NCFE Level 2

Certificate in the Principles of Cyber Security

Workbook 2

How to use your learning materials

This course is delivered on a flexible learning basis. This means that most of your study will take place away from your Assessor/Tutor. It helps to carefully plan your studying so that you get the most out of your course. We have put together some handy tips for you below.

Study Guidance

- Try to plan an outline timetable of when and where you will study.
- Try to complete your work in a quiet environment where you are unlikely to be distracted.
- Set realistic goals and deadlines for the various elements of your course.
- Plan what you are going to study during each session, and try and achieve this each time.
- After each session, reflect on what you have achieved and plan what you hope to complete next time.
- Remember that not only do you have the support of your Assessor/Tutor, but it is likely that your family, friends and work colleagues will also be willing to help.

Assessor/Tutor Support

Your Assessor/Tutor will be available to support and guide you through the programme. They are experts in your area of study and are experienced in helping many different types of learners.

They can help you to improve the standard of work you submit and will give you useful feedback on areas in which you have excelled, as well as where you can improve.

Remember to listen to, or read, their feedback carefully. Ask if you are unsure about any of the feedback you receive as your Assessor/Tutor is there to help.

Make note of any tips they give. Refer to the learning materials as they contain the information you need to complete the end-of-unit assessments.

Look out for areas in which you can improve, and set yourself an action plan to make sure you complete the required work.

Take positive feedback on board; this demonstrates you are doing things right and have a good understanding of the subject area.

Use the feedback to avoid repeating any mistakes you may have made.

Enjoy your studies!

NCFE Level 2 Certificate in the Principles of Cyber Security

Workbook 2

Workbook Contents

In this workbook, you will continue your study of the roles and issues related to Cyber Security. You will gain an understanding of some of the common threats to cyber security and how these can be combated. You will also learn about some common methods used by individuals, businesses and nations to maintain cyber security. You will also learn how to develop your work skills, so that you can work effectively in a team to deliver cyber security.

Contents

This workbook contains four sections:

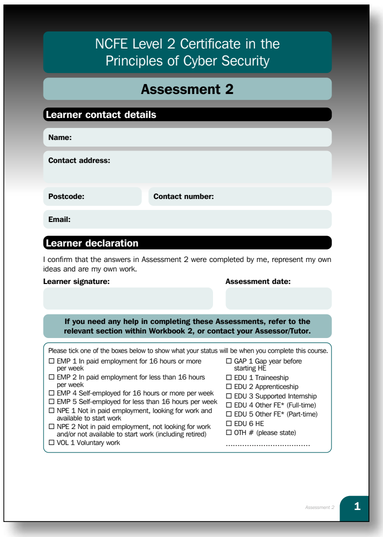
		Page
Section 1:	Understand common threats to cyber security	4
Section 2:	Methods of maintaining cyber security	25
Section 3:	Working with others in cyber security	42
Section 4:	Extension activities	64

Each section has a corresponding assessment that must be completed in order to achieve this part of the programme.

The assessments for this workbook can be found in:

Assessment 2

When you have completed this workbook, you should attempt the assessment. Your Assessor/Tutor will then give you detailed written feedback on your progress.



NCFE Level 2 Certificate in the Principles of Cyber Security

Assessment 2

Learner contact details

Name:

Contact address:

Postcode: **Contact number:**

Email:

Learner declaration

I confirm that the answers in Assessment 2 were completed by me, represent my own ideas and are my own work.

Learner signature: **Assessment date:**

If you need any help in completing these Assessments, refer to the relevant section within Workbook 2, or contact your Assessor/Tutor.

Please tick one of the boxes below to show what your status will be when you complete this course.

□ EMP 1 In paid employment for 16 hours or more per week
□ EMP 2 In paid employment for less than 16 hours per week
□ EMP 4 Self-employed for 16 hours or more per week
□ EMP 5 Self-employed for less than 16 hours per week
□ NPE 1 Not in paid employment, looking for work and available to start work
□ NPE 2 Not in paid employment, not looking for work and/or not available to start work (including retired)
□ VOL 1 Voluntary work

□ GAP 1 Gap year before starting HE
□ EDU 1 Traineeship
□ EDU 2 Apprenticeship
□ EDU 3 Supported Internship
□ EDU 4 Other FE* (Full-time)
□ EDU 5 Other FE* (Part-time)
□ EDU 6 HE
□ OTH # (please state)
....

Assessment 2 1

Upon successful completion of this qualification, learners will be awarded the NCFE Level 2 Certificate in the Principles of Cyber Security: 603/5853/1. This qualification is certificated by the Awarding Organisation NCFE.

PLEASE READ!

Every effort has been made to ensure the content of this workbook is accurate at the time of print/production. As some information (for example, legislation and government bodies) can change, we recommend that you check the latest guidance and advice to ensure your answers are accurate and current.

In this section, you will gain an understanding of malicious software and the ways in which a system can be infected. You will understand common and emerging threats as well as physical threats to cyber security.

Understand the common and emerging threats to cyber security – types of cyber attack

Please read the following as it will help you to answer question 1.

To achieve their goals of gaining access or disabling operations, a number of different methods are deployed by cybercriminals. There are always new methods being developed, and some of these categories overlap. Some of the more common methods are:

- **Phishing** – In phishing, cybercriminals craft emails to fool a target. The recipient might be tricked into downloading malware that's disguised as an important document, for instance, or convinced to click on a link that takes them to a fake website where they'll be asked for personal information, like bank usernames and passwords. Many phishing emails are relatively simple and are sent to thousands of potential victims, but some are specifically crafted to target specific individuals.
- **Spear phishing** – This is a type of phishing attack where, instead of sending out a mass email, a particular individual or individuals are targeted. As with phishing, a spear phishing attack will often involve an email and an attachment, but it will be addressed to a specific person, such as a ranking official or someone involved in confidential operations within an organisation. In a spear phishing attack, the attackers usually perform reconnaissance methods before launching their attacks. For example, determining how they format their email addresses and using social media and other publicly available sources to gather information.

- **Vishing** – This is another type of phishing attack, but one that uses a phone call. During a vishing call, a scammer uses social engineering to get you to share personal information and financial details. In one popular scenario, the scammer says they are from your bank or law enforcement and your account has been compromised, then they ask you to tell them your account details or direct you to a fake site to enter personal information.
- **Denial of service** – A denial of service attack is a brute force method to try to stop some online services such as websites from working properly. For instance, attackers might send so much traffic to a website that it overwhelms the system's ability to function, making it unavailable. A distributed denial of service (DDoS) attack uses an army of computers, usually compromised by malware and under the control of cybercriminals, to aim the traffic towards the targets.
- **Zero-day exploits** – Zero-days are vulnerabilities in software that have been announced, but not yet fixed. The name comes from the fact that once a patch is released, each day there are fewer and fewer computers open to attack, as users download their security updates.

