

Digital IT

Component 3 Learning Aim B Cyber Security- B1 Threats to Data Why Systems are Attacked

Key Vocabulary	
Intellectual Property	An idea that you invented that belongs to you, for example, an image that is copyrighted.
Ransomware	A form of malware , usually infecting unprotected digital systems, occurring when users open malicious email attachments.
Malware	A malicious form of software that is transferred to, and then executed on, a user's machine to damage or disrupt the system or allow unauthorised access to data.
Denial-of-Service (DoS) attacks	Attack a remote computer by making it unable to respond to legitimate user requests.
Cybersecurity	The combination of policies, procedures, technologies and the actions of individuals to protect from both internal and external threats.

Organisations have become reliant on digital systems to hold data and perform vital business functions. Many organisations have their digital systems attacked daily. The reasons these attacks may occur are varied

Industrial Espionage
Intellectual property (designs, business strategy etc) can be stolen through organised cyberattacks. These types of assets can be highly valuable, leading to cheaper, fake copies of products being sold and the original organisation suffering a loss of income.

Financial Gain
A very simple motive: money. Extorting money from victims of a cyberattack is common practice.

Personal Attack
The most common type of personal attack is made by ex-employees holding a grudge against their former employer, perhaps feeling they have been unfairly treated or suffered a form of emotional distress.



Data and information theft
Data and information both have value as they can be sold for financial gain. This can be done by stealing customer payment information and then using it to purchase goods illegally. Breaches of data and information are a major cause of identity theft.

Fun/ Challenge

- Hackers may attack systems for the thrill, adrenaline rush or a sense of personal achievement.
- They may view increased security as a technical challenge and enjoy trying to get past it.
- They may also get recognition from their peers when they successfully hack into systems.

Disruption
Any attack that prevents an organisation from operating normally causes operational chaos, loss of earnings and reputational damage. Disruption can be caused in many ways e.g. defacing a website or **Denial-of-service (DoS) attacks**
Motivations may be: financial/social/political reasons.

Component 3 Learning Aim B Cyber Security- B1 Threats to Data External Threats to Digital Systems and Data Security

Key Vocabulary

Social Engineering	The act of getting users to share sensitive information through a false pretext (commonly known as 'blagging')
Phishing	A cyberattack that sends spam messages to try and trick people to reply with desired information.
Pharming	A cyberattack that uses malware to direct a user to a fake website that requests information.

External attack methods include:

- Unauthorised access/hacking
- Phishing
- Pharming
- Man-in-the-middle attacks

Pharming

A type of cyber attack

User is directed to a fake website thinking it is real and they then enter confidential details such as usernames and passwords.

The cybercriminal uses these captured details to log into the real website and commit illegal acts e.g. withdrawing money, purchasing goods, downloading personal files or sending fraudulent emails

Unauthorised access/Hacking:

'Black-hat' hacking - users attempt to gain access to remote systems without permission from the owners to do so legally

'White hat' or ethical hacking - Hacking legally performed by paid specialists who are testing the security systems for a company is called

'Grey hat' hacking - hackers test security without permission, but don't exploit any vulnerabilities for personal gain.



Man in the Middle Attacks

A form of cyberattack where the communication between 2 devices, such as a user and a web server, is intercepted and potentially tampered with.

Encryption can protect against this form of hacking as any intercepted data cannot be easily used. Cybersecurity specialists also suggest that users would be safer if they did not use Wi-Fi.

Phishing

A form of social engineering and a very common form of cyberattack.

Spoof emails are sent that pretend to be from a genuine company.

The user is fooled into thinking its from a legitimate source. Usernames, passwords and credit card numbers are the most commonly captured personal information.

These can then be sold for profit to other criminals or users to illegally purchase goods or services.

Spear phishing is an attack targeting specific organisations or individuals.

Component 3 Learning Aim B Cyber Security- B1 Threats to Data Internal Threats to Digital Systems and Data Security

Key Vocabulary	
Productivity	a measure of effectiveness - how long it takes an employee to produce an item for sale.

