IT Level 3 AAQ | Pearson BTEC | 610/3960/3

AAQ BTEC National IT: Course Companion

Unit 2: Cyber Security and Incident Management

JL Hagger

zigzageducation.co.uk

POD 12912

Student Introduction

With an ever-increasing reliance on technology, cyber security is more critical than ever. Technology continues to advance, and individuals, businesses and governments face an ever-growing number of cyber threats that can compromise sensitive data, disrupt operations, and cause financial and reputational damage. Understanding these threats, identifying system vulnerabilities, and implementing effective security protection methods are essential for maintaining a secure digital environment.

The government *National Crime Agency* says on its website: *"The deployment of ransomware remains the greatest cyber serious and organised crime threat to the UK and its use threatens Critical National Infrastructure and poses a risk to national security"*.

This unit is a very in-depth look at networking and cyber security. There is a lot of detail, including technical detail, that students need to learn off by heart so they can answer what could be a very wide-ranging selection of exam questions.

To demonstrate the importance of cyber security, here are three examples of where it has failed:

- In 2010 the US and Israel developed malware called *Stuxnet* which targeted industrial control systems and used it to physically damage over 1,000 nuclear centrifuges which set back Iran's nuclear capabilities.
- In 2017 hackers gained access to sensitive data from Equifax, a credit reporting agency. Personal data of 147 million people was stolen and, as well as reputational damage, they were fined more than £11 million by the Financial Conduct Authority and paid a settlement of up to $425 million to help people affected by the data breach.
- In 2023 managed file transfer software called MOVEit had an AQL injection vulnerability which mean that more than 2,500 organisations were impacted, including the BBC, British Airways, Boots, Aer Lingus, and Transport for London. The attack was reportedly carried out by a Russian-affiliated cyber gang.

This unit is an excellent preparation for those students who want to go on to study a related undergraduate or master's degree or go into a related career. For everyone else it gives excellent skills in an increasingly dangerous world relying evermore on technology.

Here are a few key websites that contain real and up-to-date guidance on aspects of cyber security and incident management:

The National Cyber Security Centre (NCSC)	**https://ncsc.gov.uk**
Get Safe Online	**https://getsafeonline.org**
UK government security policy framework to protect government assets	**https://www.gov.uk/government/publications/security-policy-framework**
National Institute of Standards and Technology (NIST)	**https://nist.gov/cyberframework**
US National Vulnerability Database (NVD) managed by NIST	**https://nvd.nist.gov**
FAST – *campaigns against software piracy and helps organisations be compliant with licences*	**https://fast.org**

JL Hagger, September 2025

*A web page containing all the links listed in this resource is conveniently provided on ZigZag Education's website at **zzed.uk/12912***

You may find this helpful for accessing the websites rather than typing in each URL.

AAQ BTEC National IT

Cyber Security and Incident M

Content Area A: Cyber security th vulnerabilities and security protec

Contents

A1 Cyber security thre

Starter Discussion Point

What sorts of risks and dangers to IT systems can you think of? Categorise them in and into deliberate and accidental or forces of nature. What sorts of consequences organisations? How can organisations protect themselves against these risks and d

Cyber security threats usually bring to mind hackers trying to get into systems, hold a company to ransom. External threats can equally include automated ro through every existing IP address looking for weaknesses without caring who t even if there is no specific reason to be a target.

However, internal threats can be worse than external threats, e.g. a disgruntle manager who has the access and know-how to steal data or damage the syste Unintentional damage can also be great, e.g. accidentally overwriting a databa

Internal mistakes, lack of training, and not following procedures can enable a make the consequences worse. Similarly, if internal backup procedures have consequences of an internal or external cyber security failure can be worse.

Research Activity

Before we get going on the course it is a good idea to realise just how common and impactful organisations. Look up each of the following real-life case studies, and for each one identify w attack, and whether it was accidental or deliberate, and what the consequences were:

- Talk Talk 2015 cyberattack – see **zzed.uk/12912-talk-talk**
- Dixons Carphone data breach 2017 – see **zzed.uk/12912-dixons**
- EasyJet cyberattack 2020 – see **zzed.uk/12912-easyjet**

Go

A1.1 Internal threats

Employee sabotage, deliberate and accidental (A1.1.1)

Murphy's Law Enterprises is a badly run organisation suffering a series of mishaps, outlined below.

Scenario 1: An employee, frustrated with outdated company laptops, decides to 'borrow' a newer model from the IT department without permission. When it is not noticed they lent it to a family member and 'borrow' another for themselves

Scenario 2: A sales representative, intending to work remotely, transfers confidential client information onto a personal USB drive. Unfortunately, the USB drive is in a bag which is stolen on the bus. Subsequently the data appears on the Internet!

Scenario 3: An IT staff member, aiming to assist a friend's start-up, shares licensed company software without authorisation. The software company spots the additional use which leads to legal action against Murphy's Law Enterprises for violating software licensing agreements.

Scenario 4: A keen employee is waiting for IT support to give him access to a new department printer. He can't wait so he installs a print driver from the Internet. Unfortunately, it conflicts with the existing printers and no one in the company can print until the problem is investigated and fixed.

Scenario 5: An employee, attempting to bypass security protocols for convenience, installs a personal VPN on their workstation. This unauthorised VPN causes network instability, affecting the performance of all computers on the network.

Scenario 6: A disgruntled employee, seeking revenge, installs keylogging software on their manager's computer to gather sensitive information. The manager finds out and sues the company for a breach of their personal data and harassment by another employee.

Scenario 7: To evade the company's Internet usage policies, an employee utilises proxy servers to access restricted websites. Unfortunately, t to the proxy servers has been put on the Internet by hackers and contains a p into the organisation's network.

Scenario 8: To enhance productivity, an employee installs unapproved project This software is incompatible with existing systems, causing frequent crashes a multiple departments.

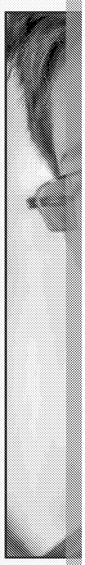
Activity A1

Study the scenarios above and map them to the list of possible types of deliberate and accide shown [illegible] the [illegible].

Accidental or deliberate damage (A1.1.2)

Scenario 1: Murphy's Law Enterprises have a burst pipe in their offices which floods their server room and damages the servers and backups. As they do not have adequate disaster recovery plans or backups in place, the data loss is significant. Furthermore, the business experiences a power loss with no UPS (Uninterruptible Power Supply) systems, causing unexpected shutdowns and data corruption. As a result, they experience severe setbacks in operations, loss of client data, financial loss from halted business activities and possible customer trust. Management had not wanted to spend money for risks they thought were unlikely to happen.

One of th
in cyber s
named E
who was
National
States, le
documen
global su
widespre
and gove



Scenario 2: FortiShield Solutions Ltd are a well-organised and security-conscious company and have a similar burst pipe incident in their office. However, thanks to their robust disaster recovery and business continuity plans, they experience no data loss or operational setbacks:

- **Prevention and early detection:** The company has water leakage sensors installed in critical areas, including the server room. The sensors detected the leak immediately and triggered an automated alert to the facilities team, allowing them to take swift action and minimise water exposure.
- **Off-site and cloud backups:** Even though a few on-site servers suffered water damage, *FortiShield Solutions* has regularly scheduled cloud-based backups and off-site redundancy. No data is lost as they can restore everything quickly.
- **Redundant power supply:** *FortiShield Solutions* has invested in UPS (Uninterruptible Power Supply) systems and backup generators. When the power went out, the undamaged servers switched preventing data corruption and downtime.
- **Disaster recovery plan:** The IT team immediately follows the predefined alternative servers at a remote data centre. Employees switch to remote ensuring business continues without disruption.

As a result, *FortiShield Solutions* only lost a few hours of data in a few places, had only a minor financial loss, and maintained customer trust.

Murphy's Law E
What do you thi

As well as attempting to prevent and minimise damage, organisations need t and recovery systems in place as there are always real risks of both acciden

Damage to systems or infrastructure can happen through:

- **Fire, flood,** or **power loss** which can severely damage equipment and d
- Acts of **terrorism** can target or disrupt essential IT infrastructure includ rogue or nefarious states.
- Other unforeseen disastrous events including **natural disasters** such as

Weak cyber security measures and unsafe practices (A1.1.3)

Physical protections should be put in place to protect important and confidential data. Physical devices are secure from unauthorised access by physically locking them away, e.g. in permanently locked server rooms with limited key access.

Normal computer devices which are connected to the physical network should have secure logins so only legitimate staff can access them.

Visitors should be accompanied and monitored so they cannot physically access devices on the network. Even if they are not able to login, they could plug a USB stick into the back when unobserved, which then collects keystrokes, including passwords. Visitors should also be security vetted if they will be accessing secure areas such as server rooms, for example to carry out maintenance.

Scenario: A cybercrime syndicate wants to make money using ransomware. They create malware that encrypts all the files on any network that a user has access to and then emails the syndicate to let them know to email a ransom request to decrypt the files. They put the malware inside an install file that also installs a legitimate print driver. They copy word for word a legitimate website that has print drivers, and create their own website called download-ace-printer-drivers.com. Then they wait to see who downloads the files from the website.

Discussion Point

If you were at a friend's house and wanted to print something to their printer, would you search Google to find the right printer driver? If Google's top link was to the website in the scenario above, would you realise that it may contain malware? How can you download the driver but avoid the situation above?

Accidental loss or disclosure of data or credentials (A1.1.4)

Many cases of personal data exposure have been in the news over the last few years. Ironically, many of these were accidents rather than malicious. One very common example is a school sending emails to a group of parents and accidentally putting all the parents' email address in to the ***To*** field, rather than the ***BCC*** field, thus revealing the email addresses to all parents.

Accidental exposure or loss of data might be due to:

- **Human factors** such as
  - **Negligence:** careless actions can lead to data being exposed, e.g. leaving a laptop on a train.
  - **Lack of training:** employees not trained in security procedures may unknowingly compromise data, e.g. not realising they should lock their computer when they leave it unattended at lunchtime.
  - **Not following security procedures:** ignoring set protocols can lead t vulnerabilities, e.g. writing down passwords on a piece of paper tha kept on their desk.
- **Inadequate monitoring and reporting:** if incidents are not noticed then t data transfer logs aren't monitored then employees or hackers may expo noticed. Similarly, if incidents are not reported then management doesn improve systems.
- **Weak security culture:** a lack of emphasis on security within the organisation means mistakes may be ignored instead of being addressed, employees skip security procedures to 'get more work done', and managers do not prioritise IT and security training.

What would yo
because the anti
there is malware

Research Activity
Look up how many ICO reported data breaches there were in the most recent three-month

Research Activity
In 2024 a company called Tile was hacked. Read about it at **zzed.uk/12912-tile**
What was the cause and how could this have been prevented?

A1.2 Function of external threats

Malicious software (malware) (A1.2.1)

Types of Malware	
Virus	Type of *malware* that attaches itself to a legitimate program or file and spre delete or modify data. Viruses are normally initiated by some user action to an email attachment, downloading a file from the Internet or plugging in a
Worm	Self-replicating malware that spreads without human interaction, exploiting widespread damage by overloading networks, deleting files, or installing ba
Boot Se	Critical part of a storage device (e.g. hard drive, USB drive) that contains c Boot sector viruses infect this area, so they load before the OS to evade det
Web Script	Small program or code executed in a web browser, often written in JavaScri used in attacks like Cross-Site Scripting (XSS) to steal user data or spread m
Macro	Set of automated commands used in applications like Microsoft Office to pe embed malicious code in documents or spreadsheets which execute when o
Rootkit	A rootkit is a collection of software tools, often at the kernel or low-level o admin access. A rootkit virus or rootkit cyberattack (sometimes confusingly the rootkit tools to enable remote access for attackers, often by disabling se
Trojan (Trojan Horse)	Malware which disguises itself as a legitimate program but secretly perform installing other malware, or creating backdoors.
Browser Hijack	A cyberattack that modifies browser settings without user consent, redirecti injecting ads to generate revenue or distribute malware.
Polymorphic Malware	A type of malware that constantly changes its code while maintaining its c traditional antivirus programs to detect and remove.

As well as the malware designed to break into systems, damage or steal data, other types of malicious software:

	Spyware	Adware
What is it?	*Type of malware that **covertly collects user data** (e.g. browsing habits, keystrokes, personal information) and sends it to attackers for **advertising, identity theft, or espionage**.*	*Software that autom displays pop-up or ba advertisements.* *Some is legitimate.*
Examples	• **Keylogger / Data Thief:** spyware that records keystrokes to steal sensitive information such as passwords and credit card details. Some keyloggers also capture screenshots and clipboard data. • **System Monitor:** software tool (legitimate or malicious) that tracks system activity, including keystrokes, applications used, and websites visited. Can be used for security monitoring or espionage. • **Mobile Device Tracker / Stalkerware:** malicious software giving unauthorised tracking of a mobile device's location, calls, messages, and activity. Used to stalk victims. • **Web Beacons:** invisible tracking elements embedded in emails or websites to monitor when and where a user interacts with content. • **Tracking Cookies:** small files stored on a browser to record user activity across websites to track behaviour, usually for advertising purposes.	• Potentially Unwa Program (PUP): s that users may unknowingly inst which often inclu unwanted adwar toolbars, or syste modifications. • Legitimate Adwa ad-supported sof that displays ads exchange for fre • Abusive or Decep Adware: tracks u excessively, hijac browsers, or pus fraudulent/scam Some forms are i

Research Activity

AI is a fantastic tool but it unfortunately also increases cyber security threats. Read the *compari*
and create a warning poster for students not studying IT who will be less aware of the risks.

In 1989 a biologist called Joseph Popp sent around 20,000 infected floppy disks labelled 'AIDS
attendees of a World Health Organization conference on AIDS. They contained what was su
Upon infection, the ransomware would count the number of times the computer had been bo
would encrypt the names of all the files on the computer and demand a $189 payment to 'PC

This attack marked the beginning of ***ransomware*** as a method of extortion. Ransomware ha
sophisticated and prevalent due to advancements in technology and the Internet, affecting in
government agencies worldwide.

Hacking – commercial, government, individuals (A1.2.2)

Hacking is unauthorised access to or manipulation of devices, services or networks. Here are some hackers' motivations:

- Financial gain through data theft (stealing personal or sensitive data to sell or blackmail), credit card and payment fraud, fraud, cryptojacking (secret cryptocurrency mining), and ransomware attacks
- Cyberwarfare
- Cyber espionage (between countries or organisations)
- To promote political or social causes (hacktivism)
- Revenge or personal vendettas
- Fun, challenge or curiosity

Hackers use a wide range of methods including:

- Malware
- Social engineering attacks (see *A1.2.4*)
- Direct network attacks such as DoS and DDos
- System and software vulnerabilities
- Browser hijacking or other PUP (Potentially Unwanted Program)
- Authentication attacks to gain or circumvent passwords
- Insider or physical attacks

Discuss th

Cyberwar
nation-sta
or disrupt
or data of
often for s
It may incl
- Disab
refine
transp
- Hacki
busin
or cau
- Sprea
social
- Launc
dama

Denial of Service (DoS) and **Distributed Denial of Service (DDoS) attacks** atte
services to make them unavailable.

	Denial of Service (DoS)	Distribu
Definition	A cyberattack where a single hacker runs a script on a computer to flood a website, server or network with excessive requests, making it slower, unavailable or possibly to crash.	A large-scale cyberatt flood a system with tr These devices may be hacker or set to run a
Detection and prevention	Easier to detect and mitigate by blocking the attacker's IP.	Harder to mitigate sin advanced filtering tec

Data tampering is the process of intentionally altering or destroying data. Th

- back end: altering databases or data storage systems.
- front end: modifying public-facing applications, e.g. websites.

Hacking may be carried out by people or by *automated bots*. Bots are progra the Internet, often used for cyberattacks, spamming, or mining cryptocurrenc computers controlled by attackers to carry out DDoS attacks, credential stuffi

Activity A2

An organisation is [illegible] helping older people to use computers. They have a simple websi computers connected to the Internet, and no bank account. Despite having nothing of value, w still at risk of hacking?

Research Activity

Read:

- *6 Motivations of Cyber Criminals* at **zzed.uk/12912-6-motivations**
- *The Psychology of Cybersecurity* at **zzed.uk/12912-hacker-mind**
- *7 of the Most Famous Hackers in History* at **zzed.uk/12912-famous-hackers**

Create a summary presentation combining information from all three, with one slide for each m

Sabotage – commercial, government, individuals, terrorism (A

Sabotage involves deliberate damage or disruption, for example:

- data poisoning: corrupting data to make it unreliable.
- data tampering or destruction
- fake creation: counterfeit images, videos, documents using software or AI.
- damage to or hijacking of infrastructure, e.g. machinery, vehicles, IoT devices, industrial processes, commercial infrastructure such as credit card payments, or critical infrastructure like power grids or water supply systems.

Discu
succe
disab
the U
the U
how I

Stuxnet is a high-profile example of cyberwarfare. It was discovered in 2010 and is believe United States or Israel because its specific target was industrial control systems used in Iran's

Stuxnet was designed to get into these systems undetected to sabotage them from the insid machine that controls how fast nuclear centrifuges spin. By secretly making the machines sp Stuxnet caused physical damage without setting off alarms or making the workers suspiciou everything was running normally. It is reported to have destroyed approximately 1,000 cen

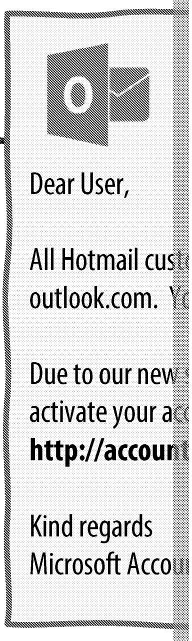
Social-engineering techniques used to obtain secure informa

Individuals are often manipulated to gain confidential information through on

- *Phishing* is sending receptive emails or messages to trick recipients into re
- *Vishing* and *Smishing* are phishing via phone (voice) or SMS.
- *Spear Phishing* is *Phishing* targeting specific individuals or organisations u customised attacks, for example creating emails using the style and emai of friends, colleagues or a boss. *Whaling* is a variation of *Spear Phishing* t targets high-level managers or high-profile targets such as politicians.
- *DNS Spoofing* is forging or corrupting *DNS records* to redirect users to ma without their knowledge.
- *Pretexting* or *impersonation* is convincing someone to reveal information

Activity A3

How do you know this is a Phishing email? If it was sent to 100,000 people, how many people do you think would follow the link and enter their email address and password when faced with a site that looks like the outlook.com site?



Dear User,

All Hotmail cust outlook.com. Y

Due to our new activate your ac **http://account**

Kind regards
Microsoft Accou

Research Activity

Research types of social engineering attacks, e.g. **zzed.uk/12912-social-eng**

Go to **zzed.uk/12912**

Create a poster for your school or college computer room which outlines the dangers.

In May 2000, a simple email with the subject line "**I LOVE YOU**" caused chaos across the glob actually a cleverly disguised computer worm, created using a scripting language called VBScri – titled "LOVE-LETTER-FOR-YOU.txt.vbs" – the worm activated, replicating itself and sendin Microsoft Outlook address book. It spread like wildfire, affecting millions of computers withi

But was as well as replicating the virus caused damage. It overwrote image files, stole passw governments, businesses, and individuals alike. Corporations shut down their email systems, reached billions of dollars. It used *social engineering* by replying on curiosity and emotional a

The creator, a 24-year-old student from the Philippines named Onel de Guzman, claimed he i concept, not a global cyberattack. At the time, Philippine law had no specific rules against ma prosecuted. The "I Love You" worm remains one of the most infamous examples of early cybe world views digital security and email threats.

Physical security (A1.2.5) and vulnerabilities (A2.1.6)

Suppose you have the job as head of security at a bank. In addition to cyber s physical ways that James Bond (or more likely a bunch of thugs) might break i

Risk	How to protect against i
Tailgating: sneaking in behind an employee or customer to bypass security checkpoints (a form of social engineering)	✓ access control systems – install badge readers, keycard syste allow one person per entry. ✓ turnstiles and mantraps – use security doors that lock behind to enter. ✓ security awareness training – train staff to challenge unkno doors open for strangers. ✓ security guards – position guards near entrances/exits to mo ✓ surveillance cameras – monitor entry points to detect and tr
Forced entry	✓ reinforced doors and windows – use bulletproof glass, reinfo impact-resistant materials. ✓ alarm systems – install motion detectors and glass-break se ✓ 24/7 surveillance – use high-resolution cameras covering al ✓ physical barriers – install bollards, security gates and fencin to break in). ✓ rapid police response – install direct alarm connections to lo ✓ secure vaults – store money and backups in reinforced, firep
Impersonation, e.g. posing as employees, delivery workers, IT staff, or even a celebrity (a form of social engineering)	✓ strict ID verification – require badges, photo IDs, and PIN au ✓ visitor management system – register and track visitors, issu at all times. ✓ multifactor authentication (MFA) – use biometric scans, pin c employee verification. ✓ uniform and equipment checks – ensure all staff and contracto ✓ training and drills – educate employees on social engineerin credentials before granting access. ✓ fake call prevention – implement a 'call-back verification sy requesting access over the phone.
Forcing employees to open safes or disable security through **coercion**, e.g. threats, blackmail, or physical harm	✓ panic buttons and silent alarms – place hidden emergency b ✓ time-locked safes – use safes that only open at preset times ✓ employee safety protocols – train staff to follow protocols li security without escalating the situation. ✓ two-person rule – require two employees to be present for a (e.g. opening vaults). ✓ escort policies – ensure high-risk employees (managers, vau handling large cash transfers. ✓ security escorts for at-risk staff – provide escorted exits for e large transactions.

Activity A4

Draw a simple plan of security bag and person check at an airport. Draw on security feature

Discussion Point

The head of IT at a bank suggests that they need better physical security to pr However, the head of security laughs and says that their security is super stron considered to stop anyone getting close to the vaults. What might the head o

Access to network devices, or stolen devices can lead to data breaches and un Sensitive business or personal data may be exposed.

If a cyber attacker can physically connect with any external device used to legi more likely they can hack into your network. Therefore, organisations need to unauthorised access to devices.

Risk	How to protect agains
Unattended devices	✓ take portable devices with you, or secure them in a draw off behind ✓ auto-logoff and screen locking – enable automatic scree
Shoulder surfing: watching someone enter their password, PIN or confidential information	✓ privacy screens – use anti-glare privacy filters on monito side-viewing. ✓ screen positioning – arrange screens so they face walls, r ✓ enforce a 'clean desk' policy – ensure no confidential inf printed bank statements) is left visible. ✓ awareness training – educate staff on how to spot and d
Theft of laptop or mobile device or data storage devices (e.g. USB stick). *Accidental loss can also mean these fall into the wrong hands.*	✓ physical locks and tethers – secure laptops, desktops, an bolted enclosures. ✓ restrict USB and external storage use – prevent employe USB drives or external disks. ✓ data encryption – encrypt all sensitive data stored on la even if stolen, it remains unreadable. ✓ two-factor authentication (2FA) – require employees to u facial recognition) or security keys to log in. ✓ device tracking (e.g. Apple's 'find my iPhone'). ✓ ensure devices have remote lock and wipe capabilities to ✓ limit portable devices – restrict which employees can ta the bank. ✓ surveillance and alarms – place security cameras and mo ✓ require employees to immediately report lost devices so issue replacements.
Devices or interfaces installed in public areas; attackers may install skimmers, keyloggers, or fake interfaces on bank-owned devices (i.e. ATMs, payment kiosks, public computers)	✓ tamper-proof ATM and kiosk designs – use anti-tamper s unauthorised modifications. ✓ regular physical inspections – train staff to check ATMs a (loose card readers, extra keypads, hidden cameras). ✓ CCTV monitoring – install cameras near ATMs and public ✓ disable unused USB ports and interfaces – prevent attac devices to inject malware. ✓ public device session timeouts – ensure workstations, ATM

Many organisations which don't consider themselves high risk have poor or e experienced con artist can blag their way into what should be a restricted area a check or repair by the organisation that owns the building.

Research activity
Use generative AI, e.g. Microsoft Copilot, to ask for the different methods that the fictional chara your choice) has used to bypass physical and electronic security systems.

A1.3 Impact of a credible threat, likely to result in s

If your laptop is stolen it might cost you £1,000 to replace, and yet the thief m the impact of a cyberattack can be much more wide-ranging with knock-on co organisation to fail. Below are different categories of loss.

Operational loss (A1.3.1)

Most organisations provide either a product or a service. After a cyberattack an organisation may not be able to carry out its normal operations:

- **Manufacturing output**: there may be direct delays or halts in production processes so the organisation cannot create its product.
- **Direct service availability**: the service the organisation offers (perhaps via its website) may affect customers.
- **Indirect service availability**: even if the direct product or service is not affected, the organisation's ability to take orders or provide customer service can directly affect the organisation, as well as user experience and satisfaction.
- **Data availability**: loss of access to important data, which could hinder operations and decision-making processes.

Ca
con
130
by t
spre
cripp
lapt
The
forc
pro
mas
$25

Financial loss (A1.3.2)

The organisation may directly lose sales due to the operational loss and may l reputational damage or intellectual property loss (more details below). Here a financial loss may occur:

- **Organisational financial strain:**
  - cash flow problems, e.g. running out of money in the bank (or not bei items cannot be ordered or suppliers paid
  - loss of profits due to interrupted business activities
  - increased insurance costs: future higher premiums due to elevated r insurance generally gets more expensive if you crash your car
- **Compensation costs:**
  - refunds to customers for unsatisfactory or delayed services or produ
  - payments to customers for compromising their data
  - remedial actions: staff costs investigating and recovering from back customers to try to hold on to sales
  - contractual defaults: penalties for failing to meet service agreement
  - discounts or write-offs: offering reduced prices or debt forgiveness to retain customers who have been affected
- **Legal liability:**
  - fines and penalties for breaking laws or regulations
  - statutory investigation costs arising from required investigations in the problem
  - legal fees: for hiring legal professionals to handle disputes resulting from the cyberattack

Research Activity

Find out about the *Colonial Pipeline* ransomware attack. What was the financial and operationa organisations affected?

Reputational loss (A1.3.3)

Reputational damage can have long-lasting effects on an organisation's succes

- a loss of trust with customers losing confidence in an organisation's abilit
- poor customer reviews: negative feedback can spread across platforms, s
  - rapid sharing of negative experiences via social media
  - persistent critical reviews on review websites will deter potential cus
  - direct negative product feedback on their own website or related fo
- reduced reputation or ratings scores on sites that assess reputational me

In addition, when an organisation has had a large data breach or financial loss from cyberattacks in the past, this is often mentioned as context in later press meetings or interviews.

After organisations have suffered a cyberattack, in addition to improving cyber defences, they need to put together a plan for mitigating any loss of reputation.

Research and Discussion Activity (with AI) – fixing reputations

Scenario: *a travel company has had its main website hacked where all the photos were changed days to fix and which generated a lot of negative press and a loss of bookings.*

Step 1: Write down a list of ways you can think of for how the company can recover their re

Step 2: Discuss this in a group, and add any suggestions from others that you didn't think of

Step 3: Use AI such as Microsoft Copilot; give it the suggestions you have come up with so fa additional suggestions.

When you present your work, ensure you clearly present which of the three steps each point is

Intellectual property loss (A1.3.4)

Intellectual property (IP) refers to an organisation's inventions, brand names, d secrets, proprietary technology, or other items which potentially give it an edg legally protected to give it a competitive advantage.

Loss of intellectual property through an attack can impede innovation and com

- exposure or theft of new product designs can lead to loss of market adva
- compromised research testing and development data can delay or ruin pr
- breaches of organisational strategy and trade secrets can reveal strategic confidential information could be exploited by others.

Activity A5

All-Tools-For-You is a fictional company based in the UK who makes highly designed bicycle to employ 100 full-time employees and have a turnover of 10 million pounds. They have protec Europe. However, a Chinese company has recently mimicked all of their products and are selli price. Explain why despite this many customers might buy the imitation products and what t

A1.4 Cyber security threats vary over time and cybe organisations provide regular updates on the curre threat landscape

Cyber criminals find weakness in new software and hardware, new weaknesse invent creative new physical and electronic methods to break in, or combine e a result, it is an area that is constantly changing and therefore defences need t updated. Below are three key organisations which provide regular updates on

National Cyber Security Centre (NCSC) UK
https://www.ncsc.gov.uk/

National Cyber Security Centre

Home | Advice & guidance | Respond to a c

The National Cyber Secu

Making the UK the safest place to live an

Experienced a cyber attack? Find resource

Find guidance and resources for…

You & your family | Small & medium sized organisations | La orga

Free resources for individuals, organisations and the public sector to help protect against and respond to cyberattacks. You can sign up to receive details of:

- the latest threat reports and malware analysis
- news (reports and advisories on recent activity) that alerts companies, governments and the public about recent cyber activities and what actions to take to protect against them

National Institute of Standards and Technology (NIST) USA
https://www.nist.gov/

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLO U.S. DEPARTMENT OF COMMER

What we do

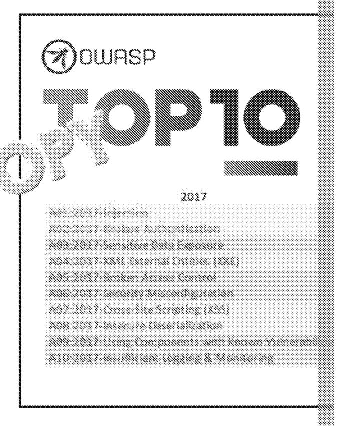
From nanoscale devices that power the most measurements and research fuel innovation a support and resources to U.S. manufacturing,

Discover how our work makes America safer, h

- Artificial Intelligence
- Cybersecurity
- Manufacturing
- Energy

An official website of the US government. NIST publishes advisories and reports similar to the NCSC to keep everyone informed about recent cyber events. They often explain how attacks took place and offer guidance on securing systems.

Open Web Application Security Project (OWASP)
https://owasp.org/Top10/



OWASP

TOP 10

2017

A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabili
A10:2017-Insufficient Logging & Monitoring

The 'OWASP Top 10' is a list highlighting the most critical security risks to web applications. It's very useful for understanding what vulnerabilities to watch out for when developing or using web applications. They are currently working on the 2025 list; the previous lists were concluded in 2017 an

Research Activity

Work through the quick training on cyber security from the *National Cyber Security Centre* websi

A2 System vulnerabili

A2.1 Vulnerabilities of different types of computer different threats they are exposed to

Network vulnerabilities (A2.1.1)

Your computer, your server, and your computer network all need to connect to the Internet. There should be a firewall (ideally a specific firewall device, or if not built into the Internet router supplied by your ISP) which stops unwanted connections to your network. Data needs to go out (for example a request from a browser for a web page) and come in (like the web page you have requested). Different types of data are allocated different ports (or holes into the network).

Standard firewall ports:

- **Port 80** – HTTP (Hypertext Tra
- **Port 443** – HTTPS (Secure HTT
- **Port 25** – SMTP (Simple Mail T
- **Port 21** – FTP (File Transfer Pr

Ports (1024 to 49151) are registere

- **Port 3306** – MySQL database
- **Port 3389** – Remote Desktop P

Dynamic/Private Ports (49152–65 used for temporary or private com chosen dynamically by the operat

Attacks on network ports		
Open Ports	Any open port is a potential entry point for attackers e.g. if port 3306 is open to connect to a database, hackers attempt brute force attacks (trying multiple passwords).	To mitigate this cl firewall rules, and Limit some open p
Spoofing	Attackers can forge packets to appear as if they come from a trusted source to bypass firewall rules and gain unauthorised access.	Use packet filterin limit exposure.
Denial of Service (DoS)	Attackers flood a port with traffic to overwhelm the system, making it unavailable.	Implement rate li configure firewall

Any external storage device which is connected to a device on a network may c save work to external storage devices to take work home, but home computer protected with outdated software and all sorts of programs installed. Then, w work computer, it introduces a virus or malware.

Devices include:

- flash/USB (universal serial bus) drives
- SD cards
- external SSD hard drives
- magnetic backup tape (a feasible risk, although rarely used by users)

Discuss the c so far on thi methods to a methods to a networked c network thr

Measures to protect against this are:

- Disable *AutoRun* functionality to prevent automatic execution of malicious code.
- Automatically scan external drives for malware with a virus checker befor
- Provide alternative methods for users to access data from other locations, Storage in the cloud such as *OneDrive* and *Google Drive* is still a risk to spr
- Purchase devices without SD card slots, CD/DVD drives or USB drives so de

Misconfigured hardware, especially firewalls, can create vulnerabilities – see s

Organisational vulnerabilities (A2.1.2)

Organisations must manage permissions, password policies, and password management effectively to prevent unauthorised access, data breaches, and system compromise.