Some emerging threats include:

- **Man in the middle** – This is a type of attack where the attacker intercepts and alters communication between two people or organisations so they can masquerade as one of those communicating and steal information.
- **Smishing** – This is any kind of phishing that involves a text message. The techniques are very similar to phishing, but use text messages instead of emails. It is particularly effective because people tend to be more inclined to trust a text message than an email. While most people are aware of the security risks involved with clicking on links in emails, they may not yet be aware of the risks of clicking on links in text messages.
- **Cryptojacking** – Cryptojacking is an emerging type of specialised attack that involves getting someone else's computer to do the work of generating cryptocurrency for you (a process which is also called data mining). The attackers will install malware on the victim's computer to perform the necessary calculations.

- **Watering hole attack** – Also called waterholing, this works by identifying a website that's frequented by users within a targeted organisation, or even an entire sector, such as defence, government or healthcare. The attacker identifies weaknesses in the main target's cyber security, then manipulates the site to deliver malware that will exploit these weaknesses. The computer of anyone visiting or downloading material from that site is then infected with malware.
- **Synthetic identity fraud** – In this rapidly-emerging type of fraud, criminals don't steal an identity, but instead create a new one. To do this, they might combine fake and real information, for example, mixing a fake name and address with a real identification number they have stolen or purchased. They then use this identity to open bank accounts and obtain credit cards. Fraudsters then use these credit cards to make large purchases or obtain bank loans. In the end, the fraudster will vanish without paying off any of the debt.

Find Out More: Choose one type of emerging cyber threat and find out more about it and how it is being combated.

What is meant by malicious software?

Please read the following as it will help you to answer question 2.

Malicious software, which is more commonly known as malware, is a piece of software that seeks to harm or compromise a computer system. Malware can be in the form of worms, viruses, trojans, spyware, adware, rootkits and more. All of these can steal protected data, delete files or install extra software not wanted by a user.

Botnet

A botnet is a network of computers that have been intentionally infected with malware so that they will perform automated tasks on the Internet without the permission (or knowledge) of the devices' owners. Personal computers, servers, and even webcams and smart devices like WiFi-enabled refrigerators can be used in botnets.

Malware

Short for malicious software, malware can refer to any kind of software that is designed to cause damage to a single computer, server or computer network. Worms, viruses and trojans are all varieties of malware and are distinguished from one another by the ways that they reproduce and spread. These attacks may be designed to render the computer or network inoperable, or grant the attacker root access so they can control the system remotely.

Trojan

A Trojan horse, or Trojan, is a type of malicious code or software that looks like a real piece of software but can then take control of a computer. A Trojan is designed to damage, disrupt, steal, or inflict some other harmful action on data or a network.

Cyber-criminals use forms of social engineering to trick users into loading and executing Trojans on their systems. Once activated, Trojans can give cyber-criminals access to a system in order to spy or steal sensitive data.

There are many types of Trojan, including:

- Backdoor – this gives attackers remote control over the infected computer.
- Rootkit – these Trojans are designed to conceal certain objects or activities in your system. Often their main purpose is to prevent malicious programs from being detected.
- Trojan-Dropper – used by hackers in order to install Trojans and/or viruses.
- Trojan-GameThief – these steal user account information from online gamers.

Ransomware

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data. Users are given instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, and are typically payable in cryptocurrency.

Spyware

This is unwanted software that infiltrates a computing device, stealing the Internet usage data and sensitive information. Spyware is a type of malware – malicious software designed to gain access to or damage a computer, often without the user's knowledge. It may gather personal information such as bank account log in details or passwords to email accounts.

Virus

A computer virus is a software program that is loaded onto a user's computer without their knowledge, and that performs malicious actions. These range from deleting files to potentially destroying hardware.

Worm

This is a type of malware that spreads copies of itself from computer to computer without any human involvement. Worms do not need to attach themselves to a software program in order to cause damage. Worms can modify and delete files, or insert malicious software onto a computer. Sometimes a worm's purpose is just to make copies of itself – depleting system resources and overloading a shared network. They can also steal data, install a backdoor, and allow a hacker to gain control over a computer and its system settings.

Knowledge Activity 1: What are some ways that you could prevent the types of threats and attacks discussed in this section?

Ways in which malicious software can infect a system

Please read the following as it will help you to answer question 3.

How malware can infect your PC

Malware can find its way on to your computer in a number of ways. Some of the most common routes are:

Spam emails

The people who create malware often use tricks to try to convince users to download damaging files. This can be an email with a file attached that says it is a receipt for a delivery, a tax refund or an invoice for something you have bought. If the attachment is opened, users could end up installing malware onto their computer without their knowledge.

A malicious email may sometimes be easy to spot – it could have bad spelling and grammar or come from an email address that people don't recognise. However, these emails can also look like they come from a real business or someone you know. Some malware can also hack email accounts and use them to send malicious spam to any contacts they find.

To prevent a computer from being infected, it's a good idea to consider the following:

- If you aren't sure who sent you the email – or something doesn't look quite right – don't open it.
- If an email says you have to update your details, don't click on the link in the email.
- Don't open an attachment to an email that you weren't expecting, or that was sent by someone you don't know.

Infected removable drives

Many types of malware can be easily spread by infecting removable drives such as USB flash drives or external hard drives. The malware can be automatically installed when you connect the infected drive to your computer. Some worms can also spread by infecting computers connected to the same computer network.

There are several things you can do to avoid this type of infection:

- Run a security scan of your removable drives every time you plug them in.
- Disable the Autorun function so that it doesn't automatically start when you plug it in.

Bundled with other software

Some malware can be installed while you are downloading other programmes. This includes software from websites.

Some malware will try to install other software that will be detected as unwanted software. This can include new toolbars on your web browser or programs that show you extra advertisements as you browse the web. There will often be an option to opt out of installing this extra software by checking a box during installation.

You can avoid installing malware or potentially unwanted software by:

- Only downloading software from the official vendor’s website.
- Taking your time to install the software, making sure you read exactly what you are installing.

Compromised webpages

Malware can enter a computer through infected websites. As soon as you enter the website, the malware will download to your computer. The website might have been created solely for the purpose of trying to get malware installed on as many computers as possible, or it could be a legitimate website that has been compromised or hacked.

Methods for removing malicious software from an infected system

Please read the following as it will help you to answer question 4.