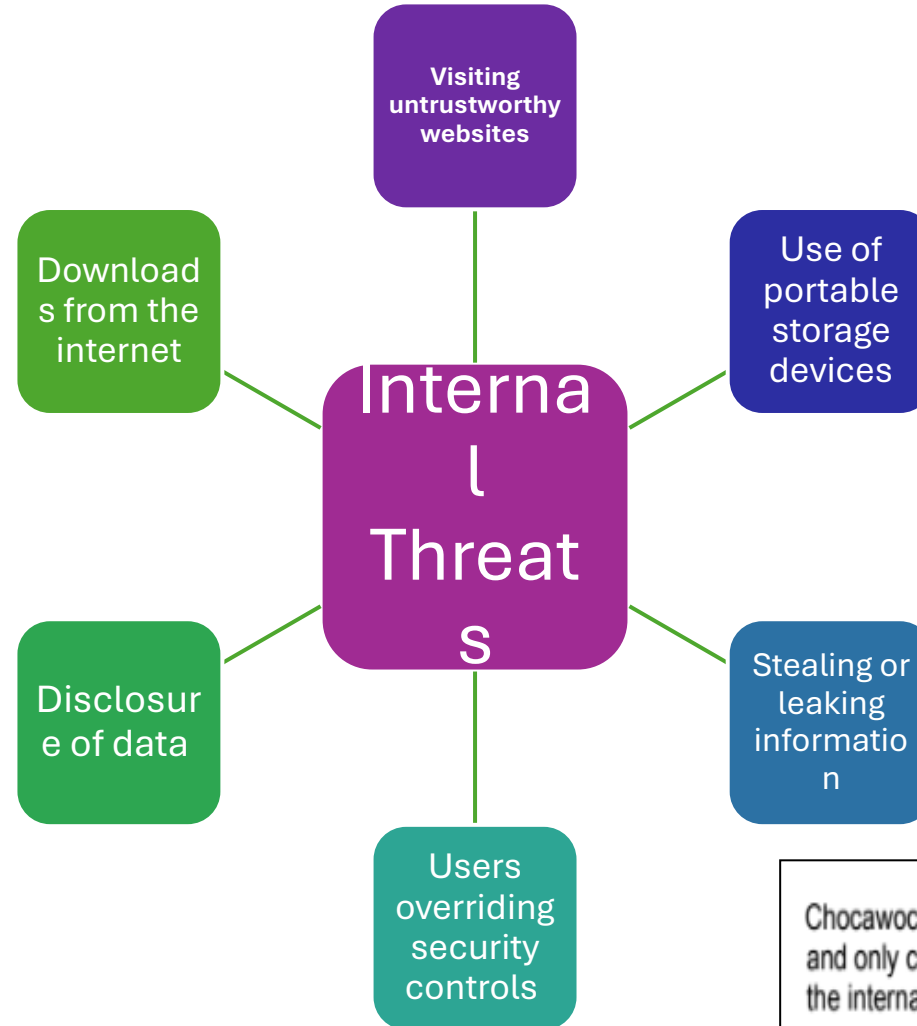
Internal Threats

Some internal threats happen because of accidents, mistakes or poor choices made by an organisation's employees. However, a disgruntled employee could do something malicious.

For example:

- Delete customer records
- Steal confidential information
- Create fake invoices that will be paid to their own bank account
- Install malware

Protecting an organisation against internal threats is as important as protecting against external ones.



Impacts of security breach	
Immediate Impacts	Longer-term Impacts
<ul style="list-style-type: none"> •Data loss •Lost sales •Downtime •Reduction in productivity 	Damage to the organisation's public image which could lead to: <ul style="list-style-type: none"> •Financial loss •Potential legal action

Example Exam Question

Chocawoca's recipes are kept on secure servers in their secret recipe rooms and only certain staff have access to these recipes. They are concerned about the internal threats to this vital data.

(b) Explain **two** possible internal threats to Chocawoca's recipes.

Component 3 Learning Aim B Cyber Security- B2 Prevention and Management of Threats to Data User Access Restriction

Physical Security

Benefits	Drawbacks
Act as a deterrent and deter attackers.	Often more expensive to purchase
Stop attackers from gaining direct and physical access to locations where data is stored.	Building work may be required.
Automatically and secretly call the police if an attacker is detected,	Some methods of physical security, such as CCTV, do not stop data from being stolen

Example Security techniques:

- Electronic Swipe Lock
- Secure Device
- CCTV Camera

Passwords

The use of passwords is a traditional security measure to control access to digital systems.

There are other forms of passwords:

- Patterns that can be drawn connecting a series of dots
- Gesture passwords - can be used with touchscreen devices where the user draws a shape.

Benefits	Drawbacks
<ul style="list-style-type: none"> • They are simple and easy to use. • There are no costs involved as they require no specialist hardware to setup. 	<ul style="list-style-type: none"> • They are only effective if users keep their passwords secret. • A strong password can be hard to remember. • Specialist software can be used by attackers to try and guess the user's passwords. • Users can find it hard to remember lots of different passwords.

Requires individuals to use part of their body to prove their identity.

- Common biometric examples include:
- Eye (retina or iris pattern) scan
- Fingerprint identification
- Hand geometry (shape of user's hand)
- Voice analysis
- Facial recognition
- Gait analysis (how a user walks)
- Handwriting analysis

Benefits	Drawbacks
<ul style="list-style-type: none"> • Users don't need to remember lots of different passwords or keep updating them. • More secure as they cannot be guessed, lost or forgotten. • Can take less management because users are less likely to be 'locked out' or need to have their user accounts reset. 	<ul style="list-style-type: none"> • More expensive as you need specialist hardware devices to set them up. • They can easily spread germs, e.g. if lots of users are using the finger print scanner then germs can be easily spread. • Some users may feel that it is an invasion of their privacy by having their biometric data stored.

Two-factor Authentication

A popular form of multifactor authentication and is used when just a password or PIN is not considered sufficient.

It works by asking the user to supply two forms of identification.

Benefits	Drawbacks
<ul style="list-style-type: none"> • It is more secure. • No extra equipment is needed as users can use items they already have to authenticate themselves, e.g. their mobile phones. 	<ul style="list-style-type: none"> • It is possible that some factors may get lost e.g. you may lose your swipe card. • The recovery options that are used to reset your account are easy to get through, which could be exploited by attackers. • It can take longer to gain access

**Component 3 Learning Aim B Cyber Security- B2 Prevention and Management of Threats to Data
Data level protection: firewalls and anti-virus software (part 1)**

Key Vocabulary	
Firewall	A device that protects an IT system (or network) from unauthorised access by blocking 'bad' network traffic.
Local Area Network (LAN)	A network based on geographical location, such as an office or a school
Access Control List (ACL)	A list that tells the network which data can be sent and received.
Shoulder Surfing	Obtaining sensitive personal information from a user by literally looking over their shoulder while they use digital devices e.g. computers or cash machines.
Session Cookies	Data stored by the web browser until it is closed
Worms	Small computer programs that can spread to other programs.
Trojans	Types of malware disguised as legitimate programs.
Rootkit	Collection of tools or programs that allow an unauthorised user to obtain undetected control of a computer system.
Spyware	Software that is installed on a device without the user's knowledge. It can gather information about their computer activities by transmitting data secretly from their hard drive.