Dis

How many passwords do yo
If not, why not? If so, do you

Category	Threats	
Permissions or Privileges	✓ Not carefully managing permissions, e.g. giving all staff admin access, can lead to unauthorised access.	✓ Follow le ✓ Implemen ✓ Regularly unused ac
Access Control on Files, Folders, Devices, and Services	✓ Unauthorised access to sensitive files and services. ✓ Poor device security allows data theft. ✓ Misconfigured group policies lead to security risks.	✓ Apply gra ✓ Use multi sensitive s
Password Policy	✓ Short or weak passwords make brute-force attacks easier. Passwords using personal details such as names and birthdays are easier to guess. ✓ Reused passwords can be exploited if previously leaked. ✓ Shared passwords increase unauthorised access risks.	✓ Set minim complexit ✓ Enforce pa ✓ Disallow c ✓ Restrict co
Password Management	✓ Storing passwords in plain text exposes them to attackers. ✓ Forgotten passwords encourage users to reuse passwords on multiple sites. ✓ Auto-fill credentials can be stolen through malware or compromised browsers.	✓ Train user ✓ Encourage password ✓ Disable br password ✓ Cloud pas multiple d
New User and Leaving User Processes	✓ New users are not yet trained. ✓ Departing employees may still have system access. ✓ Delayed account deactivation can be exploited by attackers.	✓ Implemen ✓ Automate ✓ Regularly ✓ Automatic used for a ✓ Microsoft deleting a there are s person or

Activity A6

1. How can an organisation balance security needs with convenience in its password policies?
2. When should MFA be used?
3. What's the problem with using the same password on more than one website?

In January to March 2019 the A
all Microsoft user accounts an
usernames and passwords tha
breaches at other online servic

At the same time a survey by L
from which 91% said they und
and yet **59% said they reuse**

Software vulnerabilities (A2.1.3)

Scenario: Dave is a BTEC computing student who plays drums in a band and w
He searches the web and finds some software called MusicRecorder on a site c
thinks sounds legitimate, and he downloads and installs it. Unfortunately, it i
hackers, and the software contains malware which goes across all the shared s
encrypting all the files. This happens in April just before school exams and the
school otherwise all the students who didn't backup their work will lose their c

Dave is not alone – there are many web sites which appear legitimate which a
installers contain the real software alongside malware, so it appears to have i

Another issue is that many people do not want to pay for software, which can
illegal copies of the software on the Internet, and do not download the softwa
software. Hackers know this, and many illegal copies of software contain mal

Yet another issue is where users steal software from the organisation they are
the software install files are on the network and copy them to install at home.
software cannot be registered and therefore software updates can't be downl
software updates are to remove new or discovered flaws in the software. It is
stories where a virus is affecting thousands of computers that are running an c

Increasingly, schools and organisations do not allow users to install software, and they have to request it from the IT department. This is inconvenient but protects the organisation.

If downloading software at home, you sh

- Only download software that you ha recommended or has a lot of positiv
- Use the trusted source so, for examp from the Microsoft websites
- Ensure the website is using HTTPS a in the browser
- Ensure you have up-to-date antiviru so it automatically checks install file

Some software suppliers provide a *cryptographic hash* of the software. When
software updates, you run a program to generate the hash code, and check th
software supplier's website.

Activity A7

Lawrence is a sixth-former who plays in a band and wants to download some music editing s
edit recordings of the band. He has a school laptop and isn't allowed to bring in his own devi
allow him to install his own software and says that the *GarageBand* software is not sanctione
to Lawrence to ease his frustration?

Research Activity

Find a specific example from the last 10 years where a company suffered legal issues or financia
organisation using unauthorised software. Who can find the biggest negative impact?

The table below lists different methods that hackers may use to gain access th
This may involve either accessing data on the website or gaining control of the

Vulnerability	Description	Mitigation Strategies
SQL Injection	Attackers inject malicious SQL code into input fields, manipulating database queries to gain unauthorised access, modify data, or delete tables.	Use *parameterised queries* or *prepa statements*, input validation, least privilege database accounts, web application firewall (WAF).
Cross-Site Scripting	Attackers inject malicious scripts into trusted websites, allowing them to steal user data, hijack sessions, or redirect users to malicious sites.	Input validation, output encoding, u frameworks with built-in XSS protection, HTTP-only cookies.
Cross-Site Request Forgery (CSRF)	Attackers trick users into performing unwanted actions on websites. The attack relies on the victim already being authenticated.	Use anti-CSRF tokens (synchroniser tokens), *SameSite cookies*, requirin authentication for sensitive actions, proper HTTP method usage (i.e. GET retrieval, POST for changes).
Buffer Overflow	Occurs when a program writes more data to a buffer than it can hold, overwriting adjacent memory and potentially executing malicious code.	Use safe string handling functions, boundary checks, address space lay randomisation (ASLR), data executi prevention (DEP), consider only usi memory-safe programming languag

Zero-day exploits

A **zero-day exploit** is a cyberattack that takes advantage of a software vulnerability before the software developer is aware of it or has released a fix. Since there is no patch available at the time of discovery, these exploits are highly dangerous and can be used for cyber espionage, malware distribution, and system compromise.

SQL Injecti

Suppose you go to your profile o
name, but instead of your name y
users;. In some circumstances
this query and output it on the sc

The programmers should either r
from all input at all entry points o
the database which only treats th
database fields as text (e.g. paran

Warning

You can test this on your own co
experiment on live sites as this
attempted hacking.

Read *The 10 Worst Zero-Day Attacks Ever* at **zzed.uk/12912-zero-day**

The first example is *Code Red Worm (2001)* which infected over 359,000 systems globally in le
cost more than $2 billion. It exploited a vulnerability in Microsoft's IIS which was widely usec

Operating System (OS) (A2.1.4)

As well as software, the operating system (Windows, Linux, Apple OS) can als below covers some of the weaknesses that can let hackers in.

Vulnerability	Threats and Risks	
Unsupported or Out-of-support Versions	• No security updates, leaving known vulnerabilities exploitable. • Incompatible with newer security tools, increasing risk.	• Upgrade to s • Isolate legac
Missing Patches or Updates	• Zero-day exploits become more effective if patches are delayed. • Known security flaws are advertised on the Internet to hacking communities.	• Enable autom • Periodically c been applied • Use vulnerab missing patc
Missing or Incorrect Security Settings	• Default settings may leave ports and services exposed. • Weak access controls can allow privilege escalation. • Unconfigured firewalls or antivirus leave systems open to attacks.	• Strengthen O unnecessary • *Implement G SELinux/App* automatically • Regularly au ensure compl

Cyber threats to Graphical User Interface (GUI) and Command Line Interface

Most of the threats to operating systems apply to both GUI and CLI operating few differences that need to be considered

GUIs are generally more accessible and therefore likely to also be used by use knowledge who are more likely to be susceptible to social engineering attacks configuration settings when trying to get something to work. The additional c can introduce more vulnerabilities such as buffer overflow or input validation

CLIs are more efficient and designed to automate tasks which can suit cyber a complicated, often in multiple hierarchical configuration files so mistakes can dashboards it can be harder to spot alert warnings.

Mobile devices reliant on Original Equipment Manufacturers software (A2.1.5)

One key problem with mobile devices is that often the manufacturer (e.g. Sam OnePlus, Vivo and Motorola) control the updates because they made custom So when there are updates to the underlying operating system (e.g. Android) and so there can be a considerable delay before the users get the updates.

In addition, OEMs generally stop supporting older phones after a number of y their old phone are faced with the choice of buying a newer model or sticking security updates

Physical vulnerability points (A2.1.6)

See A1.2.5

Human vulnerability points (A2.1.7)

Leaks	Sharing Security Details	F
• *Accidental* leaks occur when sensitive information is shared unintentionally (e.g. via email, social media, or insecure channels). • *Intentional* leaks can involve insiders stealing or sharing sensitive information for personal gain or malicious intent.	• Sharing passwords or login credentials compromises system security. • *Social engineering attacks* can exploit people's tendency to share sensitive information with the wrong people.	• Weak or in handling a to exploita • Ineffective passwords, easily gues • Human erro encryption sharing, or

Key best practices for addressing human-related vulnerabilities:

- Establish clear security policies for accessing and sharing sensitive data, ensuring users understand the importance of following these rules.
- Conduct regular security awareness training for all users on common threats (phishing, social engineering), secure handling of data, and how to spot suspicious activities.
- Conduct regular security audits and tests (e.g. penetration tests, internal audits) to identify vulnerabilities in human processes.
- Require the use of password managers to avoid insecure storage and sharing of passwords, and encourage strong, unique passwords for a

In
wa
Wh
th
co
bo
zz

Research Activity

Search the *Fortinet* list of *IoT Device Vulnerabilities* and make a list of all the possible vulner your house, e.g. voice-controlled speakers? What do you think are the top three vulnerabilit

Security implications of cloud computing and of the Internet o

Software used to be installed on individual computers. Then a lot of software
and then was networked through the Internet across multiple sites. Much of t
cloud-based. This centralisation has advantages but also the following risks.

Risk	Implications	
Missing, incorrect or default security settings	• Improper configurations can leave cloud environments vulnerable to attacks (e.g. open ports, weak authentication). • Default security settings may not meet an organisation's needs, leaving critical data exposed.	• Implemen ensure mi • Regularly default co
Third party or cloud provider access	• The cloud software provider can access your sensitive data. • You are likely to use third-party API integrations or credit card payments. • Your IT support may have access.	• Data encr data from • Establish and data a
Reliant on third-party security	• Organisations rely on the cloud provider's security measures, which may not align with internal security policies or standards.	• Ensure th standards • For high-r audits of t their prac
Data movement outside the organisation's network and over the Internet	• Risk of interception, theft or tampering when sensitive data moves over the Internet, especially without proper encryption.	• Use VPNs, to-end en • Limit data governanc • Regularly across net

St Jude Medical recalls 465,000 pacemakers due to security vulnerabilities!
Initially, in 2016 *St Jude Medical* denied the allegations and sued the two companies who clai
However, they subsequently made a security update to resolve some of the flaws in January 20
software update to 'reduce the risk of patient harm'. Patients had to visit a healthcare provide
home. US CERT included the following details in their advisory notes:

- The pacemaker's authentication algorithm could be compromised or bypassed
- The device's battery could be drained by an attacker repeatedly sending *RF wake-up* com
- Some versions of the pacemakers transmitted unencrypted patient information via RF co

Discussion Point

Amelia buys a remote-controlled dog which she registers on a dedicated IoT site and controls through her speaker which is connected to the Internet. What are the cyber security risks invo

IoT devices

The Internet of Things (IoT) refers to the network of physical objects, such as d sensors, and other objects, that are connected to the Internet and can collect, objects are often embedded with sensors and software to enable them to com central systems without direct human intervention. The IoT increases security devices, their interconnectivity, and potential vulnerabilities in the way they ar Below are some of the key issues:

Risk	Implications	
Weak or no encryption on IoT devices and their transmi	Data transmitted by IoT devices without encryption can be intercepted or tampered with.	• Encrypt using TL
Default passwords	• Many IoT devices come with default passwords that are often easily guessed or publicly known.	• Change installat • Enforce IoT devi
Lack of patches and updates	• IoT devices may not receive timely patches or updates, leaving them vulnerable to known exploits.	• Establis device f
Deployment by non-IT staff	• Non-IT staff may lack the knowledge to securely configure IoT devices.	• Ensure I configur • Provide and ope
Flawed or insecure control interfaces	• Weak or insecure control interfaces may allow unauthorised access to IoT devices or systems.	• Secure c authent • Use mu accessin
Poor or no compatibility with network security systems	• Some IoT devices may not integrate well with existing network security tools, such as firewalls, intrusion detection systems, or monitoring tools.	• Choose security network • Segmen isolate I
Eavesdropping, and smart devices always listening and sending voice data	• Voice-activated IoT devices, such as smart speakers, may constantly listen for commands and capture private conversations.	• Disable when no • Ensure v

Activity A8

You are the head of IT security for the UK prime minister and have been tasked with the cyber Based on the above table of risks, what actions would you propose to your team to prepare fo tips would you give to the very busy prime minister?

A2.2 Where to find up-to-date sources of informati hardware and software vulnerabilities

Staying informed about security vulnerabilities is important for protecting syst sources where IT professionals and cyber security specialists can find the lates

Manufacturers' websites (A2.2.1)

Hardware and software manufacturers maintain official security advisories an They provide **patches, firmware updates, and security fixes** when vulnerabili

Often the updates are automatic, e.g. as part of monthly operating system upd any updates each time the user opens the application.

IT support may sign up to a mailing list or for RSS feeds to receive notifications patches, e.g. to deal with a current computer virus.

Ideally the IT support department should have a monthly check that automati any manual updates are approved, and a manual check on the websites for so automatic updates. Organisation-level antivirus software normally provides a support can identify any devices which do not have up-to-date antivirus updat

Forums and technical help websites for IT professionals/cyber

Web forums and technical help websites offer discussions among IT professionals and security researchers who share real-world experiences. Security experts often provide workarounds, mitigation techniques, and best practices.

Sometimes they are run by the software manufacturers and sometimes they are independent.

Often, vulnerabilities are discussed on forums and technical help websites before official patches are released.

Stack Exchange (Security)	**https://secu** Community
Reddit (cyber security)	**https://ww** Discusses v security ne
Cisco Security Community	**https://com** **p/4561-se** Cisco-relate
Microsoft Tech Community	**https://tech** **com/catego** Discussions

Third party websites specialising in specific hardware or soft

The table contains examples of websites which collect vulnerability reports from multiple sources, including government agencies, researchers, and manufacturers.

They provide detailed descriptions, impact analysis, and exploit availability. Some sites track exploits used by hackers, helping security teams prepare defences.

National Vulnerability Database (NVD)	**https://nvd.nist.gov** Tracks known vulne
Exploit Database (Exploit-DB)	**https://www.exploi** Lists publicly availa
CERT Coordination Center (CERT/CC)	**https://www.sei.cm** Vulnerability reports Mellon University.
Common Vulnerabilities and Exposures (CVE) List	**https://www.cve.or** Identify, define and cybersecurity vulne
The Hacker News	**https://thehackern** Reports on hacking,
MITRE ATT&CK	**https://attack.mitre** Public knowledge b understand how rea

A2.3 Attack vectors

An *attack vector* is a method or pathway that cybercriminals use to exploit vul
devices. Below is a breakdown of attack vectors categorised under wireless, In
network access devices.

Wireless attacks (A2.3.1)

Wireless technologies transmit data through the air, making them vulnerable t
unauthorised access.

Wireless Technology	Security Risks	
Wi-Fi (IEEE 802.11)	Weak encryption, rogue access points, packet sniffing	Use WPA3, di access points
Bluetooth	Weak pairing protocols, unauthorised access	Use 'Not Disco
Cellular (3G, 4G, 5G)	Fake phone towers, SIM swapping, insecure mobile networks	Use encrypted
Satellite Link	Weak encryption, signal jamming, spoofing	Use encrypted
Infrared (IR)	Short-range attacks, device hijacking	Use limited IR
Near-Field Communication (NFC)	Contactless skimming, unauthorised data transfer	Disable NFC w
Radio-Frequency Identification (RFID)	Passive interception, cloning, replay attacks	Encrypt RFID t

Go to **zzed.uk/12912**

Research Activity

Read the article at **zzed.uk/12912-security** which is about ensuring wireless network security.
suggestions and categorise each one into (1) either for everyone, including home Wi-Fi network
organisations, or (3) only for large and government organisations.

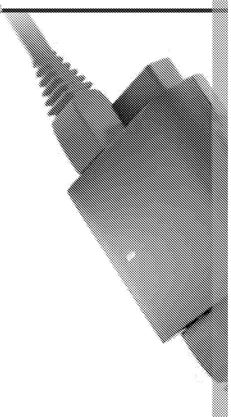
Do you need to check your home Wi-Fi setup as a result of reading this article?

Internet connection attacks (A2.3.2)

Different Internet connection types and devices introduce unique vulnerabilit

Connection Type	Device	Security Risks
Copper Cable (Ethernet, DSL)	**Cable Modem or Router**	Physical tapping, man-in-the-middle (MITM)
Optical Fibre	**Fibre Modem or Router**	Difficult, but still possible to or read signal leakage
Wi-Fi and Cellular/5G	**Wireless Router, Cellular Device, or 5G Router**	*Covered under wireless attac*

KSEC World sells specialised security tools including *hacking* tools for penetration testing. Here you can see the *KSEC Hak5 Packet Squirrel II* which is a *network sniffing and automation tool.*



Internal network access devices attack vectors (A2.3.3)

Switches, routers and WAPs manage internal communication but can be explo
disrupt network traffic.

Device	Security Risks	
Router	Default passwords, open ports, firmware vulnerabilities	Change defa
Switch	VLAN hopping (tricking a switch to send traffic on a VLAN they don't have access to), MAC spoofing	Enable MAC
Wireless Access Point (WAP)	Rogue APs, weak encryption	Use enterpri

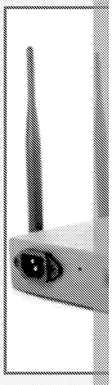
To reduce risks some general mitigation measures are to:

- Use strong encryption (e.g. WPA3, TLS, VPN)
- Disable unnecessary services (e.g. WPS, remote admin access)
- Regularly update firmware and software
- Monitor network traffic for anomalies
- Implement multifactor authentication (MFA)

You don't need to learn these technical terms, but they help you understand t
in this section:

1. **Packet Sniffing: c**apturing data as it travels over a network, often to stea
2. **Weak Pairing Protocols:** insecure methods of connecting devices (e.g. Bl
by attackers.
3. **SIM Swapping:** attackers trick a mobile provider into transferring your nu
access your accounts.
4. **Insecure Mobile Networks:** public or poorly secured mobile networks th
manipulated.
5. **Signal Jamming:** blocking wireless signals to disrupt communication betw
6. **Spoofing:** pretending to be a trusted device or user to gain unauthorized
7. **Short-range Attacks:** attacks that require physical proximity, e.g. interce
8. **Device Hijacking:** taking control of a device without the owner's permissi
9. **Passive Interception:** secretly listening to or recording data without alte
10. **Replay Attacks:** reusing captured data (like login credentials) to trick a sy

Shown here is the *Hak5 Wi-Fi Pineapple Enterprise Pro Pentesting Device* from **KSEC Worldwide**



Basic Operations

1. **Reconnaissance**:
   - Use the **Recon** module to scan for nearby Wi-Fi networks and devices.
   - Identify potential targets and gather information such as SSIDs, BSSIDs, and signal strength.
2. **PineAP Suite**:
   - Enable the **PineAP** suite to perform advanced Wi-Fi attacks.
   - Use **Deauth** to disconnect clients from their networks, forcing them to reconnect to your device.
   - **SSID Pool** allows you to broadcast multiple fake networks to lure clients.
3. **Client Management**:
   - Monitor connected clients and their activities.
   - Use the **Client** module to manage and analyse connected devices.

A2.4 Types and uses of tools and methods to assess computer systems

Assessing vulnerabilities in a computer system is essential to identifying poten exploited. Various tools and techniques, like those below, help security profes Attackers also use all of these tools to test for weaknesses, although hopefully tools from outside your network, not from inside.

Port scanners (A2.4.1)

A port scanner checks for open, closed or filtered network ports on a system o vulnerabilities by [illegible] unauthorised access.

Network mappers and system discovery tools (A2.4.2)

A network mapper (or system discovery tool) scans and maps connected devic relationships and configurations. It can help you find old devices that are still c not be connected.

Registry checker (A2.4.3)

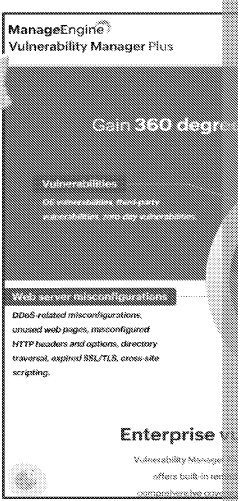
A registry checker scans the Windows registry database for unauthorised chan vulnerabilities. It can check for weak security settings, detect startup program identify malware modifications in the registry.

Website vulnerability scanner (A2.4.4)

A website vulnerability scanner tests websites for security flaws like SQL injection, cross-site scripting (XSS), and misconfigured security settings.

Vulnerability detection and management software (A2.4.5)

These tools automate the process of scanning for vulnerabilities, assessing risks, and managing security patches. They may include all the above tools and give you an overview report of weaknesses. In addition, they may identify outdated software unpatched vulnerabilities, carry out automated penetration testing to find weak spots, and manage the security policies across an organisation.



ManageEngine
Vulnerability Manager Plus

Gain 360 degre

Vulnerabilities
OS vulnerabilities, third-party vulnerabilities, zero-day vulnerabilities.

Web server misconfigurations
DDoS-related misconfigurations, unused web pages, misconfigured HTTP headers and options, directory traversal, expired SSL/TLS, cross-site scripting.

Enterprise v
Vulnerability Manage
offers built-in re
comprehensive cov

Commercial to vulnerabilities, but

Assessing user vulnerabilities (A2.4.6)

This considers the human factor and examines how users may introduce secu of training. To test the system for human weaknesses a security firm may use

1. Carry out training and test staff on the answers
2. Carry out password tests looking for weak or reused passwords
3. Create phishing simulations to test whether or not users click on fake phis

Nmap (Network Mapper) is a powerful free (open-source) tool for network discovery and **zzed.[illegible]2-NMap** which is an excellent YouTube tutorial video from NetworkChuck o information about computers and servers on your network, which can be used by hackers to

Warning: scanning or probing networks without permission can count as unauthorised a identifying open ports can be seen as *attempting to access*.

A2.5 Use of independent third-party review of a sy designs before implementation

Before deploying a new system or network, organisations can seek independe that security risks are identified and mitigated. These reviews help establish t the system's security measures.

Some industries have specific security and compliance standards. For example payments then you need *PCE DSS compliance*, and if you are a healthcare orga *ISO 27001*. All organisations need to comply with *GDPR*.

Establishing due diligence (A2.5.1)

Due diligence is the process of assessing and reviewing a system or network d identify and mitigate potential security risks. Unless the organisation happens their payroll, they are likely to hire a specialist company to carry out, for exam

- Security Audits – where external cyber security experts assess system/ne
- Penetration Testing (Pen Testing) – simulates hacking attacks to find wea
- Compliance Assessments – to ensure adherence to industry standards (e.

Third party certification (A2.5.2)

Independent third-party reviews validate whether an organisation has followed security best practices.

Third party certifi
- provides cred best practice
- helps organis compliance r
- improves tru and regulato

Research Activity

Find three companies in the UK which provide third-party support for organisations. Draw up a Also identify what recognised accreditation they help you obtain. In particularly do they offer *IS*

A2.6 Applications and features of penetration testi

Penetration testing, sometimes abbreviated as 'pen testing', is essentially *appr* experts try to break into computer systems legally, using the same tools and te weaknesses before the bad guys find them.

Use a range of techniques to find weak spots (A2.6.1)

Penetration testing uses vulnerability detection and management software, so and organisational weaknesses, and an understanding of an organisation's spe weaknesses.

Check against lists of known vulnerabilities (A2.6.2)

Penetration testing checks against known vulnerabilities which will include tho well as current threats such as those listed on the National Vulnerability Datab

Produce reports in appropriate formats (A2.6.3)

After testing, a report is created to summarise what was found and how it can clear and easy to understand for different audiences, such as technical teams a that the organisation can u what actions need to be tak

OWASP 2021 Top 10 https://owasp.org/Top10/
1 Broken Access Control
2 Cryptographic Failures
3 Injection
4 Insecure Design
5 Security Misconfiguration
6 Vulnerable and Outdated Components
7 Identification and Authentication Failures
8 Software and Data Integrity Failures
9 Security Logging and Monitoring Failures
10 Server-Side Request Forgery

** we anticipate the new 2025 top 10 soon*

The *OWASP Top 10* is a list o web applications, published *Security Project (OWASP)*.

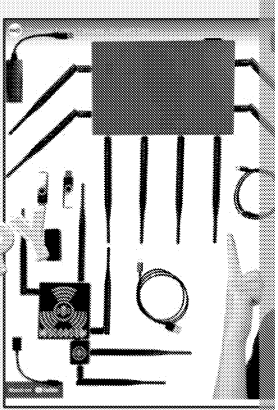
Go to **zzed.uk/12912**

Research Activity

Browse the large number of Hak5 penetration hacking tools at **zzed.uk/12912-hak5**

Also watch the video which explains what a lot of the tools do.

For those of you who have watched films where USB sticks are plugged in to hack computers – you can see that these are based on reality!



A2.7 Passive risk management measures

In cyber security, managing risks is about understanding potential problems a them. 'Passive' risk management refers to actions taken to reduce risk withou For example, it might be considered that the risk is too low or the consequen the threat.

Risk transfer to a third party (A2.7.1)

This involves moving some or all the risk to another party. The most common v paying a *service provider*. A service provider (or *Cyber security Service Provide* specialising in providing security services, such as threat monitoring, vulnerabi response, to protect clients' information systems and data from cyber threats.

> *Scenario: A school realises it is too costly or too complex to handle all its IT s they hire an external Managed Security Service Provider (MSSP) to manage school can reassure parents that they have professionals carrying out the IT succeeds, the blame can be placed on the external company.*

Risk avoidance (A2.7.2)

This strategy involves stopping an activity altogether to eliminate risk.

> *Scenario: An organisation has a software system which provides a service t and now highly vulnerable to cyberattacks. The cost of updating the syster programming, is much higher than the profits they are making from the sys offering that service.*

Risk acceptance (A2.7.3)

Sometimes, the cost of mitigating a risk is too impact of the risk event. In such cases, an orga the risk. For example, a school might decide t being hacked is low and the cost of securing it ensure that all data on the computer is encryp and to accept the low risk of being hacked, an systems instead. Only time will tell whether, or not, it was a good strategy!

Discuss exa
'accept' a ri

Activity A9

Eloise has just decided to create a range of AI-generated images and to put them on T-shirts wit the slogan 'AI Generated: Because Humans Need a Break!'. They proved popular in her village an she has already made over £1,000. She has set up her own website to start selling them on the Internet, but an IT expert friend has told her that there are many security issues with her website. She is worried that it would cost way too much money to pay someone to fix the problems, so is considering either accepting the risk or stopping the business.

Help Eloise weigh up the choices.

A3 Legal responsibili

Students should know the responsibilities in relation to current legal legislatio

A3.1 Current legislation

UK General Data Protection Regulation (UK GDPR) (A3.1.1)

EU GDPR legislation of 2016 was [illegible] top of earlier legislation; the UK was i of leaving the UK, the UK GDPR was created, which continued to make everyo responsible for following rules about how the data is used, states the rights th their da

See **zzed.uk/12912-ICO** Go to **zzed.uk/12912**

UK Computer Misuse Act 1990 (A3.1.2)

This legislation aims to protect personal data held by organisations from unauthorised access and modification. In the late 1980s, it became clear that legislation was needed to address the rise in computer use. The Computer Misuse Act of 1990 was created to protect against exploitation, defining three offences:

1. Unauthorised access to data, requiring proof of access, lack of permission, and awareness of the lack of permission.
2. Unauthorised access with intent to commit another offence, requiring evidence that the gained data would be used for further illegal actions.
3. Unauthorised modification of data, including spreading a virus.

'Obtaining access' involves actions such as copying, erasing or altering data, or causing output. Even unsuccessful attempts to access or interfere with security systems count as offences.

The Act also acknowledges that computer crimes may cross national borders, giving British courts jurisdiction when a significant link to Britain exists. Updates in 2006 and 2015 enhanced penalties, included new crimes such as distributing malware, and expanded the Act's scope.

Consequences range from six months in prison and a £5,000 fine for unauthorised access to computer material, to five years and an unlimited fine if you have intent to commit a further crime, to 14 years in prison for damage to critical national infrastructure and life imprisonment if there is significant risk of serious damage to human welfare or national security.

See **zzed.uk/12912-legislation** Go to zzed.uk/12912

The Computer Misuse Act 1990 was prompted by the 1987 case of Steve Gold and Robert S unauthorised access to British Telecom's systems and even accessed the Duke of Edinburg under [illegible] laws, was overturned because those laws didn't clearly apply to computer mi

A3.2 Areas current legislation applies to

There are some obvious ways the current legislation protects you and your da that if you order a product by email then the company cannot start using your similarly they must keep your email address secure.

Protection of data, in storage and when transferred (A3.2.1)

Your data must be protected when it is stored in a database on a server, on th other storage medium, including [illegible]. Key measures specific to stored da

- *Encrypting data and files* so that it's unreadable without the decryption k
- Implementing strong *access controls* to restrict who can access stored da
- *Maintaining regular backups* to prevent data loss in case of hardware failure o the[illegible]s be secure.
- Ensuring *physical security* of storage devices and servers.

Your data must also be protected when it is transferred, for example between networks and across the Internet. Key measures specific to data being transfe

- Using secure protocols such as HTTPS, TLS and SFTP to *encrypt data durin*
- *Encrypting email communications*, especially when sending sensitive info
- Implementing firewalls, intrusion detection systems, and other *network s*

Privacy and Personally Identifying Information (PII) (A3.2.2)

This focuses on the protection of individuals' privacy and the handling of their be used to identify an individual, such as name, address, date of birth, Nationa number, email address, phone number, biometric data, and online identifiers (

All the data protection principles outlined below apply to all personal data incl is necessary for a specific purpose, only using PII for the purposes for which it with individuals about how their PII is being used, and respecting individuals' r restrict the processing of their PII.

Unauthorised access to computers and devices (A3.2.3)

As well as following the rules for how personal data can be used, organisations must prevent other, unauthorised access to computers, devices and systems which hold personal data. This means that cyber security is essential and not optional!

Two S
(Sam
legit
caugh
for, a
offen

Unauthorised access to and modification of data (A3.2.4)

One difficult area for organisations with thousands of employees is to ensure t organisation have access to the right sets of data, and also to ensure that emp need to have access to in ways that they shouldn't. Some measures to implem

- Least privilege: giving users only the minimum necessary access to data a
- Access Control Lists (ACLs): control who can access and modify specific d
- Audit trails: to track who has accessed and modified data.
- Data integrity checks: to detect unauthorised modifications.
- Intrusion Detection/Prevention Systems (IDS/IPS): to detect and prevent u

A3.3 Legal responsibilities legislation

General Data Protection Regulation (GDPR) (A3.3.1)

See **https://ico.org.uk/** for the UK government website with the full legislatio

GDPR: UK Data Protection Act 2018 Everyone responsible for using personal data has to follow strict rules called 'data protecti information is:	
- used fairly, lawfully and transparently	Data must be handled in a way that is fair to the ind open and honest about how they are using the data for processing personal data, for example if: - the individual has consented to them having th any time) - it is part of a contractual obligation (processin - the organisation has a legitimate interest e.g. f must conduct an LIA (legitimate interests' asse valid reason and that the processing is necessa - processing the data is of vital interest, e.g. a h with emergency services - there is a legal requirement to process the dat employee's tax information to HMRC - it is in the public interest, e.g. a local council p health monitoring
- used for specified, explicit purposes	Organisations must have a clear and specific reason in the first place, i.e. they can't simply collect data a If they want to use the data for a new purpose, they
- used in a way that is adequate, relevant and limited to only what is necessary	Organisations should only collect the minimum am achieve their stated purpose, i.e. they shouldn't col
- accurate and, where necessary, kept up to date	Organisations are responsible for ensuring that the up to date. If they become aware that data is inaccu
- kept for no longer than is necessary	Organisations can't keep personal data indefinitely. how long they will keep the data, and they must de longer needed.
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage	Organisations must take appropriate physical and te data from unauthorised access, accidental or delibe enforcing strong passwords, multifactor authenticat controls, software updates, anti-malware software, a

Your personal rights (often referred to as *digital rights for citizens*)

The table on the previous page outlines the responsibilities of organisations holding your personal data. The following list outlines your rights from your perspective as an individual. People have the right to:

- access their own personal data
- be informed about how and why their data is used
- have their data corrected, removed or restricted
- object to the data being used
- portability (have data supplied in a machine-readable format)
- not to be subject to a decision based solely on automated processing (which may restrict the scope of AI systems)

If you a
a comp
to kno

Additional points to be aware of

1. There is stronger legal protection for more sensitive information, such as opinions, religious beliefs, trade union membership, genetics, biometrics health, and sex life or orientation.
2. There are separate safeguards for personal data relating to criminal convi
3. If you hold data about someone else (the data subject) you are a data contro processing data belonging to another organisation then you are a data proce (data processing agreement) with the data controller. A good example of a D **https://eRevision.uk** → Privacy and GDPR Notice → Terms and Conditions o

Activity A10

You should know the principles of GDPR and be able to recite them.

