** raising awareness of threats so employees can recognise and avoid them, teaching safe computing practices such as strong passwords and avoiding suspicious attachments or links, ensuring compliance with company security policies, and enabling early detection and reporting of suspicious activity.

Resilience Controls to Recover from an Attack

Prevention will never be perfect, so resilience also requires planning for recovery — how an organisation gets back on its feet once an attack has already succeeded:

- **Alternative facilities:** making arrangements for alternative premises, communication methods and facilities as part of Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), so critical operations can continue even if primary locations, communication systems or facilities become subject to a cyber-attack — for example, arrangements for staff to work from an alternative location, or backup phone systems and email servers.
- **Exploring what-if scenarios:** simulating hypothetical scenarios to understand how an organisation would respond to a cyber-attack, and identifying potential weaknesses in existing systems, processes and protocols — helping prioritise response and recovery efforts and improve disaster recovery and business continuity plans before a real attack happens.
- **Regular backups of data:** ensuring critical data can be restored in the event of loss — such as through ransomware or data theft — minimising the impact on operations. Backups should be stored in secure, easily accessible locations, such as off-site data centres or cloud-based storage, and regular backups also help organisations comply with data retention and privacy regulations.

Notice how prevention and recovery controls complement rather than duplicate each other: prevention controls (firewalls, access control, patching, training) reduce the chance of an attack succeeding; recovery controls (backups, alternative facilities, tested response plans) reduce the damage when — not if — one eventually does.

(d) Social Engineering

Every technical defence covered in section (c) can be undermined by a single successful social engineering attack — because social engineering does not try to break through a firewall or crack an encryption key; it targets people directly. This closing section covers the specific techniques attackers use, the UK legal framework that applies to them, and real-world examples across commerce, personal finance and process control.

Social Engineering Techniques

> Social engineering attacks use **deception and manipulation** to trick users into revealing sensitive information or making mistakes that compromise the security of their devices, using techniques such as phone, email or direct contact to gain illegal access to information or devices.

Figure: six common social engineering techniques. All of them exploit human trust or curiosity rather than a technical flaw.

Phishing is a type of cyber-attack that aims to trick individuals into revealing sensitive information — such as passwords, credit card numbers and bank account details — typically through emails, text messages or websites that appear to be from a trustworthy source (such as a bank or well-known company). The attacker often asks the victim to provide personal information and login credentials, or to click a malicious link leading to a fake website designed to steal that information. Phishing attacks are becoming increasingly sophisticated and can be difficult to detect, so it is important to be vigilant with unexpected emails or messages and never provide personal information in response to unsolicited requests.

Vishing (voice phishing) uses voice calls, voicemails or interactive voice response (IVR) systems to trick individuals into revealing sensitive information or installing malware. The attacker typically poses as a representative of a trustworthy organisation, such as a bank or government agency — possibly using caller ID spoofing to make the call appear legitimate — and may use automated systems to make large numbers of calls in a short time, increasing the chances of reaching a victim.

Baiting is a type of social engineering attack where an attacker leaves a physical item, such as a USB drive or CD, in a public place with the intention of tricking someone into taking it and using it on their computer. The

device may appear to contain valuable or interesting information, when in reality it contains malicious software that can infect the victim's computer and steal sensitive information or cause harm. Baiting attacks rely on natural human curiosity to take advantage of a seemingly good opportunity; prevention involves being wary of unexpected or unfamiliar physical items, and never inserting unknown or untrusted devices into a computer or network.

Email hacking refers to the unauthorised access or manipulation of someone else's email account or email messages, done through methods including phishing (a fake email appearing to be from a trusted source, asking the victim to enter credentials or click a malicious link), brute force attacks (automated tools trying multiple username/password combinations until access is gained), and exploiting vulnerabilities in email systems (finding and exploiting weaknesses in the software or infrastructure supporting the email service). Consequences can include theft of sensitive information, the spread of malware, and damage to the victim's reputation; protection involves using strong and unique passwords, being cautious of emails or links from unknown or suspicious sources, and regularly checking for and updating security measures.

Pretexting is a type of attack where the attacker creates a false scenario or cover story to manipulate someone into divulging sensitive information or performing a certain action. In the context of contact spamming, pretexting involves the attacker creating a fake identity, or pretending to be someone else, to trick the victim into opening an email or responding to a message — often mass emails or messages appearing to be from a trustworthy source (such as a bank, government agency or well-known company), containing a request for personal information or a link to a malicious website. The aim is to trick the victim into believing the request is legitimate, in order to obtain sensitive information for identity theft or other malicious purposes. Prevention involves being cautious with emails or messages from unknown or suspicious sources, never providing personal information in response to unsolicited requests, and verifying the sender's identity before responding.

Quid pro quo scams are a type of social engineering attack in which an attacker offers something desirable or valuable to a victim in exchange for sensitive information or access to their computer. The attacker may contact the victim claiming to be a representative of a reputable organisation — such as a technology company or government agency — offering to provide technical support, a software upgrade, or to resolve an issue with the victim's computer, and in exchange asks the victim to grant remote access or provide sensitive information such as login credentials or financial information. Once access is gained, the attacker can install malware, steal sensitive information, or cause other harm. Quid pro quo scams can be difficult to detect and have serious consequences, so it is important to be cautious with unsolicited requests for remote access or sensitive information, and to verify the sender's identity.

Exploiting Digital Footprints

Exploiting passive and active digital footprints involves using information that individuals or organisations have inadvertently made available online to gain unauthorised access to their systems or steal sensitive information.

- **Passive digital footprints:** data or information left behind as a result of online activity, such as website browsing history, social media posts or IP addresses. Attackers can use this to gather intelligence on their targets and construct more convincing phishing scams or social engineering attacks.

- **Active digital footprints:** created when individuals or organisations actively share information online, for example through social media, email or instant messaging. Attackers can use this to build trust with their targets, steal sensitive information, or carry out attacks that are more likely to succeed.

This exploitation is often just one part of a larger cyber-attack campaign, which may use multiple social engineering tactics together. Prevention involves being aware of the information you share online and following good security practices — strong unique passwords, avoiding public Wi-Fi for sensitive activity, and never clicking links from unknown or suspicious sources.

Legal Framework

The UK has several laws that specifically protect against social engineering and wider cybercrime, and you should be able to name and briefly describe each of the following for the exam:

- **The Computer Misuse Act 1990:** makes it a criminal offence to gain unauthorised access to computer systems, through hacking, viruses and other forms of cyber-attack.
- **The Fraud Act 2006:** makes it a criminal offence to carry out deception with the intention of making a gain or causing a loss — social engineering scams such as phishing and vishing are often covered under this Act.
- **The General Data Protection Regulation (GDPR):** enforced by the Information Commissioner's Office (ICO), it requires organisations to protect personal data and report data breaches to the ICO within 72 hours.
- **The Privacy and Electronic Communications (EC Directive) Regulations 2003:** regulates the use of electronic communication services, including email, voice calls and text messages, requiring organisations to obtain consent before sending marketing communications and to provide individuals the option to opt out.

Examples Across Commerce, Personal Finance and Process Control

The specification expects you to be able to discuss the risk of social engineering across three distinct sectors, ideally with a real-world example for each — these three cases are excellent ones to have ready for an extended exam answer.