Every computer should have some form of anti-virus software installed. However, most anti-virus software is not used to detect malware. Computers should also have an anti-malware program to regularly scan, clean and protect them from potential Internet threats: viruses, spyware, trojans, bots, adware and worms.

How to remove malware from your computer

There are many types of software that will help you to clear an infected system – some is designed for home computers and others specialise in clearing servers and networks. In general, clearing an infected system often involves the following:

- **Disconnect from the Internet** – this will prevent more of your data from being sent to a malware server or the malware from spreading further
- **Enter safe mode** – often referred to as safe boot, this is a way to start your computer so that it allows only the most necessary software and programs to load. This will prevent the malware from loading and make it easier to remove.
- **Check the activity monitor for malicious applications** – this shows the processes that are running on your computer, and allows you to see how they affect your computer's activity and performance. For example, you can see which applications are working the hardest – if you do not recognise the app, it may be malware.
- **Run a malware scanner** – these can remove most standard infections. You should install and run security software which provides protection against existing and emerging malware.
- **Verify your browser's homepage** – malware can modify your web browser's homepage to re-infect your computer.
- **Clear your browser's cache** – the cache is a temporary storage location on your computer where data is saved so your browser doesn't need to download it each time. Clearing it can remove any malware that is still lurking.

If all else fails, it may be necessary to entirely reinstall the operating system and all applications and programs from scratch. This is why it is vital that you always have an up-to-date backup on an external drive.

Knowledge Activity 2: Go back and look at your answer to Knowledge Activity 1. Are there any additional steps that you would take to prevent or remove the threats and attacks discussed earlier?

The importance of perimeter access control

Please read the following as it will help you to answer question 5.

Physical perimeter access control includes those systems and technologies that protect people and assets in a facility and its grounds by blocking unauthorised physical intrusions across the perimeter. In cyber security, this may involve controlling access to an entire building, or to a single room, such as the server room. The goal is to prevent unauthorised access by people who could damage hardware or software, or steal information to use in setting up phishing or other types of attacks.

Physical security perimeters are used to safeguard sensitive data and information systems. These can include fences, barriers, gates, electronic surveillance, physical authentication mechanisms, badges, fingerprint scanners, reception desks, and security patrols. It can also include having backup systems in place to ensure that operations can continue if anything should happen.

Security perimeters are often set up in layers. For example, it may be relatively easy to enter a building, but more checks are needed to enter different parts of the building, with the highest level of checks used in the most sensitive areas.

Access control systems are used to make sure that those who are entering each layer are authorised to be there. Physical security perimeters may include fences, cameras or CCTV, locked doors, and alarms; access control systems often include badges, sensors, alarms, passwords, fingerprint scanners, etc. Essentially, it involves anything that is involved in the control of people, materials and vehicles through entrances and exits of a controlled area.

The importance of check and challenge on the premises

Please read the following as it will help you to answer question 6.

Check and challenge is the process of confirming someone's identify and their reason for visiting the business premises or area. It is usually done at reception but can also be carried out by security professionals or through use of key cards or access codes.

Check and challenge is particularly important in areas where there is highly sensitive or classified data or work. Behaviour that may trigger check and challenge could include 'tailgating' (waiting until someone with a code or key card opens the door and then entering an area before the door closes and locks again), re-using visitors' passes, or people who have talked their way through reception, for example, by posing as a delivery worker.

By carrying out check and challenge, organisations can ensure that the people accessing their site are there for the right reasons and not attempting to cause damage to their computer systems or steal data.

How organisations can protect themselves from unauthorised entry

All staff to wear and display ID badges

If all permanent staff members do not wear ID badges, it makes it difficult to tell the difference between an intruder and a member of staff. If all staff members display an ID badge and all visitors are wearing a visitor pass, it becomes much easier to spot an intruder.

Allocate a single point of entry and exit for visitors

One key security measure is for all visitors to enter and leave via the same door. This will allow reception staff to monitor all visitors and ensures that when a visitor leaves the premises they sign out and hand back the visitors' pass.

Visitors must supply valid picture ID such as a Driving Licence or Passport

All visitors should provide proof of identification on arrival. This helps confirm the person coming into the building is who they say they are.

Visitor badges should not leave the premises

How many times have you visited a business and kept the visitors' badge afterwards? Preventing visitors from removing badges from the premises limits the chances of them being lost, stolen, or reused by an attacker.

Education of employees

It is vital that employees have training in security procedures. It is also important that the employees know what action should be taken should an intruder be identified.

Knowledge Activity 3: Imagine that you are in charge of security for a building where sensitive and confidential data is stored. What types of security would you put in place to make sure that only authorised personnel have access to the most sensitive parts of the building?

Identifying possible threats to a business

Please read the following as it will help you to answer question 7.

Personal devices

In addition to employees using their personal devices for company business, many organisations have started using a bring-your-own-device (BYOD) policy, where employees use their own computers, phones, etc for work, bringing them to the office or using them when working remotely.

However, this policy also has a number of risks. These include the possibility that employees' personal devices will not be as well protected as company devices. There is also an increased risk of infection from malware, for example, if the employee downloads an app from an untrustworthy source.

Because the employees will be carrying their devices to and from work, there may also be an increased risk of the devices being lost or stolen.

Personal devices also tend to lack robust data encryption, or may not be regularly updated, so they may also be easier to hack. If employees are working remotely, such as from Wi-Fi hotspots in public, this could also leave them more vulnerable to hacking and to malware.

Removable devices

Removable media and devices include:

- Optical Discs – such as Blu-Ray discs, DVDs and CD-ROMs
- Memory Cards – such as Compact Flash card, Secure Digital card and Memory Sticks
- Zip Disks/Floppy disks
- USB flash drives

Removable media provide a common route for the introduction of malware and the export of sensitive data.

Removable media is very easily lost, which could result in the compromise of large volumes of sensitive information.

Did you know?

In 2018, Heathrow Airport was fined £120,000 by regulators after a data breach caused by a lost USB stick. An airport employee lost a USB stick containing 76 folders and over 1,000 confidential files containing the names, dates of birth, passport numbers, and other details of individuals and security staff.

The USB was discovered by a member of the public, who opened the USB at a public library before handing it to the press. The information on the USB was not protected or encrypted. After the newspaper took a copy of the information, the stick was returned to the airport.

Hardware

Physical hardware theft and loss are also huge risks to an organisation. The loss of a laptop, mobile device, or storage devices such as hard drives and flash drives can result in high costs and loss of reputation.