1. What does GDPR stand for, and what is its primary purpose?
2. What is the difference between a 'data controller' and 'data processor' under the UK G
3. What are the six key principles of the UK GDPR?
4. A school collects students' names, addresses, and medical information. What legal basis s should they use to comply with the GDPR?

Discussion Point

Suppose a housing association receives requests from organisations such as utili debt collecting companies for the addresses of previous tenants who have debts they share the information?

After your discussion have a look at **zzed.uk/12912-case-study** for a case stud

Go to **zzed.uk/12912**

A4 Software and hardware secu

A4.1 Software and hardware

Physical security measures to protect software and hardware

It is pointless spending thousands of pounds on cybersecurity if someone can office and pick up a computer or hard drive or server. Protecting software and unauthorised access, theft, or tampering requires robust physical security mea

1. Site Security Locks
Locks on doors and server cabinets help restrict unauthorised access to facilities where critical hardware and software are stored. These include:

- Mechanical key-based locks; a simple solution but susceptible to lock-picking or lost keys.
- Programmable electronic keypad locks, card entry systems and biometry security. They can provide logs of access attempts.
- Network-connected smart locks integrate with security systems to allow remote access control and monitoring through the Internet.

2. Card Entry Systems
Card-based access control regulates entry into secure areas. Different types include:

- Near-Field Communication (NFC); short-range wireless technology used to verify access cards or mobile devices for authentication.
- Radio-frequency identification (RFID): uses radio waves to detect RFID keycards in users' pockets to unlock doors.
- Barcode and QR Code: entry systems that scan printed or digital barcodes and QR codes for temporary access control.
- Magnetic stripe cards: old technology using a magnetic strip to store credentials, swiped through a reader for access.
- Embedded microprocessor/chip (smart cards): chip-based cards often used with PINs or biometric authentication.

3. Biometric Security
Biometrics provide a high level of security by verifying physical characteristics unique to each individual. These include fingerprint scanners, eye iris/retina scanners, facial recognition, voice and handwriting recognition, signature and pattern recognition (which can use a touchscreen or pad to analyse writing style, pressure, and stroke patterns).

Fingerprint scanners are common on laptops; facial recognition is common for mobiles; and voice recognition is common for voice-controlled speakers and can also be used over the telephone.

4. Closed-Circu
Surveillance ca
around protec
preventing acc
door security t
Features can i

- Motion de
- Remote m
- AI-based a
  suspicious

5. Security Sta
Physical securi
access and res
roles may inclu
CCTV and alar
access points a

6. Alarm Syste
Alarms in build
security teams
breaches. They
broken windov
also be installe
drives to preve

7. Protected C
Protecting net
interception. U
stop physical a
preventing ta

8. Staff Trainin
Security is only
Training helps

- Recognise
  or phishin
- Follow acc
- Respond t

Data storage, data protection and backup, and recovery proce

Backup types

Backups are essential for protecting data against accidental deletion, corruptio cyberattacks. The three main types of backups are:

- *Full backup:* a complete copy of all selected data. It is relatively simple to in one place. However, it is also relatively time-consuming and requires t
- *Differential backup:* this copies only the files that have changed since the much faster than a full backup and uses less storage. Restoring data requ the latest differential backup
- *Incremental backup:* this copies only the data that has changed since the la backup of any type (full or differential or incremental). It is the fastest bac type with minimal storage requirements. However, restoring data can be s because it requires the last full backup plus all subsequent incremental ba

One possible strategy is to take full backup periodically (e.g. once a week) then make daily differential backups. If that is not frequent enough for the organisation, i.e. it is too big a problem if a day's work is lost, then incremental hourly backups could be taken.

Backup strategies

Suppose an organisation takes full backups of their server every day and keeps server. If the building ever burns down, then they lose the server and the back Therefore, it is a good idea to consider:

- *Onsite backups* are stored at the same location as the original data (e.g. b external hard drives, network-attached storage). Although very quick and provide a backup in case of extreme disaster, it is a good idea to keep the
- *Offsite backups* are stored at a different physical location, e.g. in remote d would have to happen at both sites at the same time. The backup can be external hard drive then taken off-site, or the backup can be made ove
- *Cloud backups* are off-site, on a remote server provided by cloud services Azure. The third-party services usually provide an additional periodic bac

Now that superfast fibre has been rolled out throughout much of the UK at rea viable to make nightly cloud backups. However, it is still normally more costly than to make your own tape backups and physically take them off-site.

Backup methods

- *Automated backups* are scheduled or continuous backups without user in specialised software and monitoring. If alerts fail, then no one may realis
- *Manual backups* require a user to initiate the backup process (and possibl external drive). They give more control over what gets backed up and wh error and may be inconsistent. Manual backups are more suitable to sma simple backup needs.

Disaster recovery sites

- A *warm site* is a backup site that, as well as a backup of the data, has som with some setup could become an operational site within a few hours o
- A *hot site* is a fully operational backup location with real-time data replication from the original site so that, in the case of disaster at the original site, it can take its place very quickly. It is used by organisations that need immediate recovery, e.g. banks and hospitals.

RAID

A redundant array of independent drives (RAID) system is a way of configuring multiple storage drives to act as a single drive for file storage. There are many levels of RAID, which use the multiple drives in different ways.

Aside from RAID 0 (which just means using multiple drives as if they are one drive) they mirror or duplicate data on more than one drive. Ideally RAID drives should be *hot-swappable*, which means it is possible to remove any one disk while the server is running and replace it with a new one. The server gives users a warning if a drive fails. Once the new disk is inserted, the storage controller copies the required data to the new drive.

This means it is much better than a backup in the case of a single drive failing. However, backups are still needed in the case of a fire or other disaster at the site.

Archiving vs backup

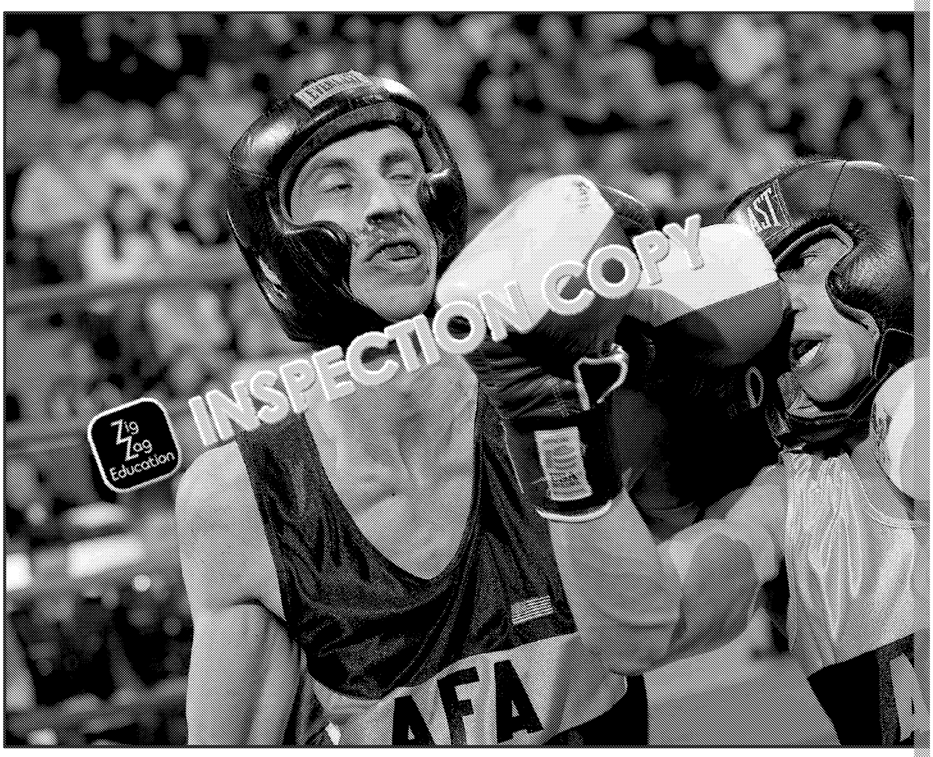
Archiving is a type of backup, normally a long-term backup that is unlikely to e

Feature	Backup	
Purpose	Creates copies of active data for quick recovery in case of loss, corruption, or system failure.	Moves inactive d reduce system lo
Data Type	Regularly updated, frequently changing data.	Historical, rarely financial reports
Storage	Usually stored on-site, off-site, or in the cloud with retention policies.	Often stored in t specialised archi
Access Speed	Designed for fast recovery.	Slower retrieval,
Retention	Short- to medium-term depending on business needs.	Long-term, some
Use Case	Disaster recovery, accidental deletion recovery.	Compliance, lega record-keeping.

Activity A11

Quick recap questions:

1. What is the purpose of site security locks?
2. How do card entry systems enhance physical security?
3. What are the common biometric security measures?
4. How does CCTV contribute to physical security?
5. What roles do sec
6. Why might cablin
7. What are the thre
8. What is a hot site



Data resilience

Data resilience refers to a system's ability to withstand failures and recover qu
downtime. Concepts include:

- *Redundancy:* keeping multiple copies of data across different locations (e.
- *Fault tolerance:* systems designed to continue working even if a compone
load balancing).
- *Disaster recovery plans (DRP):* policies and procedures to recover data in c
disasters, or hardware failure.
- *High availability (HA):* ensuring minimal downtime by using failover syster
- *Continuous data protection (CDP):* real-time backup mechanisms that allo
previous states.

Recovery types

There are many different situations where recovery is needed. An organisatio
different locations to choose from for recovery. For example:

- *File/Data Restore:* individual files or folders may need to be recovered du
or software failure. It is likely that they can be recovered from the most r
backup, cloud backup, or possibly a backup tape that has been taken off-s
- *Image Restore (Disk, Device, System):* an entire disk, device or system may
image backup (a snapshot of the system at a specific time). Different type
been taken:
    - *Disk image:* backup of an entire disk, including the operating system,
    - *Device image:* backup of a workstation, laptop or server.
    - *System image:* backup of the entire system and servers, from which t
disaster or after a ransomware attack.
- *Full/bare metal restore:* the entire system, including the operating system
is installed on new or repaired hardware. This might take around four ho
example, if practice recovery runs have been made to make the process a

Antivirus software and detection techniques (A4.1.3)

Antivirus software is a security application designed to detect, prevent and re viruses, worms, trojans, ransomware, and spyware. Organisations will normall servers and computers, and possibly for other devices and employee home co recommended to buy antivirus software for their home computers.

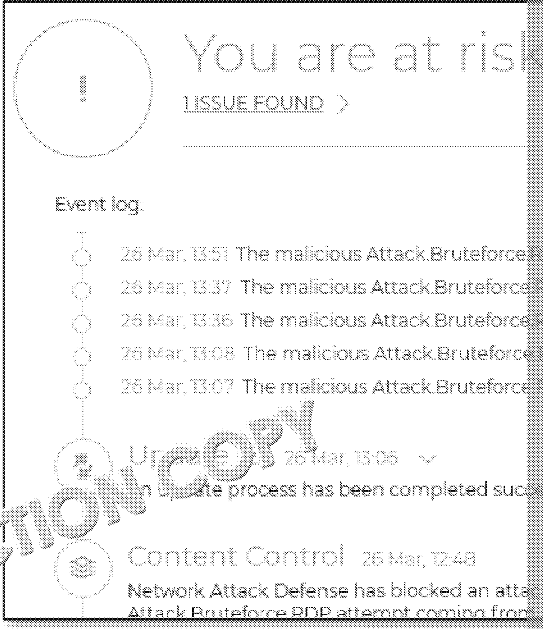
Antivirus software will normally carry out a periodic scan of all the files on you month, and in addition scan each file you open. Antivirus software detects viru

- *Virus Signatures and Scanning;* a virus signature is a unique string of bytes specific virus. Antivirus software maintains a database of known virus sig signatures and flags any files that match. This is a good method for spotti
- *Heuristic Analysis;* heuristic techniques look for suspicious characteristics, system files, self-replicating behaviour, and attempts to run unauthorised more chance of spotting new malware, although is more likely to give fal
- *File Integrity Check and Checksums;* antivirus software computes a checks saves it. When doing a periodic scan or when a user opens a file it compa one it saved last time. If the checksum has changed then it could indicate (possibly by malware).

Once antivirus software identifies a threat it may deal with it automatically or out one or more of the following actions:

1. *Warning;* the antivirus software displays a notification to the user about a The user must decide whether to allow, ignore, or take further steps.
2. *Logging;* the antivirus records details about the threat in a log file. This da malware activity and analyse attack patterns.
3. *Prevent Execution;* the antivirus blocks the file from running to stop poten
4. *Quarantine;* the antivirus moves the infected file to a secure, isolated fold files and either delete them permanently or restore them if they are sure
5. *Deletion;* the antivirus removes the infected file permanently from the sys infected and is not needed.

This screenshot shows the event log from antivirus software, demonstrating that there were multiple brute force attempts made the day before via remote desktop. The first IP address was from a location in France, the others from Russia.



Event log:

```
26 Mar, 13:51 The malicious Attack.Bruteforce
26 Mar, 13:37 The malicious Attack.Bruteforce
26 Mar, 13:36 The malicious Attack.Bruteforce
26 Mar, 13:08 The malicious Attack.Bruteforce
26 Mar, 13:07 The malicious Attack.Bruteforce
```

Update 26 Mar, 13:06

An update process has been completed succ

Content Control 26 Mar, 12:48

Network Attack Defense has blocked an atta Attack.Bruteforce.RDP attempt coming from

Activity A12

View the event log from the anti-virus software running on your home computer.

Although it reads like a *produ* **zzed.uk/12912-antivirus** i software works and software

Software and hardware firewalls and the filtering technique

A **firewall** is a security system that monitors and controls incoming and outgoi predefined rules. It acts as a barrier between a trusted network (like your hom network (like the Internet). Most routers contain a firewall to filter the traffic computers contain software-based firewalls.

However, the best solution is a hardware-based firewall which is a dedicated p WatchGuard or Cisco firewall. This means that the firewall can be one networ separate Internet network, and the only way that devices outside the network the firewall.

Firewalls use various techniques to inspect, filter and control network traffic. I

- *Packet Filtering and Inspection* which examines individual data packets m the header information of each packet such as the source and destination the protocol type (TCP, UDP, ICMP). It then accepts or blocks the packet b
- *Application Layer Awareness (Deep Packet Inspection - DPI);* this analyses headers. It is used to detect malicious content, block unauthorised apps, example blocking P2P file-sharing apps, detecting malware hidden in ema web filtering (e.g. blocking social media).
- *Inbound and Outbound Rules.* Inbound rules might, for example, block al web browsing. Outbound rules might, for example, prevent employees fr personal email.
- *Network Address Filtering (IP Filtering)* blocks or allows traffic based on IP can restrict access from certain countries or regions, block known malicio internal devices to access sensitive systems.

CloudPanel is a website management tool. This screenshot shows a security page from a web CloudPanel page.

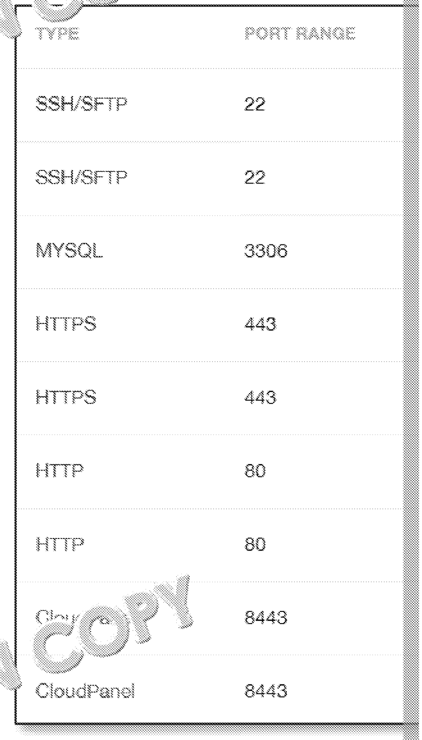
You can see that HTTP and HTTPS are allowed of course.

SSH allows the developer to connect to the machine to work on it with a digital certificate.

MySQL allows the developer to access the database on the live server.

CloudPanel allows the developer to access the *CloudPanel* settings to make changes.

There are no other ports open.



TYPE	PORT RANGE
SSH/SFTP	22
SSH/SFTP	22
MYSQL	3306
HTTPS	443
HTTPS	443
HTTP	80
HTTP	80
CloudPanel	8443
CloudPanel	8443

User authentication (A4.1.5)

User authentication is the process of verifying a user's identity before grantin network. It ensures that only authorised users can access sensitive data and re

User login procedures

The user login process typically involves:

1. Entering a username and password
2. Authentication check that the username and password match those in a d
3. Granting or denying access based on authentication results
4. Optional Multi-Factor Authentication (MFA) for additional security
5. Account throttling which progressively increases the delay between login lockout after between five and ten login attempts

Strong password and password policy compliance

A strong password is difficult for attackers to guess. The UK National Cyber Security Centre recommends, when passwords are used:

- Ideally use machine-generated passwords and save them in a password manager
- Advise users to generate passwords with three random words such as *smashbugshirt*
- Users should avoid using the same password, or variations of the same password, for different logins

Password policy compliance

The UK National Cyber Security Centre also recommends:

- Enforcing a minimum length to avoid very short passwords
- Using password deny lists which contain a list of the most common passw
- Do not force passwords to expire
- Do not use complexity requirements or maximum length requirements

Biometric authentication

Biometric authentication is covered in *A4.1.1*. It uses unique physical or beha fingerprint scanning, eye iris or retina scanning, facial recognition or voice rec

Single-factor (SFA) and Multi-Factor Authentication (MFA)

SFA uses one method to log in a user, most commonly a password.

MFA requires two or more authentication factors. If there are two types of a code that is texted or emailed to you, it may alternatively be called Two-Facto different types of authentication can be categorised as follows:

1. Knowledge (Things You Know) – passwords, PINs, security questions
2. Possession (Things You Have) – security tokens, smart cards, authenticati
3. Inherence (Things You Are) – biometrics (fingerprints, voice, face)
4. Location-based factors – IP address, device MAC address, GPS location
5. Behavioural factors – typing patterns, mouse movements, writing style

Security tokens

Security tokens generate temporary authentication codes for login. They inclu

1. Physically connected tokens such as USB security keys (e.g. smart cards w YubiKey, Google Titan Security Key and Nitrokey).
2. Contactless tokens which are wireless/Bluetooth/NFC that auto-authentic
3. Disconnected tokens which generate authentication codes independently
   - Smartphone security apps (Google Authenticator, Microsoft Authen
   - Dedicated security devices (Bank OTP generators, RSA SecurID).

Kerberos network authentication

Kerberos is a secure authentication protocol used in Windows® and Linux® ne wristband at a festival – once you have been *authenticated* at the entrance by entitles you to go to some areas in the festival but not others, for example you tent but your wristband isn't the right one to get through internal security to t

1. The client requests access to a service, e.g. when logging on.
2. The Authentication Server (AS) verifies the user and provides a Ticket-Gra
3. The client uses the TGT to request a Service Ticket (ST) from the Ticket-Gr
4. The client presents the ST to the service, which grants access, if the user h

Basic key exchange process

Secure communication relies on setting up *cryptographic key exchanges* betwe

1. Client request – the client asks for a secure connection.
2. Server response – the server sends a digital certificate.
3. Authentication of server response – the client also verifies the server's ce
4. Key exchange – a secure session key is generated using encryption (e.g. Di

This ensures that during the session only the client and server can decrypt dat

Certificate-based authentication

Although less common than it used to be, you may sometimes go to a website are taking a risk by going to the website. This is because either (a) the website (http) instead of a secured connection (https), or (b) because the website is usi than one issued by the *Certificate Authority (CA)*. The latter option used to be now gives this warning. So, when someone sets up a new website, they must may be semi-automated by the software they are using.

Concept	Definition	Rea
Public Key Infrastructure (PKI)	A system that manages encryption keys and digital certificates	PKI uses public-key cryptogra • a *Public Key* (shared wit • a *Private Key* (kept secre
Certificate Authority (CA)	Trusted organisation that issues verified *SSL/TLS certificates*	Let's Encrypt, DigiCert, Globa certificates that allow websit
TLS (Transport Layer Security)	Encrypts data between client (browser) and server	e.g. when you visit https://w connection so hackers can't s is the current standard.
SSL (Secure Sockets Layer)		SSL is no longer regarded as
Self-signed certificate	A certificate created without a CA – not trusted by browsers	May be used for internal com website before buying a real where security isn't a concern
Client/device certificate	Digital certificate used to authenticate a user or device	A company laptop has a *devi* to the corporate Wi-Fi witho

zzed.uk/12912-authentication gives more detail about some of the above aut use them.

Go to **zzed.uk/12912**

Access controls and the methods to restrict users' access to res

Access control ensures that only authorised users can access specific resourc data and devices. There are different types of access control models used in cy

Discretionary Access Control (DAC)

DAC is when users have control over their own files and resources. The owner of a resource decides who can access it. For example, if you create a document and save it in *OneDrive* or *Google Drive*, you can share that file with anyone.

I can share photos in my OneDrive with my mum 😊

Role-Based Access Control (RBAC)

With *RBAC*, the administrator assigns access based on roles or groups. Users belong to groups (e.g. in school, there will be a teacher group and a student group) with predefined permissions. This ensures that students can only access shared student files. Similarly in a workplace it ensures that employees only access what they need for their job; for example, only Human Resources (HR) staff should be able to access employee records.

If I'm ill and miss a lesson the teacher puts them on the student shared drive so I can catch up 😊

Access control can apply to these resources, for example:

Resource Type	Example
Applications	Restricting access to HR software only for HR employees
Folders	Only finance staff can open the budget folder
Files	A CEO's confidential report is locked to only the CEO and executives
Data Sets	Customer data is restricted to authorised analysts
Physical Devices	Only authorised staff can access server rooms, printers, and company la

Trusted computing (A4.1.7)

Trusted computing is a concept where the memory of the computer (boot dri RAM) are all encrypted with a key that is known only by the operating system The advantages are that:

- unauthorised code cannot be run at start up to hack into the system
- only software and hardware authorised by the operating system can be i
- only files verified by the operating system can be saved so there is reduce unauthorised access
- if the hardware is stolen the data on it is encrypted

However, there are opponents to the concept on the basis that it shifts the co manufacturer so for instance:

- Users may be forced to use software and hardware from a specific manuf
- Users cannot install software that is not pre-approved by the system.
- It can allow companies to track and verify devices, reducing anonymity.
- Governments or corporations could enforce restrictions on users.

Windows users can opt to install *BitLocker* which encrypts their hard drive. Se This works in conjunction with a Windows hardware component called a *Trust*

Device based security (A4.1.9)

There are a few methods that phones, tablets, laptops and desktop computers unauthorised people accessing them:

- timed lockout: if a device is inactive for a set period (e.g. 10 minutes), it a password, PIN, or biometric login to regain access
- repeated failed login attempts lock the device out for a period of time to p all possible combinations of passwords
- memory wipe or factory reset after failed login attempts or attempts to lo generally only appropriate for high-security data
- devices can be instructed to be wiped remotely so the data is not stolen

Finding lost or stolen devices (A4.1.8)

Device tracking and location reporting software is commonly used by users. For example, Apple has the option to find your registered friends and family through their phones, a lot of people use SnapMaps to see where their friends are, and many devices have the ability to find them if they are lost or stolen.

Phone Home on Connection: devices such as mobile phones have multiple methods of connecting to the Internet, commonly by Wi-Fi, by the mobile network to phone masts, and by GPS. Each time it makes a connection IP and location information is logged centrally by the oper

GPS (
satelli
deter
signal
to sat

There are a few concerns about location tracking software:

- Privacy; some software tracks users without their consent.
- Cybercriminals can exploit tracking software if they gain access to the dev
- It relies on Internet connectivity; while the device is offline, tracking is del

Group Discussion

A military officer fell asleep on the train and woke up at his stop. Worried he migh realised too late that he'd left his laptop on the train. It contained highly confiden wasn't backed up and so he only wants to remote wipe it as a last resort. Discuss

A4.2 Use of encryption

Storage encryption (A4.2.1)

Storage encryption involves encrypting data before it is saved and then saving
This means that the data has to be decrypted with the correct password or ke

- *Safe Password Storage:* programmers or hackers used to be able to acces user database directly. Passwords are now hashed with a one-way encry a user logs in, the password they type is also hashed and the two hashed
- *Digital Rights Management (DRM):* encryption is used to lock digital conte The encrypted files can therefore be made freely accessible, but only aut key can access the content.
- *File, Folder, Disc, Device Encryption:* data files stored on devices are encry those with the decryption key.

Communications encryption (A4.2.2)

Communications encryption involves encrypting a message before it is sent, a only decode the message if it has the key. Encryption is built into most mode encryption technologies are also embedded into smart, mobile, and other dev

There are two main types of encryption method:

- *Symmetric Encryption:* uses the same secret key for both encrypting and Encryption Standard (AES) is a widely used symmetric encryption algorit encryption such as BitLocker, VPNs and messaging apps such as WhatsAp encrypting data in blocks of 128 bits using either a 128-, 192- or 256-bit k multiple transformations on the encrypted data such as shuffling the dat A 256-bit key means there are 2^{256} possible keys.
- *Asymmetric Encryption:* uses two keys, a public key (shared publicly) and

These two common algorithms are used for slightly different purposes for co

- *Rivest–Shamir–Adleman (RSA):* a secure method to send encrypted mess signatures with which to prove the identity of the sender. The keys must the communication. *RSA* has been replaced in many applications by **ECD** curve mathematics) and offers the same level of security with smaller ke efficient. However *RSA* is still common for backwards compatibility.
- *Diffie–Hellman Key Exchange:* a secure method to create a shared secret can subsequently be used for encrypting their communication.

There are various reasons why people might want to hide their IP address and browsing the Internet and communicating over the Internet. Some are legiti investigating criminal gangs or using the Internet in heavily censored countrie reasons are for illegal use such as communication between criminals, to acces the *dark web* or to carry out cybercrime. There are two common methods, *T* table below.

Feature	The Onion Router (TOR)
How it works	Encrypts internet traffic and routes it through multiple servers (like the layers of an onion)
Advantage	Maximum anonymity
Disadvantage	Slower than VPN as it is more complex and goes through multiple layers. Some websites block TOR traffic to prevent abuse.

Certificate Authorities (see *A4.1.5 User authentication*) are trusted organisati certify the ownership of a public key by the named subject of the certificate. V website using https, the website server sends its SSL/TLS certificate, which wa to the device to confirm its identity, and provides its public key. The device ca to encrypt the rest of the communication and send it to the server; only the se this communication and get the session key to be used to encrypt the rest of t

End-to-End Encryption (E2EE) ensures that data is encrypted on the sender's d recipient's device, preventing third parties from accessing the data. For examp the AES key between the user and the WhatsApp server, then uses AES to en E2EE is an additional layer to ensure that the WhatsApp server cannot read th

Application	En
Wi-Fi (WPA2/WPA3)	CCMP, SAE (for WPA3)
HTTPS	AES and RSA/ECDSA
BitLocker (Windows) and FileVault (MacOS)	AES (128 or 256)
VPNs	AES-128, AES-256, IKEv2/IPS
WhatsApp	E2EE, AES and RSA
Telegram (Secret Chats)	E2EE, AES and RSA
Telegram (Cloud Chats)	AES
Cryptocurrencies and blockchain (e.g. Bitcoin)	ECDSA

Activity A13

Quick recap questions:

1. Explain the difference between symmetric and asymmetric encryption.
2. When would you use each: *Rivest–Shamir–Adleman (RSA)* and *Diffie–Hellman Key Ex*
3. Explain what a certificate is (in the context of cyber security).
4. What is the difference between normal encryption of communication and *end-to-end e*

Go to zz

Research Activity

Study the article *File Encryption 101: Safeguarding Your Sensitive Data* from Veritas at **zzed.uk/1** the options you have to encrypt the files on your computer and highlight the ones that you thin

A4.3 Protecting a Wireless Local Area Network (W unauthorised access

Wireless connections to a network, e.g. through a wireless router or wireless access point (WAP), are often publicly accessible, either by someone outside the window of the office, or a guest, e.g. in the reception area or in a coffee shop.

Media Access Control (MAC) address filtering and hiding the Service Set Identifier (SSID) (A4.3.1)

At home, schools, businesses and cafés you can generally see the Wi-Fi networks that are available. Most will be secured with a password. However, you can tell a Wi-Fi router to not display their SSID (their name). This way only people that you tell the SSID to can access your Wi-Fi, which makes it harder for someone to hack in (although they still fi

Every device that can connect to a network has a unique identifier called a MA when connecting to a wireless network. If you log into your home wireless ro listed with its MAC address, as well as every other device that has connected i your friends' mobile phone MAC addresses who you've allowed to access you

MAC Address Filtering can be used to only allow specific devices (with known M network, adding an extra layer of security (although it is possible to spoof MA

Wireless encryption (A4.3.2)

WPA2 and *WPA3* are security protocols that encrypt the data traveling over yo unauthorised users can't easily read intercepted data. WPA3 is the most recen enhanced protections compared to WPA2. WPA stands for *Wi-Fi Protected A*

Wi-Fi Protected Setup (WPS) is a feature that makes it easier to connect device pressing a button on the router, or by entering a PIN code. It can be very conv recommended to disable it if you don't use it.

Here are some wireless vulnerabilities:

- Piggybacking is unauthorised use of a network, i.e. when someone connects to your open network without permission, potentially consuming bandwidth or accessing sensitive data. This can happen in cafés where the Wi-Fi deliberately has no password, or the password is on the counter in plain sight.
- Unsecured access point: an access point that does not have encryption or security features enabled, leaving it open for unauthorised access.
- A fake access point (also known as an *evil twin attack*): a fake Wi-Fi network set up by an attacker to trick users into connecting.
- Wireless sniffing or eavesdropping is when attackers intercept and capture data sent over the network to extract sensitive information.

Mitigation methods for attacks on Wi-Fi:

- Ensure your network uses at least WPA2 or WPA3 if it is available.
- Change the default password and names because many default admin an the Internet.
- Use *block and allow* lists to dictate which devices can and cannot con
- Use a Virtual Private Network (VPN) to encrypt your Internet traffic if yo confidential information.
- Check the firewalls settings; these help to block unauthorised access and m network traffic based on predetermined security rules. For a home netwo router is normally sufficient, but for organisations a separate hardware fire

A4.4 Building in security issues during network an

Expect that attacks will happen (A4.4.1)

The government National Crime Agency says on its website *'The deployment o cyber serious and organised crime threat to the UK and its use threatens Critic a risk to national security'*. When designing a network, expect that attacks wil

- Assume your system could be targeted by attackers; even if you don't thi use automated programs to go through every network where it can find w
- Plan for potential security breaches by implementing strong protective m
- Conduct threat modelling and risk assessment to understand where attac responses in place.
- Regularly update your security measures to tackle new threats.

Design the system to run on 'fewest privileges' (A4.4.2)

Use the principle of least privilege, which means giving users and systems the to perform their functions. This limits the potential damage from compromise access more than they need. Ensure that permissions are regularly reviewed a requirements evolve.

Do not rely on secrecy (assume hackers can work out your syst

Design your system in a way that it remains secure even if details about its de applying the various principles of security outlined in this course companion, e updates, access controls. It is a very bad idea to rely on secrecy of the system'

Compliance with information security standards (A4.4.5)

Organisations should follow established security standards, e.g. *ISO 27000*, the *NIST Cyber security Framework (CSF)* and controls from the *Center for Internet Security (CIS)*. There are also specific standards, for PCI DSS (Payment Card Industry Data Security Standard) to receive online credit card payments.