Commerce

Risk: social engineering attacks targeting retail or e-commerce employees to steal customer data or payment information. Example: the 2017 Equifax breach, in which attackers used social engineering to exploit a vulnerability in third-party software, resulting in the theft of the personal information of millions of customers.

Personal finance and home banking

Risk: attacks targeting individuals to steal login credentials or sensitive financial information. Example: in 2020, a UK man lost £20,000 after falling victim to a scam in which the attacker posed as a bank representative and asked for the victim's login credentials and a one-time passcode, which was then used to transfer money out of the victim's account.

Process control

Risk: attacks targeting employees of critical infrastructure organisations — such as power plants or water treatment facilities — to gain access to sensitive systems or disrupt operations. Example: the 2017

WannaCry ransomware attack targeted the UK's National Health Service (NHS), exploiting a vulnerability in the Windows operating system and spreading through the NHS network, causing significant disruption to patient care.

Across all three sectors, notice the same underlying pattern: the technology involved differs enormously (a third-party software vulnerability, a phone call, an operating system flaw), but in every case it was ultimately a person's trust — an employee's, a customer's, or a member of the public's — that the attacker exploited to get in. This is the single most important idea to take away from this whole topic: cyber security is never just a technical problem, and no amount of firewalls, encryption or antivirus software can fully replace an alert, well-trained human being.

2.3.3 Digital Technology Networks

This is the final topic of Unit 3, and it brings together everything that makes digital technology genuinely 'connected' — the hardware, software and infrastructure that let devices talk to each other, the protocols and standards that make the Internet work as a single global system, the way data physically gets from one place to another, the rise of cloud services, and the mobile networks that now sit in almost everyone's pocket. This is the largest single topic in Unit 3, so it has been split into four clearly defined sections, matching the WJEC specification exactly: (a) Communications Networks; (b) Data Transmission; (c) Cloud Services; and (d) Mobile Technologies.

(a) Communications Networks

A computer network exists to connect devices together so that they can share resources and communicate. To build and maintain a network, an organisation needs three broad categories of component working together: hardware (the physical devices), software (the programs that manage and secure the network), and infrastructure (the larger-scale physical systems that support it all).

Hardware Components of a Network

The specification identifies eight main hardware components that make up a typical network. You need to be able to define each one precisely — exam questions frequently ask you to identify a component from a description of what it does.

> A network router **connects multiple networks** and **directs and controls data packets between them**.
>
> A network switch **provides network connectivity by forwarding data between devices to a specific device**.
>
> A network firewall **monitors, filters and controls incoming and outgoing network traffic**, protecting networks from **external security threats**.
>
> A network hub **allows multiple computers to connect to a single network segment**.
>
> A network bridge **connects separate network segments together**, acting as a single larger network.
>
> A wireless access point **provides wireless connectivity to devices** to access Wi-Fi and the Internet.
>
> A network modem **provides internet connectivity** by **converting digital signals to analogue signals** for transmission over **telephone lines**.
>
> A NIC (Network Interface Card) is a **hardware component in a computer enabling network connection**.

Hardware Component	Core Function
Router	Connects multiple networks and directs packets between them
Switch	Forwards data to the specific device it is intended for
Firewall	Monitors and filters traffic to block external threats
Hub	Connects multiple computers to a single network segment

Bridge	Joins separate network segments into one larger network
Access Point	Provides wireless connectivity to Wi-Fi devices
Modem	Converts digital signals to analogue for telephone lines
NIC	Hardware inside a computer that enables network connection

Table 1: the eight main hardware components of a network, at a glance.

Software Components of a Network

Hardware alone cannot manage a network — it needs software running alongside it to control access, secure traffic, monitor performance and keep the network operating smoothly. The specification identifies eight main software components.

> Network operating systems are **specialised software that manages and controls network resources** for connected computers and devices, enabling **centralised administration**.
>
> Remote access software **allows remote users from different locations to connect to the network**.
>
> Backup and recovery software **provides services to protect and preserve data** in the event of data loss, e.g. real-time cloud saving.
>
> Network security software **protects the network from security threats by preventing unauthorised access and malware** using cyber security software.
>
> Network management software **monitors and manages network hardware components and services**, e.g. configuring router settings.
>
> Communication protocols are the agreed rules that allow devices to exchange data across the network in a consistent, predictable format.
>
> Network performance monitors **measure and analyse network performance, identifying bottlenecks and improving efficiency**.
>
> VPN software **enables secure remote network access while masking the user's information via encryption**.

As part of data transmission specifically, network operating and accounting software offers a wide range of facilities beyond these headline definitions. Resource and application management dynamically allocates computing resources such as CPU, memory and storage based on current and predicted demand, and automates the deployment and configuration of applications. Data security features encrypt data, require credentials such as passwords or fingerprints, and detect and remove viruses and other malicious software. Data storage facilities manage and organise large amounts of data, automatically back it up, and compress it to save storage space and cost. Backup facilities provide recovery from stored backups, encrypt those backups, and can be scheduled to run automatically at set times. Monitoring facilities cover system and resource monitoring, application monitoring, event logging, alerts and notifications, customisable dashboards, network monitoring and cloud monitoring — often integrating with other IT tools such as ticketing systems. Finally, activity management facilities monitor, manage and analyse network activity, giving administrators visibility to detect, diagnose and resolve performance, security and reliability issues, and providing detailed analysis of network traffic patterns to identify bottlenecks and security threats.

Infrastructure Components of a Network

Beyond the individual hardware devices and the software controlling them, a network also depends on larger physical infrastructure — particularly once an organisation scales up to running its own data centre. The specification identifies seven main infrastructure components.

> Network servers **provide centralised resources such as storage, processing and applications for network clients**.
>
> A SAN (Storage Area Network) is a specialised network that **connects servers to data storage devices** at a block-level for high-speed access.
>
> A WAP is a device that **allows Wi-Fi enabled devices to connect to a network wirelessly**.
>
> Data centres are a large network of servers that provide **centralised and secure locations** for storing and processing **large amounts of data**.
>
> Network racks and cabinets are **physical storage units** that are used to **organise and store components of a network**.
>
> Power backup systems **provide backup power to the network hardware** in case of power outage to **maximise uptime**.
>
> Cooling systems **regulate the temperature** in data centres and network racks **to prevent overheating and damage**.

Infrastructure Component	Core Function
Network Servers	Centralised storage, processing and applications for clients
SANs	Connect servers to storage devices at block-level for speed
WAPs	Allow Wi-Fi devices to connect to the network wirelessly
Data Centres	Centralised, secure sites housing large amounts of data
Racks & Cabinets	Physically organise and store network components
Power Backup Systems	Provide backup power to maximise uptime
Cooling Systems	Regulate temperature to prevent overheating

Table 2: the seven main infrastructure components of a network, at a glance.

Network Servers in Detail

A server is a **software or hardware device** that **receives and responds to requests** made over a network. Devices making the requests are the clients. Four types of server appear regularly in the specification: file, print, internet (proxy) and mail servers.

> A file server **provides storage for files shared across the network**, allowing **multiple users to access and store data** in a **centralised location**.

A file server has three main uses:

- Facilitates **file sharing** among users.
- Provides **backup & recovery** capabilities.
- **Access control** for security.