Understanding how hardware theft and loss happens, and how to reduce the risks of both physical device and data loss, helps organisations to reduce the risks and the impact of a loss on their business.

Human error is one of the largest risk factors in hardware loss. Employees may accidentally leave laptops, phones and other devices in public places, such as on trains, and these may be found by fraudsters or those who sell them to fraudsters.

While most of us think that we would never lose a laptop, one study by Kensington showed that 84% of businesses surveyed had reported a lost or stolen laptop. In fact, data shows that, in the US, more than 12,000 laptops are left in airports each week, and most of these are never returned to their owners.

Networking infrastructure

Network infrastructure refers to all of the resources of a network that make network or Internet connectivity possible. Network infrastructure includes both hardware and software, along with elements like servers, network hubs and switches, firewalls, Wi-Fi access points and routers.

Making sure the network infrastructure is robust, secure and protected is critical to cyber security.

Just like a secure physical perimeter can safeguard the material inside a building, a secure networking infrastructure can help safeguard data from hackers. A network perimeter is the secured boundary between the private and locally managed side of a network, such as a company's intranet, and the public facing side of a network, often the Internet.

Network infrastructure could include:

- Border Routers: These direct traffic into, out of, and throughout networks. The border router is the final router under the control of an organisation before traffic appears on an untrusted network, such as the Internet.
- Firewalls: This is a set of rules specifying what traffic will be allowed to pass through or denied access. A firewall is usually more thorough at filtering traffic than a border router.
- Intrusion Detection System (IDS): This acts like an alarm system for your network. It is used to detect and alert on suspicious activity. This system can consist of a single device or a collection of sensors placed at strategic points in a network.
- Intrusion Prevention System (IPS): Compared to a traditional IDS which simply notifies administrators of possible threats, an IPS can attempt to automatically defend the target without the administrator's direct intervention.
- De-Militarized Zones / Screened Subnets: DMZ and screened subnets are small networks connected directly to a firewall or other filtering device.
- Secure open Wi-Fi: an unsecured, or open, wireless network is one that does not require a Wi-Fi Protected Access (WPA, WPA2 and WPA3) code for access. Organisations should use either WPA2 or the newer WPA3 standard for encryption. Employees who work remotely should also use this security standard and should never connect to an open network.
- Administration passwords: These give access to the router and should be changed regularly to prevent hackers gaining access to the network through the router.
- Router: These are used to connect devices to the Internet and to each other, as well as to create LANs. Routers may be vulnerable to unauthorised access from an attacker, such as through a rerouting attack, when the attacker manipulates router updates to cause traffic to flow to unauthorised destinations; or through a masquerade attack, when an attacker manipulates IP packets to falsify IP addresses.

Threats presented by remote working

Please read the following as it will help you to answer question 8.

Security challenges of remote working

The willingness to work remotely has never been greater than right now. However, companies who offer more remote work opportunities must look at a wide range of security challenges and so must respond accordingly to prevent unauthorised network access.

Allowing employees to access company data from offsite locations raises serious concerns about data encryption, the security of wireless connections, use of removable media and potential loss or theft of devices and data.

The following are some of the security challenges presented by remote working, to both workers and the organisation.

- Fewer layers of security: Organisations often use perimeter access controls, local area networks and other security tools, such as firewalls and dedicated work computers that come with encryption. Without these multiple layers of security, remote workers are more vulnerable to security threats.
- Reduced security on BYOD and mobile devices: Using personal devices and open Wi-Fi can expose data to threats from hacking. Many phishing attacks now use text messages or WhatsApp. Using a device that has these apps installed can leave the device, and the data on it, exposed to this type of attack. All employees should be required to use secure passwords and secure Wi-Fi, or a VPN with end-to-end encryption, on any devices they use for work. Organisations can also provide security themselves by installing authorised antivirus and security software.
- Loss or theft of devices: If employees are working outside their home, for example, in a coffee shop, there is added risk of losing a device or having it stolen.
- Tracking and managing data in the cloud: Many businesses, especially those that operate almost entirely remotely, store and share work in the cloud. This can leave the data open to risks in the event that the cloud server is hacked. Cloud-based IT management platforms can be used to allow businesses to connect, monitor and secure data on the cloud, without any geographical boundaries.
- Inadequate backup and recovery systems: In case of an accidental data loss, remote employees using their own devices often do not have adequate backups in place. This can be solved by having a centralised data backup and recovery programme for all remote devices used for work, or by using a cloud backup.

- Damage to equipment: This may be more likely to happen when people are working remotely and in a less-controlled environment. For example, they may be working around pets or small children or in a place where food and drink can more easily be spilled on a device.
- Mixing up work and personal use: Remote employees who are using a BYOD device are probably using the same device for work and personal use, and could mix up personal and business data. So, if an employee's laptop crashes due to malware that was accidentally downloaded on software for personal use, the business data is lost too. This is why having a backup is very important.
- Legal compliance: Small businesses employing freelancers and remote staff can have a harder time ensuring they strictly abide by the rules of GDPR. This is because it is unclear how some of the rules apply to employees using BYOD devices. For example, how would the rules apply to an American citizen working for a US-based company, who is living and working remotely in the EU? All businesses with remote employees should have a clear policy on how they handle business data at all times.

Knowledge Activity 4: Compare and contrast the main threats to cyber security from working in an office and working remotely.

Best practice to minimise physical threats to cyber security

Please read the following as it will help you to answer question 9.

What is physical security and why it matters

Gaining access to a property can provide criminals with the ability not only to steal physical items from the premises, but also to potentially infect computers with malware or access data through the IT infrastructure.

Physical security includes any security measures that are taken to ensure that only authorised personnel have access to equipment and resources in an office or building. A well-designed physical security system protects the building, resources and equipment against theft, vandalism, natural disaster, sabotage, terrorist attack, cyber attack and other malicious acts.

Practices to minimise physical threats

Physical security becomes more important in case of critical systems and facilities, for example: server rooms, production bays, data centres, nuclear reactors, electricity power grids, etc.

The following are examples of different system measures which can be used to protect against potential threats:

- Access controls – Organisations need to have some way of controlling access to the premises. If the business is based at a small office with a single door for entry, a simple lock can be enough. But if there are many ways to gain entry, then more advanced methods are needed.

  This could include high-tech options such as finger-print scanning or a PIN-entry system.
- Issue ID cards – One useful and effective security measure that all organisations should implement is providing ID cards for staff. It’s a simple step, but doing so ensures that anyone who wants to get access to an organisation’s building needs to show an ID card. When combined with a swipe system for access to the building or to different areas of the building, this adds another layer of security.