ISO 27000 – set of standards designed to help organisations establish, implement, maintain and improve Information Security Management Systems (ISMS)

- ISO/IEC 27001: d that organisation
- ISO/IEC 27002: p information secu selecting and im
- ISO/IEC 27005: f context of inform assess and mana security systems
- ISO/IEC 27003: o ISMS based on IS
- ISO/IEC 27004: p performance of a
- ISO/IEC 27006: o certification bod

Key Information Security Standards		
Standard	Focus	Appli
ISO 27001	Information Security Management Systems (ISMS)	All industries
Cyber Essentials	Government certification scheme to protect against the most common threats	All industries
NIST CSF	Cyber security risk management framework	Government, fi infrastructure
PCI DSS	Payment card security	Retail, bankin
SOC 2	Data security for cloud services	SaaS, cloud, te
HIPAA	Healthcare data protection	Hospitals, insu
UK GDPR DPA 2018	Personal data privacy	UK citizens' da
EU GDPR	Personal data privacy	EU citizens' da
FISMA	Federal information security	Government a
COBIT	IT governance and risk management	Enterprises, fi
ITIL	IT service management security	IT service pro

AAQ BTEC National IT

Cyber Security and Incident M

Content Area B: Use of ne architectures and principles

Contents

B1 Network types

Students should apply their knowledge and understanding of the security issu
to secure them in organisational contexts. Students should be able to interpre

B1.1 Applications and features of networks

A computer network is two or more computers or devices connected togethe
printers) or for users to communicate.

Types of network (B1.1.1)

Local Area Network (LAN)

A LAN is a network that connects computers and other devices within relative
building or a school campus, so that a direct physical connection is possible. A
fibre-optic cables to connect buildings and rooms. Normally Ethernet cables c
devices within a room or area. The set-up costs can be high due to the installa
in place, adding new devices is easy and affordable.

Wireless Local Area Network (WLAN)

A WLAN is a type of LAN that uses wireless signals (Wi-Fi) instead of cables to
laptops, tablets and smartphones to connect to the network without needing
commonly found in homes, schools, offices, and public places such as coffee s
using wireless routers or Wi-Fi access points to send and receive data.

Many workplaces and schools use a mixture of physical connections for the m
computers and also provide wireless access points (WAPs) for laptops, tablets
desktops in places where it is difficult or expensive or undesirable to install ph

Wide Area Network (WAN)

A WAN is made up of multiple interconnected networks. WANs can use differe
to each other including undersea cables, satellites, microwave signals, and tel
voice, video and data over long distances. WANS typically connect multiple L

Storage Area Network (SAN)

A SAN is a special type of network designed specifically for storing and manag
computers and devices like a LAN, a SAN links together storage devices (such
large amounts of data can be stored and accessed efficiently. SANs are mainl
and cloud storage providers that need to manage vast amounts of data secure

Personal Area Network (PAN)

A PAN is a small network that connects devices around an individual person's
someone is working in a café on a tablet, they might also be connected to a B
smartphone via Wi-Fi and a Bluetooth headset for phone calls.

The Internet

The Internet is the term for the global network of interconnected computers
devices all over the world to communicate and share information. It mainly u
across each country and between countries, including undersea cables, which
servers. The way the Internet works using DNS and IP addresses is outlined la

Private network types (B1.1.2)

An **intranet** is a private network used by an organisation (such as a school, bus to share web-based tools, documents, and communication. Normally only em access it. For example, a school may have an intranet where teachers and st timetables, and announcements.

An **extranet** is similar to an intranet, but it also allows authorised external use suppliers, or customers) to access specific parts of the network. For example, parents to access the intranet from home to check what homework has been s extranet where suppliers can log in to check stock levels and place orders.

A **cloud network** is where data, applications and services are stored on remot These services can be accessed over the Internet from anywhere in the world. *Microsoft OneDrive* allow users to store and access files from any device with

Over the last decade or so there has been a trend away from intranets and ex websites, third-party suppliers (for example to host email services, accountan file sharing.

Wired and wireless integration (B1.1.3)

Most modern networks combine both wired and wireless technologies to provide flexibility, reliability and efficiency. Wired connections (Ethernet) are fast and stable, while wireless connections (Wi-Fi) offer convenience and mobility. In an office, desktop computers may use wired Ethernet for speed, while employees' laptops and smartphones connect via Wi-Fi for mobility.

Bandwidth determin transferred across a c
1 Kbps = 1 thousand
1 Mbps = 1 thousand
1 Gbps = 1 thousand

Ethernet standards for wired and wireless

The *IEEE 802* family of standards defines how devices communicate over netw

- The Ethernet Standards (*IEEE 802.3*) define wired connections whi Mbps, 100 Mbps, 1 Gbps or 10 Gbps) or fibre optic (100 Gbps).
- The Wireless Ethernet Standards (*IEEE 802.11*) define wireless network c (802.11a) operated at a frequency of 5 GHz, had a maximum speed of 54 (802.11ax (Wi-Fi 6)) has a maximum speed of 9.6 Gbps and can operate a

Compatibility/interoperability issues

Generally, there is not a problem with using a combination of wired and wirel wireless devices connect to a wireless access point (WAP) or router, which is c However, there are a few compatibility issues with some wireless communicat

- Older Wi-Fi devices may not support new standards.
- Some devices only work with specific access points.
- Some old devices don't support strong encryption (WPA3).

Admin issues

Network administrators must manage settings to ensure seamless wired-wirel

Issue	
Wireless networks use **different frequency channels**; too much overlap causes interference.	Set **non-overlapping channel**
Devices on wired and wireless networks need **unique IP addresses** to communicate.	Use **Dynamic Host Configura** IP assignment.
In terms of network security; wireless networks are more vulnerable than wired.	Use **WPA3 encryption and M**

Common technical issues

The IT support team can spend a lot of time with technical network set-up issu and even more so when new equipment has been installed. Below are the so the day in the life of an IT technical support engineer:

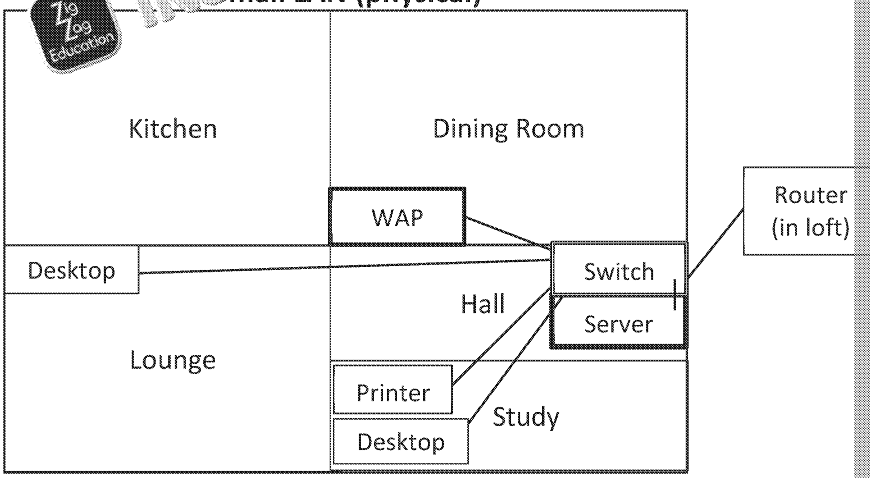
Rank	Issue	Cause	
1	**Weak Wi-Fi signal**	Distance from router, obstacles (walls, floors), interference.	Move or a
2	**Interference** (from other devices or networks)	Nearby Wi-Fi networks, microwaves, Bluetooth devices, cordless phones.	Chan use
3	**Bandwidth bottlenecks** (slow speeds)	Too many devices streaming/downloading at once.	Use route
4	**Latency** (delay in data transfer)	High congestion, poor routing, overloaded network.	Use impo
5	**Overloaded access points** (too many devices on Wi-Fi)	Too many users connected to a single access point (AP).	Add
6	**IP address conflicts**	Two devices assigned the same IP address.	Enab auto
7	**Wi-Fi channel overlap**	Multiple networks using the same frequency.	Use 11 fo
8	**Packet loss** (unreliable connection)	Wireless interference, damaged cables, or overloaded network.	Use chan
9	**Jitter** (inconsistent latency)	Network congestion, poor router settings.	Opti use
10	**DNS issues** (slow or no Internet)	Incorrect DNS settings, slow DNS servers.	Use (1.1
11	**Hardware failures** (routers, switches, cables)	Ageing or faulty network equipment.	Repl regu
12	**Network segmentation issues** (security risks)	Poor separation between wired/wireless networks.	Use
13	**Crosstalk** (wired signal interference)	Data signals from one cable interfere with another.	Use
14	**Network loop** (switching loop)	Improperly connected switches create continuous loops.	Use preve
15	**Power over Ethernet (PoE) problems**	Devices don't support PoE, or power is insufficient.	Use powe

Schematic diagrams (B1.1.4)

As you can see from the long list of possible technical issues above, it is import network works to be able to troubleshoot and to design new networks, or add can look at a network design in two ways.

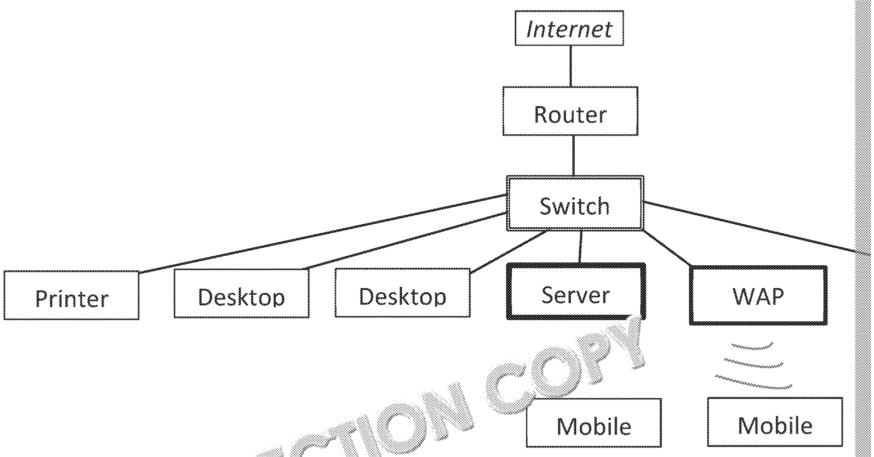
A **physical network diagram** shows the physical locations of hardware devices including server rooms, routers, switches, and end devices. It helps IT teams set network. *A physical diagram is like a floor plan of a building, showing where d are physically placed.*

Small LAN (physical)



A **logical network diagram** focuses on data flow and communication between It will represent IP addresses, subnets, and routing paths, so if some users are their data flows from their laptop through a router to the Internet. It might, f external networks and lines and arrows to show connections. *A logical diagra routes and maps but doesn't focus on physical distances.*

Small LAN (logical)



Features/requirements of networks (cyber security related) (

Following are key features and requirements of networks to consider from a c

Feature	Explanation	Cybersecu
Scalability	The ability to expand the network without affecting performance.	• Use hardware that can b • Plan in higher specificati
Software and Hardware Sharing / Compatibility	Ensuring different devices and systems work together.	• Secure authentication (e. • Regular security updates • Preventing legacy device
Data and File Sharing / Transfer	Secure transfer of files across devices.	• Encryption for data in tra • Secure file-sharing proto • Access control policies a
Performance / Response Time	Speed and efficiency of network communication.	• Optimised security tools • DDoS protection to preve • Load balancing to distrib
Backup Management	Creating and maintaining copies of important data.	• Encryption of off-site/clo • Use of *immutable* backu • Regular backup testing a
Security Settings	Configuration settings to protect the network.	• Strong passwords and MF • Network segmentation to • Regular patching, firewal
Reliability	Ensuring the network is always available.	• Redundant network conn • Failover mechanisms for • Security audits and netw
Fault Tolerance	Ability to keep functioning despite failures.	• Redundant hardware (ba • RAID hard drives and hot
Communications	Secure exchange of data.	• End-to-end encryption. • Zero Trust security mode • Regular audits of commu

Activity B1

1. What are the differences between Ethernet and fibre cables, and what are their maximu
2. What is the maximum bandwidth of standards 802.11a and 802.11ax?
3. What is the difference between a WAN and the Internet?

B1.2 Applications and features of network topolog

Physical topologies (B1.2.1)

Star network topology

A star network has one central message-switching device through which all th computers communicate. In this system, each workstation is connected direct central device – normally a switch – by its own unique cable.

The major disadvantage is dependency on the central device; nothing can communicate if it breaks down. It requires a lot of cable, and if there are a lot devices then the switches can be expensive.

However, its advantage is that it is easy to track problems because each wo has its own separate cable. Also, this means that a problem with one cable or of the system. Performance doesn't degrade when new nodes are added so th the central switch can copy with the additional connections.

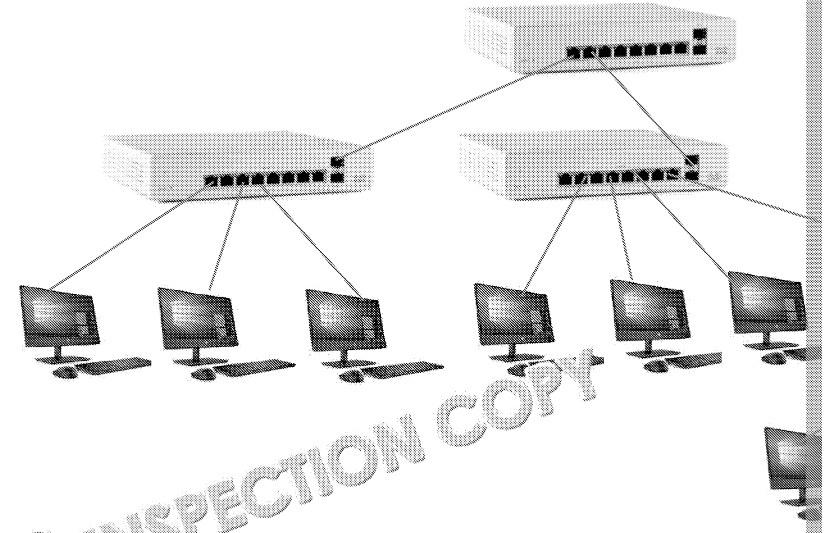
If you have a single Internet router in your home which you run physical cables and/or Wi-Fi for mobiles, tablets and TV, then your home network is a star!

Extended star network topology

An extended star network topology is a specific variation of the star topology interconnected through additional hubs or switches. For example, you might classrooms in a school, where the central switch in each classroom is connecte scaling up without disrupting the structure of individual stars. If a single centr that star lose connection, but nothing else is affected.

Hierarchical network topology

In a hierarchical topology, the central switch connects to other switches, whic other switches which connect to computers. This means it is very easy to scal if a switch goes wrong then only devices below it lose connection to the rest o the whole network is affected if a central switch goes wrong or loses power.



Wireless mesh

Wireless mesh networks consist of a mix of WAPs. Some of the WAPs may wo are connected to other WAPs wirelessly. Others may be connected by wired c Internet. The WAPs covered can overlap with each other meaning that if one WAPs can find other WAPs to maintain the network connection, i.e. there is a

This is very useful for users on a campus where they can move about the camp can seamlessly move between WAPs to maintain their connection. It is also usefu enemy may destroy a WAP with limited impact on their communications.

Mixed and ad-hoc network topologies

Note that a star network can be redrawn as a one-level hierarchical network, a similar to an extended star network. The reality is that many networks are a c A medium-sized organisation on a large site is likely to have a central server r to a super-fast switch with high bandwidth, which in turn is linked to a numbe the site. Any one area on the site is likely to have one or two cables going to a topology with all network ports in the room or area going to that one switch.

In addition, many or all areas of the site may have WAPs providing wireless ac employees/students **BYOD (Bring Your Own Device)**.

Logical topologies (B1.2.2)

This describes how data moves across a network, regardless of its physical de

- In a *Logical Bus Topology* all devices on the network share the same com all devices but only accepted by the intended recipient. This is easy to un there is a problem with the main line, the whole network can be disrupte
- In a *Logical Ring Topology* data travels in a circular pattern around the rin Each device on the network has exactly two connections to other devices and each device only needs to handle its own data, but a failure in any ca entire network

Activity B2

1. Define physical topology and logical topology in the context of computer networks.
2. Describe the key characteristics of the following physical topologies:
   a. Logical bus topology
   b. Logical ring topology
   c. Physical star topology
   d. Wireless mesh topology

B1.3 Network architecture

Peer-to-peer (B1.3.1)

Peer-to-peer networks are those where there is no central server and every co communicate with others. There is no central management. Peer-to-peer is us computers do not need to interchange information with each other. Small com networks since having independent computers doesn't require an expensive s manage and maintain. This is now more feasible when many of the business se software, email and storage can all be on cloud servers.

On most peer-to-peer networks the data is stored locally on each machine and syncing [illegible] cloud or regular backups to prevent data loss. However, someti have shared directories on individual computers, i.e. individual devices act like

The Internet has made global peer-to-peer networking possible and cheap. He peer-to-peer networking. (For this course you don't need to learn the example

Category	Software Examples	
File sharing and content distribution	**BitTorrent** (qBittorrent, uTorrent, Transmission)	P2P file-sharing protoc efficiently.
	IPFS (InterPlanetary File System)	Decentralised storage a
Communication and messaging	**Jami**	Secure, decentralised V
	Tox	Encrypted, P2P messagi
	Briar	P2P messenger that wo Bluetooth or Wi-Fi).
Blockchain and cryptocurrencies	**Bitcoin**	Decentralised digital cu
	Ethereum	Blockchain supporting s (DApps).
Decentralised cloud and storage	[illegible]	Distributed cloud storag
	Sia	Blockchain-based cloud
Gaming and media streaming	**Popcorn Time**	A P2P-based movie stre
Collaborative and distributed computing	**Freenet**	Anonymous P2P platfor
	BOINC (Berkeley Open Infrastructure for Network Computing)	Distributed computing p

Client/server (B1.3.2)

Servers f to client

- Int
- File
- Pri
- Da thr
- Em

The client–server model is a network architecture that dominates network design. The basic principle is that most or all computers in the network are either a server or a client. A client is the machine or application that is usually interacting with the user. It is responsible for sending a request for data via the network to a server, or a small group of servers. A server receives these requests, processes them accordingly and then returns the requested data to the client over the network.

Many organisations that used to have their own servers on site are now either they can be accessed by users outside the site or from home more easily, or a provided by third parties.

Thin client (B1.3.3)

'Thin' computers are reliant on a powerful server for most of their processing s
large amounts of memory. This separates the computer into two parts where t
interactions with the user, containing only the minimum number of parts, whe
computations and stores the data. If the server has any 'downtime' then all da
application useless until the server reconnects.

If your school has given you a li
Microsoft Word and other apps
means you can use it on your la
your device only needs access t
most of the processing is done o
works fine for basic documents
desktop software for complex d

The advent of cloud applications makes thin-client more feasible. For example, businesses can have their email, word processing, spreadsheets, customer management software and accountancy software all in the cloud rather than installed on the computer, so the computer doesn't need to be as powerful.

Further advantages are that there is less complex software on the client, and software updates are managed by the central server, and little data is stored on the clients so there is less of a security risk.

Disadvantages are that the server(s) must be more powerful and therefore more costly to cope with the demands of the clients accessing it at the same time, a fast and robust network to ensure a good connection is needed, and losing connection means no work can be done.

Discussion Point

Smartphones are a type of thin client. If you have a smartphone, which applications do you prefer to use o
computer or laptop than on a smartphone?

B1.4 Modern trends – applications and security issu

Virtualisation (B1.4.1)

Virtualisation is the process of creating virtual versions of physical computing networks, storage, or even entire operating systems. Instead of relying on ded allows multiple virtual instances to run on a single physical machine using soft This technology is widely used in cloud computing, including for whole websit

One key advantage of this virtualisation is *segmentation*, which involves dividi smaller, isolated sections. This ensures that if one part crashes, or is comprom move to other areas.

It also means that resources can be shared more efficiently. Suppose a server h virtual servers. Each server could be allocated 32 GB of RAM, but as long as at an average of less than 12.8 GB of RAM no one will be affected. Normally you dedicated RAM, compared to shared RAM where you get a lot more for your m

Isolation, sandboxing and **containerisation** are three closely related concepts

- *Isolation:* separates different environments so that they cannot interfere running multiple virtual machines on a hypervisor, each with its own oper
- *Sandboxing:* creates a restricted environment where applications can run This is commonly used for testing software, but also for running suspiciou for malware.
- *Containerisation:* uses lightweight, virtualised environments (containers) system to avoid duplicating the OS in every container, but aside from tha *Docker* and *Kubernetes* are popular container systems. *Docker Desktop* ca to create a Linux virtual machine for developing code.

The attack surface is the total number of possible entry points where an attac *the attack surface* means minimising these entry points, making it harder for h Virtualisation helps with this by:

- having fewer physical machines; instead of managing multiple physical se workloads into fewer, more secure virtual environments.
- controlled access; virtual machines and containers can restrict access to s vulnerabilities.
- easier patching; virtual environments can be quickly updated or reverted are found.

Discussion Questions

1. What is the difference between *isolation* and *containers* and when would ea
2. Discuss the limitations of sandboxing. Are there any scenarios where sandbo
3. How does containerisation help in reducing the attack surface of a system?

Cloud computing (B1.4.2)

Cloud computing is the on-demand delivery of computing services (such as se networking, software, and analytics) over the Internet. Instead of maintainin and individuals can rent resources from cloud providers like *Amazon Web Serv Cloud* and *Digital Ocean*. Cloud computing offers scalability, flexibility, and co security risks, like those outlined below, that must be managed carefully.

Configuration issues and default access settings: Many cloud services come with default settings that may not be secure. If an organisation does not properly configure these settings, unauthorised users could gain access to sensitive data. Examples of misconfigurations include:

- Publicly accessible storage *buckets*: breaches sometimes happen when organisations accidentally leave Amazon S3 buckets, Google Cloud Storage, or Azure Blobs exposed to the public.
- Overly permissive access controls: giving users more privileges than necessary can lead to data leaks or insider threats.
- Unsecured databases: Cloud-hosted databases may not be password-pro passwords that were used for development.

In 2021 m different online fr types of d personal i tracing, C social sec employee addresses employee

Reliance on service provider: when using cloud services, companies trust thir protect their data. If the provider experiences an outage, cyberattack, or polic critical data. In addition, employees of the cloud provider could accidentally o stored data; in 2012 hackers stole 60 million user credentials after gaining acc stored password. Users may be able to reduce the risk by encrypting sensitive cloud to prevent unauthorised access and use more than one provider for re their own backups of critical data.

Application Programming Interfaces (API) and vulnerabilities in cloud services/storage: *APIs* allow applications to interact with cloud services. However, insecure APIs can create vulnerabilities that attackers can exploit to access cloud resources. Common API vulnerabilities are weak authentication and no rate limiting issues to prevent repeated brute-force API attacks to gain unauthorised access.

On 19th Janua was accessing over a year in numbers, dat was further to agreeing to pa

Account hijacking: cloud-based accounts can be compromised if attackers steal login credentials. This allows them to access sensitive data, launch attacks, or use cloud resources for criminal activities (e.g. cryptojacking, sending spam, or deploying malware). Attackers hijack accounts by phishing, testing to see if users reuse passwords that were exposed in previous breaches or exploiting weak authentication (not using [illegible]

In 2017 Uber revealed tha account (a programming c breach including names, e 57 million users and 600,0 to implement reasonable former Chief of Security O convicted for covering up

Activity

Outline the pros and cons of using cloud applications through a browser compared to deskto future all applications will be cloud-based?

BYOD (B1.4.3)

BYOD (Bring Your Own Device) policies allow employees to use their personal for work purposes. Similarly, universities allow students to BYOD. While this productivity, it also introduces security, privacy and management challenges.

Issues	
Non-endorsement of password policies: personal devices may not enforce strong password policies, making them easier to compromise, or employees might reuse weak passwords across personal and work accounts. They may store passwords insecurely (e.g. in notes app) and not use multifactor authentication (MFA).	*Enforce st accounts a employee store all w*
Owners' vs organisation's privacy: employees may feel uncomfortable if an organisation has remote access to their personal device. On the one hand employers need visibility over work-related data, but this could conflict with the employees' right to personal privacy and there are legal implications if organisations monitor personal activities without consent. Privacy concerns may lead employees to disable security settings or refuse device monitoring. Companies may accidentally collect personal data, leading to legal and ethical issues.	*Some Mob exist that personal u to implem what the c employee using con*
Data security (on-device and during transfer): work data stored on personal devices is at higher risk of theft, loss or exposure. Employees might use unsecured cloud services, email, or messaging apps to transfer work data. Personal devices might lack encryption, making stolen and lost devices a major risk.	*Encrypt al Use secur encrypted unauthor Google Dr*
Patches, maintenance, updates and compatibility: personal devices may not receive regular security updates. Employees may use outdated operating systems or applications with vulnerabilities. Corporate applications might not be compatible with all personal devices.	*Require a accessing employee versions t*
Organisation vs personal applications: employees may install work apps on personal devices, mixing corporate and personal data. They may download apps for personal use (e.g. social media, gaming apps) which contain malware or data tracking.	*Use applic approved personal p jailbroken*
Erasing/wiping data after use or when no longer required: when employees leave a company, corporate data may still exist on their personal devices, or they may deliberately leave it on there to use in the future. If a device is lost or stolen, work data could be exposed, and personal devices may not have secure deletion methods.	*Use remo to return Support to*
Tracing and auditing data use/movement: organisations need visibility over corporate data but cannot intrude on personal data. Employees may use personal storage solutions, making it difficult to track where work data is stored or shared. A lack of logging makes it hard to investigate security incidents and so data breaches may go undetected if tracking mechanisms are weak.	*Use Data monitor d only use c activity lo complianc*

Software-Defined Networking (SDN)

SDN is an approach to network management that centralises network controls administrators to manage and configure network traffic dynamically, rather th based network management. SDN is commonly used in cloud computing, data to improve flexibility, security and efficiency. Key aspects of SDN follow.

- **Segmentation:** SDN logically divide a physical network into multiple virtu isolated to reduce security risks. For example, a hospital network could u from administrative systems.
- **Remote management:** traditional networks require manual configuration whereas SDN enables centralised control to manage entire networks rem can be diagnosed and fixed remotely, changes can be deployed across the across devices, and IT teams can enforce policies even for remote bra
- **Automation:** SDNs automate network configuration, traffic management predefined rules. AI and machine learning can be integrated into SDN to automatically. This can reduce human error by preventing misconfigurati vulnerabilities, speeds up deployment of new services and applications, a detect network failures or cyberattacks.
- **Scalability:** traditional networks require new physical hardware (switches allows networks to scale by adjusting configurations via software, without resources can be added or removed as needed, bandwidth can be dyna applications, and can scale during peak times
- **Reduced hardware requirements:** SDN reduces expensive proprietary ne dedicated firewalls, load balancers, and routers, replacing it with program These white-box SDN can be supplied as *bare-metal*, where you choose w (some are open-source), and others are bundled with a vendor network O

Storage Area Network (SAN)

A SAN is a scalable solution for multiple storage devices, e.g. an array of hard centralised storage management. A SAN may be expandable – for example, b but also uses hardware to link drives together and a management system t right component. Key features of SANs are:

- **Redundancy:** redundancy in a SAN ensures that data remains available e It is achieved through RAID, having multiple physical paths between the s controllers and power suppliers, and backup power (USPs).
- **Scalability:** new disk arrays can be added without downtime, *Logical Volu* allocation of storage resources, and as storage demands increase, worklo across available resources.
- **Access controls:** to prevent unauthorised access and ensure proper data *zoning* (restricting which devices and servers can communicate within the *Control (RBAC)* to define permissions for administrators and users based
- **Encryption and digital certificates:** security is a major concern in SAN en data integrity and confidentiality (both on the storage, and when data is i used to authenticate devices and prevent unauthorised access.

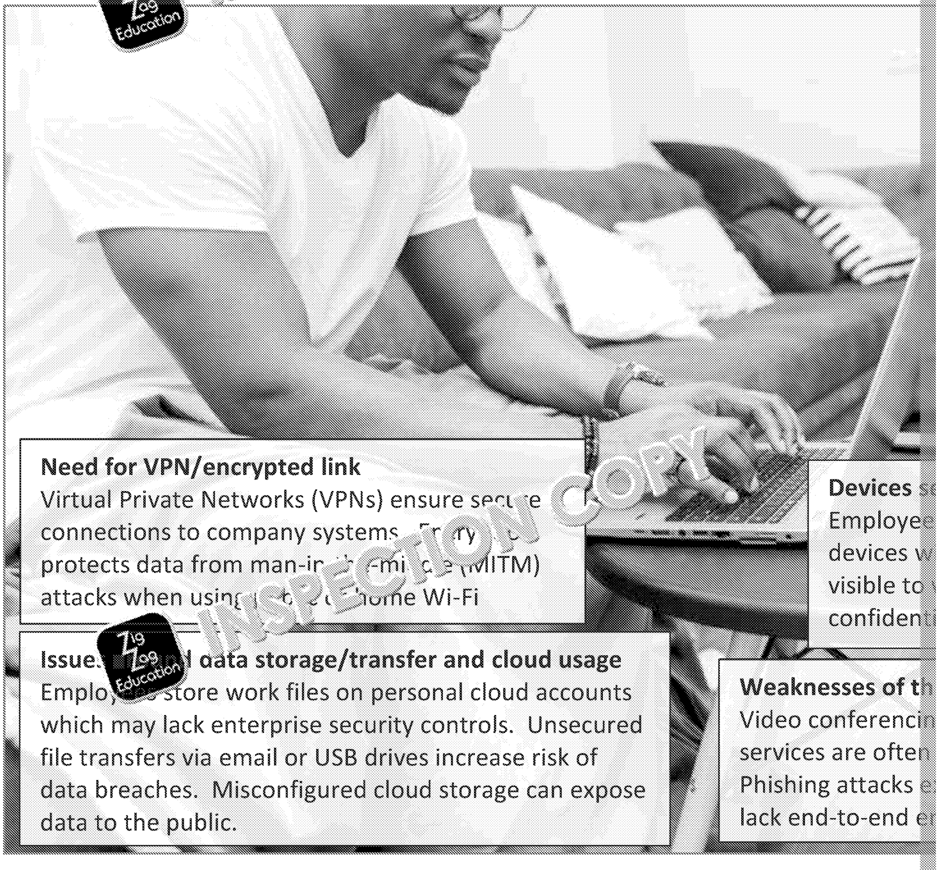
Internet of Things (IoT)

The *Internet of Things (IoT)* refers to a network of interconnected devices that other networks without direct human intervention. IoT devices include smart medical equipment, and connected vehicles. These devices collect share, and automation and convenience. However, IoT security remains a major concern exploited by cybercriminals.

IoT Security Issue	Description	
API Security Issues	IoT devices use APIs to communicate with cloud services, but weak authentication and encryption can expose sensitive data.	Hackers ex IoT camera
Default Passwords / Security	Many IoT devices come with default credentials that users don't change, making them easy targets.	2016 Mirai passwords
Lack of Patches / Updates	IoT manufacturers often fail to provide security updates, so devices are vulnerable.	Older smar vulnerabili
Low-Power Wireless Technologies	Weak encryption on Zigbee or Bluetooth 5, makes it easy to intercept signals. Limited range forces users to install more devices, increasing the attack surface.	Attackers e trackers or
Botnets	IoT devices can be hijacked and controlled as part of a botnet, launching DDoS attacks, spam, and cryptojacking.	The Mirai b into attack Internet le
Spying via Networked Cameras, Smart Hubs, and TVs	Hackers can access cameras and microphones in smart devices for surveillance and data collection.	This can be identify va
Exposure of Non-Traditional Networked Devices	Critical IoT systems, including medical equipment, home appliances, industrial machines, and vehicles, are at risk of cyberattacks.	Smart cars and acceler insulin and attacks and

Remote working

Remote working offers flexibility and convenience but also introduces several



Need for VPN/encrypted link
Virtual Private Networks (VPNs) ensure secure connections to company systems. Encryption protects data from man-in-the-middle (MITM) attacks when using public or home Wi-Fi

Devices s
Employee
devices w
visible to
confident

Issues around data storage/transfer and cloud usage
Employees store work files on personal cloud accounts which may lack enterprise security controls. Unsecured file transfers via email or USB drives increase risk of data breaches. Misconfigured cloud storage can expose data to the public.

Weaknesses of th
Video conferencin
services are often
Phishing attacks e
lack end-to-end e

B2 Network compone

B2.1 Application and features of hardware compo

End-user devices, with connectivity and processing (B2.1.1)

Mobile devices

The key features of mobile devices are [illegible] as well as being compact and por Wi-Fi or Bluetooth, and they are battery powered so need to be recharged.