A file server also supports various network protocols such as SMB, NFS and FTP, provides version control (tracking changes and reverting to previous versions), and can be scaled to meet growing storage and processing needs.

> A print server allows **multiple users on a network** to **use the same printer**, **eliminating the need for individual printers** per user.

A print server has three main uses:

- **Manages print jobs**, ensuring correct print order.
- **Provides tracking capabilities**, allowing users to see the print job status.
- **Security features**, ensuring the privacy of documents and prevention of unauthorised access.

A print server can also distribute print jobs across multiple printers to avoid overload, supports protocols such as LPD, IPP and SMB, manages printer drivers, and provides user authentication and access controls.

> An internet (proxy) server **acts as an intermediary between a client and a server**, forwarding responses and requests between them.

The specification identifies five main uses for internet servers:

- **Caching** frequently accessed content to reduce data transmission and improve response time.
- **Filters content** based on pre-determined rules, blocking certain websites.
- **Network security** via the use of a firewall.
- **Bandwidth optimisation** via compression.
- **Remote access.**

A proxy server can also provide anonymity, hiding a user's IP address for safer, more private browsing, and can act as a gatekeeper for Internet access, allowing or denying access based on organisational policy.

> A mail server provides **email services** to users.

The specification identifies five main uses for a mail server:

- **Email storage.**
- **Email delivery and reception.**
- **Virus protection.**
- **User authentication.**
- **Backup and recovery.**

Mail servers also provide spam and virus protection (filtering unwanted or malicious e-mails), mailing list management, and message retrieval via standard protocols such as POP3 and IMAP.

Requirements Analysis for Network Infrastructure

Before an organisation builds or upgrades a network, it must carry out a thorough requirements analysis. This can involve surveys, focus groups or interviews with key stakeholders to identify specific needs, goals and constraints. The process follows a clear sequence of steps:

- Gather **user requirements** (needs, goals, constraints).
- **Evaluate** network requirements (number of users, type of software).
- Determine network **components** (cost, reliability, performance).

- Produce a network **architecture** (how components will be used).
- Create detailed **specifications** (specs for hardware and software).
- Validate & **test**.
- **Finalise** the network.

LAN, WAN, VLAN, WLAN and VPN

Networks come in several distinct forms, distinguished largely by their scale and how devices connect to them. You need to be able to define each of the five network types below and, for LAN, WAN and VPN, weigh up their advantages and disadvantages.

> A LAN (Local Area Network) is a network **covering a small, specific geographic area**, such as a single building.

A LAN operates over a relatively small area — a single building or group of buildings, such as a school or small manufacturing business — usually limited to a few dozen to a few thousand devices. LANs can be secured using firewalls, access controls and encryption, and configured in topologies including star, bus, ring and mesh, using protocols such as Ethernet, TCP/IP and Wi-Fi.

Advantages of a LAN:

- **High data transfer speeds** (10 Mbps to 100 Gbps).
- Generally **cheaper** than other networks.

Disadvantages of a LAN:

- Only covers a **small area.**
- Potential **security risks.**

> A WAN (Wide Area Network) is a network that **spans a large geographical area**, **connecting multiple networks** (such as LANs) together, e.g. a video game network spanning across the entirety of Wales.

A WAN usually covers a large geographic area — a city, country or the entire world — connecting an unlimited number of devices, and typically offers lower data transfer speeds than LANs (a few kilobits per second to several gigabits per second) due to the distances involved. WANs are vulnerable to security threats such as hacking, eavesdropping and man-in-the-middle attacks, and can be configured in point-to-point, star, mesh and hybrid topologies, using protocols such as frame relay, ATM, MPLS and VPN.

Advantages of a WAN:

- Spans a **large geographical area.**
- Connects an **unlimited number of devices.**

Disadvantages of a WAN:

- Generally **more expensive** to implement and maintain.
- **Requires strong security** measures.

> A VLAN (Virtual LAN) is a type of network that **allows multiple isolated networks to exist on a single physical network**.

VLANs have four key characteristics:

- **Logical Segmentation** (their main characteristic).
- Increased **Security.**

- Improved **flexibility.**
- Reduced **broadcast traffic** (by dividing traffic across segments).

VLANs segment a network into smaller logical networks to improve performance, security and management — improving scalability (allowing more devices to be added without physically reconfiguring infrastructure) and reducing network complexity (by reducing the size of broadcast domains). Building a VLAN requires five key components: a switch, router, NICs, cables and network management software.

> A WLAN (Wireless LAN) is a type of LAN that uses **wireless communication** to connect devices within a **small geographic area**.

WLANs have four key characteristics:

- **Wireless connectivity.**
- **Flexibility.**
- **Limited range.**
- **Automatic connection.**

A WLAN uses wireless communication technology to connect devices within a limited area such as a home, small office or campus, giving users the ability to connect to network resources from any location within its coverage area, dynamically connecting and disconnecting as users move. WLANs are standardised through the IEEE 802.11 standard, and rely on WPA/WPA2 encryption and authentication to mitigate the risks of eavesdropping and unauthorised access that wireless signals introduce. Building a WLAN requires five key components: WAPs, a wireless network adapter, a router, cables and network management software.

> A VPN (Virtual Private Network) is a type of network that **allows users to securely access resources over a public network** through **encryption**.

VPNs have four key characteristics:

- **Remote access.**
- **Secure communication.**
- **Tunneling.**
- **Authentication.**

VPNs use tunnelling protocols such as PPTP, L2TP/IPSec or OpenVPN to create a virtual tunnel between the client device and the network, encapsulating transmitted data for an extra layer of protection. VPNs can also be used for network segmentation — allowing different departments or users to access different resources — and are compatible with a wide range of devices, including laptops, smartphones, tablets and servers. Building a VPN requires five key components: a VPN server, client devices, a router, cables and network management software.

Advantages of a VPN:

- Increased **Security.**
- **Remote Access.**
- Increased **Productivity** — access to resources from anywhere, at any time.
- **Cost savings**, eliminating the need for expensive leased lines or dedicated network connections.

Disadvantages of a VPN:

- Potentially **expensive.**

- Decreased **visibility.**
- **Complexity.**
- **Security concerns** — a VPN server can be hacked or compromised, and a VPN is only as secure as the encryption methods it uses.
- **Dependence on third-party hardware**, increasing the risk of outages and the cost of management.

Distributed Networks

> A distributed network is a **decentralised network** of **nodes that work together**. The **operating system** manages and shares resources in the network, so the **user does not have to**.

In a distributed network, the operating system automatically manages and distributes resources to users without requiring manual intervention — for example, if a user wants to access a file on a remote server, the OS automatically manages the communication and data transfer. This enables users to access network resources seamlessly and efficiently, improving productivity. Distributed networks also allow for load balancing and fault tolerance, as the OS can dynamically allocate resources and redirect traffic to other nodes in the event of a failure or overload.

The Benefits of Computer Networks

Beyond the technical detail of how each network type works, the specification expects you to be able to explain why organisations build networks in the first place. These benefits fall into four broad categories.

Efficient use of software and hardware resources: networks enable centralised resource sharing (printers, scanners, storage devices — reducing costs), load balancing (distributing processing load across multiple computers), and improved collaboration and remote access.