Firewalls	Hardware firewall	Software Firewall
	<ul style="list-style-type: none"> Form the first line of defence in protecting digital systems from external threats such as cyberattacks and viruses. Can be hardware or software based Work by using a set of rules that filter and reject unwanted or suspicious network packets arriving from a remote network. 	Sit between an external network and an internal connection e.g. the internet and a local area network (LAN)

Benefits of firewalls	Drawbacks of firewalls
They can stop attackers from gaining unauthorised access to a device.	Firewalls can block legitimate things.
You can customise the firewall settings to meet the needs of your organisation.	Can make the performance of a computer or network a lot slower.
Software firewalls are easy to install.	Highly effective firewalls can be very expensive.

**Component 3 Learning Aim B Cyber Security- B2 Prevention and Management of Threats to Data
Data level protection: firewalls and anti-virus software (part 2)**

Modern software design aims to make applications easier to use, often including various tricks that can assist user inputs. Some techniques can improve security; others can cause issues.

Common techniques used to make applications easier to use

Obscuring data entry	Common technique to solve shoulder surfing when using secure logins in a public place is to obscure the entry of sensitive data e.g. passwords.
Autocomplete	Autocomplete is a technique where an application will recognise a familiar input and make suggestions from previous inputs. If used on a publicly accessed IT system it can be a security risk.
"Stay logged in"	Web applications often use session cookies to keep a user logged in, even if they leave a page and later return to it. Can be a security risk if a different user gains access to the IT system before the web browser is closed and the session cookie is cleared.

Anti-Virus Software

Anti-virus software monitors a digital system, attempting to identify and remove malicious software before it can cause damage. Most viruses infect a digital system when the unsuspecting user opens infected email attachments. Worm viruses can replicate themselves from device to device via the network.

Different types of viruses include:

- Ransomware
- Worms
- Trojans
- Rootkit
- Spyware

Benefits of anti-virus software	Drawbacks of anti-virus software
Can stop files that contain viruses from accessing your computer system.	Needs to be continually updated to ensure it can detect new viruses.
Some anti-virus software is free to download.	Can make the performance of a computer or network slow.
If a virus is not yet known, anti-virus software is able to monitor the behaviour of files to see if they are showing any virus characteristics	Highly effective anti-virus software can be very expensive.

Example Exam Question

At present, staff who work at Chocawoca use a card entry system to gain access to their secret recipe rooms, cards are swiped at the entrance. They are considering changing this to use a biometric system as they think this will improve security.

(c) Explain **two** benefits of biometric systems to Chocawoca.

(4)

Component 3 Learning Aim B Cyber Security- B2 Prevention and Management of Threats to Data
Data level protection: device hardening and encryption

Key Vocabulary	
Vulnerable	Describes a flaw of weakness in the design, implementation or configuration of a system. Known vulnerabilities can be exploited by 'black hats' to attack a digital system.
Security patches	Additional settings or program codes that fix vulnerabilities in applications, operating systems and device firmware, and are usually downloaded from the manufacturer.
Privilege	A set of rules that allows users to use specific components or access data folder or files.

Device Hardening

Digital systems may have default settings or weaknesses that can make them (and their data) **vulnerable** to attack. The process known as 'device hardening' attempts to resolve these issues.

Device hardening techniques:

- Installing a firewall
- Installing anti-virus (and anti-spyware) software
- Applying **security patches** and updates
- Using encryption
- Closing unused network ports
- Removing non-essential programs or services
- Restricting user access (called the principle of 'least **privilege**')


Encryption

It is common practice to encrypt data when it is stored and when it is being transmitted between IT systems. Stored data is a popular target for cyberattacks and unencrypted (plaintext) data is considered insecure and a security risk. - One solution is to encrypt this stored data.

Vast quantities of personal data are transmitted from web browsers to web servers and back again, especially in web applications e.g. social networking and online banking.

Organisation web servers can use a digital signature that can be transmitted to a web browser to prove its identity and encrypt data transmissions between them.

You can tell if a connection is secure when you see a padlock and the HTTPS prefix on a website address.




Benefits	Drawbacks
<ul style="list-style-type: none"> •Scrambles data so that others cannot easily read it. •Ensures that organisations comply with data protection laws. 	<ul style="list-style-type: none"> •Does not stop data from being stolen. •Encrypting a large amount of data can take time. •Encryption methods need to continually 'evolve' and change as attackers find new ways to access data.

Component 3 Learning Aim B Cyber Security- B2 Prevention and Management of Threats to Data

Finding weaknesses and improving system security

Organisations have responsibility to secure their IT systems to protect the personal and sensitive data they store and process.
Assessing the security of IT systems objectively can be difficult to do, so sometimes external help is required

Ethical Hacking

A process where an individual or a team of penetration testers are asked by an organisation to simulate an attack on its IT system to highlight any weakness and vulnerability.

To start with, the hackers are given little information about the system and will identify weaknesses and then exploit them to see if sensitive data or services can be accessed.

White hat hacker - an IT specialist who is invited to discover vulnerabilities in a system and report them to the organisation or author.

Grey hat hacker - an IT specialist who discovers vulnerabilities in a system, typically without invitation, but does not exploit them for personal gain (although they might make the information publicly known).

Benefits	Drawbacks
Can see if the security of your network is able to withstand the skills of expert attackers.	Can be very expensive to hire professionals with the necessary skills.
Can help to find 'loopholes' in your network security in order to make it better.	Depends on the trustworthiness of the ethical hacker. Some may abuse their position.
The security of a system can keep evolving when loopholes in the network security have been found.	Some people may view ethical hacking as an invasion of privacy if others are able to view their data.

Penetration Testing

Aka 'pen' testing.

A systematic process used by ethical hackers to determine how secure an IT system is.