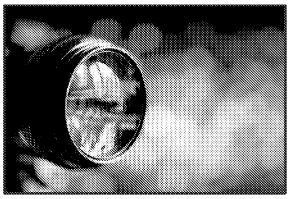
Most mobile phones are *smartphones* which are handheld devices w same tasks as a computer or laptop, albeit with a much smaller touchscreen. by making calls and access the Internet using the mobile phone network. The using Wi-Fi, and connect to other devices such as smart watches and headpho

Laptops (interchangeably called netbooks a version of a desktop computer with a built- portable, the components need to be adap and they also need to be more robust, so la same specification, are designed to consum connect using wireless.

Initially, the key difference between a *tablet* and a laptop was that a tablet ha touchscreen rather than a keyboard. However, many laptops now have touchscreens, and wireless keyboards can be used with tablets, so the two ty devices are now merging. The key difference between a smartphone and a ta was often size but the lines are blurred with bigger smartphones, widespread Internet telephone and increasing use of video calls.

There are many *portable gaming devices* which have built- capabilities. Examples are Nintendo Switch, Steam Deck, Portal. Some smartphones support gaming through cloud GeForce Now).

Smartwatches and fitness trackers are wearable devices that sync with smartphones for notifications, fitness tracking, and health monitoring. They c provide apps, GPS tracking, payment, and phone call capabilities. Fitness trackers, with Fitbit and Garmin being the biggest brands, specialise in heart r steps, and sleep tracking.



Digital cameras are dedicated devices to take high- videography. They include both DSLR cameras, mi such as GoPro. Many cameras now feature Wi-Fi a images and video.

Virtual Reality (VR) headsets (e.g. Meta Quest, HTC Vive, PlayStation VR) imm users in 3D virtual worlds. *Augmented Reality (AR) devices* (e.g. Microsoft HoloLens, Apple Vision Pro) overlay digital elements onto the real world. The are used in gaming, virtual collaboration, training, in education and have medical applications.

***Multi-functional device** refers to devices that have features traditionally in ot smartphones have cameras (largely replacing digital cameras), watches can m phone calls, and gaming devices can be used to surf the Internet.*

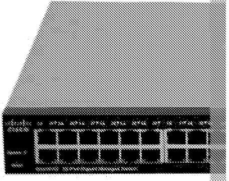
Fixed, networked devices with processing and/or storage

Fixed devices are permanently installed devices that handle data processing, s
They are traditionally connected to networks through physical cabling for spe
increasingly PCs, printers and scanners make use of faster Wi-Fi networks. As
restrictions of portable devices, they are often more powerful and are usually
relying on batteries.

Device Type	Description and Features
Server	A powerful computer designed to manage network resources and security, run shared applications, and store data. Can run 24/7 to support continuous services. As a result, it normally has faster, bigger and more reliable hot-swappable hard drives, processors, RAM, as well as redundant power supply and is linked to a UPS.
Network Attached Storage (NAS)	A dedicated storage device connected to the network. Provides centralised, shared data access to multiple users. Often includes RAID configurations for redundancy and backup.
Personal Computer (PC)	Non-portable computer, sometimes called a desktop computer, for personal or business computing. Traditionally *workstation* referred to higher specification computers.
Printer	A peripheral device that produces physical copies of digital documents. Network printers connect directly to LAN/Wi-Fi for shared access. Most common are laser printers, but inkjet and thermal printers are available too.
Scanner	A peripheral device that captures physical documents or images and converts them into digital formats. There are flatbed, sheet-fed and portable handheld models. Network scanners allow scanned documents to be emailed directly to a user.
Multi-Functional Devices (MFDs)	Combines printing, scanning/copying and emailing in one device. Often networked to allow shared access. May include security features to protect confidential data.

Connectivity devices (B2.1.2)

Connectivity devices are the hardware components used to create network co
other networks and the Internet.



Switches have ports to connect multiple devices within a LAN, most commonly using an Ethernet connection. Either computers and servers can plug into them directly using a CAT5 or CAT6 cable, or they plug into a wall network connection which has a cable that connects to the switch. *Unmanaged switches* are basic plug-and-play with no configuration. *Managed switches* can manage traffic better by forwarding data to specific locations, by including security features, and sometimes can be controlled remotely.

Routers connect a network to the Internet. They handle the traffic sent out from the network, sending it to the ISP (Internet Service Provider) and incomi traffic. Home routers normally have an inbuilt firewall for security and to dire traffic to and from specific computers, although larger businesses have a separate physical firewall device to do this. Wired routers have at least one Ethernet or fibre connection, although some contain a mini switch with four o more Ethernet ports. Wi-Fi routers allow multiple devices to connect to gain access to the Internet. Most provide both physical ports and Wi-Fi.

Gateways connect networks that use different protocols. This may include co computer networks [illegible] most of the old analogue phone network has be devices [illegible] systems to the Internet. They also provide a link betwe A router is a type of gateway, linking network traffic with the Internet.

Bridges connect two networks together. They are generally lower cost and lo may have just one in and out connection. However, they can link networks wi protocols and can also be useful to connect legacy systems that do not suppo

Repeaters boost and retransmit signals to extend network range. They are us Fi and wired networks. If you have an area in your house that doesn't reach t can buy a relatively cheap Wi-Fi repeater to receive the Wi-Fi signal from else house and boost it.

Wireless Access Points (WAP or AP) convert wired si as a hub for Wi-Fi devices, and a *mesh* of WAPs can a site.

USB hubs expand the number of USB ports available. For example, if you hav USB slots in your laptop and want to have a USB mouse, keyboard and charge phone, then you can get a USB hub which converts one USB slot into four, for example. If you use a laptop for work and home, you can have all your periph plugged into the USB, so you only have to plug the USB hub into your laptop w you arrive. *Passive hubs* rely on the power through the USB connection. *Acti* need to be plugged in for power but can support more devices.

Modems (Modulator-Demodulator) are devices that connect your network to t signals from your network to analogue signals for transmission and vice versa Types of modem are:

- *DSL/Copper Cable Modems* convert signals to/from copper telephone lin These are often called legacy lines as most of the UK is converted to fibre
- *Optical Fibre Modems* convert signals to/from fibre-optic cables using lig data transmission.
- *Wireless Modems* connect to the Internet via cellular networks. A mobil is a mobile hotspot. 4G is relatively slow but can be helpful in areas with available this can provide a faster service than legacy copper phone lines

Many of these connectivity devices have overlapping capabilities. As mentio and often has a switch and a WAP.

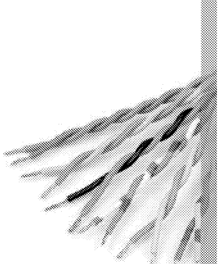
Activity B4
Explain the differences between gateways, bridges, switches a

B2.1.3 connection media

This table contains more technical detail about the different types of wired an

Connection	Type	Technical specification	Advantages	Di
Wired	**Ethernet**	Twisted-pair cable (Cat5e, Cat6)	Reliable, fast, low latency, secure	Limited installat cable w
	USB	Wired input connection for peripherals and data transfer. (USB 1.1, 2.0, 3.0, 3.1, and 4.0)	Universal compatibility, fast data transfer (USB 3+).	Short ca slower s versions
	Optical Fibre	Uses light pulses to transmit data through fibre-optic cables.	Extremely fast, low latency, long-distance.	Expensi fragile, with tha
Wireless	**Wi-Fi (802.11 standards)**	Wireless connection using radio waves (2.4 GHz, 5 GHz, 6 GHz).	Convenient, flexible, fast speeds (Wi-Fi 6).	Interfere range, s vulnerat
	NFC	Wireless, short-range (4 cm) communication using 13.56 MHz radio waves.	Contactless, low power, quick authentication.	Limited transfer
	Bluetooth	Short-range wireless communication (2.4 GHz) for device pairing.	Low power, easy pairing, wide compatibility.	Short ra speeds,
	Cellular (5G)	Mobile connectivity using radio towers (millimetre-wave and sub-6 GHz).	High-speed data, low latency, supports many devices.	Limited expensi security
	Optical Li-Fi	Data transfer using visible light instead of radio waves.	Very fast speeds, secure, immune to electromagnetic interference.	Limited line of s technolo

16-core fibre-optic cable



10
1

B2.2 Application and security issues of external me

External media and storage refer to *physical devices* or *digital platforms* used t outside of a computer's internal storage. These devices can be *removable*, *por* them ideal for temporary or long-term data storage and sharing. Removable p drives, external hard drives, SD cards, CDs and DVDs, and tape. Network-base *attached storage (NAS)* and cloud storage platforms.

Encryption (B2.2.1)

Encryption is used to protect data on external media by converting it into unr decryption key. Although this helps prevent your data being accessed or stole to be compliant with data protection regulations (e.g. GDPR) if it contains pers encryption (built into devices) and software encryption (BitLocker, VeraCrypt) issues with encryption are:

- outdated or weak encryption methods can be easily cracked
- losing or mismanaging encryption keys renders data unrecoverable
- encryption can slow down data transfer speeds
- encrypted media may not be readable on all devices or operating system

Secure disposal (B2.2.2)

When external media comes to the end of its life (for example if it has some e broken) it's important that it is disposed of in a way that any sensitive data ca individuals. Disposal methods include *physical destruction* (shredding, demag secure erase tools). Security issues with secure disposal, which can be avoide

- disposal companies may claim they wipe the data but cut costs and send
- incomplete erasure may leave residual data accessible
- simple file deletion or formatting does not completely erase data
- some media retains metadata even after deletion

Loss or theft of media (B2.2.3)

External media is portable which makes it prone to being lost or stolen. Also, transfer, or temporary storage, it may contain more than just current workin considered a risk in the case of loss or theft:

- lost media without encryption or password protection exposes sensitive
- stolen devices with confidential data can lead to legal and financial conse
- unlike cloud storage, physical media cannot be remotely wiped
- unlike smart devices, it can be difficult to trace or locate lost and stolen m

Interception/copying (B2.2.4)

Data transfer between a computer and an external device gives more potenti during transfer between devices. This can occur through physical tampering o wireless transfers through Bluetooth or Wi-Fi. Considerations for security are

- media contents can be copied quickly and covertly
- data transferred without encryption is easily intercepted
- employees may copy data from external media without permission

Data loss or corruption (B2.2.5)

Data loss or corruption occurs due to accidental deletion, physical damage, or often in temporary storage as they are not kept stationary. Therefore, good b cater for the following possibilities:

- media failure or file corruption can make data unreadable
- incomplete writes or improper ejection can lead to corruption
- a power failure during transfer can result in corrupted or incomplete file

Media lifespan leading to failure (B2.2.6)

External media has a finite lifespan, depending on usage and quality; cheap fl lower quality than those built into devices. Over time media may become unr which can render stored data permanently inaccessible. In addition, old medi speeds or data inconsistencies. It is a bad idea to rely on a single external me any files.

Malware vector (B2.2.7)

External media can carry and spread malware (e.g. viruses, ransomware); com drives, SD cards, and external hard disks. This is because users can use extern laptops with less protection and oversight, and some users such as consultant organisations. Problems specific to external media are:

- some operating systems automatically *autorun* executable files on externa
- files on external media can contain *hidden malware* or *payloads*
- *cross-device infection*: infected media can spread malware to multiple sy
- media without proper *antivirus scanning* before use may introduce threa

Key mitigation strategies for IT departments to consider implementing for employees using

- Use strong encryption (AES-256) for sensitive data.
- Implement strict media disposal policies (e.g. shredding, degaussing).
- Enforce access controls and require multifactor authentication (MFA).
- Use secure file transfer protocols (e.g. SFTP, FTPS).
- Regularly back up data stored on external media.
- Employ anti-malware scanning tools before connecting external media.
- Implement media usage policies (e.g. disable autorun, restrict unknown devices).

Activity B5

A family member has started a business. They take a tape backup of all their files each night. Write them a short bullet point list of suggestions for an IT policy based on the points in B2.2.

B2.3 Application and features of network softwar

Network and device operating systems (B2.3.1)

Network and device operating systems are specialized systems designed to m switches, firewalls) or devices with network capabilities (servers, IoT devices). following interfaces:

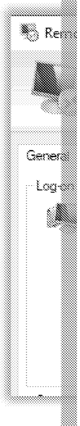
- **Graphical User Interface (GUI):** this provides a visual representation of ne it easier for administrators to manage and configure them. Like in Windo navigation, visual dashboards to monitor performance, and drag-and-dro training to use them.
- **Command Line Interface (CLI)**: this involves typing commands. Although commands, and the output is often harder to read and understand, it do low resource usage, faster execution particularly for bulk operations, and for repeated processes and setup.
- **Web Interface (Internal Web Page for Device Control and Configuration** firewalls, access points) have built-in web interfaces for remote managem normally have a password protected login to access them. It is a massive so multiple devices can be configured and monitored over the network fr this from home by going to your home router; the IP address will be on th 192.168.0.254, 192.168.1.1, 192.168.1.254 or 10.0.0.1.

Network monitoring, management and troubleshooting tool

Large networks can be difficult to administer so several tools have evolved to h

Category	Application	Key Feature
Remote Access Administration	Remote access tools to manage multiple network devices and servers from a single location	• Secure encrypted co • File transfer capabili • Multi-platform suppo
	VPN (Virtual Private Network) can give secure remote access to other internal networks	• Encrypted tunnel • IP masking • Bypass geo-restrictio
Performance Monitor	Real-time performance to monitor network resource usage	• Live resource stats • Historical data • Alerts and notificati
Events and Logs Viewer	Log management tools to analyse and display system and network event logs	• Log filtering and sea • Time-stamped recor • Exportable logs
Vulnerability Scanner	Security assessment tools to scan for security vulnerabilities in devices and networks	• Automated scanning • Generates vulnerabi • Compliance checks
Network Analyser / Packet Sniffer	Traffic analysis tools	• Packet inspection • Real-time monitori • Protocol filtering
Network Management Tools	Network configuration managers	• Automated device c • Performance trackin • Alerts and reporting
Network Troubleshooting	Diagnostic and repair tools	• Ping and tracerout • Route analysis • Latency measureme

RDP stands for *Remote Desktop Protocol* and is a technology developed by Microsoft to enable users to connect to and control another computer over a network or the Internet. It is often used by employees working from home to access their work computers. Ideally it should be used in conjunction with a VPN, which adds another layer of security to prevent cyberattacks.



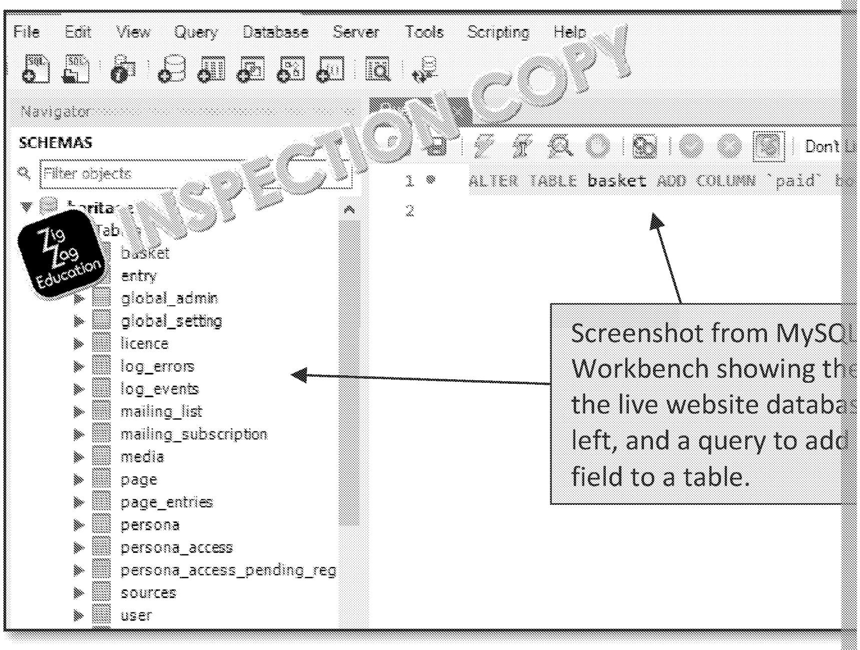
Network Applications (B2.3.3)

There are a number of applications available with a specific focus on managin

Remote desktop tools enable remote access to network devices, workstation

- VPN or Remote Desktop to connect and use workstations and servers
- SSH clients for remote management of routers and switches
- Cloud-based remote monitoring by applications such as Cisco Meraki and time network monitoring, alerts and remote configuration

Remote database management software such as MySQL Workbench, phpMy enable you to connect to databases on other services or SANs to edit data, ch corruptions and import new or updated data.



```
ALTER TABLE basket ADD COLUMN `paid`
```

Screenshot from MySQL Workbench showing th the live website databa left, and a query to add field to a table.

Document Management Applications (DMAs) are software solutions that ena access, manage, and collaborate on documents over a network. These tools in control, and document security, making them essential for businesses handlin

Network discovery and mapping tools are software applications used to iden devices and infrastructure. These tools automatically scan the network, detec network topology maps. They help IT administrators understand, manage and by offering detailed visual representations of network components.

B3 Networking infrastructure servi

B3.1 Application and function

Transmission Control Protocol/Internet Protocol (TCP/IP) (B3.

The four-layer model

TCP/IP stands for *Transmission Control Protocol / Internet Protocol*. It is a seri
communications on LAN and WAN networks and is widely considered the sta
The protocol is arranged in a stack with four layers, which are shown here:

Application layer	The *application layer* defines the protocols for the application (which th interface (communicate) with the *transport layer*. The application layer Naming System), HTTP (Hypertext Transfer Protocol), FTP (File Transfer Transfer Protocol), DHCP (Dynamic Host Configuration Protocol), RDP (R Shell) and Telnet.
Transport layer	The *transport layer* permits source devices and destination devices to s defines the level of services and the status of the connection used whe protocols included are TCP (Transmission Control Protocol) and UDP (U
Internet layer	The *Internet layer* splits the data up into data packets known as *IP data* destination address. The *Internet layer* also determines the route that t arrive from a source in a different order from that in which they were se layer to put them back in the right order.
Network access layer	The *network access layer* defines the protocols of how data is physicall bits are electronically or optically signalled by the hardware devices tha cable. The most common protocol is *Ethernet*.

Transport Layer Security (TLS)

TLS is a cryptographic protocol used to provide secure communication over a
the *Transport Layer* of the TCP/IP model, sitting above the TCP layer and ensu
between client and server is encrypted and authenticated.

Packets and headers

For data to be sent across a network, it is broken down into a structure know
broadcast by a device across the network. To give you some idea, a single pac
800 bits, so a 2-megabyte file will be broadcast as 20,000 packets. This will ca
the most direct route to the destination will change during the course of tran
in a different order to that which they were sent.

To enable packets to reach the correct destinations and then be assembled in
up of a *header,* the *body (or payload)* and a *trailer* or *footer*. See more on pac

Error correction

A *checksum* is a simple calculation – e.g. adding up the bits in the package and g
calculated again when the package arrives. If the checksum after arriving is diff
it means that there must have been an error in transmitting one or more of the
have been accidentally swapped during transmission, then the checksum wou

A *cyclic redundancy check (CRC)* does the same job as a checksum, but it uses
formula that still picks up an error if the same digits are sent in a different o

Packets are retransmitted if there is packet loss (when a packet doesn't arrive
happen if, for example:

- there is network congestion because the network hits maximum capacity,
- electrical interference causes packet corruption, or
- faulty hardware fails to transmit packets correctly

Ports (B3.1.2)

Hardware switch ports are the physical ports in a network switch that device network devices) plug into for communication with other network devices. T i.e. RJ45 ports for Ethernet or fibre-optic ports. The switch forwards traffic fr their *MAC addresses*; they maintain a MAC address table which maps the MA ports. Switches with port security block or allow specific MAC addresses to se unauthorised devices from accessing the network. [illegible] ports will be normal or more *trunk* or *uplink* ports that can transfer data at a higher speed to conn prevent bottlenecks.

Software or virtual ports, commonly referred to as *Internet Protocol (IP) port* communication between applications running on devices over a network. The applications/services on a device (like a web server or an email service). An number ranging from 0 to 65535; see *section A2.1.1* for more information abo

Packets (B3.1.3)

Here is an example structure of a packet:

Header	Payload	Footer
Destination	Data (content)	CRC (Cyclic Redundancy Che check whether the data has during transmission
Source		
Protocol		
TTL		Padding (if required to ensu the packet matches what is
Checksum		
Sequence		

Time To Live (TTL) prevents a packet from circulating indefinitely in case of ro each router, and if it reaches zero, the packet is discarded.

Protocol [illegible] TCP/IP and UDP:

- **IP (Internet Protocol):**
  - Responsible for addressing and routing.
  - Used for routing data between devices across different networks.
- **TCP (Transmission Control Protocol):**
  - Establishes a connection before transmitting data.
  - Used with IP.
  - Ensures data is delivered in order, with error correction and retrans
  - Used for web browsing (HTTP/HTTPS), email (SMTP), file transfer (F
- **UDP (User Datagram Protocol):**
  - No connection set-up before sending data.
  - Does not guarantee delivery, order, or error checking beyond a simp
  - Used for streaming, DNS, VoIP and online gaming where speed is m

Network address translation (NAT) (B3.1.4)

Each device active on a network has a unique IPv4 IP address. IPv4 addresses a between 0 and 255, separated by dots. This IPv4 addresses can therefore be b 255.255.255.255 (with some limitations, more on this below).

In addition, if you are connected to the Internet, then your router will have an allocated by your ISP. You can see what this is by searching the Internet for "W understand that every router in the world connected to the Internet will have that each network can also have the full range of IPv4 addresses.

NAT (network address translation)

A website on Internet web server will have an internal IP address. But the v IP address has been given to the server by the web hosting company in th an IP address. When you send a request to the server, it converts its domain n server has a NAT table that maps the public IP address to the website internal mapping. This is helpful for security because it means that all connections mu and cannot communicate with it directly.

PAT (port address translation)

A local area network might have 1,000 devices with IP addresses, but only one IP address, so it needs to have a one-to-many mapping, with each internal dev a unique port number.

If your computer communicates with another computer through the Internet, e.g. if you are v following process happens:

1. Your communication goes from your computer to your Internet router.
2. The Internet router makes a note of your (private) IPv4 address and logs it against a uni
3. It then sends your request, identified by your router's (public) IPv4 address as well as yo sending your friend's router's (public) IPv4 address and their (public) port ID.
4. Your friend's Internet router will look up your friend's (public) port ID to find their (priva send them the communication.
5. The whole process happens in reverse when your friend's computer sends commu

Static and dynamic IP addresses

In terms of **public IP addresses**, a web server, mail server or VPN server needs can be found by the address which is verified against the public DNS records. Y connection may be dynamically allocated by your ISP each time you restart yo IP addresses, or they may be static which means they don't change.

Similarly on your network the internal IP addresses can be dynamic (they can c *for more details.*

IPv6

IPv6 (Internet Protocol version 6) was developed to replace IPv4 due to severa including the maximum number of addresses and the need for improved effici the huge number of IoT devices.

The IPv4 address is made up of four sets of numbers up to 255 which can be sto The IPv6 address is made up of eight sets of 4-digit hexadecimal numbers which e.g. 2a00:23c7:d43c:8101:333c:da5c:5c6b:cde7. IPv4 can hold up to 4.3 billion 340 trillion trillion trillion unique IPs!

Currently most networks currently run dual IPv4 and IPv6 addresses, but this w years; in 2025 just over 50% of Internet traffic used IPv6.

RFC 1918 private addresses

For internal networks, the *RFC 1918* standard specifies that the following rang use in local networks and cannot be used as public Internet IP addresses:

- Class A: 10.0. 0.0 to 10.255. 255.255 (16,777,216 possible addresses)
- Class B: 172.16. 0.0 to 172.31. 255.255 (1,048,576 possible addresses)
- Class C: 192.168. 0.0 to 192.168. 255.255 (65,546 possible addresses)

There are also a few reserved IP addresses:

- Automatic Private IP Addressing (APIPA) for DHCP (dynamic IP allocation) 169.254.254.255
- 127.0.0.1 loopback address (localhost) – used for internal testing
- 255.255.255.255 broadcast address for local networks
- 224.0.0.0 – 239.255.255.255 multicast IP range for streaming and confere

Activity B6

Sasha is talking to her friend James on WhatsApp. WhatsApp is not peer-to-peer, so all traffi address *157.240.3.54*. Sasha's mobile IP address is *192.168.0.5* and James' IP address is *10.0.* address *62.31.148.219* and James' Internet router has IP address *62.30.148.69*.

Draw a diagram to illustrate a packet of information travelling from Sasha to James, and how

B3.2 Application of domains, sub-domains and seg

A *domain* is a group of devices, users and resources that are managed togethe policies; for example, a domain may cover all devices, storage and users in an

- A *sub-domain* is a smaller, distinct part of the main domain, often used fo e.g. dividing network resources into the sales department, the developme HR department.
- *Segmentation* refers to dividing networks into smaller, manageable sectio security, e.g. the HR department may be separated into payroll and new

Go to zzed.uk/12912

Research Activity

Read **zzed.uk/12912-Network-Segmentation** on the topic of Network Segmentation. Extra and illustrate them as an infographic or a poster.

Hierarchy (B3.2.1)

The hierarchical structure of domains and sub-domains ensures:

- Centralised management: network administrators can apply global policie
- Granular control: each sub-domain can have different security rules and a
- Efficient resource allocation: network traffic and resources are organised sub-domain membership.

Trust relationships (B3.2.2)

A *trust relationship* defines how different network domains or sub-domains in permissions. It determines whether devices or users in one domain can access sub-domain. This means that:

- Users can access shared resources across trusted domains without additi
- Network admins can selectively allow or block trust, protecting sensitive
- There is no need to create duplicate user accounts across domains.

Access control (B3.2.3)

Access control in network segmentation defines who can access what resources based on user identity, device, and trust level. It ensures that only authorised users can interact with specific devices, data and applications. Types of network access control include:

- Role-Based Access Control (RBAC) → access based on user roles (e.g. admin, employee).
- MAC Filtering → restricts access by specific device MAC addresses.
- IP-based Access Control Lists (ACLs) → limits access based on IP address r

Security benefits (B3.2.4)

Benefits of structuring network around domains, sub-domains and segmentati

- limits access to devices data, and applications as they are allocated to spe individual segments. For example, a finance VLAN may be set up that onl guest VLAN can be set up that is isolated from the main network, preventi
- restricts lateral movement of malware, e.g. if malware infects the finance sideways into the main or HR departments.
- creates a smaller attack surface: isolating network segments reduces the making it harder for attackers to gain access; for example, IoT devices ca prevent them from exposing core business systems.
- resulting in simpler damage control in that if a breach occurs, only the co which reduces downtime and speeds up recovery.

B3.3 Application of network devices to configure n

Previously we've covered what each of the following devices does. We outlin used in networks:

- An organisation normally has one or more *servers (B3.3.1)* to manage use control centralised printers and manage backups. Other services such as software may be on an internal server or a cloud server.
- Each server normally connects to a master (expensive and fast) network s a switch in each room or location to which computers and printers can co
- There are likely to be *Wireless Access Points (WAPs) (B3.3.4)* around the si Ethernet to switches, or in a wireless mesh to other WAPs.
- The master switch will probably also link to a *router (B3.3.2)* which in tur connected via a fibre-optic connection to the *ISP* (Internet Service Provid
- The Internet is also made up of *routers* which direct traffic on to the next
- If the network has a lot of traffic in separate zones, then a *bridge (B3.3.6)* which will intelligently send traffic for one zone through one port, and tr another port. For example, if an organisation has a very busy printing de data through to the network printers, then the bridge enables this traffic the network.
- A *gateway (B3.3.7)* can be used to connect part of the network using diff rare now. It can also be used to deal with email data, but this is now nor gateway on the email server. However, credit card payment machines li gateways between the network and the phone system.

Activity B7

Draw a diagram of a network that illustrates all the network devices men

B3.4 Application and function of network infrastr

Domain Name System (DNS) (B3.4.1)

The Domain Name System (DNS) is a network service that translates human-r (e.g. *google.com*) into the IP address (e.g. *108.177.98.101*) that identifies whe DNS you would have to remember IP addresses instead of domain names.

DNS resolution process

The **DNS resolution process** is the sequence of steps through which a domain na

1. The user enters the domain name, for example **www.eRevision.uk**, into t
2. The device first checks its local cache to see if it already knows the IP add use[illegible]ec[illegible]
3. If th[illegible] not cached, the request is sent to a recursive DNS resolver pro service (e.g. Google provides DNS 8.8.8.8 and Cloudflare provides 1.1.1.1)
4. The recursive resolver contacts one of the 13 root servers to find informati
5. The TLD server (e.g. .com, .net, .org, .uk) directs the resolver to the authoritative name server responsible for the requested domain.
6. The authoritative name server provides the IP address for the domain.
7. The recursive resolver returns the IP address to the client device, which can now connect to the server hosting the requested website.

Reverse DNS resolution (rDNS)

This is the opposite of standard DNS resolution; it maps an IP address back to the corresponding domain name. This is used to verify that an email serve name to reduce spam.

1. The client sends a reverse DNS query to identify the hostname associated
2. The resolver queries the reverse DNS zone of the IP range.
3. The server looks for the PTR record which contains the domain name lin
4. The hostname is returned to the client.

DNS cache

DNS cac[illegible]mporarily store previously resolved domain names and IP addre times and network latency. Users frequently access the same sites and access site. Occasionally, if a website moves to a new server, users will not be able t has been refreshed; each DNS record has a TTL value that indicates how many (website developers will temporarily reduce this during a website move). DNS

- The browser on your devices and the operating system cache DNS entrie
- Your ISP stores frequently requested domains for faster resolution.
- The *recursive resolver* caches responses for future queries.

IPv6 DNS handles **domain name resolution** for devices using **IPv6 addresses**. for a site, if it has an IPv6 address it is stored in the **AAAA records** instead of t don't yet have AAAA records, but they will be created by the hosting compani

Activity B8

Go to **zzed.uk/12912**

Go to **zzed.uk/12912-DNS** and search for **www.eRevision.uk** to find its IP address. It wil (46.101.67.170 at the time of checking) and the **AAAA** record (doesn't yet exist at the time o for email, the name servers and a series of text records used for site security and verification address[illegible] sec[illegible]ds, so the server will check for any update approximately every two and

Directory services (DS), identity and access management (IA

Directory Services (DS) are centralised systems that store, organise and manag and resources in a network. They are essential for *Identity and Access Manage* only authorised users and devices can access specific resources. *IAM* involves:

- Authentication: verifying a user's identity (e.g. login with username and p
- Authorisation: determining what a user is allowed to do after successfully applications).
- User management: adding, modifying, and removing user accounts.
- Single Sign-On (SSO): enabling access to multiple systems with a single au

Two of the main directory services are Microsoft's Active Directory, which is li operating system and Apple's Open Directory which is licensed with the macO OpenLDAP which is free and open source, designed for Linux platforms.

Authentication services (B3.4.3)

Authentication services are systems and protocols used to verify the identity o attempting to access a network, service or system. It plays a key role in *Identit* ensuring only authorised individuals or systems gain access to resources.

Types of authentication

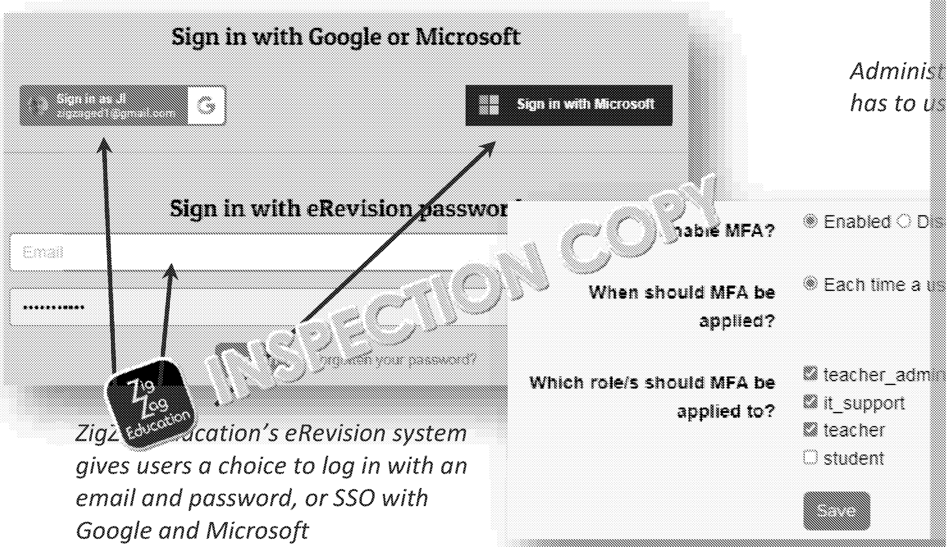
Single-Factor Authentication (SFA) uses only one factor to verify a user's identi This is the least secure, as it relies on a single piece of information, and is vuln brute-force attacks.