Data access and sharing: networks provide centralised data storage, improved data access from any location, data backup and recovery, enhanced data security (via encryption and other measures), and improved data management.

Collaborative working: networks enable improved, real-time, multimedia communication, shared workspaces, remote working, and improved decision-making through collected and analysed data.

Central management and monitoring: networks allow centralised management of users, security and data; improved security through firewalls, antivirus and encryption; centralised backup; user account management; monitoring and tracking of network usage to identify security threats; and remote management of network resources from any location.

The Internet as a Global Communication Network

The Internet is an interconnected network of computers, servers and other devices that communicate using standardised communication protocols, enabling individuals, businesses and organisations worldwide to share information, communicate and collaborate in real time regardless of location. It has enabled entirely new technologies, forms of communication and e-commerce that would not otherwise be possible.

The specification identifies five essential physical components that form the Internet's backbone:

- **Servers** — powerful computers that store and manage data, websites and applications.
- **Data Centres** — secure facilities housing and managing large numbers of servers.

- **Network Routers** — directing data traffic between computers and networks.
- **Fibre Optic Cables** — high-speed data transmission lines connecting data centres, routers and other network parts.
- **Wireless Towers** — structures allowing wireless data transmission via Wi-Fi and cellular networks.

These components communicate using protocols such as TCP/IP, which is covered in detail below.

Internet Standards

> An Internet standard is a **predefined protocol** that should be followed to allow **different systems to interoperate seamlessly**, providing common ground, e.g. HTML or TCP/IP protocols, universal data formats.

Standards are predefined protocols and practices followed when transmitting information, providing common ground for communication between different devices and systems. Two key organisations develop and maintain the standards the Internet depends on.

The W3C (World Wide Web Consortium): focuses on developing standards for the World Wide Web (e.g. HTML, CSS, JavaScript), aiming to ensure the web is accessible to everyone.

The IETF (Internet Engineering Task Force): develops and maintains technical standards for the Internet as a whole, including the Internet protocol (IP), the transmission control protocol (TCP) and the domain name system (DNS).

Working together, the W3C and IETF ensure the Internet remains a stable and secure platform for communication, commerce and innovation, and that it continues to evolve to meet changing user needs and new technologies.

TCP/IP and Packet Switching

> The TCP/IP model is a **four-layer networking framework** that **defines how data is transmitted, routed, and received** across the Internet.

The Internet is a packet switching network built on TCP/IP (transmission control protocol / Internet protocol). A TCP segment — which forms part of the IP data portion of an IP packet — carries fields including the source port number, destination port number, sequence number (of the first byte of data), acknowledgement number (identifying the position of the highest byte received), offset, checkbits (URG/ACK/PSH/RST/SYN/FIN flags identifying the segment's purpose), window size (how much data the destination can receive), checksum, urgent pointer, and options/padding.

> Packet switching is the process of **breaking data down into smaller 'packets' (or datagrams)**, which are **sent independently over a network** to the destination, where they are **reassembled**.

Each network packet's header carries a set of standard fields:

Field	Description
Version	Indicates which version of IP is being used.
Length	Specifies the length of the header in 32-bit 'words'.
Total Length	Indicates the total length of the datagram, including header and data.
Identification	Provides a unique integer that identifies the datagram.

Flags	Manages fragmentation and indicates if this is the last fragment.
Fragment Offset	Specifies the location of this fragment within the entire datagram.
Time to Live	Maximum time the datagram can remain on the Internet (default 255 seconds), preventing packets remaining indefinitely.
Header Checksum	Provides validation of the header.
Source Address	The IP Address the packet came from.
Destination Address	The IP Address the packet is going to.
Options	Network testing and debugging options.

Table 3: the fields that make up a network packet header.

Transporting packets across a packet switching network involves six distinct steps: data segmentation, applying a packet header, transmission, reassembly, error checking and flow control.

> Data Segmentation: **dividing data into smaller units called packets, ranging from hundreds of bytes to a few kilobytes.**
>
> Packet Header: **each packet is given a header, containing information about the packet such as the source, destination, sequence number, and data type.**
>
> Transmission: **packets are transmitted individually over a network using the IP protocol, taking different paths to reach their destination depending on network conditions.**
>
> Reassembly: **when packets reach their destination, they are assembled back into the original form. This is done using the sequence number.**
>
> Error Checking: **the data link layer is checked to ensure the packet is transmitted correctly with no corruption or packet loss.**
>
> Flow Control: **regulates the flow of data between the sender and receiver, moderating network congestion and preventing packet loss**, e.g. TCP's sliding window mechanism.

Figure: a simple network topology, showing core hardware components

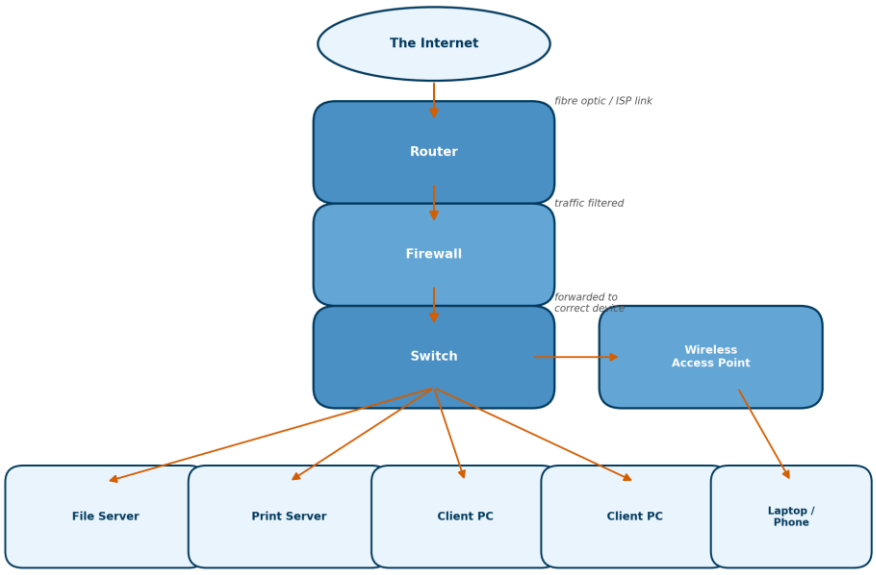

Figure 1: a simple network topology, showing the router, firewall, switch and access point working together.

Routing and DNS

> Routing is the process of **determining the path that an IP packet should take** to reach its destination using its IP address.

The routing process follows a consistent sequence:

- Identifying **Destination IP Address.**
- **Routing Tables** used to identify the pathway.
- Determining the **next hop** towards the destination.
- **Routing protocol** is used to update the routing table.
- **Packet forwarding** occurs to the next hop.

IP routing is essential for the Internet and TCP/IP networks to function, but it carries a number of risks. Security is a concern because routing protocols and tables can be exploited by malicious actors injecting false information to redirect packets — known as a 'routing attack' or 'route hijacking'. Network congestion can occur because routing algorithms may make suboptimal decisions, passing through congested links and increasing delay. Configuration errors are also a risk, since complex routing configurations can easily be misconfigured, causing routing problems. As networks grow, scalability becomes an issue, as routing algorithms must handle large amounts of routing information efficiently — and interoperability can suffer where routing protocols from different vendors are not fully compatible, causing difficulties connecting different parts of a network.