Frequent vulnerabilities that ethical hackers uncover when attacking a system:

- Unpatched operating systems and applications.
- Web applications that have not been well programmed, leaving them insecure.
- Data that has not been encrypted.
- Poor security practices

Stages of penetration testing:

1. Authorisation to penetration test
2. Discover vulnerabilities and weaknesses
3. Exploit weaknesses (without disruption)
4. Document weaknesses
5. Recommend security improvements

Penetration Testing Report

The findings of penetration testing are presented to the organisation as a formal report, including recommendations that may resolve the issues found.

The report is used to harden the security, addressing the issues found.

The process may then be repeated until the organisation is sufficiently confident in its systems

Component 3 Learning Aim B Cyber Security- B3 Policy Security Policies

Security Policies

To make sure that all employees in all locations follow the same code of conduct organisations create policies that set out the responsibilities of staff.

These policies detail how staff are expected to behave and what procedures they should follow in the event of a disaster.

Most security policies are implemented by IT and technical staff..

Examples of security policies include:

- System security
- Data security
- Compliance (with regulations and legislation)
- Environmental (including disposal of old equipment and waste products)
- Disaster recovery
- Data recovery
- Infrastructure (updating and replacing hardware and software)
- Responsible use policies (including email and internet use policies)



Planning for disaster recovery

Policies exist to increase the robustness of IT systems and data and to plan for what should happen in the event of a disaster.

Disasters can come in many forms:

- Theft of data (having systems hacked or laptops/devices stolen)
- Virus or other malware infection
- Data loss (accidental deletion or intentional sabotage)
- Fire or flood
- Mechanical failure of equipment

To ensure the organisation can become operational again as quickly as possible, a detailed plan is created.

Disaster Recovery Plan

Consideration	Description
Identifying potential risks	Identify potential risks to the system and how each risk will affect the computer system and data
Who is responsible for which actions in the event of a disaster	Staff are given specific recovery tasks to avoid anything being duplicated or forgotten.
What staff should and should not do	Ensure that all staff know the procedures even if they do not have any direct tasks
How the systems will be backed up (including what will be backed up, how often and which media will be used)	Ensure that regular backups are taken. Decide where the backups will be stored and which media will be used to store the data e.g. cloud, magnetic tapes.
A timeline to establish how quickly the systems will need to be backup and running	After a disaster not all operations will be needed immediately. A plan should be made to define how long the organisation can be without each system. Critical systems must be identified and will need to be recovered first.
An alternative location for operation (hardware, software and personnel).	After disaster the organisation may need to move quickly to another location. Hardware, software and personnel should also be available (along with the backups) so that the organisation can function again quickly.

Component 3 Learning Aim B Cyber Security- B3 Policy Passwords

Key Vocabulary

Parameter	A parameter is a set of rules to be followed or behaviours that need to be demonstrated.
Default password	A password that is automatically allocated when your account is set up. Users are always advised to change default passwords on first use.

Password Policy

Organisations that take data security seriously usually have a comprehensive password policy that they ask employees to follow.

This policy usually covers the creation and protection of passwords.

Passwords should be suitably complex. Complexity is increased by:

- Greater password length
- Combination of upper and lower case characters, numbers, punctuation and other symbols
- Passwords SHOULD NOT use words found in a dictionary, familiar names (family or pets) or be easy to crack
- Using initial letters from a memorable phrase, mixing lower and upper case letters and numbers

Protection of Passwords:
Passwords are our first point of defence for our files and personal information.

Usually an organisation's software will prevent the creation of passwords that:

- Don't match the organisation policy, have been used before or are in a dictionary.

Password Strength	Description	Examples
Weak	An obvious password using either standard letters or numbers, often personal to the user (e.g. family name, birthday) so can be easy to guess	PASSWORD,123456
Medium	Uses a combination of letters and numbers, but could use more special characters and less recognisable words to make it more difficult to guess.	LiverPool5
Strong	Makes use of special characters, numbers and upper/lower case letters, making it very difficult to guess.	A?vEr8gS!



Component 3 Learning Aim B Cyber Security- B3 Policy Security Policies

Key Vocabulary

Software Audit

A manual or automated process that lists the name, version and installation date of all software found on a digital device. The process may be carried out remotely, for example, across a network, or in person.

Acceptable Use Policies

Unapproved software could contain malware that might infect the organisation's systems and network.

It may conflict with the hardware or other software on the digital system.

An acceptable software policy explains what will be done to help prevent any attempted installation and use of unapproved software.

Use of unapproved software

The use of unapproved software is usually disallowed by an acceptable software policy. Breaching the policy may result in disciplinary action e.g. verbal or written warning even if the employee did not install the software. Most operating systems can prevent the use of certain software applications. Preventing the use of unapproved software helps to protect the organisation from malware and potential external threats.

The AUP reinforces the need for the installed software to be used responsibly and legally. It also usually prohibits unauthorized duplication of the software for home use unless permitted by the software's licence.

Installation

- Users are usually forbidden from installing unapproved software or updates.
- Users may ask for approval for new software or be asked to select from an approved list.
- Users may need support from their manager or another department for their request to be considered.
- Users will need to justify why this new software is required for their job.

Security policy statements may state the following:
You may **not** install software on digital systems used within the organisation.

All software requests **must** be justified and approved by a manager and then sent to the IT department or Help Desk in writing or by email.

New software **must** be selected from the IT department's approved software list unless no match can be found that meets your needs.



Enforcing AUPs

The operating system applies the safeguards that prevent the installation of software if the user does not have sufficient administrative rights.

Other techniques that prevent unwanted installation of software:

- CCTV monitoring of employees
- Software audit of digital systems

Example Exam Questions:

1. Identify the risks of installing and using unapproved software.
2. Describe how an acceptable software policy might be enforced.
3. Describe what a software audit is.
4. Give two reasons why employees are not automatically allowed to duplicate software for home use.