Two-Factor Authentication (2FA) or *Multi-Factor Authentication (MFA)* uses tw categories to authenticate users. Although it is much more secure it also has i can be more difficult to recover from if you lose a password. Factors include:

- password (something you know)
- SMS code or smart card (something you have)
- biometric fingerprint (something you are)

Single Sign-On (SSO) allows users to log in once and access multiple applicatio authenticate again. This is more convenient for users and removes the need t However, if the SSO system is compromised, all linked services are vulnerable.

- The user logs in to a central authentication server.
- The server generates a token or session cookie.
- The user accesses multiple services using the same token without re-ente



Sign in with Google or Microsoft

Sign in with eRevision passwor

ZigZag Education's eRevision system gives users a choice to log in with an email and password, or SSO with Google and Microsoft

Enable MFA? ● Enabled ○ Di

When should MFA be applied? ● Each time a u

Which role/s should MFA be applied to?
☑ teacher_adm
☑ it_support
☑ teacher
□ student

Administ has to u

Authentication protocols
These are standardized rules and procedures used to verify the identity of use access a network, application or service. Having standardised protocols creat different platforms and services.

RFC documents issued by the IETF (Internet Engineering Task Force) contain t organisational notes. For example, they define how credentials (username, p transmitted, verified and validated between the client and the server. They in

- *RFC 1334: Password Authentication Protocol (PAP).* This is a basic and ou uses plaintext passwords for authentication where the client sends the u in plaintext and they are matched to the credentials in the database th used for some legacy systems with minimal security requirements it is ins passwords in plaintext.
- *RFC 1994: Challenge Handshake Authentication Protocol (CHAP).* This is a using a challenge-response mechanism for authentication. It is used for V works as follows:
  1. The server sends a random challenge code to the client.
  2. The client hashes the challenge with the password.
  3. The server checks if the hashed response matches its own hash.
  4. If they match, access is granted.
- *RFC 5247: Extensible Authentication Protocol (EAP).* This is a flexible aut supports multiple authentication methods. It is used for VPNs and wirel defines a set of standard messages and procedures but delegates the act methods. Common *EAP* methods are:
  - EAP-TLS: uses certificates for authentication.
  - EAP-TTLS: combines TLS with password-based authentication.
  - EAP-PEAP: secure channel with MS-CHAPv2 authentication.

Activity
Explain the difference between PAP, CHAP and EAP and when you would u Then have a look at the DNS records for your school domain.

Dynamic Host Configuration Protocol (DHCP) (B3.4.4)

DHCP is a network management protocol used on IP networks whereby a DHC addresses to each device on a network, so they can communicate with other d means that network administrators don't have to manually assign IP addresse

A *DHCP server* is a device (often a router or a dedicated server) that runs the D IP addresses and leases them to clients. It also provides other configuration i default gateways, and DNS server addresses.

A *DHCP client* is any device (computer, smartphone, printer, etc.) that request information from a DHCP server. When a client joins a network, it broadcasts configuration information.

The *DHCP IP address allocation process* typically involves four main steps, ofte

1. The client broadcasts a *DHCPDISCOVER* message to find available DHCP s
2. DHCP servers that receive the DISCOVER message respond with a *DHCPO* an available IP address, subnet mask, lease duration, and other configura
3. The client chooses one of the offered IP addresses and broadcasts a *DHC* acceptance of the offer.
4. The DHCP server that offered the chosen IP address sends a *DHCPACK* (a client, confirming the assignment and providing the complete configurati

IP address ranges

- A DHCP server is configured with a range of IP addresses that it can assign to clients.
- This range is defined by a start address and an end address.
- Example: 192.168.1.100 - 192.168.1.200. This example would allow the DHCP server to lease 101 different IP addresses.

DNS server address

This is the static IP address that is assigned to the DHCP server itself. Clients need to be able to locate the DHCP server, so the server needs a consistent IP address. This address is not in the range of IP addresses that are allocated to clients.

Basic configuration setti

DHCP servers provide va clients, including:

- *IP address:* the uniq each device on the
- *Subnet mask:* deter host portion of an IP
- *Default gateway:* th allows the client to other networks, mo
- *DNS server address:* Name System serve names to IP address
- *Lease duration:* how IP address before it

Lease duration

A DHCP lease is the duration for which a client is granted the use of an IP addr expire, the client attempts to renew it with the DHCP server. If a client does n returned to the pool of available addresses.

IP addresses are allocated in one of three ways:

Dynamic IP Address Allocation	Reservations (Static IP Addresses)	Autom
Dynamic allocation is the standard DHCP process where IP addresses are assigned automatically to clients as they join the network. The server assigns an IP address from a defined range of IP addresses. This is the most common use of DHCP.	DHCP servers can be configured to reserve specific IP addresses for particular devices by associating a device's MAC address with a specific IP address. This is useful for devices that require a consistent IP address, such as printers or servers. This is also known as a static DHCP lease. The server should not allow two devices to reserve the same IP address.	Automatic allocation i DHCP server semi-per client the first time th table of past assignme address to the client a This is different from does not manually co address and IP addres by the DHCP server. A device then the origin a different IP address

Routing (B3.4.5)

Routing is the process of selecting a path for data packets to travel across a ne destination. Routers are the devices responsible for making these path selecti commonly manually configured (static) whereas more complex larger network

Static routing is manually configured with fixed routes that do not change unle predictable paths for data packets, and routes can be configured with security t domains to use a path. It does mean that manual updates are needed when a link fails the data cannot be sent down another available route if it has not been

Dynamic (adaptive) routing uses routers that automatically learn and update r condition. Routers use routing protocols to exchange information and deter it can adapt to network changes and failures and make efficient use of networ However, it can be more complex to configure and troubleshoot if more sophi needed. Also, it can create routing loops if not configured properly.

Routing tables are data tables stored in a router that lists the best paths to va determine where to forward packets. Each entry in the table typically include

- Destination network address
- Subnet mask
- Next-hop IP address (the address of the next router in the path)
- Outgoing interface
- Metric (a value that indicates the "cost" of the path)

Different protocols are used whether it is an internal or external packet:

- *Interior Gateway Protocols (IGPs)* are used for routing within a network u (e.g. a corporate network). Common IGPs include:
  - *RIP (Routing Information Protocol):* a simple distance-vector protocol t
  - *OSPF (Open Shortest Path First):* a link-state protocol that uses a more bandwidth. It is more scalable and efficient than RIP.
  - *EIGRP (Enhanced Interior Gateway Routing Protocol):* a Cisco-propriet features of distance-vector and link-state protocols. Fast convergenc
  - *IS-IS (Intermediate System to Intermediate System):* a link-state routir service provider networks.
- *Exterior Gateway Protocols (EGPs)* are used for routing separate network
- *Border Gateway Protocol (BGP)* is the standard EGP used for Internet rou that exchanges reachability information between networks. BGP makes and path attributes, rather than just hop count or link cost, and is crucial scalability of the Internet.

Remote access services (RAS) (B3.4.6)

Remote access services refer to the technologies and methods that allow user the device from a remote location. These services enable users to access files printers, and other resources without being physically present at the location *handshake* is the initial communication process to verify identity and establis

RAS Type	Description	Connection Proce
1. Dial-up (Telecommunications Services)	Uses traditional phone lines and modems to connect to remote networks. Used for legacy systems, emergency remote access and remote terminal connections.	Client uses a modem to server's phone number. server authenticates th access to resources is g
2. VPN (Over the Internet)	Secure remote access over the Internet which creates an *encrypted tunnel* between the client and the server. Protects data over public Wi-Fi.	Client initiates VPN con request. Server authent user. A secure, encrypte established.

Handshake/connection processes (client-host/server)

The *handshake process* is the initial communication between the client and th secure and authenticated connection.

- In a *dial-up handshake* the client dials the server's phone number. Mode audio signals. Authentication through username and password.
- In a *VPN handshake* the client sends a connection request to the VPN ser challenge, requesting authentication details. If authentication is successf encryption protocol, and the client is assigned an internal IP address. If a is rejected.

Activity B10

Teachers at a school can connect to the school file system in the evening when planning thei can access Internet files and the intranet. Describe how the VPN works.

B3.5 Application and function of network services a

File and print services (B3.5.1)

File services

File services enable the storage, retrieval, sharing and management of files ove multiple users to access shared files simultaneously, enhancing collaboration a networks have a centralised storage location, providing easy access to shared on one or more *file servers* which have large hard drives or dedicated *network*

Having centralised storage means that individuals can hot-desk (desktop and d computer when the user logs on) as well as collaboration and file sharing acros simplifies backup and recovery.

File services are specifically set up for *file management* for multiple users on a file access control and permissions (e.g. no access, read-only, or write access).

- *Tracking*: monitoring who accesses, modifies or deletes files. It may also i (e.g. Git) to help track file changes.
- *Sharing*: users to access files from different locations. File permissions co specific files.
- *Security*: encryption protects files from unauthorised access, and backup a file safety in case of hardware failure or data loss.

Print services

Print services manage and control the printing process over a network, allowin efficiently. These services optimise print jobs by managing queues, prioritising configurations.

A *networked printer* is a printer that is capable of being connected directly to t (via Ethernet or Wi-Fi) rather than needing to be connected to a desktop comp This means it can be accessed by multiple users without the need for a dedica machine. It will often be configured with a static IP address to help with print

A *print server* is a server or device that specialises in managing print jobs from printers on the network are listed on the printer server, and when a client req provides the printer drivers if it is not already installed on the client. It receive sends them to the appropriate printer. It may have the capability to improve p prioritising jobs. Print management includes:

- *Sharing* of network printers by multiple devices and users, reducing the n permissions control who can access and manage print jobs.
- *Queueing:* print jobs are placed in a queue and processed in order. Users their print requests.
- *Prioritising:* admins can prioritise specific print jobs, or users may be able may be allocated by user or department. Higher priority jobs are printed

Adding a new printer to the network involves:

- *Printer configuration:* setting up the printer's IP address, network name, a define default print settings (e.g. black-and-white vs colour) and *print qu*
- *Driver management:* print drivers translate print jobs into commands the must ensure correct drivers are installed on the print server to automatic them on all client machines for each printer type they use. Drivers need t compatibility and performance improvements.

Web, mail and communications services (B3.5.2)

Web services

Web services are software applications that enable communication and the sh
systems over the Internet or a network using standard protocols.

HTTP or HTTPS are web protocols that are used to send information between a
web browser:

- *HTTP (Hypertext Transfer Protocol)*: the client sends a GET, POST, PUT, or
  processes the request and sends a response.
- *HTTPS (HTTP Secure)*: the secure version of HTTP, using SSL/TLS encrypti
  prevent eavesdropping, tampering, and man-in-the-middle attacks. It is p
  credit card payments over the Internet.

The response from the web services is normally *HTML* data, or files such as ima
to be displayed in a web browser. The response is more likely to be *XML*, *JSON*
from an API or an AJAX call or if the data is to be processed in some way.

<table>
<tr><th colspan="2">Comparison of HTML, XML and JSON to return details of some book info</th></tr>
<tr><th>Format</th><th>Representation</th></tr>
<tr><td>HTML</td><td><pre>
<!DOCTYPE html>
<html>
        <head>
                <title>Book Information</title>
        </head>
        <body>
                <h1>Book Details</h1>
                <p><strong>Title:</strong> The Hitchhiker's Guide to t
                <p><strong>Author:</strong> Douglas Adams</p>
                <p><strong>Year:</strong> 1979</p>
        </body>
</html>
</pre></td></tr>
<tr><td>XML</td><td><pre>
<?xml version="1.0" encoding="UTF-8"?>
 <book>
        <title>The Hitchhiker's Guide to the Galaxy</title>
        <author>Douglas Adams</author>
        <year>1979</year>
</book>
</pre></td></tr>
<tr><td>JSON</td><td>json { "title": "The Hitchhiker's Guide to the Galaxy", "author": "D</td></tr>
</table>

Web protocols allow applications to exchange data and interact with each oth
language or operating system they use. For example, a Python application run
an https request to a PHP-based web service running on a Linux web server.

Mail services

Mail services are the systems and protocols involved in sending, receiving and
involves a physical server (sometimes a dedicated mail server), mail server sof
and receiving email, and client software or website code to create and send th

Originally Yahoo, Hotmail, Google and others hosted free email on dedicated e
and Google now provide businesses with managed email services which are pa
services. Many businesses used to host mail server software on their own serv
lot of technical knowledge is needed to keep everything updated to comply wi
treated as spam, so many have moved to managed mail services.

Mail client software for desktop computers includes Microsoft Outlook. Outl available on devices including tablets and mobiles. Users can also manage th needing no software other than an Internet browser.

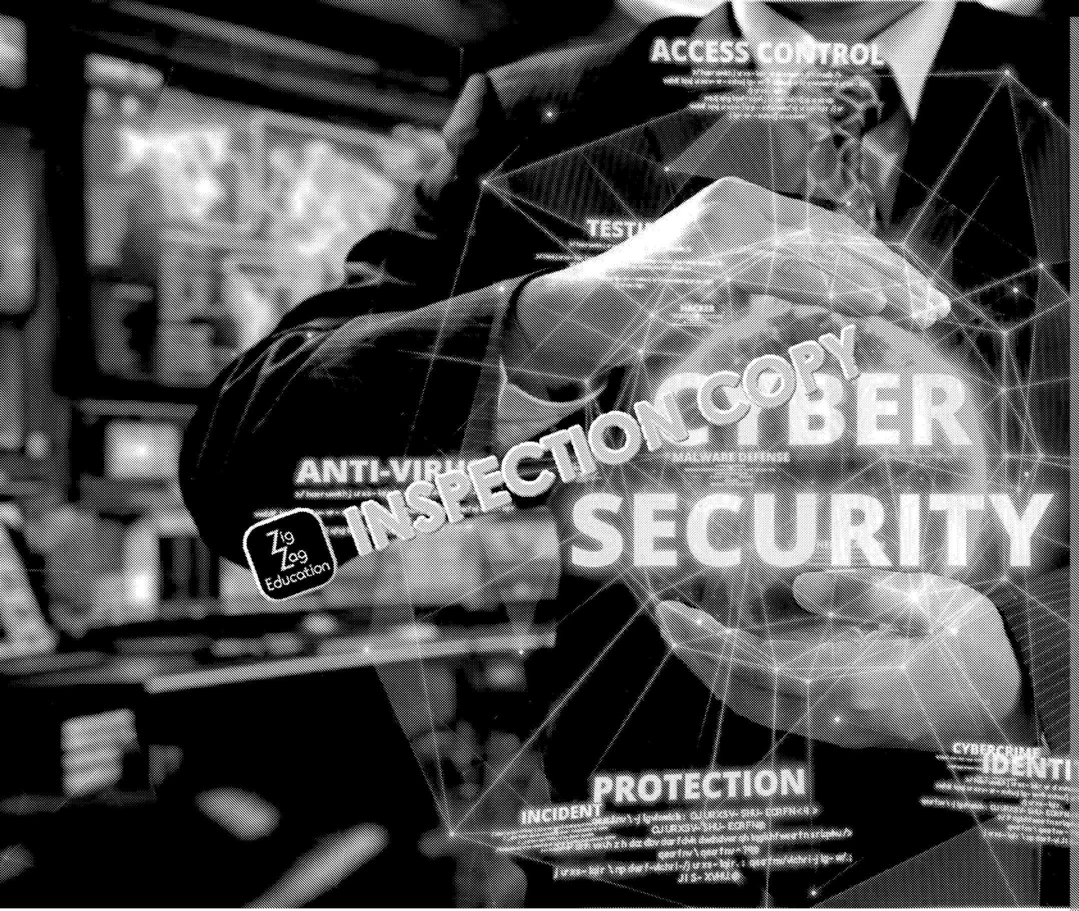
Mail protocols include:

- SMTP (Simple Mail Transfer Protocol) which is used to **send** email from a mail servers. It handles the transmission of email messages.
- POP (Post Office Protocol) which is used for **retrieving** email from a mail email to a mobile phone.
- IMAP (Internet Message Access Protocol) is an alternative to POP, allowin email on the server without downloading it. IMAP is better for keeping e multiple devices.
- MIME (Multipurpose Internet Mail Extensions) extends the format of em other than ASCII and non-text attachments such as images, audio and vid

These old protocols have a lack of built-in encryption and transmit data in pla eavesdropping. To address this, SMTPS, POP3S and IMAPS have been develop

When an email is sent, the sending mail server uses DNS (Domain Name Syste Exchange) record of the recipient's domain which specifies which mail server for that domain. The sending server then connects to the destination server t

Communication Methods		
Communication Service	**Description**	
Email	Digital messaging system for exchanging messages over a network.	G M
VoIP (Voice over IP) / Internet Calling	Voice communication over the Internet. Converts voice signals into digital data packets.	S C D
SMS/Text Messaging	Short Message Service for text messages on mobile phones. Uses cellular networks.	S p
Video Conferencing	Real-time video and audio communication between multiple participants. Used for remote meetings.	Z T W
Social Networking Applications	Platforms for connecting, sharing information, and communicating. Offer various communication features such as messaging, posts, comments.	F In
Online Collaboration Tools	Applications facilitating teamwork and collaboration. Provides features such as shared documents, project management, and team messaging.	G M T
Communication as a Service (CaaS)	Cloud-based delivery model providing communications tools and services over the Internet. Businesses can access advanced communication features without investing in infrastructure. Includes VoIP, video conferencing, messaging, and collaboration tools. CaaS providers handle the maintenance and upgrades of communication systems.	R V



AAQ BTEC National IT

Cyber Security and Incident M

Content Area C: Cyber security

Contents

C1 Internal policies and gener

C1.1 Use of general security-related IT policies and

You need to know and understand the governance policies and documents ne security on an ongoing basis.

Cyber security policies (C1.1)

Cyber security policies should apply the Plan-Do-Check-Act loop (PDCA loop) derived from ISO of the International Organization for Standardization ISO27001:2022 (previously 2013). The *PDCA cycle* ensures that the *ISMS* evolves with changing threats, risks, and organisational needs. It promotes a proactive approach by identifying vulnerabilities and addressing them through continuous feedback loops. The cycle is *iterative* – each time it completes, the organisation refines and strengthens its security:

1. **Plan:**
   - Define the scope of the ISMS (Information Security Management Sys
   - Identify internal and external risks and requirements.
   - Set security goals and policies.
   - Create a risk assessment and treatment plan.
   - Assign roles and responsibilities.

2. **Do:**
   - Put the security controls and processes into practice.
   - Ensure employees are competent and aware of security measures.

3. **Check:**
   - Check how well the ISMS is working.
   - Monitor and measure its performance.
   - Carry out internal audits.
   - Review the risk assessment results and spot any issues.

4. **Act (Improve):**
   - Take corrective actions to fix problems.
   - Update policies, procedures, and controls as needed.
   - Use audit findings and incidents to improve the ISMS continuously.

Activity C1

Overleaf is an example security policy on the use of Internet and email at an organisation. Th need to know about for your exam. Compare this security policy to your school security policy suggesting any improvements, if there are any, to your school policy.

Exam Tip! It may be primarily larger businesses that need and pay for ISO certification, but small businesses also need comprehensive security policies.

Internet and Email Use Policy

1. **Inappropriate, Offensive, or Illegal Material**
   - **Prohibited Content:** employees must not access, download, store, or share content that is inappropriate, offensive, or illegal, including but not limited to:
     - pornographic, obscene, or sexually explicit material.
     - hateful or discriminatory content.
     - material promoting violence or illegal activities.
     - content that may be considered harassment, bullying, or abusive.
   - **Consequences:** any attempt to access or distribute such content will be considered a serious violation of company policy and may result in disciplinary action, including termination. Illegal activities may be reported to law enforcement.

2. **Sending Confidential Information**
   - **Confidentiality Protection:** employees must not send confidential or sensitive information (e.g. financial data, customer details, or intellectual property) via unsecured email. When sending confidential information:
     - Use encryption.
     - Apply email classification labels (e.g. 'Confidential') where available.
   - **Unauthorised Disclosure:** sending confidential information to unauthorised recipients is a breach of policy and may lead to disciplinary action. Any accidental disclosure must be reported immediately.

3. **Privacy Issues**
   - **User Privacy:** employees should not assume privacy when using the organisation's Internet or email systems. The company may monitor, log, and review usage to ensure compliance with security policies.
   - **Personal Use:** limited personal use of Internet and email is allowed but must not interfere with work responsibilities. Personal use must comply with the same security and privacy rules.

4. **Upload/Download of Copyrighted Material, Music, and Video**
   - **Prohibited Downloads:** employees must not upload or download copyrighted material (e.g. music, films, software) without proper authorisation or licensing. Peer-to-peer (P2P) file sharing of copyrighted content is strictly forbidden.
   - **Legal Compliance:** violating copyright laws could result in legal consequences for both the employee and the organisation. Employees involved in unauthorised distribution may face disciplinary action.

5. **Download of Exe**
   - **File Downlo** download o .msi) from th IT departme increase the
   - **Software In** permitted. U system vuln

6. **Visiting Potentia**
   - **Restricted W** websites tha
     - flag a softw
     - host il
     - promo
   - **Web Filterin** filtering too Attempts to of policy.

7. **Organisation's Ri Monitor Activitie**
   - **Monitoring** reserves the
     - Monito visited
     - Scan n
     - Retain
   - **Email Reter** emails for le purposes. E audits or inv
   - **Employee N** of the organi expectation provided sy

Acknowledgment and
All employees must re Failure to comply may termination. The orga this policy as needed security requirements

Activity C2

Below is an example set of security and password procedures. The headings match the points your exam.

Read the article called '**The logic behind three random words**' at **zzed.uk/12912-rando** ways should the password length and strength policy below be updated?

Go to zz

Security and Password Procedures

1. **Password Length and Strength Policy**
   - **Length Requirements:** all passwords must be at least 12 characters long. For privileged accounts (e.g. admin, root), passwords must be at least 16 characters. Passwords must not be more than 20 characters.
   - **Complexity Requirements:** Passwords must include:
     - at least one uppercase letter (A-Z),
     - at least one lowercase letter (a-z),
     - at least one number (0-9),
     - at least one special character (e.g. !@#$%^&*).
     - Passwords must not contain usernames, email addresses, or repeated or sequential characters (e.g. 123456, aaaaaa).

2. **Management and Enforcement Tools**
   - **Password Management Software:** the organisation uses password management tools to generate and store strong, unique passwords. Employees are required to use company-approved password managers.
   - **Enforcement Measures:** the IT department enforces password policies through Active Directory (AD) or equivalent systems. Password complexity and expiration rules are automatically applied.
   - **Self-Service Reset:** a self-service password reset (SSPR) portal is available for employees, with multi-factor authentication (MFA) verification.

3. **Deny Lists of Common/Weak Passwords**
   - **Blocked Passwords:** the organisation maintains a deny list of common and weak passwords such as 123456, password, qwerty, letmein, admin. It also denies variations with numbers or special characters (e.g. P@ssw0rd).
   - **Automatic Checks:** the system also checks new passwords against a database of known compromised credentials. If a password is on the deny list, the user is required to choose a stronger password.

4. **Monitoring and Log**
   - **Failed Login A** logs all login a after multiple
   - **Logging Detai** username and attempt, IP ad failure status
   - **Incident Resp** automated se result in temp to the security

5. **Lockout Policy for I**
   - **Account Locko** login attempts minutes. Furth lockout period
   - **Automatic Log** log out inactiv
   - **Re-authentica** authenticate a

6. **Use of Technology t Passwords**
   - **Multi-Factor A** uses MFA to r required for e cloud/remote a
   - **Biometric Aut** authentication used instead o
   - **Single Sign On** solutions (e.g. A of individual pa SSO integrates
   - **Passwordless** organisation a methods, such authenticator a

Staff responsibilities in cyber security policies

Staff IT security training aims to empower employees to become a strong first threats. It's not just about compliance; it's about creating a security-conscious

1. **Complete required security training:** all staff members should be required security training as part of their joining process and at regular intervals. Re of current threats and know how to protect company data. Training covers password management best practices, secure handling of sensitive data, in

2. **Follow security procedures and report problems:** employees should adhe procedures. This includes following password policies, locking computers using company-approved software. Staff should immediately report any sharing passwords), using unauthorised software or system errors or failu problem. Consistent adherence to security protocols minimises vulnerabi

3. **Respond to/report suspicious activity:** employees should recognise and r phishing emails, unexpected login attempts, unusual system behaviour a data. Staff should avoid interacting with suspicious links or attachments a the IT team because quick reporting of suspicious activity enables faster i potential damage.

4. **Maintain security in own workspace/behaviour:** employees should secu workspace by locking screens when away from their desks, securing confi shredders and locked cabinets), following clean desk policies (no sensitive company-approved devices and software only. Remote workers should u ensure their home office environment is free from unauthorised access. P unauthorised access and reduce the risk of data leaks.

Activity C3

At All4One Solutions, several security failures were discovered during a routine IT review. Emma, skipped mandatory cybersecurity training and fell victim to a phishing attack, compromising her Meanwhile, [illegible]d, a software developer, accessed confidential HR files on an unlocked computer report the breach, allowing the incident to go unnoticed. Mark, a marketing associate, ignored m and didn't report the suspicious activity, letting a hacker bypass security measures. Jessica, work left her laptop unattended, and malware was injected into her device via a USB. To make matters passwords without enforcement tools in place, making it easy for hackers to break into accounts unnoticed due to the lack of a proper lockout policy.

Outline the key failings of staff responsibilities at All4One.

Key elements of effective staff IT security training

By implementing a comprehensive and engaging staff IT security training prog significantly reduce their risk of cyberattacks and create a culture of security a

1. **Leadership/management commitment:** if leadership must recognise cyb investment, they will allocate sufficient budget, staffing, and the necessar This includes allocating time for all staff to train and ensuring that the IT s create and deliver training. Leadership can start by clearly communicatin and how it impacts the organisation's overall success in addition to makin prioritised activity.

2. **Flexibility of training programme:** training should be accessible to all em technical expertise, location, time zone or work schedule. This can be ac training formats (online modules, in-person workshops, webinars). Traini training content is customised to specific roles and responsibilities of diff example, finance personnel may need specialised training on phishing an may need training on secure coding practices.

3. **Range of training resources/learning styles:** utilise a variety of training m and cater to different learning styles. Ideas for this are interactive online simulations, in-person workshops with hands-on exercises, short, engagin simulations to test employees' awareness and gamified training. It is also examples and case studies to illustrate potential threats and demonstrate

4. **Progress tracking:** in any area of business just asking for things to be don monitoring is needed by implementing mechanisms to track employee pa assessments and simulations can be used to evaluate knowledge and skill rates, quiz scores, and the number of reported phishing attempts. Repor where employees may need additional support.

5. **Incentives rather than punishment:** focus on positive reinforcement and demonstrate good security practices. Offer incentives such as certificates company newsletters or meetings, and small gifts or rewards. When emp constructive feedback and additional training rather than resorting to pu environment where employees feel safe to report security issues.

6. **Provide ongoing training:**
   - Reinforcement and updates: cyber security threats are constantly ev Regularly reinforce key security concepts and provide updates on ne regular training is often better than infrequent long training.
   - New threat awareness: conduct training sessions to address emergi techniques or ransomware variants. Provide regular security bulleti
   - Annual refresher: conduct a yearly review of security policies and pr

Activity C4

Imagine that the IT students studying cyber security are offering their services to parents wh brief suggestion, under the six headings above, that you could present to a parent running a employees, outlining what you suggest they would put together for their staff IT security trai

Security audits and their application to check compliance aga

A security audit is a systematic evaluation of an organisation's security structu policies, and practices. Its primary goal is to determine whether there are vuln from internal or external threats, either deliberate or accidental. Part of the a organisation's security measures comply with internal policies, external regula well as identifying vulnerabilities, audits mitigate risks and ensure continuous i

Audit goals and scope

The **goal** of a security audit is to assess how effective the current security con weaknesses in security practices and check compliance with external standard actionable recommendations for improvement.

The **scope** specifies what will be audited, which could include physical infrastr apps, storage and databases including encryption and access controls, process with industry standards (e.g. ISO 27001) and legal frameworks (e.g. GDPR).

Identifying problems, gaps, and weaknesses

Methods used may include penetration testing, reviewing configurations and s event logs, and comparing current policies with industry standards. During th to detect:

- *Vulnerabilities:* outdated software, misconfigurations, unpatched system
- *Weak authentication:* insecure login methods or lack of multi-factor auth
- *Access control issues:* overprivileged accounts, weak role-based access co
- *Data handling gaps:* improper encryption, insecure data transfer/storage.
- *Incident response gaps:* lack of proper logging, monitoring, and response

Checking against internal policies

Auditors review the organisation's internal security policies to ensure:

- *Consistency and completeness:* are all necessary security measures define
- *Enforcement:* are the policies actively followed in practice?
- *Documentation:* are the policies well-documented, accessible, and regula
- *Employee adherence:* are employees aware of and compliant with policie

Checking against external regulations and laws

Auditors ensure that the organisation complies with industry standards and le PCI DSS (credit card data protection), ISO 27001, and NCSC best practices. The areas of industry, e.g. the NHS DSPT (Data Security and Protection Toolkit) wh healthcare organisations in the UK.

Reporting of results, required improvements, and changes

After the audit, the findings are compiled into a comprehensive report that in

- *Executive summary:* high-level overview of the audit findings.
- *Detailed findings:* specific vulnerabilities, gaps, and non-compliance area
- *Severity assessment:* classification of issues by severity (low, medium, hig
- *Compliance status:* evaluation of how well the organisation adheres to in or regulatory standards.
- *Recommendations:* steps to address identified weaknesses including inve improvements, staffing, policies and security controls, and training.

Once all the findings and recommendations are agreed, a remediation plan sho actionable steps with deadlines to address issues.

Activity C5

An organisation had a professional security audit five years ago. List reasons they need to rev

Backup policy (C1.1.3)

Below is an example of an organisation's security and password procedures. T you need to know about for your exam. There are a few weaknesses in the po by doing the activities below and reviewing your answers against the answers

Happy Cards Backup Policy

Happy Cards charges customers for creating greetings cards. This policy outlines the procedures for backing up critical data at Happy Cards to ensure business continuity and data recovery in the event of data loss, system failure, or cyberattacks, including ransomware. This is crucial for maintaining our online platform, customer data, and design assets.

1. **Selection of Data; critical data is:**
   - Website database including details of all products, customer accounts including purchase history, order and payment information.
   - Website configuration files and website server operating system images.
   - Cloud marketing platform including all customer emails and names.
   - Cloud accounting system including all financial records.
   - Cloud email service and archives.
   - In-house design asset libraries (card designs, templates, graphics), website code and other user files

2. **Backup Methods;** carry out periodic immutable encrypted backups for each of the following:
   - Tape backups of local files, e.g. design assets, user files and website development code base.
   - Hosting provider system image backups for web servers.
   - Cloud-based backup services for website database, and the marketing, accounting and email services.

3. **Backup Type and Frequency**
   - Monthly full backups of all datasets, cloud services and website images at 1am on the 1st of each month.
   - Weekly differential backups of all datasets except the website database on Sundays at noon.
   - Daily incremental backups of the website databases at 2am each morning.

4. **Storage Strategy:**
   - **Off-site Storage:** use a reputable cloud backup service for website and cloud services' remote storage. Take the monthly backup tape off-site to be stored in a manager's home.
   - **Encryption:** all backups are encrypted using AES-256 encryption.
   - **Retention:** daily incremental backups retained for 7 days, weekly differential backups for 4 weeks, monthly off-site backups for 12 months.

5. **Responsibility, A**
   - The IT Ma
     - ○ Impl back
     - ○ Moni succ
     - ○ Perf
     - ○ Ensu
   - All employ loss or bac
   - Manageme backup pol

6. **Backup Testing**
   - Apply auto backup is r
   - Carry out a been succe
   - Document,

7. **Legal/Regulator**
   - Annually, e PCI DSS (if
   - Maintain d and compli to manage

8. **Emergency/Rec**
   - In the eve building b customers suitable al internal se house files know that
   - In the eve up new we import dat
   - In the eve purchase a recover in- tape. Isola if necessar the netwo

Activity C6

Scenario 1: *a gas explosion at 11pm one evening on Thursday 22nd January 2026 destroys the w which will take two years to rebuild. Fortunately, this didn't affect their website or cloud service*

Scenario 2: *on Wednesday 7th January 2026 the accounts team arrived to work to find that the c with ransomware and the supplier goes out of business.*

Scenario 3: *one afternoon the accounts department discover that a virus has infected their comp random. It has only affected files that the accounts department can access and has not affected*

1. What would be the negative impacts of each of these three scenarios, despite them rob each one, split the negative impacts into those which are definite impacts, and those th

2. On the previous page is the Happy Cards backup policy. Propose improvements to the b ac[illegible]e negative impacts you have identified.