- Car park security – The car park for a property is a surprisingly vulnerable area, and it is important that organisations put the proper safety precautions in place. Car parks can be used as an area to conduct surveillance of your property. If there is no access prevention, getaway vehicles can be parked right next to the building to allow criminals to escape in the event of a physical breach.

  There are a number of different steps that can be taken to make a car park more secure. These include installing a security barrier, having a key card system or using a guard.

- Automatic lighting – Another great physical security feature that can make a big difference to a business is to add automatic lighting. Motion sensing lights will illuminate anyone who is not where they are supposed to be, making it harder for people to sneak around. Often the threat of being seen is more than enough to put off a criminal from attempting to gain access to an area.

- Surveillance – This can be a strong deterrent against criminal activity. One common type of surveillance is CCTV.

  Another option is to hire a professional security firm to conduct patrols. This is expensive and is usually used by large organisations where the risk of a breach is worth the costs involved.

- Create a security culture/human firewall – One of the most important things that a business can do for their physical security is to ensure that all staff take security seriously. If staff are aware of the need to keep an eye out for any suspicious activity and report it as soon as possible, they can be a very valuable line of defence in terms of surveillance.

  Provide regular training sessions to staff about the importance of good security practice and the things that they can be doing to help the business be more secure.

- External barrier – This can include fences, walls, razor wire, etc. and provides a first line of defence against intruders.

Fort Knox

The saying "as secure as Fort Knox" implies that a place has much stronger protection than normal. So, how secure is Fort Knox? The United States Bullion Depository (the proper name of Fort Knox) is home to about half of the U.S. gold reserves, and has been called the most secure vault on the planet.

The complex is surrounded by a steel fence and the building is made of concrete-lined granite, reinforced with steel. While the U.S. Treasury won't say what protective devices the building and underground vaults are equipped with, it will say that the door to the vault is made of steel and concrete and weighs more than 20 tons. No single person knows everything about how to get in. Instead, certain staff members know just one of several combinations, and they need to all be dialled separately to open the vaults.

Aside from armed guards, who practise their skills in an on-site gun range, the site also shares its home with 40,000 soldiers at the Fort Knox Army post. The building also has its own emergency power plant and water system.

Knowledge Activity 5: Carry out a security assessment on your workplace or home. What physical security features are currently used? How would you make the building more secure?

Summary

In this section, you have learned about:

- common and emerging threats in cyber security
- different types of malicious software
- ways of identifying and removing malicious software
- different types of physical threats to cyber security
- threats from remote working, personal devices, removable devices, hardware and networking infrastructure

Section 2: Understand methods of maintaining cyber security

In this section you will understand the preventative methods used to maintain cyber security, the principles of user access control and the use of firewalls.

Routine ways to maintain cyber security

Please read the following as it will help you to answer question 10.

Every organisation is a potential victim of a cyber attack. All organisations have something of value that is worth something to others, even if that is simply money from ransomware. Organisations that do not take routine precautions will almost certainly experience some form of cyber attack.

Common elements of routine cyber security

The following are a few of the precautions that are routinely used. Not every organisation will use every one of these.

- Boundary firewalls and Internet gateways – Establish network perimeter defences, such as web proxy, web filtering, content checking, and firewalls. These will help to detect and block executable downloads, block access to known malicious domains and prevent users' computers from communicating directly with the Internet.
- Malware protection – Set up and maintain malware software to detect and respond to known attacks. This could include installing security software and ad blockers, as well as restricting the use of personal email on work computers.
- Patch management and software updates – Updating your software regularly with the latest version will ensure that new vulnerabilities and bugs are patched quickly, before they can be used by hackers.
- Whitelisting and execution control – This is a security feature that allows you to create lists of trusted IP addresses or IP ranges from which your users can access your domains. It also prevents unknown software from being able to run or install itself.
- Secure configuration – This restricts the functionality of every device, operating system and application so they cannot be used in an unauthorised way.
- Password policy – Ensure that an appropriate password policy is in place and followed. This should include the use of secure passwords, not writing down passwords or keeping them near the computer, etc.

- User access control – This includes limiting users' execution permissions so that users only have permission to access certain files and folders, rather than every file and folder in the system.
- Employee education – Make sure that every employee is fully trained in how to recognise and prevent cyber attacks. This should include a clear statement of what employees can and cannot do; procedures for handling a suspected data breach; encryption of all devices used for work, including BYOD devices; specifying the particular information and documents that should never leave the secure workplace; rules for online behaviour.
- Back-ups – All data should be backed up regularly to an external drive or server, or to the cloud.
- Policies and procedures – Have detailed and clear policies and procedures in place that set out what employees must and must not do and what to do should a cyber attack happen.

Vulnerability testing

Please read the following as it will help you to answer question 11.

A vulnerability test or assessment is the process of identifying and prioritising the vulnerabilities in a system. This type of test is performed in different kinds of systems, including IT systems, energy supply systems, communications systems, etc. The tests may be conducted for organisations ranging from small businesses up to large regional infrastructures. Vulnerability tests usually include cataloging the assets and resources of the system; ranking the assets in terms of importance to the organisation; identifying potential threats to each asset or resource; finding the best ways of mitigating or eliminating the threats. This process usually includes the following:

Vulnerability assessment

A vulnerability assessment is a way to evaluate the security risks in the software system in order to reduce the probability of a threat. It is also called vulnerability testing.

A vulnerability is any weakness in the IT system's security procedures, design, or implementation that may result in systems becoming hacked.

The purpose of a vulnerability assessment is to reduce the possibility for intruders (hackers) to gain unauthorised access. To complete an assessment, a number of different tools are used. The first is a vulnerability scan, which is usually completed along with penetration testing.

Vulnerability scanning

A vulnerability scan is an application that identifies and creates an inventory of all the systems (including servers, desktops, laptops, virtual machines, containers, firewalls, switches, and printers) currently connected to a network.

For each device that it identifies, it will also identify the operating system it runs and the software installed on it, along with other key information, such as open ports and user accounts.

Vulnerability scanners will also attempt to log in to systems using default or other credentials, in order to build a more detailed picture of the system.

Once it has built the inventory, the vulnerability scanner checks each item in the inventory against one or more databases of known vulnerabilities to see if any items are subject to any of these vulnerabilities. This identifies if any critical updates have not been applied.

The result of a vulnerability scan is a list highlighting any systems that have known vulnerabilities that may need attention.

The vulnerability management process

Once a scan has been completed, the information is then used to produce a detailed report.

The report would include key information which is extremely useful to IT departments.