Component 3 Learning Aim B Cyber Security- B3 Policy

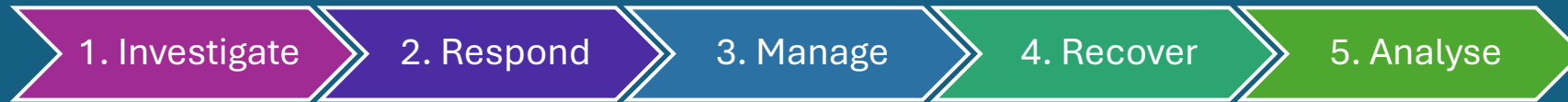
Actions to take after an attack

Key Vocabulary

Data Protection Controller	The named person in an organisation who takes responsibility for the safety and security of the organisation's data.
Remedial Action	An action taken to fix something that has gone wrong; a remedy

Actions to take after an attack

After an attack it is crucial that an organisation and its employees have a clear idea of the actions to take to resolve the situation and reduce the likelihood of it happening again.



Investigation

The organisation will investigate the nature of the attack. It will want to find out the following:

- **The type of attack** e.g. malware, network attack, data theft, phishing
- **The severity of the attack** e.g. Level 1 (low risk) to Level 5 (severe risk)
- **Which processes or services are affected.**
- **When it happened.**

The information gathered at this point is vital to help the organisation determine how to respond, manage and recover from the incident.

Response

The type of response will vary depending on the severity of the attack.

- An organisation will inform:
- Stakeholders (employees, shareholders, customers, suppliers, business partners etc)
 - Appropriate authorities (law enforcement including police, National Crime Agency, **Data Protection Controller**, etc)

Notifying stakeholders

This is important as data breaches might include confidential details (usernames and passwords) that customers might use for other services.

Informing stakeholders may lead to a damage to public image.

Not telling the authorities could result in legal action and potential fines.

It is also important that interested parties are kept updated as more information becomes available from the investigation.

Manage

The priority is to isolate the problem by containing the threat as close to the source as possible.

e.g. disconnecting an infected computer from the network or blocking unauthorised network traffic by using a firewall.

Recover

The organisation will have a separate disaster recovery policy that it will follow in the event of an attack.

- This will include:
- Employees responsible for specific tasks
 - The expected timeline
 - The **remedial action** involved.

Analyse

Analysis will focus on the following:

- What went wrong,
- How it happened (internal or external threat),
- How it could have been prevented,
- How effectively the organisation responded to the attack
- What lessons have been learned.

Business Studies



Business Studies

Learning Journey

SUCCESS COMES FROM HARDWORK

Theme 2
L1r 45

Theme 1
L1r 45

2.1 Making human resource decisions

2.3.2 Accrual
2.3.2 Effective provision

2.3.1 Organizational structure

2.4.2 Understanding performance

2.4.1 Business calculations

2.1 Making Operational decisions

2.1-2.2 research (3
Basic Test)

2.1.1 Business operations

2.1.2 working with suppliers

2.1.4 The sales process

2.1-2.3 research (3
Basic Test)

2.1.3 research (3
Basic Test)

2.2.5 Marketing mix & Decisions

2.2.4 Price

2.2 Making marketing decisions

2.2.5 Promotion

2.2.2 Price

2.2.1 Product

YEAR 11

2.1.5 Basic Test

2.1 research (3
Basic Test)

2.1.4 Price

2.2.3 distribution & Business

2.1 Drawing the business

Theme 1
stock exam

Theme 1
research (3)

2.1.1 Business growth

2.1.2 Changing aims & objectives

1.5.1 Legislation & Business

1.5.2 Technology & Business

1.5.3 Economy & Business

1.5.4 External influences

1.5.5 Finance

1.5.6 Business plan

1.4.4 Business Marketing mix

1.4.3 Marketing mix location options

1.1 Understanding external influences

1.1.1.4 research (3)
Basic Test

1.1.1.3 Basic Test

1.4.4 Business plan

1.4.3 Marketing mix location options

1.4 The options for start up and small businesses

1.1 Putting a business idea into practice

1.1.1.2 research (3)
Basic Test

1.1.1.1 aims & objectives

1.1.2 Revenue, cost & profit

1.1.3 Cash & cash inflow

1.1.4 Sources of finance

1.2.3 Market Segmentation

1.2.4 Competitive environment

1.1.1.3 Basic Test

1.1.1.2 research (3)
Basic Test

1.1.1.1 aims & objectives

1.1.2 Revenue, cost & profit

1.1.3 Cash & cash inflow

1.1.4 Sources of finance

1.1 Spotting a business opportunity

1.1.1.3 Basic Test

1.1.3 Size of business activity

1.1.2 Risk and Reward

1.1.1 Dynamic nature of business

YEAR 10

1.1 Examples and Entrepreneurship

1.1.1.3 Basic Test

1.1.3 Size of business activity

1.1.2 Risk and Reward

1.1.1 Dynamic nature of business

1.2.2 Market Research

1.2.3 Customer needs



Topic 2.3.1 Operations

Key Vocabulary

Good – a tangible item that exists in a physical sense, e.g. a car

Service – an experience or non-physical item, e.g. a trip to a theme park

Job production – one-off production of a one-off item for each individual customer

Batch production – producing a limited number of identical products

Flow production – continuous production of identical products, which gives scope for high levels of automation

Productivity – a measure of efficiency, usually output per person per time period

Automation – using machines that can operate without people

Robots – machines that can be programmed to do tasks that can be done by humans, e.g. spray painting

Flexibility – the ability to switch quickly and easily from one task to another

CAD – Computer Aided Design

CAM – Computer Aided Manufacture

Core Knowledge

The purpose of production is to create **goods** and **services**.