Activity C7

How might the **3-2-1 Rule** be incorporated into the Happy Cards backup policy?

Activity C8

The customer decides to classify all their data into one of three categories below. How migh

- Customer data and financial records are classified as 'Highly Sensitive'.
- Design assets and website databases are classified as 'Sensitive'.
- Email archives and general operational data are classified as "General".

Data protection policy to ensure organisational compliance (C

A data protection policy tries to ensure that an organisation remains complia upholds the privacy and security of personal data. The organisation should en associated parties familiarise themselves with and adhere to the policy.

Research Activity – Data Protection Policies

Use the Internet to research what should be covered in a data protection policy and put togethe key points. Also explain why it is needed to ensure organisational compliance.

zz[illegible]29[illegible]-data-protection explains that the DPO's minimum tasks are:

- to inform and advise the controller, its employees, and any associated processors a with the UK GDPR and other relevant data protection laws such as Part 3 of the A
- to monitor compliance with data protection laws, including managing internal da data protection impact assessments; train staff and conduct internal audits; and
- to be the first point of contact for the Information Commissioner and for individua (employees, customers, etc.).

Activity C9 – Quick Quiz

Use the *Example Data Protection Policy* on the next page to answer the following quick quiz q

1. Which of the following is NOT considered personal data under data protection laws?
   A) Email address
   B) Date of birth of an employee
   C) Employee ID num
   D) Age of anonymo

2. According to data protection principles, personal data should be kept for:
   A) As long as convenient
   B) Only as long as necessary
   C) Indefinitely
   D) Until requested

3. What is the main role of a Data Protection Officer (DPO)?
   A) Approving company policies
   B) Overseeing compliance
   C) Handling complai
   D) Managing IT

4. If a company suffers a data breach, it must:
   A) Keep it confidential
   B) Report it
   C) Fire the employe
   D) Delete all data

5. What is the purpose of data minimisation?
   A) Collect as much data as possible
   B) Delete data immediately
   C) Collect only nece
   D) Store duplicate c

6. An employee requests a copy of their personal data. What should the company do?
   A) Ignore the request
   B) Provide the data within the legal time frame
   C) Charge a fee
   D) Ask for a reason

7. An employee loses a USB stick with customer data. What should the company do first?
   A) Fire the employee
   B) Wait to see if [illegible]
   C) Follow breach re
   D) Call the café

8. A [illegible]ng company sends promotional emails without consent. What principle is bei
   A) Purpose limitation
   B) Data minimisation
   C) Lawfulness, fairn
   D) Accuracy

9. Personal data must always be encrypted when stored digitally. **True or False?**

10. A company can share customer data with third parties without consent if it benefits th

Example Data Protection Policy

Introduction

We are committed to ensuring the protection and lawful processing of personal data in compliance with relevant data protection laws and regulations including the UK Data Protection Act 2018 (DPA). This policy outlines our approach to safeguarding personal data, maintaining security, and ensuring accountability across the organisation. For any queries or concerns regarding data protection, contact the Data Protection Officer at **dpo@business.co.uk**

For the purposes of this policy, personal data refers to any information relating to an identifiable individual. This includes but is not limited to:

- Names, addresses, phone numbers, and emails.
- Identification numbers (e.g. employee IDs).
- IP addresses.
- Sensitive data, including medical records or financial information.

***Non-personal data**, such as general statistics or anonymous data, is excluded from this definition.*

1. **Data Protection Officer (DPO)**
   We have appointed a Data Protection Officer (DPO) responsible for overseeing compliance with data protection laws, providing guidance and serving as the primary contact for data protection matters.

2. **Data Protection Principles**
   We are committed to processing data in accordance with our responsibilities under the DPA:
   - Data must be processed lawfully, fairly, and in a transparent manner, ensuring individuals are informed of how their data is used.
   - Data must only be collected for specified, explicit, and legitimate purposes and not further processed for other purposes.
   - The minimum necessary personal data required for the intended purpose should be collected and processed.
   - Personal data must be accurate and kept up to date; inaccurate data must be corrected or deleted without delay.
   - Data must be kept only for as long as necessary for the purposes it was collected, with appropriate retention and disposal policies.
   - Data must be processed securely to protect against unauthorised access, loss, or damage.
   - Compliance with data protection principles must be demonstrated through documentation, policies, and audits.

3. **Protection of Rights and F**
   We are committed to uph
   their personal data, includ
   - Be informed about
   - Access their persona
   - Rectify inaccurate d
   - Erase personal data
   - Restrict or object to
   - Data portability
   - Not be subject to au
     without consent

4. **Staff Training**
   All employees handling pe
   protection training to ens
   requirements, and organis

5. **System Security Procedu**
   To safeguard personal dat
   measures, including:
   - Secure storage of ph
   - Access controls and
   - Encryption and pseu
     and highly sensitive
   - Regular system audi
   - Incident response p

6. **External Contractors, Co**
   All external parties proces
   comply with this policy. C
   include data protection cl
   legal obligations.

7. **Breach Response Procedu**
   In the event of a data brea
   organisation will identify a
   assess the impact on perso
   authorities and affected in
   law, and record the breach

8. **Responsibility and Accou**
   - The DPO ensures po
     monitoring.
   - All staff members m
     data protection con
   - Management is resp
     support for data pro

9. **Policy Review and Update**
   This policy will be reviewe
   necessary to reflect chang

Cyber security incident response policy (C1.1.5)

Contacts

A clear list of internal and external contacts is essential to ensure timely and co
This section should include names, roles, and multiple contact methods. Belo
may be in this list.

Contact Role	Responsibilities in case of cyber secu
Incident Response Team (IRT) leader	Oversees and manages the overall incident response process. Make mitigation and recovery. Coordinates between all teams involved i senior management to provide updates and guidance.
IT Team leader	Leads technical analysis of the incident to identify the cause and im strategies to stop the spread of the incident. Works to restore syste Coordinates with other teams to ensure affected systems are isolat
Senior Management	Approves strategic decisions related to the incident, including reso direction and oversight during high-severity incidents. Makes decis including public relations and legal notifications. Ensures continuit
Legal	Advises on legal implications of the incident, including potential da regulatory reporting requirements. Coordinates with law enforceme manage the legal aspects of communications with customers, partn
Public Relations (PR)	Manages public and media communications to control the narrative public statements or press releases. Coordinates with external agen inquiries. Ensures the messaging is consistent with legal and organi
Human Resources (HR)	Manages any employee-related issues during the incident, such as i Coordinates with legal and senior management on disciplinary actio employees are informed and supported during the recovery process and organisational impact.
Insurance	Assesses the incident's impact on the company's cyber insurance co insurance claims for damages or losses. Works with legal and mana legal liabilities. Ensures that claims are made in a timely and accura

Communication

It is very important to ensure reliable communication during an incident. The
key contacts should be immediately compiled as well as backup details in case
mobile numbers, messaging apps, email addresses.

A conference call facility should be set up to enable real-time communication
secure dial-in with details distributed to all authorised participants and the ca
incident tracking in real time.

Procedures, flowcharts, and checklists

These should be created for:

1. **Initial decisions, triage, and escalation:** the incident's severity should be
response level, which is likely to fall into the following classifications:
    - Low: Minor technical issue, no data exposure → report only
    - Medium: Limited data exposure, localised disruption → some action
    - High: Significant data loss, major business impact → escalate to a ful

2. **Main response, analysis, containment, mitigation, and recovery:** the ai effectively and fully, and to minimise damage.
    1. Analyse the incident including identifying attack vectors (phishing, m scope of affected assets.
    2. Contain the incident by isolating infected systems and changing com
    3. Mitigate the impact, e.g. applying patches or updates and enhancing
    4. Recover systems from backups; but verify system integrity before go signs of recurrence.
3. **Reviewing, reporting, and closing the incident:** ensure proper documen improvement to response to enhance for future incidents:
    1. Review and document: create a detailed incident report. Include the
    2. Report to authorities (if required): this may include regulatory bodie activity is suspected.
    3. Debrief and lessons learned: hold a post-incident review meeting to improvements.
    4. Close the incident: verify all systems are operational and ensure no

Activity C10 – Role Play

You are working for a large organisation which specialises in providing IT security systems. Y all the computers in the organisation are locked with ransomware. The organisation immedi respond to any ransom demands.

In groups of between 3 and 6, each take on the role of someone in the initial triage meeting a response and actions will be. Someone must take the role of IRT Leader.

Disaster recovery policy (C2.6)

This is the general disaster recovery policy for the business, to try to minimise business in the meantime, trying to help the organisation survive. If the disaster i will work in conjunction with the Cyber Security Incident Response Policy.

1. **Purpose and scope**
    - Purpose: this policy outlines the procedures for responding to and r that may affect Happy Cards' operations, data, and systems. It aims t business continuity, and protect the organisation's assets and reputa
    - Scope: this policy applies to all Happy Cards' employees, contractors, access to the organisation's systems and data. It covers all IT infrastru processes, including website operations, customer data, financial sy
2. **Triage, possible events, severity, and response**
    - Triage: when disaster strikes, the leadership will designate personne determine the severity and impact of the event.
    - Possible events, severity and response. In all cases the stakeholders situation and progress. Here are three different types of events:
        - Cyber attack and/or ransomware attack: initiate the Cyber Secu
        - IT-related, e.g. server failure, website failure, database corrupti backups. If a primary server is unrecoverable, failover to secon
        - Natural disaster: may include physical damage to facilities, pote downtime. The primary priority is to ensure personnel safety, a Continuity Plan which might involve relocating to an alternative systems and restoring set-up and data from offsite backups.

3. **Activation procedures: depending on the situation, the appropriate pro**
   - Activate Cyber Security Incident Response Plan in the event of a cybe
   - Activate Disaster Recovery Plan: in the event of a system failure, data l
   - Activate Business Continuity Plan in the event of a major disruption t to operate from its primary location.

4. **Roles and responsibilities**
   - Leadership: responsible for activating the appropriate recovery plan a needed. Also responsible for overseeing communication with the sta
   - IT Manager: responsible for implementing and maintaining the Disas Security Incident Response Plan and reporting to leadership.
   - Individual department managers, e.g. the Accounts Manager is respo accounting data and assisting in the recovery of financial systems an reports if cash flow or profits are affected.
   - All employees are responsible for reporting potential disasters or sys security procedures and for following instructions given during a dis

5. **Contact lists**

   Organisations should have pre-compiled sets of contact lists which are ke someone joins or leaves the organisation or gets a promotion there shoul should be on the list). Key roles and contacts that should be on the list ar the IT manager, members of the cyber security response team and depar contact list should have key IT-based suppliers including any cloud backup email hosting providers.

6. **Monitoring and reporting requirements**
   - Backup monitoring: daily monitoring of backup logs to ensure succes verification of backup integrity.
   - System monitoring: continuous monitoring of critical systems for per Regular security assessments and vulnerability scans.
   - Incident reporting: all disaster recovery incidents must be document A post-incident review will be conducted to identify areas for improv
   - Policy review: review and update the various recovery policies and pl needed.
   - Compliance reports: annual reports to management regarding GDPR backup and recovery procedures.

Activity C11

You are the head of IT for a programming company and receive a call at home to say that there h everything in your basement server room. There is also infrastructure damage so the building wi months at least. You are informed that there will be an emergency meeting the next morning in

Put together a bullet point list of the key suggestions you will make in the meeting, and wha

External services policy (C1.1.7)

An *external services policy* is a set of rules that explains how a company works storage, hardware vendors, or software providers. It aims to ensure these serv the law. The policy covers such things as who can access the services, how the what to do if something goes wrong (e.g. a security breach). It also sets rules fo quickly problems should be fixed and who to contact if issues aren't solved. Ov information safe and ensures outside services are held responsible for their pa

Extract from an Example External Services Policy

Key internal and supplier contacts are emailed to key personnel on the 1st of every month.

Authorisation and Access Control

- Users must use MFA to access the cloud email platform. Passwords must meet the organisation's complexity and rotation requirements.
- Only IT admins can modify email configurations and permissions. User accounts must be assigned least privilege access to minimise risk.
- Inactive or terminated user accounts will be deactivated within 24 hours. Regular access reviews will be conducted every six months.

Acceptable Use

- The platform is strictly for business communication and related activities. Users may send and receive work-related files (following data protection rules). Sending personal, offensive, or inappropriate content is forbidden. Sharing sensitive data with unauthorised recipients is strictly prohibited.

Data Protection

- Encrypt all emails in transit and at rest to prevent unauthorised access. Sensitive information (e.g. financial data) must be encrypted using end-to-end encryption tools.
- Retain emails for 5 years, in compliance with legal and business needs. Deleted emails are permanently removed after 30 days.
- The platform performs automatic daily backups. Backup data is stored in multiple locations for disaster recovery.

Service Agreements and Support

- The cloud email provider guarantees 99.9% uptime. The platform will notify the organisation of planned maintenance or downtime at least 48 hours in advance. Issues wi be reported through the IT support helpdesk. Response time to minor issues is within four hours, to major incidents within 1 hour. If unresolved within the agreed time frame, issues are escalated to the cloud provider's senior support team.

Incident Response

- The platform is to be monitored for suspicious activity (e.g. login from unusual locations). Suspicious emails are automatically flagged or quarantined.
- In case of a security breach: isolate affected accounts and restrict access, notify affected users within 24 hours. Report incidents to compliance officers and external authorities (if required). A full review will be conducted after incidents to identify causes and apply fixes.

Compliance and Audits

- The cloud email platform must comply with GDPR and ISO 27001 standards. Annual security audits will be conducted to ensure the platform meets compliance standards.

Responsibilities

- IT team: manage platform security settings. Perform regular access and compliance reviews.
- Employees: follow acceptable use guidelines. Report suspicious emails or activity immediately.
- Cloud provider: ensure service uptime and data protection. Provide technical support as per the SLA.

Cloud services

Cloud services require careful consideration because (a) you have responsibility to ensure that they look after your confidential data, (b) they may be in direct contact with your customers, and (c) they, not you, are in control of their systems. The policy should also outline how your users interact with cloud services.

- *Cloud resources requiring protection:* it is important to identify the critical assets (e.g. customer data, proprietary information) that require protection.
- *Acceptable use:* defines how your employees should behave when using cloud services. For example, it may prohibit them from unauthorised sharing, downloads, or modifications of cloud data. It may outline the use of VPNs and secure connections when accessing cloud services remotely.
- *DPA:* the cloud service will be processing your data so, under GDPR, you will need to have a *DPA (Data Protection Agreement)* with them which is a them which outlines the responsibilities of both parties. You need to che protected; for example, that databases should be encrypted, files containi be encrypted, and communication should be encrypted in transit, includi backup systems should be in place.

Hardware

A hardware section of the policy will outline:

- *Authorised suppliers and contractors:* if the company requires a high level organisations, defence, biotech) then suppliers and contractors may need procedures before they can become an authorised supplier.
- *Service agreements:* as standard hardware will come with a basic warrant consumables then there is likely to already be a basic service level agreem
- *Maintenance and support:* if the business relies on key hardware (e.g. pri support machines in a hospital) then this may be a negotiated agreement call-out, stocks of consumables on site, and penalties if printers have dow will be specified whether parts are included in the cost for repairs, and w

Software

The software section of the policy will contain:

1. *Authorised suppliers and contractors:* as with hardware, the higher the level of security required, the more detailed this section will be. Off-the-shelf software requires regular security assessments. Bespoke software development requires thorough vetting of contractors.
2. *Service agreements:* the organisation needs to carefully read and understand the service agreement and any terms and conditions. They will be looking out for details of patch management, update frequency, and security fixes. They also need to ensure that software providers adhere to the organisation's security policies.
3. *Licensing:* this section is to ensure compliance with software licences and usage terms. To do this the organisation outlines how it will track licence usage to prevent violations or overuse, and procedures for renewing or terminating licences.
4. *Software support:* specifies support levels offered by the vendor (e.g. basic, premium) and response times and how problems will be resolved.

Support

Support has been mentioned briefly on the previous page within the hardwar bit more detail about what to look for in a support contract.

1. *Service time and availability* defines the operational hours for external se support availability or standard business hours. It may include provision f
2. *Response time – report to support starting* defines expected response tim outlines the process, e.g. ticketing systems, phone or email support.
3. *Troubleshooting and solution time* specifies timelines for diagnosing and r between minor, moderate and critical issues. May include provisions for permanent solution.
4. *Escalation procedures* define what happens when issues are not resolved agreed time frames. Who are the contact points for higher-level support? which can be initiated? Are there penalties or opt-out clauses if a satisfac

Activity C12

Your organisation is intending to move from a bespoke in-house email service to either Micro systems. Someone else is researching the technical features and the pros and cons of each se your organisation's *External Services Policy* to each one.

Create a bullet point list of the things you will have to find out to apply the policy.

AAQ BTEC National IT

Cyber Security and Incident M

Content Area D: Forensic p

Contents

D1 Forensic collection of e

Digital forensics uncovers, analyses and can be used to reconstruct criminal ac exciting as the forensics you see in crime dramas such as *CSI* and *Silent Witnes* and methodologies. Digital forensics are just as deadly serious and urgent wh hospitals which have been hacked, and in cyber warfare in Ukraine and Russia.

Students should apply their knowledge and understanding of the methods fo following a security incident

D1.1 Forensics on devices – servers, PCs and mobile

Meeting requirements for forensics (D1.1.1)

Confiscation of devices

When investigators **seize (take) devices** such as servers, computers, or phone ensure that any evidence they take will be admissible in court. The evidence n scrutiny of the defence lawyers.

Investigators need to **be prepared** for different devices (e.g. laptops, servers, p very old or uncommon models, custom built or from other countries. They sh store each type of device without damaging data.

Key points they need to consider are:

- If the device is locked, investigators will try to get the **PIN, password, or b** from the suspect. If they can't get the password they may use forensic to
- They need to have the **correct chargers and cables** to keep the devices cha **cables** to access data.
- They need to **retain current power state**, if possible, i.e. if the device is al to keep it that way. This is because some data might be only accessible w as running programs or temporary files.
- If the device could be remotely accessed or wiped, it must be **cut off from t** **are on**. Network cables should be unplugged, and they need to know how communicating, or to turn on *airplane mode* which disconnects all wireless
- They need to carry **appropriate packaging** to avoid damage. If they want t need special *Faraday bags* to block communication signals. They should k they found with the device.
- The **document chain of custody** is very important if it goes to court to de tampered with. A chain of custody is a record of who handled the eviden date of seizure, the names of the investigators handling the device and a
- Investigators need **legal authority**, e.g. a search warrant, to confiscate an permission, the evidence could be thrown out of court.

Taking an image of the system

Before analysing a device, investigators make a *forensic image* (an exact copy the original evidence from being altered. Investigators can then work on the c intact. It's done by using forensic tools to make a *bit-by-bit copy* of the device'

Using a forensic analysis tool

Forensic tools are special programs used to analyse data without changing it. A used to create and view the image, and then tools such as *autopsy* can be used Sophisticated tools such as *EnCase* can be used for network analysis.

Reviewing files and settings

Investigators look through the files, folders, and system settings to find clues. Fo

- Documents and images to see if anything suspicious or illegal is saved.
- Hidden files or encrypted folders which might hold concealed evidence.
- System settings to check for tampering or suspicious modifications.

Reviewing system logs

System logs are records of what the device did, e.g. which programs have bee and error logs. They can help to construct a timeline of what happened when malware was introduced, and its effects, including:

- *Login history:* shows who accessed the device; this means you can consul compare behaviour or perhaps identify the person who introduced the ma
- *File access logs:* lists recently opened, edited, or deleted files, which may the malware.
- *Internet history:* displays websites visited or downloads made which coul

Reviewing user activity

Investigators look at user behaviour on the device. For example, they might c find any suspicious communication, or social media activity to see their posts, will also see which files have been modified when the user was logged on to s (legitimate or otherwise) and also to check if the user tried to delete or alter e

Malware analysis and alerts

If the device is infected with *malware*, investigators examine it carefully. If th will then analyse its behaviour to see what it does, e.g. replicate itself, send e access, steal or damage data, or spy on the users.

Activity D1

1. What must investigators ensure when seizing devices?
   A) Devices are [illegible] C) Devic
   B) Devices are new models D) Eviden
2. What should investigators do if a device is locked?
   A) Try to get the PIN, password, or biometric info from the suspect C) Turn o
   B) Connect the device to the Internet D) Discar
3. Why is it important to retain the current power state of a device for forensic investigatio
   A) To access data that will be lost when the device is turned off C) To pre
   B) To save battery life D) To ens
4. What is the purpose of a chain of custody?
   A) To track the battery life of the device C) To rec
   B) To prove evidence wasn't tampered with D) To list
5. What is a forensic image?
   A) Photograph of the device C) Screen
   B) List of the device's files D) Exact c
6. What might investigators look for in system logs?
   A) Battery usage C) Device
   B) Login history, file access logs, and Internet history D) User m

The challenges of live forensics (D1.1.2)

Live forensics, the practice of acquiring and analysing digital evidence from a r
set of challenges compared to analysing powered-off systems. Some of the ke

Challenge	Description	
Changing data in situ	A running system is constantly changing. Processes are running, files are being accessed, and network connections are being made. In addition, any interaction with the system, even for forensic purposes, is likely to alter the evidence.	Use specialised fore without changing an methods to view file so you can show wh on the system.
Recovering corrupted data and preventing further corruption	Malware or system errors can corrupt data. The malware can continue running while you carry out live analysis, and some actions (e.g. running programs) could restart the malware.	Use professional sof fast and so give the that focus on data r techniques that min
Capturing data in active memory (RAM)	RAM is volatile and requires specialised tools; the capture itself can alter the data.	Use dedicated RAM the RAM without ch memory analysis on
Capturing remote data	Data can be stored on remote servers, cloud services, or other devices, anywhere in the world. Cloud services may restrict your access, or they may wipe the server when you tell them about the malware on their system.	Obtain legal authori (e.g. SSH, HTTPS) to devices. The cloud can take a snapshot agree how you will
Avoid losing temporary files	Operating systems and applications create numerous temporary files that might contain evidence. These files are often deleted when the system is shut down or when applications are closed.	Identify and preserv file recovery tools. file activity. Use to that is often delete include the tempora

The *ACPO (Association of Chief Police Officers)* has published a **Good Practice Guide for Digi**
interesting information which is relevant to this course. Here are a few extracts:

> *'By profiling the footprint of trusted forensic tools used to gather volatile data, the digital foren impact of using such tools and can explain any artefacts left by the tools. … Regardless of the capturing the contents of RAM, the volatile memory.'*
>
> *'If other tools are used before the contents of the RAM are stored, it is very likely that running t of the RAM .'*
>
> *'The tools used to capture this volatile information are generally run from removable media lik floppy disk. A USB stick is generally most convenient, as the output of the tools can be written t to the original drive should be avoided whenever possible, as this changes the contents of the h evidence. Again, principle 2 does allow the investigator to do this, it is a conscious decision wil written down.'*
>
> *'And, it should be noted that in live forensics it is not always possible to know upfront which ap Whichever method is chosen, remember to take meticulous notes.'*

Activity

1. Why is it challenging to change data in situ on a running system?
2. Why is meticulous documentation important when interacting with a system for forensi
3. Why is live analysis risky when dealing with malware?
4. What should be obtained before capturing remote data?
5. Why is it important to identify and preserve temporary files quickly?

Network forensics (D1.1.3)

Network forensics are more complicated than device forensics in that you can' away for analysis, or take a snapshot. Also, networks may be shared between or to public networks. It is more complicated than signing a DPA and policy agr and permissions may need to be sought from supervisory or legal bodies befo permission you are likely to need to present justification and evidence of why network, possibly to a court. Unauthorised scanning could be considered hackin

Once you have written permission you can begin testing. But the network is li your methodology must not disrupt the live system. Steps you can take to hel

1. Use non-invasive, low-impact tools to avoid adding too much load to the r
2. Use passive tools where possible which monitor the network without dire
3. Active tools test by sending data across the network or sending probing r active scans during low-traffic hours to reduce the chance of overloading

Investigate individual network hardware in the following ways to look for mal

- Suspicious traffic patterns such as constant outbound communication to communication to non-UK locations.
- Flagged malware files in antivirus software.

Device/Component	Why It Matters	
❶ **hardware firewalls** sitting between Internet routers and networks; ❷ **software firewalls** built into routers, servers and computers)	Firewalls control incoming and outgoing traffic; they only allow traffic through that meets the rules. They detect suspicious connections and blocks threats and keep a log of failed and successful connections.	Traffic logs unexpected rules and po misconfigura
Switches	Directs internal network traffic to devices via other switches, routers and WAPs. Logs can reveal communication patterns between devices.	Check port port scannin spoofed or
Routers	Connects the internal network to the Internet. Stores logs of incoming/outgoing traffic.	Traffic logs patterns. Ch suspicious r traffic which firewall.
Wireless Access Points (WAPs)	Provides wireless network access to devices. Logs reveal device connections and signal activity.	Analyse the suspicious d or WPA2. Ch are strong.
Client or Server Logs	These log user and system activity, so can be a key source of evidence for detecting breaches.	Check for fa force attack unauthorise service cras

If malware is identified it needs to be analysed to understand it, which can hel likely to have spread to new locations, whether it has released any data to thi any way *backdoors* for third parties to access the network, whether it has into the network.

Always use *sandboxing* when analysing malware, which means running the m environment to see how it behaves and what files and devices it interacts wit

Documenting the scene (D1.1.4)

Prior planning

Before the search and seizure of digital evidence from a scene, a planning mee charge of the investigation and personnel of other specialities who will be inclu you may be investigating a cybercrime, or a crime such as online fraud where t central element, or criminals involved in the drugs trade where communicatio part of the evidence but the initial action at the crime scene will be to arrest a and samples.

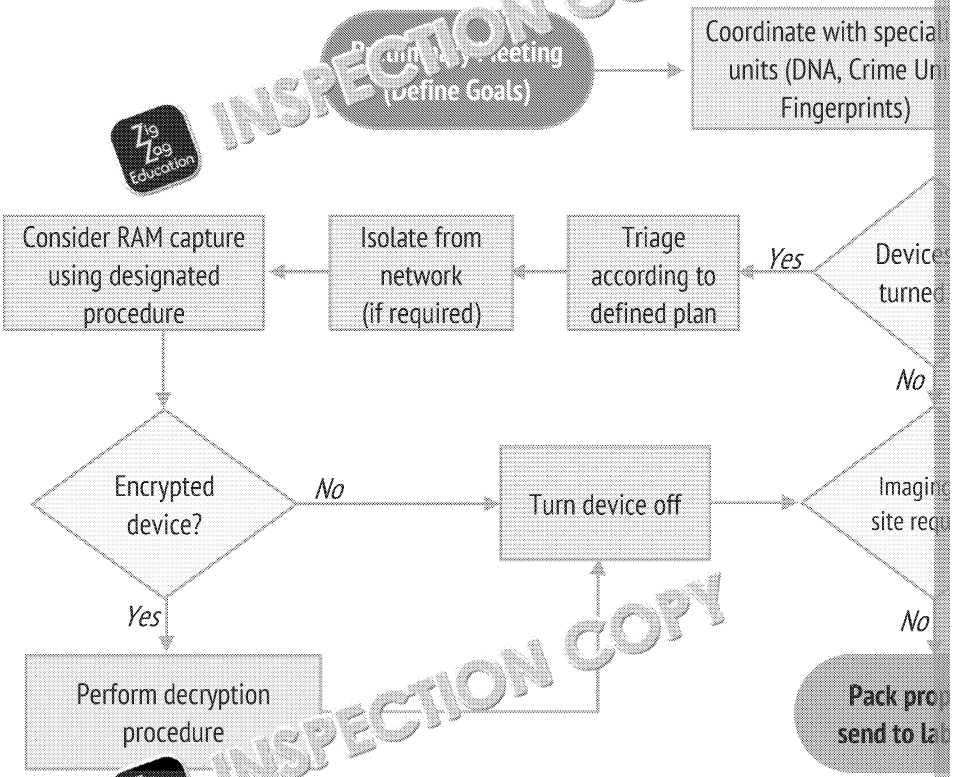
Also, planning is needed because there may be multiple locations where crimi sometimes in a different jurisdiction where additional legal authorisation is re

Key planning considerations in terms of the digital forensics:

- Permissions for the seizure, and for any additional access to passwords fo and cloud services.
- Which devices need to be analysed on-site (for example, before power is off-site before analysis starts.

Equipment also needs to be planned and checked. It will include laptops with hardware, spare cables, write blockers, blank hard drives and other media to n cutters, cameras and video cameras, evidence boxes, bags and tags, markers a magnifying glasses and masks.

Personnel involved in the operation should wear appropriate protective clothi contaminate the scene in any way. Even if the primary focus is the forensic in will be a search for fingerprints and DNA.


Preliminary Meeting (Define Goals)
Coordinate with speciali units (DNA, Crime Uni Fingerprints)
Device turned
Yes
Triage according to defined plan
Isolate from network (if required)
Consider RAM capture using designated procedure
No
Encrypted device?
No
Turn device off
Imagin site requ
Yes
Perform decryption procedure
No
Pack pro send to la

Flowchart adapted from the Interpol Guidance fl

Securing the scene

The aim is to prevent the loss, alteration or destruction of possible evidence. S

1. Stop anyone at the scene from using mobile phones, computers or other damaging it. Ask them for their PINs and passwords to access their devic this jurisdiction).
2. Remove and forbid unauthorised personnel from accessing the scene.
3. Remove any wired network devices and disable wireless communications
4. Tag equipment as either being available to take away, or for investigation This investigation may start immediately while another member of your t other devices.

Excellent, very detailed guidance for securing the scene can be found in th **zzed.uk/[illegible] guidelines**. It also includes details of specific tools useful for f

Plans, photos and diagrams of the scene

The crime scene should be accurately recorded before any evidence recovery starts (except where there is risk of losing evidence, e.g. if there is bad weather in which case markers should be used to indicate where evidence has been recovered from).

Ho
an
-
-
-
-

The methods to document the scene can include:

- Still photography (wide-angle shots of rooms and close-ups of devices and screens)
- Video photography
- 360° imaging
- Drawing plan
- Contemporaneous notes

How
- T d
- B
- S
- S
- S
- L
- S
- C n

If it is important to, for example, unplug network or Internet cables before properly documenting the scene, it may be best to use a live video camera to document the unplugging of the cables.

Contemporaneous notes

These are notes made at the time or shortly after an event occurs. Therefore, they are the best recollection of what you witnessed. They should include the date, time and location, and details such as:

- Environmental details: was it hot, cold, damp? Were computers on or off? Was there any noise or music playing?
- What were the names and roles and contact information of anyone on-site, and what did they say?
- What was displayed on screens when you arrived? Was there any literatu
- What could you determine visually about the makes, models and serial n
- What were your actions and the actions of others in the team?

Witness statements

Whether the scene is from a police raid or an office of an organisation that ha can be invaluable. Witnesses who are suspects may be interviewed under poli Witnesses in the building may be taken out to a neutral office away from the c Other witnesses may include security staff or third parties, e.g. cloud software off-site technical support.

Witnesses may be asked questions such as:

- When did you first notice the issue?
- What unusual activity did you observe, either before or after you noticed the issue?
- What action did you take, e.g. to run antivirus software or reboot the device?
- Who did you tell, and what did they say or do?
- Have you shared any passwords, or clicked on any email links, or noticed any USB drives plugged in or seen anyone unfamiliar in the area?

Elem

Activity D3

You are the chief forensics investigator and have arrived at a scene where five laptops, three t found. The laptops are all on with some sort of program running; the tablets and mobiles are and have been apprehended.

You have a team of five. List your role and draw up a list of tasks for each team member to do

D2 Systematic forensic analysis of a

Students should apply their knowledge and understanding of the requirements a

D2.1 Requirements for maintaining an accurate re or as soon after the incident as possible

Activity D4

Follow the story below using a highlighter to carefully match each relevant point in the story you need to know from the specification.

My statement

I was reviewing the report of a recent cyber security incident when my work m frantic, from one of our clients. 'Something's wrong,' he stammered, his voice t strange characters, code, just... appeared on all the accounts department scre We've been hacked, I'm sure of it.'