> DNS (Domain Name System) is a **distributed database** whose primary task is to **enable users access to websites and other Internet resources** by **translating IP addresses into human-readable domain names**.

DNS is essentially the Internet's equivalent of a phone book, translating human-readable domain names (such as 'www.wjec.com') into the IP addresses that machines actually use. DNS provides four key functions:

> Load Balancing: **DNS distributes the load of incoming requests across multiple servers by returning multiple IP addresses for a single domain.**
>
> Redirection: **DNS redirects incoming requests from one domain to another, allowing network administrators to control traffic as required.**

- **Authentication.**
- **Service discovery.**

Because DNS is so central to how the Internet functions, it is also a common target for attack. The specification identifies five DNS vulnerabilities:

> Cache Poisoning: **an attacker injects false information into the DNS cache, causing it to return incorrect IP addresses.**
>
> Spoofed Responses: **an attacker sends spoofed DNS responses to a resolver, used to redirect traffic to a malicious site, steal sensitive data or interfere with network operation.**
>
> Zone Transfer Attacks: **an attacker requests a copy of the entire zone file from a DNS server, which contains information about the server's domain names. The information is then used for further attacks.**

> DDoS Attack: **flooding the server with requests so that it becomes overwhelmed and unavailable, making it difficult for users to access the server.**
>
> Name Server Hijacking: **an attacker compromises a DNS server and changes the information stored, allowing them to steal sensitive data or spread malware.**

Some DNS servers can be configured to use cryptographic signatures to authenticate the source of DNS information, which helps prevent cache poisoning attacks specifically.

Environmental Concerns of the Internet

The Internet's infrastructure requires significant power to build and run, and this has a real environmental cost. The specification identifies five key environmental impacts of the Internet:

- **Energy Consumption** — data centres use large amounts of electricity, contributing to greenhouse gas emissions.
- **E-Waste** — electronic waste generated from producing network components.
- **Resource Depletion** — the extraction of finite natural resources, such as rare earth minerals.
- **Water Usage** — required for energy production and electronics manufacturing, potentially causing water shortages.
- **Land Use** — the construction of data centres can destroy natural habitats.

It is essential for organisations to implement sustainable practices — such as using renewable energy, improving cooling efficiency and recycling old hardware — to minimise these impacts.

Selecting an ISP

> An ISP (Internet Service Provider) is a company that **provides Internet access to users** for a monthly fee.

The specification identifies four key factors to consider when choosing an ISP:

- **Speed.**
- **Reliability.**
- **Cost.**
- **Customer Service.**

In practice, these four factors expand into a wider checklist: the desired Internet speed for bandwidth-heavy use or gaming; whether the ISP actually services your location and any coverage gaps; its reputation for network uptime and consistency; pricing plans, installation and equipment rental fees; usage restrictions (data caps); response time and available customer support hours; contract length and termination fees; and any service level agreement guaranteeing network uptime and response times.

(b) Data Transmission

Once a network's components are in place, data still has to physically move between them. This section covers the hardware that moves data around a network in more technical detail, the software that manages and secures that movement, the physical media data travels across (both wired and wireless), and how to calculate how quickly a given file will transfer.

Network Hardware for Data Transmission

You have already met the eight core hardware components in section (a). As part of data transmission specifically, the specification expects a deeper, more technical understanding of how several of these devices actually operate.

Hubs: a hub is a networking device operating at the physical layer of the OSI model, functioning as a central point for transmitting data. When a device transmits data to a hub, it broadcasts the data to every other connected device, regardless of the intended recipient, meaning all connected devices must process the data to determine if it is meant for them. Hubs lack the ability to detect data collisions (which corrupt data if multiple devices transmit simultaneously) and operate at a fixed speed, usually 10 or 100 Mbps.

Switched hubs (switches): an advanced version of a hub offering improved performance, operating at the data link layer. A switch provides dedicated connections between devices for faster transmission and reduced congestion, using address learning to build a table of device addresses so that data is sent directly to the intended recipient rather than broadcast to all devices. Switches also use collision detection, temporarily blocking transmission when two devices try to transmit simultaneously, and typically operate at 100 Mbps to 10 Gbps or higher, with some models including port security features.

Routers: routers forward data packets between computer networks, using routing tables and protocols to determine the best path and prevent loops. They receive packets, store them in memory, examine the destination address, consult the routing table, and send the packet to the next device along the best path. Routers exchange information with other routers using routing protocols to keep their tables updated, and can be configured to block or filter certain types of packets.

Repeaters: a repeater extends the range of a network by receiving a weak or degraded signal, amplifying it, and retransmitting it. Repeaters can support multiple devices and are typically transparent to the devices on a network — meaning devices are unaware a repeater is even present.

Wireless access points (WAPs): WAPs enable devices to connect to a wireless network using radio waves, with the range and strength of the signal depending on the WAP's specifications and the surrounding environment. WAPs can be strategically placed throughout a building to extend wireless range.

Media converters: media converters convert signals from one type of physical medium to another (e.g. copper to fibre optic), can convert between different data rates (e.g. fast Ethernet to gigabit Ethernet), and can extend network distance by allowing a signal to continue over fibre optic cable.

Firewall Software and Appliances

> A firewall is a **network security system** that **monitors and controls network traffic** based on **predetermined security rules**, creating a barrier between a trusted internal network and an untrusted external network.

A firewall can perform four key tasks:

- **Traffic filtering** — examining and blocking/allowing traffic based on defined rules.
- **Packet inspection** — inspecting the header and payload of individual packets against security rules.
- **Network address translation (NAT)** — translating internal device addresses to a single external address, hiding devices behind the firewall.
- **Intrusion detection & prevention** — detecting and preventing threats such as malware, viruses and unauthorised access attempts.

Firewalls can also provide a centralised management interface, allowing administrators to monitor and configure the firewall's rules from a single location, whether the firewall exists as software running on a device or as a dedicated physical appliance sitting at the edge of a network.

Wired Contemporary Communication Infrastructures

Data does not just travel wirelessly — a great deal of network traffic, especially within buildings and between data centres, still travels along physical cabling. The specification identifies three types of wired communication infrastructure.

> UTP (Unshielded Twisted Pair) cables have **no metal shield around the twisted wires**, making them **light and flexible**. Cheap and can transmit data at speeds of **up to 10 Gbps**.

UTP cables are widely used in modern communication networks because they are relatively cheap and easy to install, transmitting data at speeds up to 10 Gbps over short distances.

> STP (Shielded Twisted Pair) cables have **a metal shield around the twisted wires** to protect against electromagnetic interference (EMI). More expensive and less flexible than UTPs, but offer better protection.

STP cables are typically used in environments with high levels of electromagnetic interference, such as industrial settings or near high-voltage electrical equipment.

> Fibre optic cable is a type of cable used to transmit data **using light**, consisting of a glass or plastic fibre core with a protective coating.

Fibre optic cabling has three key advantages over copper cable:

- **Higher Bandwidth.**
- Better for longer **Distances.**
- Immune to electromagnetic **Interference.**

A fibre optic cable's core is designed to transmit light in the form of pulses, and is used extensively in telecommunications, internet connectivity and data centres. Fibre optic cables usually consist of a bundle of individual fibres, used in single-mode and multi-mode applications, and are generally more reliable, secure and efficient than copper cables for transmitting data over long distances.