Production Method Job	Advantages	Disadvantages	Examples
	<ul style="list-style-type: none"> • Unique products • High quality • Higher prices 	<ul style="list-style-type: none"> • Need highly skilled workers • Lengthy process • Higher cost per unit 	Tailoring, bridges, Olympic Stadium
Batch	<ul style="list-style-type: none"> • Variety and choice for customers • Materials purchased in bulk, lowering production costs 	<ul style="list-style-type: none"> • Work is repetitive • Equipment must be cleaned after each batch 	Bread, clothing
Flow	<ul style="list-style-type: none"> • Bulk buyer leads to lower unit costs • Production 24/7 • Consistent quality 	<ul style="list-style-type: none"> • High capital investment • Less flexibility to adapt products • Very repetitive work 	Canned food, bottled drinks

Impact of technology:

- Lower costs in long term due to lower labour costs; improved quality so less wastage
- Increased productivity due to no breaks or holidays
- Improved quality / consistency
- Lower costs can lead to competitive prices

Don't be a "man on the street"

- Remember not all production happens in a factory: a bakery is also manufacturing
- Introducing technology does not lower costs immediately: in the short term there are high costs and this will affect cash flow and profit margins

Wider Business World

Morgan cars – produced by job production

Ford cars – considered to be the first mass produced car in the world

Synoptic Links

Technology – has had an impact on production

Marketing – creates the demand for the product

Finance – introducing technology will incur costs and affect cash flow

Human Resources – if staff lose their jobs they will be entitled to redundancy payments

Legislation – operations will need to follow Health & Safety law

Key Vocabulary

Stock – items held by a firm for use or sale. Also called inventory

Bar gate stock graph – a diagram to show changes in the level of stock over time

Maximum stock level – highest level of stock to be held by a business

Minimum stock level – also called buffer stock level. The lowest level of held to avoid running out

Re-order level – the level of stock that will trigger the business to order more

Lead time – number of days or weeks that it takes from ordering stock until it arrives

Order quantity – the number of items ordered by the business

JIT – Just in Time. Running the business with so little stock that supplies have to arrive 'just in time' before they run out

JIC – holding buffer stock levels, 'just in case' there is a sudden increase in demand

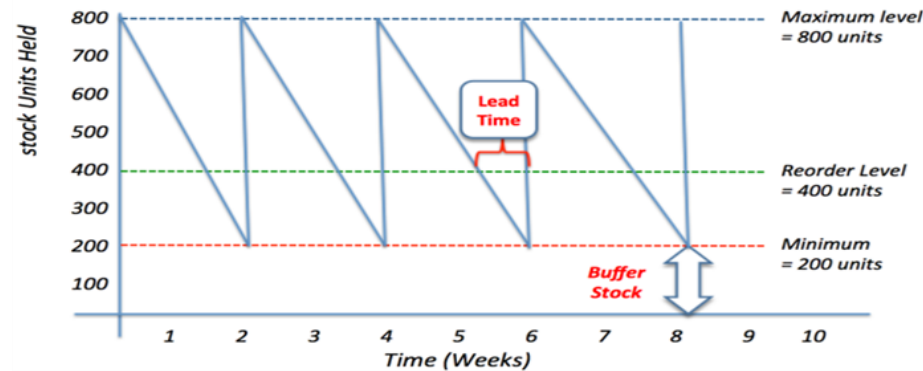
Procurement – obtaining the right supplies from the right supplier

Logistics – ensuring that the right supplies will be ordered and delivered on time

Core Knowledge

The operations department has a role to ensure that there is enough stock to meet demand, so they must work closely with suppliers as well as managing the stock that is in the business effectively.

The amount of stock held is shown in a bar gate graph:



Benefits of JIT	Limitations of JIT
Less storage space needed saving costs	Greater risk of running out and disappointing customers
Fresher produce due to more frequent deliveries	No bulk-buying discounts
Less capital tied up in stock	

Don't be a "man on the street"

- Remember not all business that hold stock are shops – it could be a factory, restaurant, bakery
- The cheapest supplier may not be the best if they are not reliable
- Not all businesses will be able to get trade credit from a supplier – trust may need to be built first

Wider Business World

Supermarkets – most run JIT systems to have more selling space and save costs on storage

Restaurants – may limit their menu choices to ensure ingredients are fresher and less stock is wasted

Synoptic Links

Cashflow – holding less stock improves cashflow because the stock is more likely to be sold before payment to suppliers is due

External factors – changes to economic factors can affect the type of products consumers demand

Customer needs – if quality is a concern more than price, this will need to be considered when choosing a supplier

Location – this could affect the logistics for a business

Topic 2.3.3 Managing Quality

Key Vocabulary

Quality control – putting measures in place to check that the customer receives an acceptable level of quality

Quality assurance – a system based on preventing quality problems by involving all staff within the production team to understand their role in maintaining highest quality standards

Warranty – the guarantee by a producer that it will repair any faults in a product for a specific period of time

Core Knowledge

Quality is about meeting a minimum standard to satisfy customer expectations

Quality control

- Finished goods are inspected
- Checks for defects rather than preventing them
- Costly as it can lead to a high level of wastage
- Workers less involved in process so may be less motivated

Quality assurance

- Quality is checked at every stage in the production process – more time consuming, but defective products are dismissed before being completed
- Aims to prevent defects
- Staff need training – costly in short term; more motivating in long term

Importance

- Lowers costs through less wastage
- As production costs lower, profit margins increase
- Quality can improve reputation and build brand loyalty leading to a competitive advantage

Don't be a "man on the street"

- Remember quality is important for goods as well as services
- Don't confuse quality control and quality assurance
- Quality assurance can not be put in place quickly – staff need to be trained and it takes time to be embedded into the culture of the business

Wider Business World

Gordon Ramsey – in his restaurant the Head Chef will check every plate of food before it is sent out

Hotels – have a check list for cleaners to ensure that all rooms are same standard