My stomach clenched as it always does when I need to kick into urgent action real time. 'I'm on my way,' I said, grabbing my go-bag. Arriving at the compa atmosphere was thick with tension. Mr. Henderson, his face pale, met me at t and have disconnected everything from the network and have turned off half o on,' he explained. Every minute counted. The malware, or whoever was behin lying dormant, waiting to strike. But this wasn't just a technical problem. This v balance speed with meticulous procedure, ensuring every step was documente was ticking, and the digital ghost was still out there somewhere.

My personal camerawoman had arrived just before me. She filmed me arrivin and followed me through the door into the building. I had to explain to the security guards that she was with me to document all actions including any items that I seize as evidence for the police. She had also created some gre video snippets for my marketing YouTube channel, but I didn't mention that!

Before even touching a keyboard, I retrieved a pre-prepared document from m bag. Mr. Henderson, the most senior person present, looked surprised that I wasn't going straight to an infected computer. 'This,' I said, holding out the document, 'is crucial. It's an authorisation. It grants me, as your representative full administrative access to your systems and files. Without it, I can't effectively investigate. It's also a formal acknowledgment of my obligations.'

I pointed to the lines requiring his signature. 'This confirms your consent. And h face him, 'is my signature, binding me to your privacy policy and the UK GDPR processor, handling sensitive information, and I want to assure you that I take seriously.'

Mr. Henderson scanned the document, his brow furrowed. 'GDPR? Is that reall 'Absolutely,' I replied, my tone firm but calm. 'Even in a crisis, we can't compro obligations. Protecting your data is paramount. This document ensures everyt accountable.' He said, 'oh yes of course' and signed the document. I signed as

With the authorisation secured, the real work began. The delicate balance between preserving evidence and preventing further damage was a tightrope walk. 'We need to isolate the affected area,' I said, addressing Mr. Henderson and a few anxious-looking staff members. 'But we can't just power everything down.' 'But the malware is still running?' someone queried. 'Malware often resides in volatile memory,' I explained. 'Turning off the power erases that data, wiping away crucial clues. But we also can't risk it spreading further or deleting more files.' As they looked to me, I explained further:

- *'First,' I said, gesturing towards the network cables snaking across the floor, 'we need to ensure complete isolation. I need to double-check every device, including printers, and disconnect any network cables leading out of this department.' I began tracing cables, including to and from the department switch, ensuring nothing was connected to the wider network or the Internet. Any wireless devices should have their Wi-Fi and Bluetooth turned off and put into airplane mode if they have it.*
- *'Secondly,' I continued, turning to Mr. Henderson, 'I need you to confirm that no one who was here this morning has taken any electronic devices – mobiles, tablets, laptops – out of the office. If they have, we need them back, immediately. They could be carriers.'*
- *'Thirdly,' I added, 'I need all mobile phones belonging to staff present to be placed in a box. We'll examine them later. It's a precaution.'*
- *'Fourthly, I need all of your staff either here, or in a room nearby. I may h some of them may be able to help me with the investigation.'*
- *'Fifthly, please put the entire company on high alert. Anyone who sees an needs to report it to me immediately.'*
- *'Sixthly,' I said, a sense of urgency creeping into my voice, 'if any members office today, on holiday or otherwise, we need to recall their devices – lapt turn them on. We need to preserve their current state.'*
- *'Finally,' I said, looking directly at Mr. Henderson, 'I need you to contact y encryption keys or certificates that might be used to access encrypted files seen anything.'*

Mr. Henderson nodded, his face grim. 'I'll get right on it.' The room buzzed wit and a desperate hope that we could contain the damage.

Creation of visual evidence of findings (D2.1.4)

The immediate priority was clear: secure the digital scene and document everything. 'Right,' I said, addressing the room, my voice firm and focused. 'We need to treat this like a crime scene. Every action, every image, must be preserved.'

'My first step is to photograph every screen that's currently displaying anything,' I stated, pulling out my digital camera. 'This captures the current state of the compromised systems. It's vital for establishing a baseline.' I systematically moved from computer to computer, taking high-resolution photos of each screen, ensuring the images were clear and detailed.

'Has anyone taken any photos or videos of the screens before I arrived?' I asked. 'Anything at all, even if you think it's insignificant.'
A few hesitant hands went up. 'I took a picture with my phone,' one of the sta slightly blurry image. 'Just when it first started happening.' 'Excellent,' I said, phone to be placed in the evidence box after the image was copied. 'Every det

'Is there any video surveillance footage that might have captured what was o that might have shown the code appearing?' Mr. Henderson looked thoughtf hallway, but I'm not sure if they'd capture the screens.' 'We need to check,' I s worth investigating.'

I then turned my attention to my own equipment. I had brought a set of video cameras, each carefully selected for its forensic capabilities. 'These cameras,' I announced, holding one up, 'are set up with specific parameters. I've noted the make, model, and serial number of each one. The metadata and location settings are preset, ensuring accuracy and preventing any later challenges in court.' I checked the date and time on each camera, ensuring they were synchronised.

'I'm going to set up a camera pointing at each active screen,' I explained. 'This will capture both the ongoing activity of the malware and my own keystrokes. It's vital to demonstrate that I'm not altering evidence or creating false information.' I began positioning the cameras, carefully framing each screen and ensuring a clear view of the keyboard. The cameras began to record, thei red lights blinking steadily, documenting every digital flicker and keystroke. The digital crime scene was being meticulously captured, every action recorde for potential legal scrutiny.

'Now,' I said, turning to the task of capturing a snapshot of the infected systems, 'we need to create forensic images of the affected drives. This is critical for analysis and preservation of evidence.'

I began with one of the powered-down computers, ensuring it was completely off and no longer being altered by the malware. 'We'll start with this one,' I explained, 'because it's in a static state. We need to preserve that.'

Carefully, I removed the hard drive, and any other storage devices. 'I'll be usin my FTK Imager,' I stated, holding up my laptop. 'It's a trusted forensic tool for creating bit-by-bit copies of storage media. We'll create two identical images of each drive.'

'Why two?' someone asked. 'One for evidence,' I replied, 'which will be seale and stored securely, and one for analysis. This ensures we have a pristine cop for court, and a working copy for examination.'

'But how will the court know that it's definitely the same hard drive?' someon piped up. 'Excellent question! Firstly, my FTK Imager generates a unique checksum from the data on the original hard drive which it saves to a file and also print a copy. Then I do the same for the pristine copy. The printouts and drives go in the number evidence folders and are sealed in full view of the vide recorder and then will be taken to the evidence locker in the police.'

I meticulously imaged each drive, including hard drives, any server hard drives that may contain virtual machines, any USB drives found, and even the SIM cards from the mobile devices. I even took a copy of the BIOS; in case the malware had altered anything at a low level. In addition, I put a request in for any backup tapes made in the last week to be locked (sliding the physical tab that stops them being overwritten) in case it was zero-day malware that was already on the system before the last backup.

Each original device was placed into a static-proof evidence bag, sealed, and clearly labelled. The analysis copy was placed in a separate, equally well-labelled bag.

'Unfortunately,' I said, 'the RAM from these powered-down machines is lost. Volatile memory disappears when the power is cut. But we can still get a RAM capture from one of the active machines.'

I moved to a powered-on computer, aware of the delicate dance between capturing data and potentially altering it. 'This will be a live capture,' I explained. 'The data may change as we copy it, but it's crucial to get a snapshot of the RAM while it's still active. We'll use a specialised tool to create a flash copy of the RAM.' I carefully initiated the RAM capture, knowing this data could hold vital clues to the malware's behaviour.

'Ideally,' I continued, 'we'd want a complete image of the entire machine, but with the boot disabled. That way, we can inspect it without running the malware. We can create a full disk image, and then, using the imaging software, ensure that the boot sector is not copied or that the boot sector is edited to not boot the OS. This allows us to mount the drive on an analysis machine, and see the file system, without running the malware.'

'One crucial question,' I said, pausing my analysis, 'does the accounts department utilise any virtual disks or virtual machines?'
Mr. Hend[illegible] looked perplexed. 'Virtual... machines? I don't think so. We jus have our regular computers and the server.'
'That's a relief,' I admitted, a genuine sense of ease washing over me. 'Virtual machines add another layer of complication.' 'Why?' someone asked.

'Imagine,' I began, 'a virtual machine is like a computer within a computer. It has its own operating system, its own file system, its own memory. If the malware had infected a virtual machine, we'd have to image and analyse not just the physical hard drives, but also the virtual disk images, which can be massive. 'Essentially,' I concluded, 'although there may be some helpful snapshot backups, it is another layer of complexity. The fact that you're using physical machines simplifies the process considerably.'

Ret
(D2

Starting a cold analysis

It was past noon, the infected computers still had code scrolling down their scr start the investigation, I plugged my laptop into my own encrypted 5G SIM rou without going through the infected network. I downloaded a fresh copy of the infected computers, as well as the bios for their specifications, and copies of th This enabled me to compare their infected version with a new version. Of cour my cyber software could analyse which files are different and advise whether t changed.   This includes the databases used by the software and the registry k

In addition, my cyber toolkit was running the latest antivirus software from multiple suppliers to run through all files in all the folders on all the drives to look for any hidden malware, including system files, software files, user data files, temporary files, downloads and even deleted files in the user's recycle bi Even if it found some, it is not necessarily the malware that is currently causin the problem.

Starting a hot analysis

While my analysis was running, I turned my mind to the infected machines tha were still running. 'Now,' I announced, setting up another analysis workstation, 'we need to delve into the data. We're looking for patterns, anomalies, anything that will shed light on what happened.'

'I'll be focusing on process and sub-process output and activity that is happeni at the moment,' I explained, opening my forensic analysis software. 'This invol at the time of the incident, their parent-child relationships, and any unusual a We're looking for rogue processes, hidden services, anything that doesn't belo

I began parsing the RAM image, searching for evidence of malicious code injec and any unusual resource consumption.

'We're also looking at network information,' I continued, switching to a netwo addresses, user logins – these can reveal communication with external servers the malware took.' I meticulously examined the network traffic logs, searching malicious IP addresses, unusual port activity, and any signs of data exfiltration

'User login data is also critical,' I explained, scrolling through authentication logs. 'We need to see who was logged in when the incident occurred, and if there were any unauthorised logins. This can help us identify potential points o entry and compromised accounts.' 'For example,' I said, pointing to a series of log entries on the screen, 'look at these login attempts. Multiple failed logins from an unusual IP address, followed by a successful login with administrativ privileges. This suggests a brute-force attack, although this happens all the time so it may not be related.'

I then turned my attention to the hard drive images. 'We'll also be examining file system activity,' I said, opening a file analysis tool. 'Looking for recently modified files, hidden files, and any suspicious file creation or deletion. We're searching for the malware itself, its configuration files, and any other traces it might have left behind.'

'We will also look at event logs, and the registry. These are the windows operating system's record of what has happened, and the configuration of the machine. The registry often holds keys and values that show what programs have been run, and what network connections have been made.'

I ran some commands to stop all the services running on the computer, which v giving me a chance to investigate it. I know that would mean that this particul used in [illegible], but I needed to open files, affecting the time stamp, a down th[illegible]e of the malware.

'The goal is to reconstruct the timeline of the attack,' I explained. 'To understa system, what it did, and what data it compromised. Every piece of informatio potential clue.'

'But I've heard that the malware will delete its original file and will attempt to *said one clearly knowledgeable member of the team. 'That's right', I said, 'but* *network activity we can delve into the system's hidden corners. System-genera* *that attackers overlook.'*

'Take the System Volume Information folder for example,' I explained, navigati *folder stores system restore points, volume shadow copies, and other critical sy* *files, previous system states, and even remnants of malware activity.'*

I carefully examined the volume shadow copies, looking for evidence of file modifications or deletions that might have occurred before the incident. 'Shadow copies are snapshots of the file system,' I explained. 'They can show us what files looked like at different points in time.'

'Next, we'll analyse the hibernation files,' I continued. 'These files store the contents of RAM when a system enters hibernation. They can contain sensitive information, including passwords, encryption keys, and even fragments of running malware.' I loaded the hibernation file into a specialised memory analysis tool, searching for any unusual patterns or anomalies.

'Crash dumps are another valuable source of information,' I said. 'These files a *and they can reveal the state of the system at the time of the crash. They can h* *crash and potentially reveal the malware's behaviour.'*

'We'll also examine the page file,' I stated. 'This file is used by the operating sys *RAM. Like hibernation files, it can contain fragments of sensitive information.'* *I ran a specialised tool to analyse the page file, looking for any traces of malicio* *synchronisation files; these files are used by cloud storage services and other a* *between devices. They can reveal files that were recently accessed or modified* *was exfiltrated.'*

I examined the synchronisation logs and files, searching for any unusual activit *generated files often hold the key to understanding the full scope of the attack* *activities, deleted files, and even the attacker's tools and techniques.' 'It is like* *system itself leaves behind, often without the user knowing that they are there*

Hours passed and I worked into the night, drawing together the evidence. I tra *stick that someone had plugged into a computer. The USB had some meta da* *called 'Dmitri Popov' had previously saved a document on the USB stick; the vi* *I discovered this.*

Over the day my support team had arrived and now were taking over so I coul *in my chair with a contented smile on my face – I had earnt a lot of money tod* *on the dark web to plug in the USB stick with my code when he delivered a pa* *probably been arrested but it couldn't be tracked back to me as I used an encry*

Prologue

The cold steel of handcuffs bit into my wrists, the metallic click echoing the fin *lights painted the whole fiasco. Detectives swarmed around the room colle* *own tools, instruments of digital truth, were now being used against me. '* *commit cybercrime, unauthorised access to computer systems, and data theft.'* *broken an encryption used on a dark web marketplace and had recorded my c*

Ensuring the evidence is relevant and not a false positive (D2.

It can be very frustrating when a legitimate email from a friend goes into your positive, i.e. an email that has falsely been flagged as positive for spam. In the software used to find and identify malware can identify false positives. Aside f undermine the case in court.

Defining file signatures, search criteria, etc.

When looking for malware there are several things that may flag up a file for fur

- a malware *file signature* is like a 'fingerprint' of a malicious program; it ca sequence of bytes, or a hash value that is unique to that specific malware
- malware detectors will have a number of *search criteria* to look forward a types, filenames or keywords inside files
- the *metadata* in a file may match those from known malware, or may be on the system

Those attempting to hack or who create malware understand how anti-malwa new ways to work around it to hide their malware.

Known/estimated error rates of tools and target data types

Forensic tools and algorithms are tested on known data to give their accuracy error rate helps determine how reliable the evidence is and how important it i manual review:

- *False positive* rate: the percentage of irrelevant data mistakenly flagged a
- *False negative* rate: the percentage of known actual evidence that is miss

Feedback of false positive data to improve detection method and algorithms

When false positives are detected, they should be used to improve the system This might be a case of:

- Updating an algorithm to change how it is detecting malware.
- Adding and removing key search words.
- Where systems give a probability of containing malware the *sensitivity thr*
- Machine learning or AI tools can be given the false positives as feedback t

Regularly updating the tool with feedback data improves its reliability and pre more likely to pick up new variants of malware.

Alert fatigue for high false positive rates

Alert fatigue occurs when investigators receive too many *false positives*. As w this can mean that analysts may start missing or ignoring alerts and real threa the system needs to be analysed and a *mitigation strategy* put in place, which

- Lower alert thresholds if still very likely to pick up issues.
- Group and prioritise alerts by severity or confidence level to focus on the
- Automate initial filtering, e.g. use AI to dismiss low-confidence alerts.

Manual review of all positives to filter obvious false positives

Even when using automated tools, all flagged evidence should undergo *manua* For example, if a forensic tool flags a common Windows system file as suspicio whether or not it is legitimate.

Further investigation and check of filtered positives

Once false positives are removed, the focus is on the remaining positives to in their validity before they can be confirmed as a definite lead. Questions to ask

- Does the context match: do surrounding files, logs, or user activity match
- Is there other evidence supporting or contradicting the flagged item?
- Do other forensic tools confirm the findings?

For example, if a flagged email contains a suspicious link, further investigation destination, analysing related email headers for inconsistencies and checking i known malicious activity.

Activity D5

You are a digital forensics investigator assigned to a case involving suspected malware on a com department has provided you with several flagged files that the anti-malware software identifi are concerned about the high number of false positives and want to ensure that only relevant evi

Outline the steps you would take to support the IT department.

D2.2 Assessing the findings

Provide evidence of a crime and/or an incident (D2.2.1)

Different types of crimes and incidents will require slightly different variations

Type of incident	Key Evidence Types
Criminal offence *(e.g. hacking, fraud, identity theft)*	• Logs and timestamps of unauthorised access or suspicio • Hard drive images (with hash values to show they are t • Evidence of wrongdoing, e.g. malware code samples, or financial records showing fraud. • Witness statements, e.g. observing suspicious activity.
Regulatory breach *(e.g. GDPR, HIPAA, PCI DSS)*	• Proof of unauthorised or improper data access. • Details of when and how the breach was detected and r • Proof/lack of compliance checks and scans. • Copies of correspondence with regulatory bodies. • The effects of the breach, e.g. what personal details we
Civil liability *(e.g. contractual breach or damages)*	• Contracts and SLAs proving contractual obligations. • Evidence of breaches of contract and associated commu • Expert reports, records and calculations of financial los
Internal policy non-compliance *(e.g. violations of company rules)*	• Logs and timestamps of unauthorised access or suspicio • Evidence of showing deviation from security policies. • Internal communications showing disregard for policies. • Evidence from witnesses.
Cyberattack *(e.g. ransomware, phishing, DDoS)*	• Logs showing IP addresses or domains linked to the att • Network logs showing suspicious activity patterns. • Malware evidence. • Forensic hard drive or device images of compromised sy • Ransom demands or fraudulent emails.
Negligence or mismanagement *(e.g. lack of due care)*	• Policies and procedures. • Proof of employee security training (or lack of training). • Incident response demonstrating delayed or ineffective r • Assessment of mismanagement or insufficient security p

For all crimes it will also be key to include the chain of custody (who handled t forensic tools used.

Demonstrate that a system has been externally and/or intern

Unusual traffic

Both inbound and outbound traffic logs may contain thousands of entries fro viewed. Users from different countries and airports and cafés may connect to complex. In some cases, AI might be used to look for patterns and to rule out l

Here are some things to look out for:

- Inbound or outbound traffic that is to or from IP addresses on watch lists, or from IP addresses that are unknown to the organisation (i.e. rule out t mainstream websites)
- Inbound or outbound traffic that is from unexpected or blacklisted locatio organisation doesn't have employees, suppliers or clients in Asia.
- Repeated sustained traffic at a higher rate than normal, even if from mul may be a DoS or DDoS attack.

Unusual login attempts

Examples may include:

- Logins or attempted logins to multiple accounts from the same IP addres
- Logins at unusual hours or from uncommon locations.
- Brute-force attempts or account lockouts for unknown reasons.
- Users with unexplained increased access, or unknown logins appearing o

Unusual DNS requests

Examples may include:

- DNS request to domains that do not exist.
- A higher-than-normal number of DNS queries in a period.

Increase in file or data reads or requests

A spike in the number of files that are being read in a second, or in a minute, o hacker or malware has accessed the network and is viewing lots of files. Simila going through the network, or database record requests may indicate malwar

Unusual port usage

Ports have standard usage, e.g. 22 for SSH, 443 for HTTPS and 110 for POP3 e ports for traffic that doesn't normally go through that port would be a red flag Similarly, using ports that are not on the standard list of ports could indicate a should close any ports that are not needed; therefore, traffic attempting to ac a problem.

Suspicious changes to files or data (including system files and data)

Sometimes users will report that a file has been unexpectedly changed and co code), or a file is trying to run a macro that they didn't create, or that a databa code. These would be suspicious.

Similarly, unexpected file modifications or deletions of files that don't normally c files, or changes to configuration or registry settings, are an indication of possi

Activity D6

Below is an example of an extract from a log of email-related traffic which contains a numbe explain why each looks suspicious.

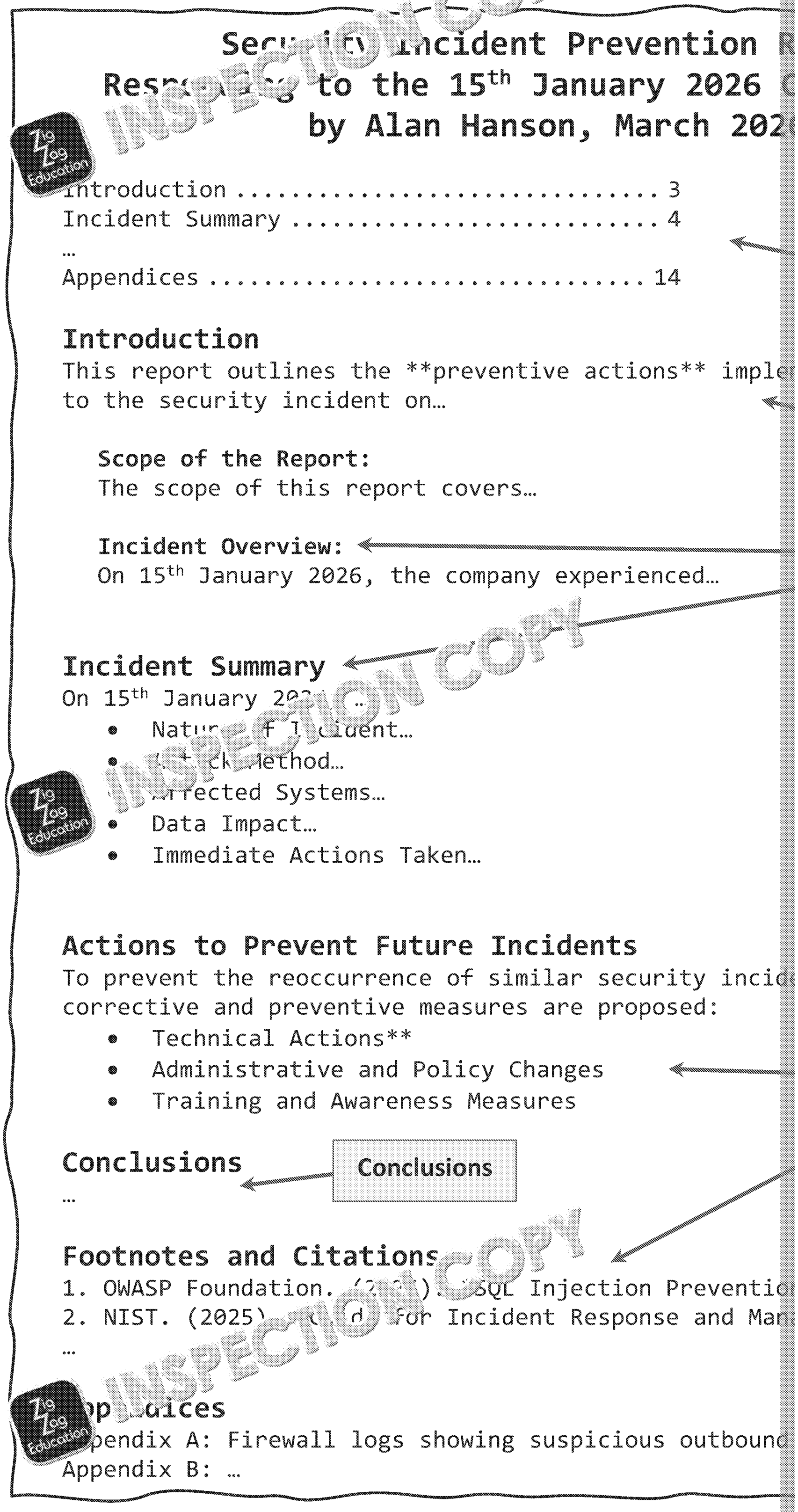
To do this task you will need to use your understanding of what the different ports are used f look for patterns in the data.

Date	Time	Source IP	Destination IP	Protocol	B
2025-03-30	[illegible]	192.168.1.10	62.31.137.89	TCP	1
2025-03-30	08:09:57	192.168.1.10	62.31.137.89	TCP	2
2025-03-30	08:10:01	192.168.1.10	62.31.137.89	TCP	5
2025-03-30	08:19:23	192.168.1.20	10.0.0.5	TCP	4
2025-03-30	08:19:23	192.168.1.10	10.0.0.5	TCP	1
2025-03-30	08:22:13	192.168.1.25	10.0.0.5	TCP	8
2025-03-30	08:22:18	192.168.1.10	10.0.0.5	TCP	1
2025-03-30	08:38:11	192.168.1.30	10.0.0.5	TCP	1
2025-03-30	08:55:45	62.31.113.5	192.168.1.10	TCP	2
2025-03-30	08:55:47	62.31.113.10	192.168.1.15	TCP	4
2025-03-30	08:56:09	62.31.113.15	192.168.1.20	TCP	1
2025-03-30	08:56:10	62.31.113.20	192.168.1.25	TCP	5
2025-03-30	09:00:17	62.31.113.25	192.168.1.30	TCP	8
2025-03-30	09:02:22	62.31.113.30	192.168.1.10	TCP	4
2025-03-30	09:10:00	62.31.147.202	192.168.1.15	TCP	1
2025-03-30	09:22:20	62.31.113.40	192.168.1.20	TCP	1
2025-03-30	09:22:28	62.31.113.40	192.168.1.25	TCP	2
2025-03-30	09:22:37	62.31.113.40	192.168.1.30	TCP	5
2025-03-30	09:32:15	62.31.113.55	192.168.1.20	TCP	8
2025-03-30	09:32:27	[illegible]	192.168.1.15	TCP	4
2025-03-30	[illegible]	62.31.147.202	192.168.1.20	TCP	1
2025-03-30	[illegible]	62.31.137.89	192.168.1.10	TCP	1
2025-03-30	09:48:14	62.31.137.89	192.168.1.10	TCP	2
2025-03-30	09:48:28	62.31.137.89	192.168.1.10	TCP	5
2025-03-30	10:03:51	62.31.113.85	192.168.1.15	TCP	8
2025-03-30	10:04:11	62.31.113.90	192.168.1.20	TCP	4
2025-03-30	10:10:00	62.31.147.202	192.168.1.25	TCP	1
2025-03-30	10:18:41	62.31.113.100	192.168.1.30	TCP	1
2025-03-30	10:19:23	62.31.113.120	192.168.1.10	TCP	2
2025-03-30	10:19:24	94.181.146.37	192.168.1.15	TCP	1
2025-03-30	10:19:25	94.181.146.37	192.168.1.15	TCP	1
2025-03-30	10:19:26	94.181.146.37	192.168.1.15	TCP	1
2025-03-30	10:19:27	94.181.146.37	192.168.1.15	TCP	1
2025-03-30	10:19:28	94.181.146.37	192.168.1.15	TCP	1
2025-03-30	10:19:29	94.181.146.37	192.168.1.15	TCP	1
2025-03-30	10:19:30	94.181.146.37	192.168.1.15	TCP	1
2025-03-30	10:19:31	94.181.146.37	192.168.1.15	TCP	1
2025-03-30	10:19:28	62.31.113.12[illegible]	192.168.1.10	TCP	8
2025-03-30	10:19:36	[illegible]	192.168.1.10	TCP	4
2025-03-30	10:20:[illegible]	62.31.147.202	192.168.1.30	TCP	1
2025-03-30	[illegible]	62.31.113.130	192.168.1.10	TCP	1
2025-03-30	10:20:33	62.31.113.135	192.168.1.15	TCP	2
2025-03-30	10:20:57	62.31.113.140	192.168.1.20	TCP	5
2025-03-30	10:21:42	62.31.113.145	192.168.1.20	TCP	8

D2.3 Writing security reports

Actions to prevent security incidents from reoccurring in the f

The security report is an official document to communicate the details of a sec recommendations, which you want to be taken seriously, so it should be a pro is an example of the outline of a report illustrating the key features that shoul



Security Incident Prevention R
Responding to the 15th January 2026 C
by Alan Hanson, March 202

Introduction 3
Incident Summary 4
…
Appendices 14

Introduction
This report outlines the **preventive actions** imple to the security incident on…

Scope of the Report:
The scope of this report covers…

Incident Overview:
On 15th January 2026, the company experienced…

Incident Summary
On 15th January 20[illegible]…
- Nature of Incident…
- Attack Method…
- Affected Systems…
- Data Impact…
- Immediate Actions Taken…

Actions to Prevent Future Incidents
To prevent the reoccurrence of similar security incid corrective and preventive measures are proposed:
- Technical Actions**
- Administrative and Policy Changes
- Training and Awareness Measures

Conclusions
…

Footnotes and Citations
1. OWASP Foundation. ([illegible]). SQL Injection Preventio
2. NIST. (2025). Guide for Incident Response and Man
…

Appendices
Appendix A: Firewall logs showing suspicious outbound
Appendix B: …

Analysis of the incident

The analysis of the incident is likely to be a detailed and technical report whic report. It will address the following points, even if only to indicate that there

- Were there any **errors or omissions in preventative measures?** Are all t complete, e.g. for firewalls, error monitoring, antivirus software, etc.? W
- Were there any **errors or omissions in our procedures** and were all the p training and documentation good enough? Were there checks that proce why not?
- Were there any **unforeseen problems?** For example, were there any une vulnerabilities which didn't flag up a weakness? Did any external factors contribute?
- Were there any **errors or delays in detection or alerting?** How long did i alerts generated promptly and accurately, then effectively communicate
- Were the **remedial actions** satisfactory, or did they not fix the situation w Were the remedial actions taken promptly and effectively? Was the reco downtime at a minimum? Have the lessons learned already been incorp

Activity D7

Match up these weaknesses with the analysis points above:

- The recovery took three weeks, and we lost a lot of business in that time.
- Staff were ill so checks were not carried out or updates not installed.
- Cloud software didn't enforce 2FA and a password was guessed.
- The hardware firewall was replaced, and the new configuration didn't block unnecessar
- The malware was detected but was missed for three weeks because it was in a very lon

Improvements to the content of IT policies (D2.3.2)

IT policies are the procedures and rules that the members of the organisation IT-related processes. They ensure that the organisation's technology resourc include [illegible] such as access control, password management, software instal recovery, and incident response.

Once the incident has been analysed, improvements may need to be made to improvements may be within the scope of the IT manager to make immediat needs to be approved, possibly waiting for the conclusions of the Incident Pre

Improvements to security protection measures (D2.3.3)

Depending on what problems were found, improvements may be needed in o
Although not an exhaustive list, the table contains those that are more likely.

Security Area	Improvement Measure	Possib
Physical Security	Access Control	• Add biometric access control. • Install turnstiles, scanners and secu • Restrict access to server areas. • Improve visitor management syster
	Surveillance and Monitoring	• Upgrade CCTV with analytics. • Implement motion sensors and intr
	Environmental Security	• Add air conditioning to server room
	Asset Protection	• Implement cable locks to desktops. • Ensure all servers are in locked cup
Software Security	Vulnerability Management	• Automate vulnerability scanning an • Conduct penetration testing and au • Add a monthly checklist that all softv
	Access Control and Authentication	• Enforce strong passwords and MFA. • Implement or extend least privilege
	Data Protection	• Implement better encryption (at re • Improve frequency of backups.
	Application Security	• Improve secure coding practices. • Conduct code reviews and security t
	Endpoint Security	• Implement antivirus software with c
Hardware Security	Secure Boot and Firmware Updates	• Implement secure boot processes. • Establish timely firmware update pr
	Hardware-Based Encryption	• Utilise hardware encryption for stor
	Network Hardware Security	• Secure network hardware with stro • Physically secure network hardware
Processes and Procedures	Incident Response Plan Refinement	• Develop incident responses to a ran • Conduct incident response drills. • Establish clear communication prot
	Security Policy Development and Enforcement	• Develop comprehensive security po • Regularly review and update policie
	Change Management	• Implement a formal change manage • Conduct risk assessments before ch
	Disaster Recovery and Business Continuity	• Test Disaster Recovery and Busines
Training	Security Awareness Training	• Conduct regular security awareness • Tailor training to specific roles. • Test employee knowledge periodica • Implement phishing simulations.
	Technical Security Training	• Provide specialised cyber training fo • Offer formal certification to IT staff.
	Role-Based Security Training	• Provide specialised training for sen

Activity

What improvement measures might be considered after each of the following scenarios?

1. A protester against an organisation's commercial practices has thrown a smoke bomb into
2. An employee has downloaded and installed a program to install a new printer driver, bu the company intranet.
3. A data breach has occurred on your company website through an SQL injection attack.