This includes:

- identification of vulnerabilities
- evaluation of the risk posed by any vulnerabilities identified, e.g. how much risk is the organisation in currently
- the treatment of any identified vulnerabilities
- reporting on vulnerabilities and how they have been handled, e.g. what has been done and what needs to be completed in the future

Find Out More: Find out more about different types of vulnerability testing and when they are used.

What is meant by penetration testing

Please read the following as it will help you to answer question 12.

A penetration test, also known as a pen test, is a simulated cyber attack against a computer system that checks for vulnerabilities that hackers can use. It is a way to test the security of an IT system by attempting to breach that system's security, using the same tools and techniques a cyber attacker would use. It can be thought of as a type of White Hat attack.

Penetration tests are used to identify the amount of risk from software, hardware and social engineering vulnerabilities. In the UK, pen tests are often performed by qualified and experienced companies that have been certified under a particular certification scheme, such as CREST or the Cyber Scheme.

There are different types of penetration testing, including:

- Whitebox testing – In this case, all of the information about the target software, hardware or employees is shared with the testers.
- Blackbox testing – In this test, no information is shared with the testers about the target. This type of test is more accurate at identifying the risks from outside the organisation, but can also mean that some vulnerabilities remain undiscovered.

The following penetration tests can be run as either whitebox or blackbox tests:

- Vulnerability identification – This is often used to test web applications. It gives feedback to web developers on coding practices to use to avoid any vulnerabilities that are found.
- Scenario driven testing for vulnerabilities – In this case, the penetration testers explore a particular scenario to discover whether it leads to a vulnerability in your defences. Scenarios may include a lost laptop or an unauthorised device connected to the internal network, but there are many others. Organisations choose the scenarios they are most concerned about.
- Scenario driven testing of detection and response capability – This type of test is also used with certain scenarios, such as a phishing attack, etc. But its aim is to find out how well the organisation can detect and respond to the vulnerability.

Security updates and 'patching'

Please read the following as it will help you to answer questions 13 and 14.

Security updates are issued regularly by the software developer (the company that makes the software). They may be issued for many reasons.

Often, security patches are included in software updates. Software updates can also include fixes for performance bugs, the addition of new features, compatibility fixes and may address any security issues that have been identified since the last update was deployed. Software vulnerabilities enable cybercriminals to access a person's computer, allowing them to take control of the computer and access personal data, such as financial information and passwords. Updates sometimes run automatically in the background. Other times, updates come in the form of a free download. They may also be necessary for software to continue running when changes are made to the host operating system.

?

Did you know?

On the second Tuesday of each month (nicknamed Patch Tuesday) Microsoft usually releases a security update to protect customers against the most recent threats.

Microsoft provides concurrent mainstream support and extended support periods for its operating systems after their release.

During the five-year mainstream support period the OS will get regular updates including security improvements and design features. Once this is over the operating system heads into the extended support period, which means it doesn't get new features, but will get security updates and fixes.

Patching

While a software update is designed to improve the performance of the software, a patch is a type of update that is designed to fix a particular security flaw, bug or vulnerability. The patch is a small piece of software that the software developer issues whenever a security flaw is uncovered. The patch covers the flaw, keeping hackers from further exploiting it.

It is very important that all computer users update their software with the latest patches, as a delay can allow hackers to access their system. For example, the WannaCry ransomware infected more than 200,000 computers and networks before a cyber security expert found a way to stop it. The software developer Microsoft had actually issued a patch for the flaw that the attackers used, but many organisations and users had not installed the patch, so their systems were exposed to the malware.

When cyber security experts or White Hat hackers discover a software flaw or bug, they alert the developer, and do not make the discovery public. This is to keep the flaw secret from malicious hackers who could take advantage of it to launch attacks. This also means that developers often release important patches before anyone knows about the problem. That's why it's very important to always update software on schedule – you could be eliminating a dangerous flaw.

The importance of keeping accurate and up-to-date cyber security information and maintenance records

Please read the following as it will help you to answer question 15.

We have already seen the risks involved with not keeping software updated and regularly patched. Cyber security is a constant cat and mouse game between organisations and attackers, with new vulnerabilities being discovered and closed all the time. This makes it very important to keep track of all maintenance and updates, to make sure that your organisation is always up-to-date with the latest fixes.

This will also minimise any disruption to the business. For example, in 2017, the personal data of 147 million people was stolen from the US company Equifax. The cause of the breach was an application that hadn't been updated, allowing hackers to access the data. However, a patch for this vulnerability was released months before the attack happened. This means that the attack could have been avoided by keeping up-to-date records to inform the IT managers that an update was needed.

Log management is another important record-keeping tool. Logs are the files that detail all the events that occur within a company's systems and networks, including servers, firewalls, and other IT equipment. Each device, system, network, and application is called a log source. The event logs can show deviations from expected activity, alerting you to potential software, hardware, and security issues.

Logs provide data about a wide array of activities across the system, including login failures, password changes, denial of service attacks, file name changes, exported data, new user logins, malware detection, etc. Tracking this information can help alert you to an unauthorised user or download, or a data breach.

Any systems connected to the Internet all require active monitoring. Any seriously suspicious behaviour or critical events will generate an alert that can then be checked and acted on by IT teams.

The logs will provide clear audit trails when investigating any incident and help identify where the attacker accessed the systems and outcome.

Maintenance records are also vital to keep systems and software safe.

The maintenance records need to be continually kept up to date so that IT professionals can ensure all the systems have the latest security patches installed. Records are used to identify which machines have which hardware and software installed on them so that when a vulnerability is identified, this can be addressed quickly. When IT teams are not sure of this key information, systems can be left vulnerable for a considerable amount of time, which gives hackers time to access the system.

Knowledge Activity 6: Imagine that you are in charge of IT for a large company. Outline some of the ways that you could make sure all of the hardware and software was kept up to date.

User access control

Please read the following as it will help you to answer question 16.

Access control is the way an organisation decides who should be allowed to see different types of data. For example, the company CEO may be able to see all of the data in the entire company; a division manager may be able to see the data for their division but not other divisions; an entry-level worker may be able to see only the data for their particular team. Each of these people has a different level of access.

The access control system verifies the identity of users and determines whether a particular user should be given access to particular data. Without appropriate access control, there is no data security. This is because giving people access to data they do not need can increase the chances of a data breach or data loss. It makes it easier for hackers to take advantage of uncontrolled administrative privileges to gain access. Failure to manage user access control can also lead to employees unknowingly or deliberately accessing and misusing data they shouldn't be authorised to see.

The granting of high-level administration privileges should be carefully controlled and managed. This principle of only giving people access to the data they need is sometimes referred to as 'least privilege'.