Synoptic Links

Motivation – motivated staff are more likely to deliver a high-quality service

Customer needs – quality is one of the needs of customers

Promotion – quality can be used as a promotion tool

Consumer law – products must be 'fit for purpose'; a minimum quality measure

Technology – led to an increase in reviews online, which impacts a firm's reputation

Key Vocabulary

Sales process – the process of persuading a customer to buy the products

Product knowledge- how well staff know the features of the products and service issues, e.g. such as the precise terms of a warranty

Customer engagement – the attempt to make a customer feel part of something rather than an outsider

Customer feedback – comments, praise or criticisms given to the company by customers

Post-sales service – anything provided after you have paid for and received the product, e.g. updates, perhaps because something has gone wrong or a way of promoting customer engagement

Core Knowledge

To succeed in the sales process the following need to be provided:

- Strong **product knowledge** and therefore helpful advice from staff
- Speedy and efficient service
- Customer **engagement**
- Responses to **customer feedback**
- Excellent **post-sales service**

Benefits of good customer service:

- Customers feel valued, are loyal and more likely to repeat purchased
- Harder for competitors to steal customers if they are loyal
- Satisfied customers tell others – this could attract more customers to the business
- Satisfied customers can create a positive working environment and make a business a reputable employer
- Developing a reputation for good customer service can develop into a competitive advantage

Don't be a "man on the street"

- Do not assume that negative reviews will make a business fail – these can be ignored or people may have little choice
- Remember that not everyone uses social media so this may not be a good way to get customer engagement for some businesses

Wider Business World

Kia – have a 7 year warranty on new cars

Pizza Hut – have a guarantee of receiving your starter within so many minutes of ordering

Burberry – send regular email updates to customers to make them feel part of the brand, rather than just a customer

Synoptic Links

Customer needs – the sales process is about meeting those needs

Recruitment – to provide excellent service the right staff need to be employed

Training – staff will need to be trained about products

Quality and operations – information about the product will need to be provided

Technology – more customer feedback is available

Topic 2.4.1 Business Calculations

Key Vocabulary

Revenue – the money that a business receives from selling its goods and services. Also called Turnover or Income

Cost of sales – the name for the costs that are directly involved in the making of a product for a manufacturer or the provision of a service for a service provider

Gross profit – the amount left after the cost of buying or making the product has been deducted from revenue

Expenses – costs of the business that are not directly involved in the making of the product, e.g. rent, rates

Net profit – overall profit made by a business. What is left after deducting all costs.

Gross profit margin – expressed gross profit as a percentage of sales revenue

Net profit margin – expresses net profit as a percentage of sales revenue

ARR – Average Rate of Return. Expresses the average yearly profit as a percentage of the sum invested. Shows profitability and can be compared with interest rates on bank deposits

Core Knowledge

Key formulas:

Gross profit = Revenue – cost of sales

Net Profit = Gross profit – expenses

Gross profit margin = (Gross profit ÷ Sales revenue) x 100

Net profit margin = (Net profit ÷ Sales revenue) x 100

ARR = (lifetime profit ÷ years the investment will last) ÷ initial investment x 100

In all cases the higher the number the better, BUT these must be compared to other businesses and previous performance

Wider Business World

RyanAir – has a greater Net profit margin than other airlines as it keeps costs down by not offering meals on board

Synoptic Links

Revenue & costs – knowledge of these terms is built on in this topic; fixed costs are expenses; variable costs are cost of sales

Don't be a "man on the street"

- Remember not all investments will be profitable
- Even if an investment is not profitable, this does not mean a business should dismiss it – it may be needed to maintain a competitive position
- A business can not lose profit – it makes a profit OR a loss
- A loss in one year does not always indicate failure – this may be due to high one-off costs

Topic 2.4.2 Understanding Business performance

Key Vocabulary

Line graph – shows data represented as lines, making it easy to identify trends

Bar graph – data represented so that the height of the bar represents the quantity involved. Good for making comparisons

Pie chart – shows data represented in a circle, with each slice of the pie representing a proportion of the whole, e.g. market share

Core Knowledge

Data can be figures or visually represented. The most common types of visual representation are graphs.

	Line graphs	Bar charts	Pie charts
Pros	Good for data shown over many time periods and for comparisons with how one factor affects another	Good for data over 2-3 time periods Good for comprising size / number of several different items	Good for showing proportions
Cons	Too many lines can be confusing Assumptions can be made about trends continuing	Cannot be easily used to compare data over many time periods	Show big differences clearly but not small differences Cannot show trends over a number of years

A business can use a variety of data:

- **Financial data** – profit margins, profit levels, ARR, break-even point, cash flows
- **Marketing data** – analysis of sales figures, market research data
- **Market data** – analysis of data such as market size, changes in market size, figures for different segments

Limitations of data:

- A need to understand why trends are happening and the causes of these trends
- Bias can be in place when interpreting data
- Some numbers will be estimates not facts

Wider Business World

Government – use line charts to show changes in taxation, inflation etc; pie charts to show how taxation is distributed

Synoptic Links

Business calculations – profit and profit margin calculations can be used to assess financial performance

HR – data on staff retention and performance can be used

Operations – productivity and quality data can also be measures of performance

Marketing – data on sales figures and market research

External influences – economic factors may affect a business performance

Aims – the importance of each measure can be different depending on the aims of the business

Don't be a "man on the street"

- Remember that data may be biased or unreliable – always check the source
- One set of data alone is not much help – a business will need to compare to previous years or competitors to put the data into context
- Financial data alone is not the whole picture – consider what external factors may have caused a change, as well as HR and Marketing data
- Don't confuse market data and marketing data