Wireless Contemporary Communication Infrastructures

Alongside wired infrastructure, four wireless communication methods make up the specification's coverage of contemporary infrastructure — each suited to a different range and use case.

Radio waves: radio waves have longer wavelengths, can easily penetrate walls and obstacles, and are used for both indoor and outdoor communication, including broadcast radio, television, mobile phones and Wi-Fi.

Infrared: infrared has shorter wavelengths, is not visible to the human eye, and is used for short-range communication such as remote controls. Unlike radio waves, infrared cannot penetrate walls.

Microwave: microwave has shorter wavelengths than radio but longer than infrared, used for both short- and long-range communication including microwave ovens, cell phone towers and satellite communication. It can penetrate walls to a limited extent.

Satellite: satellite communication uses satellites orbiting the Earth to communicate with each other and with ground devices, used for global communication and navigation such as GPS and satellite television. It is extremely reliable with broad global coverage, but signal can be disrupted by the Earth's atmosphere.

Calculating Transmission Speed

The transmission speed of a file — and, more usefully, the time it takes to transfer — can be calculated using a formula relating file size to transfer rate:

Transfer time = file size ÷ transfer rate

Worked example (as given by WJEC): a 4GB file is transferred via wireless transmission at a transfer speed of 100 Mbps.

File Size	Transfer Speed	Transfer Time
4GB	100 Mbps (wireless)	40 seconds

Worked example: calculating file transmission time. Always convert file size and transfer rate to matching units (e.g. both in megabits) before dividing.

In an exam question, always check carefully what units you have been given — file sizes are usually quoted in bytes (GB, MB), while transfer speeds are usually quoted in bits (Mbps, Gbps) — and convert both to the same unit before applying the formula. Four key factors affect the real-world transmission speed and delivery time of a file: congestion, latency, file size and file type. To improve the end-user experience, it may be necessary to optimise these factors or provide alternative methods of file transfer, such as compression or streaming.

(c) Cloud Services

Cloud services have transformed how individuals and organisations store, access and process data, moving much of the responsibility for infrastructure away from the customer and onto third-party providers. This section covers how data is protected and managed within the cloud, how cloud services actually work, their advantages, disadvantages and environmental impact, the three main service models, the three ways cloud services can be delivered, and where the future of cloud computing is heading.

File Synchronisation, Backup and Archive Systems

Before looking at cloud services in general, it is worth distinguishing between three closely related systems for managing files over time, each of which can be run locally through an organisation's own infrastructure or through cloud services.

File synchronisation systems: keep the contents of two or more folders or devices identical in real time, so that a change made on one device is automatically reflected on the others.

File backup systems: create a copy of important files and data at a specific point in time for recovery purposes in case of data loss.

File archive systems: store files that are no longer needed day-to-day but may need to be accessed in future. These files are usually compressed and stored in a way that minimises space usage while still allowing easy retrieval.

How Cloud Services Work

Cloud services are a wide range of services delivered on demand to organisations and customers over the Internet by third-party service providers, via remote servers accessible from anywhere with an Internet connection. They provide access to a shared pool of computing resources — servers, storage, applications and services — that can be easily scaled up or down as needed.

When a user accesses a cloud service, their request is routed to the appropriate server and the data or application is returned over the Internet. The user typically pays on a subscription or pay-per-use basis, with the provider managing the underlying infrastructure and ensuring availability and security. Well-known examples of cloud service providers include web-based e-mail (Gmail), file storage and sharing (Dropbox), and SaaS applications (Microsoft Office 365).

It is important to distinguish cloud computing from cloud storage, as the two terms are often confused. Cloud computing involves the delivery of a wide range of computing services over the Internet — which may include cloud storage, but also processing power, software and much more. Cloud storage refers specifically to the storage of data on remote servers, and is only one part of what cloud computing offers.

Advantages and Disadvantages of Cloud Services

Advantages of Cloud Services:

- **Scalability** — quickly and easily adding or removing computing resources.
- **Flexibility** — accessing resources from anywhere with an Internet connection, using any device.
- **Cost-effective** — pay-as-you-go pricing so users only pay for the resources they use.
- **Easy to set up** — most infrastructure and maintenance is handled by the provider.

Disadvantages of Cloud Services:

- **Reliance on Internet** connectivity — a problem in areas with poor or no connectivity.
- **Security concerns** — storing data on remote servers, especially sensitive or confidential data.
- **Ongoing costs** — subscription and usage charges can add up significantly over time.
- **Limited control over infrastructure** — a problem for organisations with specific security or compliance requirements.

Environmental Impact of Cloud Services

The specification identifies four key environmental impacts of cloud services:

- **Energy consumption** — cloud servers require large amounts of energy to power and cool equipment, contributing to greenhouse gas emissions.
- **Carbon emissions** — the energy used to power cloud servers is often generated from fossil fuels.
- **E-waste** — the rapid growth in cloud computing is increasing the volume of electronic waste.
- **Water usage** — data centres require significant water for cooling, a growing concern in water-scarce areas.

Beyond these four, cloud services also raise land use concerns, since data centres require large amounts of land and can contribute to deforestation and other environmental damage.

SaaS, IaaS and PaaS

> SaaS (Software as a Service) is a **cloud computing model** where the **3rd party service provider hosts software applications**, making them available to users over the Internet.

SaaS users do not install and run software on their own computers or servers — instead they access it through a web browser or mobile app, typically on a subscription or pay-per-use basis, with the service provider managing the underlying infrastructure (servers, storage, networking). Well-known examples include Google Workspace, Salesforce and Asana.

> IaaS (Infrastructure as a Service) is a **3rd party service** provided through **cloud services**, offering **virtualised computing resources** over the Internet, e.g. access to servers, storage, and networking infrastructure.

IaaS gives users access to servers, storage, networking and other computing infrastructure to build, deploy and manage their own software applications and services, with complete control over the computing environment — the operating system, middleware and applications. Users can create, manage and delete virtual servers as needed without investing in physical hardware. Well-known examples include AWS, Microsoft Azure and Google Cloud Platform.

> PaaS (Platform as a Service) is a cloud computing model where a **3rd party service offers a platform** enabling developers to build, deploy and manage **their own applications** over the Internet.

PaaS gives developers access to a complete development and deployment environment — tools, frameworks and services — with the provider managing the underlying infrastructure, providing pre-built components, application templates and automated deployment processes, plus additional services such as databases and application monitoring. Well-known examples include Heroku, Microsoft Azure App Service and Google App Engine.

The exam expects you to be precise about who manages what under each model: under IaaS, the customer manages the operating system, runtime, applications and data; under PaaS, the customer manages only their applications and data; and under SaaS, the customer manages just their data and settings, with the provider handling everything else.

Model	Customer Manages	Provider Manages
IaaS	Operating system, runtime, applications, data	Servers, storage, networking (physical infrastructure)
PaaS	Applications and data only	OS, runtime, middleware, servers, storage, networking
SaaS	Data and settings only	The entire application and all underlying infrastructure

Table 4: IaaS vs PaaS vs SaaS — what the customer is responsible for managing at each level.