Methods of restricting user access

Please read the following as it will help you to answer question 17.

Establish effective account management processes: Have a system in place for managing user accounts, including keeping track of special account privileges; documenting user access permissions; and removing or disabling user accounts when no longer required. Unauthorised user accounts should be denied access to applications, computers and networks.

Establish policies and standards for user authentication and access control: A strong password and username policy should be developed that balances security and usability. Consider using two-factor authentication. This is a security system that requires two separate, distinct forms of identification in order to access something. The first factor is a password and the second includes either something you have or something you are – such as a text with a code sent to your smartphone, or biometrics using your fingerprint, face, or retina.

Limit user privileges: Use the principle of 'least privilege' – granting users the permissions to access only the systems, services and information that they need to fulfil their business role.

Limit the number of privileged accounts: Control the number of people who have administrative or highly privileged access. Accounts with a high level of privileges should not be used for high risk or everyday activities, for example web browsing and email. Administrators should use normal accounts for standard business use.

Monitor: Monitor user activity through the use of logs. Activity logs from network devices should be sent to a dedicated accounting and audit system that is separated from the core network.

Have training and education for employees: All users should be aware of the policies on proper account usage and their personal responsibility for following security policies.

How Microsoft Windows stops standard users from accessing privileged accounts through UAC

User Account Control (UAC) is a feature added to Windows. It is designed to improve security by limiting application software to standard user privileges until an administrator authorises a change. This way, only applications trusted by the user receive administrative privileges, which should keep malware from infecting the operating system. In other words, applications that the user runs do not automatically have administrative privileges unless they are approved beforehand or the user explicitly authorises it.

How to create a user access control system

Please read the following as it will help you to answer question 18.

To protect the privacy and integrity of information stored on a computer, it is important to control who can access the information.

Computer access is managed through user accounts. Each individual user of a computer signs in with their own account. Each user will also be assigned their own username and password. Usernames will often follow a set pattern. For example, first name.last name@companyname.com. Assigning usernames and passwords is usually the first step in creating a user access control system.

There are different levels of user account, such as administrator or user. The access level depends on the rights or permissions that are assigned to that account.

The system actions that a user can perform are governed by the type of account they sign in with. An administrator account has higher-level permissions than a standard user account, which means that an administrator account owner can perform tasks on a computer that a standard user account owner cannot.

Standard user account credentials allow a user to do things that affect only their own account, including:

- Change or remove the password.
- Change the user account picture.
- Change the theme and desktop settings.
- View files stored in their personal folders and files in the Public folders.

Administrator account credentials are necessary to do things such as:

- Create, change, and delete accounts.
- Change settings that affect all of the network's users.
- Change security-related settings.
- Install and remove apps.
- Access system files and files in other user networks.

Tasks that require administrator permission are indicated in dialog boxes by a Windows security icon.

One of the key reasons for setting up an access control system is to restrict the files and folders a user can access and what they can do with the files. The Windows platform uses NTFS permissions to set up this file access.

NTFS permission allow detailed control over the files and folders on the system. You can set NTFS permissions on a per file basis, as well as a per folder basis.

To set NTFS permission on a file, you should right click and go to properties then go to the security tab.

To edit the NTFS permissions for a User or Group, click on the edit button.

As you can see, there are a number of NTFS permissions, so let's review them individually. First, let's look at setting NTFS permissions on a file.

- Full Control allows you to read, write, modify, execute, change attributes, permissions, and take ownership of the file.
- Modify allows you to read, write, modify, execute, and change the file's attributes.
- Read & Execute will allow you to display the file's data, attributes, owner, and permissions, and run the file if it's a program.
- Read will allow you to open the file, view its attributes, owner, and permissions.
- Write will allow you to write data to the file, append to the file, and read or change its attributes.

NTFS permissions for folders have slightly different options. (adapted from How to Geek).

- Full Control allows you to read, write, modify, and execute files in the folder, change attributes, permissions, and take ownership of the folder or files within.
- Modify allows you to read, write, modify, and execute files in the folder, and change attributes of the folder or files within.
- Read & Execute will allow you to display the folder's contents and display the data, attributes, owner, and permissions for files within the folder, and run files within the folder.
- List Folder Contents will allow you to display the folder's contents and display the data, attributes, owner, and permissions for files within the folder.
- Read will allow you to display the file or folder's data, attributes, owner, and permissions.
- Write will allow you to write data to the file or folder's data and read or change its attributes.

Try it out

Set up access control on a network or operating system. Practise setting different permissions on the folders.

Knowledge Activity 7: Outline the steps you would take to create a user access control system. Include steps such as allocating usernames and passwords, and what types of actions the administrator would have permission for (such as blocking users from installing unauthorised software or applications and making system changes that affect security).

Firewalls

Please read the following as it will help you to answer question 19.

A firewall is a network security device that monitors incoming and outgoing network traffic and allows or blocks specific traffic based on a defined set of security rules. Firewalls establish a barrier between secured and unsecured networks, such as between a company server and the Internet. By blocking access to unsecured sites, a firewall can prevent malware from being accidentally downloaded.

In protecting private information, a firewall is considered a first line of defense; firewalls are generally designed to protect network traffic and connections, and therefore do not attempt to authenticate individual users when determining who can access a particular computer or network.

Software firewalls

Software, or host, firewalls include any type of firewall that is installed on a computer or server rather than a separate piece of hardware. The big benefit of a software firewall is that it’s highly useful for creating customised rules for what can be accessed.

Hardware firewalls

Hardware, or network, firewalls act in a manner similar to a network router to intercept data packets and traffic requests before they’re connected to the network’s servers. Physical firewalls like this excel at perimeter security by making sure malicious traffic from outside the network is intercepted before the company’s network endpoints are exposed to risk.

The major weakness of a hardware-based firewall, however, is that it is often easy for insider attacks to bypass them. Also, the actual capabilities of a hardware firewall may vary depending on the manufacturer – some may have a more limited capacity to handle simultaneous connections than others, for example, and this can slow down network access.

Some types of firewall

Most firewalls use one or more of the following methods to control traffic flowing in and out of the network:

- Packet filtering – Packets are small chunks of data. The firewall software analyses the packets based on a particular set of filters. Packets that meet the criteria are sent through and those that don’t are discarded.
- Proxy service – This is an early type of firewall that acts as a gateway between networks or between an internal and external network. Information requested from the Internet is retrieved by the firewall and then sent to the requesting system.
- Stateful inspection – Instead of examining the contents of each packet, this type of firewall compares key parts of the packet to a database of trusted information. If the packet matches the trusted comparison, the information is allowed through. Otherwise it is discarded.
- Application Gateway – This is a security mechanism that is applied to specific applications, such as Telnet and FTP servers. It secures the server but can slow down performance.
- Next Generation Firewall (NGFW) – A next generation firewall is a newer class of firewall. It filters Internet and network traffic based on the type of traffic and uses particular ports. NGFWs feature the basic functionalities of a standard firewall but can provide deeper and smarter inspection.