Computer Science

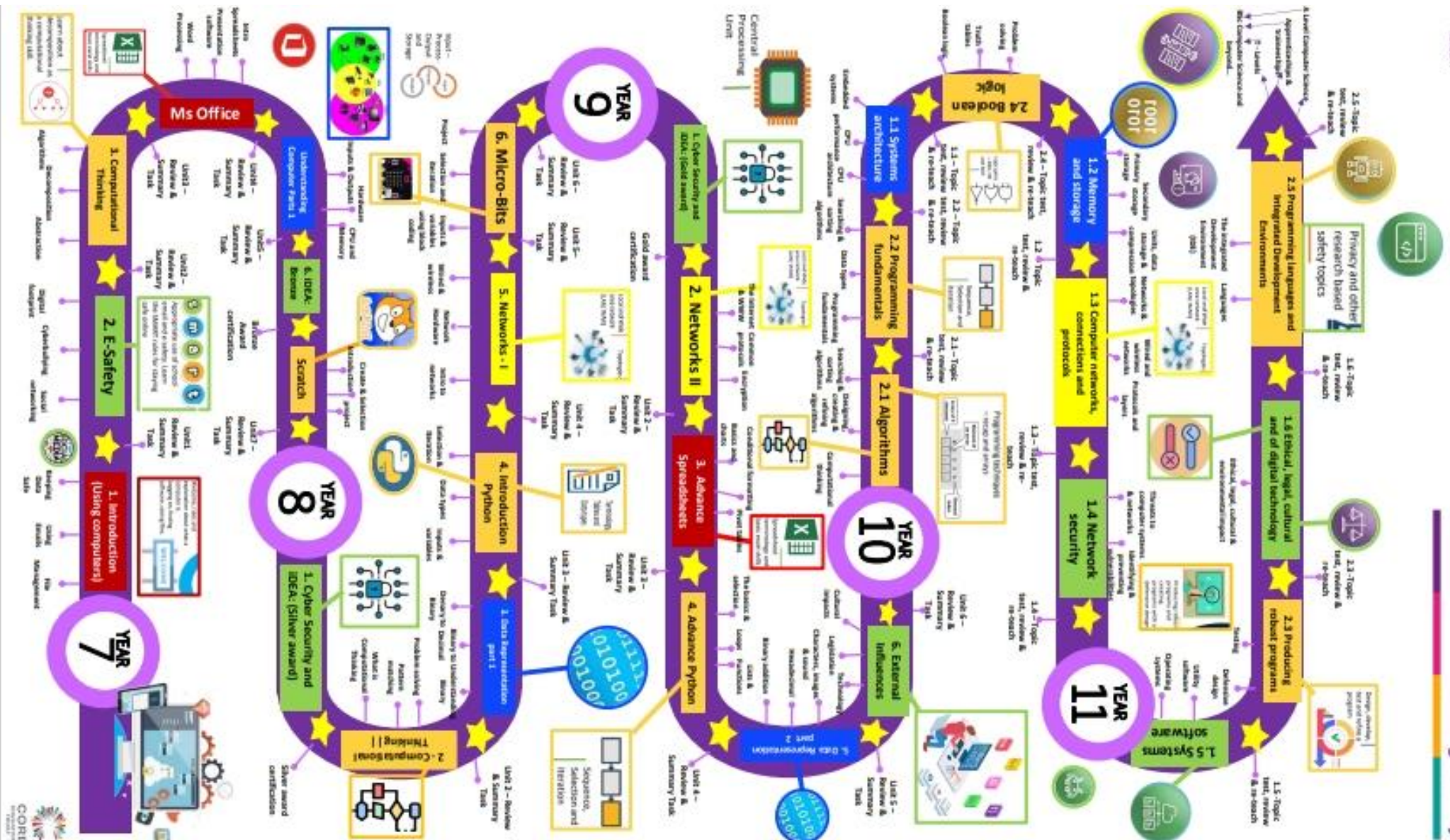
Topics covered from the beginning of the academy year to the end of this half-term.

AUT 1:

- 1. System software**

AUT 2:

- 2. Producing robust programs**



Defensive Design

Programmers try to protect their programs by testing them to reduce the number of errors, predicting how users might misuse their program and trying to prevent it and making sure their code is well maintained.

Input Sanitisation - removes any unwanted characters that have been entered into a program

Input Validation - Checks if the data meets certain criteria before passing it through the program.

Authentication - Where a program confirms the identity of a user before giving them access to the full program. This could be done through usernames and passwords.

Maintainability - Code that has been well maintained is easy to edit without causing errors. A well maintained code will have **comments** to help other programmers understand the code, as well

as **appropriate names for variables and sub programs**, and **indentation** so that it is easy for programmers to see the flow of the program. Global variables should only be used where necessary so that they don't impact on the rest of your code.

Presence check	Checks that data has been entered
Length check	Checks the data is the correct length
Range check	Checks the data is within a set range
Format check	Checks it's in the correct format (Eg: dd/mm/yy)
Check digit	Checks numerical data is entered correctly
Look-up table	Checks against a table of accepted values



Producing Robust Programs

Key Words

Authentication
Maintain
Testing
Defensive Design
Syntax Error
Logic Error
Input Sanitisation
Input Validation

Testing

A program should be tested to check for any errors.

Final Testing - The program goes is tested once at the end of development. Everything is tested in one go.

Iterative testing - a program is tested and then changes are made as it goes through the development cycle again. It may go through this process a few times to make sure it is exactly what the customer wants.

Test data can fit into 3 different categories:

Normal	Data which is likely to be entered into the program and should be accepted
Extreme/boundary	Data on the limit of what should be accepted
Erroneous	Data that should not be accepted

Types of Error

A program should be tested to check for any errors.

Syntax Error - something which doesn't fit the rules or grammar of the programming language.

Logic Error - the program runs but not as expected.
Eg: < user instead of >.