Public, Private and Hybrid Cloud Delivery

Cloud services are delivered over the Internet by third-party providers who own and manage the underlying infrastructure, offering computing power, storage, networking and software applications that customers access on demand. The specification identifies three ways in which cloud services are provided.

> A public cloud is owned by 3rd party providers, and **resources are shared amongst multiple users** over the Internet.

Public cloud uses a multi-tenant architecture where multiple customers share the same physical infrastructure, separated via virtualisation for security and isolation. It offers high scalability, flexibility and cost-efficiency, with access to the latest technologies without customers having to invest in their own hardware. Well-known examples include AWS, Microsoft Azure and Google Cloud Platform.

> A private cloud is **dedicated to a single organisation**, offering exclusive access to resources. Can be hosted by a 3rd party but on a **private network**.

A private cloud is delivered using virtualisation and cloud management technologies deployed on dedicated hardware within an organisation's own data centre, or a service provider's data centre. This gives the organisation complete control over infrastructure dedicated to its own use, ensuring high levels of security and data privacy — it can be deployed on-premises or hosted by a third party, with deployment models such as dedicated private clouds or virtual private clouds. Well-known examples include VMware, Dell Technologies and IBM.

> A hybrid cloud environment **combines public and private cloud environments**, allowing data and applications to move between them.

In practice, organisations can run some workloads on-premises in a private cloud while using public cloud services for others — for example, using the public cloud for customer-facing applications while keeping sensitive internal applications on a private cloud, connected via a hybrid cloud management platform. A hybrid cloud offers increased flexibility, scalability and cost-efficiency with a higher level of control and security than public cloud alone, but can be more complex to manage. Well-known examples include AWS Outposts, Microsoft Azure Stack and Google Anthos.

The Future of Cloud Services

Cloud-based content collaboration services, such as Microsoft SharePoint, Google Drive and Dropbox, are likely to become more integrated and connected with project management tools and communication platforms, and more intelligent and automated using machine learning — for example, automatically tagging and categorising documents, or suggesting relevant content based on preferences.

Cloud-based access control solutions — multi-factor authentication, role-based access control, identity management — are likely to become more advanced using AI to provide intelligent, context-aware access control based on user behaviour. Cloud-based application delivery management solutions, such as load balancing, content caching and application acceleration, are likely to use AI to optimise delivery based on user behaviour, automatically routing traffic to the nearest and fastest data centre and addressing performance issues before they impact end users.

Finally, cloud-based virtual desktop solutions, such as Amazon WorkSpaces, Microsoft Azure Virtual Desktop and VMware Horizon Cloud, are likely to use AI to optimise the end-user experience, automatically adjusting display resolution and quality based on network conditions.

(d) Mobile Technologies

Mobile technology is arguably the most rapidly evolving area of this entire specification. This final section covers the wider impacts of mobile technology's proliferation, how mobile networks actually locate and connect to individual devices, the signalling protocols and identifiers that make mobile communication possible, the evolution of mobile network generations from 2G to 5G, and what the future may hold.

Impacts of the Proliferation of Mobile Technology

The specification identifies four broad impacts of the rapid increase in mobile technology use:

- **Social impacts.**
- **Accessibility to information and services.**
- **Health impacts.**
- **Privacy concerns.**

In more depth, the social impacts of mobile technology include changes in social behaviour — how people interact, consume information, and engage in social and political activism — alongside improved access to information and services, particularly in areas with limited infrastructure. There is also an economic impact, with new industries and job opportunities emerging in app development and device manufacturing. Health impacts can be both positive (improved access to healthcare) and negative (increased sedentary behaviour and addiction), while privacy and security concerns centre on the collection and use of personal data by companies and governments.

Mobile technology's rapid growth also carries several environmental impacts:

- **Energy consumption** — operating cell towers and data centres requires significant energy, contributing to carbon emissions.
- **Electronic waste** — from the production and disposal of mobile devices and infrastructure.
- **Land use** — construction and maintenance of mobile infrastructure can cause deforestation and habitat fragmentation.
- **Water use**, particularly for cooling data centres.
- **Resource extraction** — production requires extracting natural resources such as rare earth metals, causing pollution and habitat destruction.

Mobile Phone Masts, Cells and Handoffs

> Mobile phone masts work by **transmitting and receiving radio waves between a mobile device and mobile network**. The towers receive a signal from the mobile device, which sends the same signal to the nearest tower to the recipient's device via **copper cabling**, which then sends it to the recipient.
>
> Cellular networks (cells) work by **dividing a geographic area into smaller areas called cells**, which are each served by **base stations** to communicate with devices.
>
> A mobile handoff is the process of **transferring a device's communication from one cell to another** as the device moves its location, ensuring the communication is **uninterrupted and the transfer is seamless**.

The Base Station Controller (BSC)

> A BSC (Base Station Controller) is a key component of a cellular network, **controlling multiple base stations within each cell**. The BSC **acts as an intermediary** between devices and the mobile network.

Connecting a mobile device to the mobile network involves five steps managed by the BSC:

> Call Setup: **the BSC allocates a unique ID to the device (called a TMSI) and a traffic channel (TCH), where the call goes through.**
>
> Call Routing: **the BSC selects the appropriate BTS (base transceiver station) for the cell.**
>
> Handoff Management: **the BSC coordinates handoffs if the device moves from one BTS to another.**
>
> Call Control: **the BSC provides real-time call control, such as call forwarding or waiting services.**
>
> Performance Management: **the BSC monitors the performance of the BTSs to ensure upmost efficiency.**

Identifying Mobile Devices: IMEI and IMSI

> An IMEI (International Mobile Equipment Identity) is a unique **15-digit number** assigned to each mobile device, used to **identify the device on the network**.
>
> An IMSI (International Mobile Subscriber Identity) is a **15-digit unique identifier** assigned to each mobile device's SIM card on a network.

An IMSI is itself made up of three separate parts:

> MCC (Mobile Country Code): **3-digit code identifying the user's registration country.**
>
> MNC (Mobile Network Code): **a 2 or 3-digit code identifying the mobile network operator.**
>
> MSIN (Mobile Subscription Identification Number): **a 10-digit number identifying the user on the network.**

Signalling Protocols: SIP, SS7 and IPv6

> SIP (Session Initiation Protocol) is a **stateless signalling** protocol used for setting up real-time communication like Voice Over IP (**VoIP**) and media streaming.
>
> SS7 (Signalling System 7) is a protocol suite used for **signalling and controlling communication services** in telecommunication networks, including mobile networks.

Advantages of SS7:

- **High speed connection.**
- **Efficient.**
- **Supports various communication services.**

Disadvantages of SS7:

- **More complicated switches.**
- **Potential security issues.**

> IPv6 is the latest version of the Internet protocol, providing a **larger and more flexible address space** to accommodate the growing number of mobile devices and applications requiring network connectivity.

IPv6 addresses the limitations of IPv4, which has a limited 32-bit address space unable to accommodate the growing number of mobile devices. IPv6 instead has a 128-bit address space, providing trillions of unique addresses. IPv6 also supports improved security and quality of service (QoS) mechanisms, and features supporting seamless mobility, allowing mobile devices to maintain network connectivity as they move across different networks and locations.

Stateful and Non-Stateful Communication

Mobile communication can be classified as either stateful or non-stateful, depending on whether a persistent connection is maintained between the device and the network.

Stateful communication: requires establishing a persistent session between the mobile device and the network, where session information (the status and context of the communication) is stored on the device and network and updated as communication progresses, remaining open until one endpoint terminates the connection.

Non-stateful communication: does not require a persistent session — communication is managed through individual packets of data, each containing all necessary information to route it to the destination, sent independently of other packets. A well-known example of non-stateful communication is SMS (short message service).

The Mobile Switching Centre and the PSTN

The mobile switching centre (MSC) is a core component of a mobile network, responsible for routing voice calls, SMS and data between mobile devices and other parts of the network. It provides connectivity between mobile devices and the public switched telephone network (PSTN) and other mobile networks, and manages the mobility of subscribers as they move between cells or locations.

When a call is made from a landline or another mobile phone to a mobile device, the call is routed through the PSTN to the MSC, which uses the mobile device's unique identifier to locate it and route the call to the appropriate cell or base station. When a mobile device initiates a call, the MSC checks whether the device is authorised, then establishes the connection to the PSTN. SMS messages and data transmissions follow a similar process, with the MSC serving as a gateway between the mobile network and the PSTN.

The History and Evolution of Mobile Technology

Mobile technology has evolved through a series of distinct generations, each bringing significantly faster speeds and new capabilities. In 1973, the first mobile phone was invented by Motorola — large and expensive, and not widely available. In the 1980s, the first analogue cellular networks were launched. In the 1990s, the first digital cellular networks were introduced, offering better call quality and data transfer speeds; GSM became the dominant standard in Europe, while CDMA was adopted in the US and other regions.

In the early 2000s, the first 3G networks were launched, offering faster data transfer speeds and enabling video calls and mobile Internet browsing. The late 2000s saw widespread smartphone adoption, led by the launch of the iPhone in 2007, bringing touch screens, app stores and high-speed Internet access. In the 2010s, 4G LTE networks became the standard, providing faster speeds and enabling mobile video streaming and augmented reality. In recent years, 5G technology has promised even faster speeds, lower latency and

more reliable connectivity, alongside the growth of the Internet of Things (IoT) and innovative form factors such as foldable phones.

> GPRS (General Packet Radio Service) uses **packet switching technology**, which enables data to be transmitted in **small packets over a GSM network** rather than in a continuous stream.

GPRS delivers data at speeds of up to 114 kbps, suitable for moderate data use such as e-mail and web browsing, and provides an 'always-on' Internet connection that is widely available and compatible with many device types.

Edge: provides faster data transfer rates than the original GSM network (up to 384 kbps), is backwards compatible with GSM networks, and uses more efficient modulation schemes to transmit more data within the same spectrum. Edge also provides improved voice quality with less background noise, and has widespread coverage that makes it popular for global roaming.

3G: provides faster data transfer rates than 2G (144 kbps to 2 Mbps), improved network capacity for more simultaneous connections, and supports multimedia applications such as video streaming, video calls and mobile TV. 3G also provides global roaming capabilities and enhanced security features — encryption and authentication — to protect user data.

4G and LTE: provide significantly faster data transfer rates than previous generations, with LTE peak download speeds of up to 1 Gbps. 4G offers low latency, support for high-quality voice and video calling and streaming of high-definition content, and more efficient modulation and multiple access schemes. It provides seamless connectivity between different networks (Wi-Fi, cellular, broadband), backwards compatibility with 3G and 2G networks, and advanced security features.

5G: provides significantly faster data transfer rates, with peak download speeds of up to 20 Gbps, and very low latency. 5G supports connecting many IoT devices with low power consumption and extended battery life, and can be divided into multiple virtual networks for customised service offerings and efficient resource use. Its high-speed data transfer enables new applications such as virtual and augmented reality.

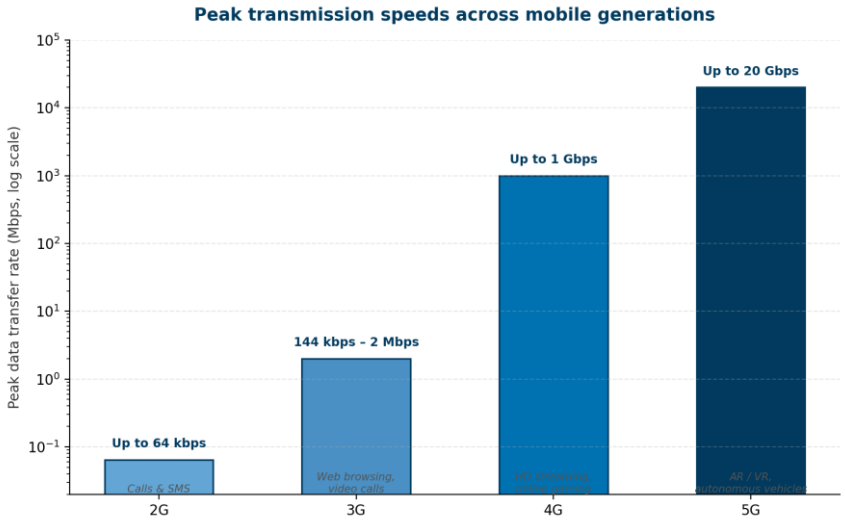

Figure 2: peak transmission speeds across mobile generations, from 2G to 5G.

The specification also identifies two further wireless transmission concepts, alongside the mobile generations above:

> Wideband: **wireless systems that operate at a wider frequency range than a conventional narrowband system, allowing for more data transmission in a given amount of time.**
>
> UWB (Ultrawide Band) provides **very high data transfer rates** (up to 1 Gbps), and requires **very little power** to operate, making it well-suited for IoT devices.

UWB is usually used for short-range wireless communication, such as wireless USB and wireless sensor networks, and can also be used for precise location tracking — including asset tracking and indoor navigation.

The transmission speed and typical uses of each mobile generation can be summarised as follows:

Generation	Transmission Speed	Typical Uses
2G	Up to 64 kbps	Sending text messages, making voice calls
3G	144 kbps to 2 Mbps	Web browsing, video streaming, video calls
4G	Up to 1 Gbps	High-quality video streaming, online gaming, large file downloads
5G	Up to 20 Gbps	Augmented reality, virtual reality, autonomous vehicles

Table 5: transmission speed for each mobile generation. Actual data transfer rates may vary depending on network conditions, device capabilities and other factors.

The Future of Mobile Technology

The future development of mobile technology is likely to be driven by consumer demand, technological advancement and market trends. Several developments are already emerging, or being actively researched.

- **Borderless technologies** — no-bezel or very thin-bezel devices, allowing larger screens in smaller form factors and a more immersive user experience.
- **'Transparent' phones** — research into transparent screens, allowing unique futuristic designs and new user experiences.
- **Chip phones / 'bionic interface' devices** — mobile devices becoming smaller and more integrated with the human body, such as implanted chip phones, allowing seamless communication without holding a device.
- **Foldable phones** — already on the market, with room for improvement in durability and design.
- **Augmented reality (AR) and virtual reality (VR)** — already used in mobile apps and games, with potential to become far more mainstream.
- **Artificial intelligence (AI) and machine learning (ML)** — already used in mobile applications, with potential to become more sophisticated and integrated.