Did you know?

In Windows and macOS, firewalls are built into the operating system.

Functions of a firewall

Please read the following as it will help you to answer question 20.

An efficient firewall monitors both incoming and outgoing traffic. It also makes your computer 'invisible' when you're online, helping prevent attempted intrusions in the first place. Most firewalls are capable of continuously updating the list of malicious applications. This way, your computer's protection is always up-to-date. A firewall has a number of security functions, including:

- In packet filtering, the firewall acts as a type of gatekeeper that determines what can pass through, based on the network's rules.
- Acting as an application proxy, or application level gateway. In this case, the firewall can identify and stop malware.
- Preventing the loss of valuable information – for example, a firewall can be installed to manage File Transfer Protocol (FTP), so that users cannot accidentally send confidential files or data to anyone outside the network.
- Record User Activity – every time a user accesses data, they will go through a firewall, which then records this in the log files.
- Modifying incoming data package. Also known as NAT (Network Address Translation), this is a way to map multiple local private addresses to a public one before transferring the information. Organisations and home routers that want multiple devices to employ a single IP address use NAT. Using NAT allows information from a computer to the Internet to make it back to the computer using the router's public address, not the computer's private one.

Advantages and disadvantages of a firewall

Please read the following as it will help you to answer question 21.

Advantages of using a firewall

The main advantage of having a firewall in place is that it provides an additional line of defence against attacks.

The main advantages of a firewall are that they:

- **Monitor traffic** – A firewall monitors all of the traffic entering your computer network.
- **Detect malware** – Having a firewall can help keep malware out of your network.
- **Control access** – Firewalls have an access policy as well. You can either use a default access policy or customise the settings to match your needs.

Disadvantages of using a firewall

The main disadvantage is that they often require trained professionals to support their configuration and maintenance. If a firewall is not used properly, it could give a false impression that the network is safe. They also often cannot protect against an insider attack. Firewalls cannot protect against viruses once they are in the network, such as Trojans, worms and spyware that spread through flash drives and portable hard drives. They may restrict authorised users from accessing valuable services. They do not protect against backdoor attacks.

Knowledge Activity 8: What are some of the main advantages and disadvantages of a firewall for an employer and for employees?

What is network traffic?

Please read the following as it will help you to answer question 22.

Network traffic is the amount of data that moves across a network at any point in time.

Examples of network traffic could be:

- Uploading a file to Dropbox .
- Carrying out a webinar over Microsoft Teams or Zoom.
- Browsing the Internet.
- Downloading a file from a website.

- Sending and receiving emails.
- Uploading photos to Facebook.

Network traffic monitoring, or network flow monitoring, is a process for tracking what devices are connected to a network, what kinds of data the devices are accessing, and how much bandwidth each device is using. It is essential for network security teams to detect zero-day threats, attacks, and other anomalies that need to be addressed.

Large companies are where network traffic monitoring tools are most often used. At this size, businesses can have hundreds or even thousands of devices joined to the same corporate network. It's just too difficult to watch that many devices without help, and that's where network monitoring tools come in. With bandwidth monitoring, automatic alerting and report generation, network administrators responsible for ensuring the network is running smoothly can stay on top of all the traffic on a company's intranet with relative ease.

Summary

In this section, you have learned about:

- different routine ways of maintaining cyber security, including vulnerability testing and penetration testing
- the importance of security updates and patches
- user access control and methods of restricting user access
- how to set up a user access control system
- the use of firewalls

In this section, you will develop an awareness of team dynamics and understand how to communicate effectively within a cyber security team. You will also learn about different types of written communications used in cyber security.

Team dynamics

Please read the following as it will help you to answer question 23.

Team dynamics describes the behaviour and relationships between the people in a group. This could include how the interact, communicate and cooperate with each other. Teams that are able to do these things well can often accomplish more.

Team dynamics involves both psychology (for example, how well do people with different personalities work together) and practical issues, such as what types of written or verbal communication are most effective.

Team dynamics can also be impacted by company culture and structure, and by the senior management's leadership style, but the strongest influences often come from within the group itself.

A group with a positive dynamic and attitude to teamwork is often easy to identify. Team members trust one another, they work towards a group goal or decision, and they help each other to make things happen.

Recent research has also shown that when a team has a positive dynamic, its members are twice as creative as an average group.

In a team with poor group dynamics, people's behaviour may disrupt work. Because of this, the group may not come to any final decision, or it may make the wrong choice be inefficient or unproductive, or make poor choices, because group members did not work together.

Some causes of poor team dynamics

Group leaders and team members can contribute to a negative group dynamic. Some of the ways in which this can occur are:

- **Weak leadership**: When a team lacks a strong leader, more dominant members can compete to take charge. This can lead to a lack of direction, infighting, or a focus on the wrong priorities.
- **Too much deference to authority**: This can happen when people want to be seen to agree with a leader, and therefore hold back from expressing their own opinions.

- **Blocking**: This happens when team members behave in a way that disrupts the focus of the group. Blocking behaviour includes:
    - Being aggressive, disagreeable or inappropriately outspoken.
    - Being highly critical of others' ideas.
    - Not participating in the discussion.
    - Being boastful or dominating the session.
    - Using humour at inappropriate times.
- **Free riding**: Some group members take it easy, and leave their colleagues to do all the work. Free riders may work hard on their own, but limit their contributions in group situations; this is also known as "social loafing."
- **Groupthink**: This happens when people place a desire for agreeing above their desire to reach the right decision. This prevents alternative solutions from being fully explored.
- **Evaluation apprehensio**n: This happens when people feel that they are being judged very harshly by other group members, and they hold back their opinions as a result.
- **Micromanagement**: When team leaders or managers make all the decisions for the group, causing team members to stop putting in effort as they feel nothing they do will have any influence.

Some strategies for strengthening group dynamics

- Know your team.
- Tackle problems quickly with good feedback.
- Define clear roles and responsibilities.
- Break down barriers.
- Focus on communication.
- Pay attention.

Team dynamics in a formal setting compared to an informal setting.

In a formal group, the relationship between the members is very professional. Formal groups tend to have stated goals, timelines for achieving these goals and a clear and defined plan for success. For example, a team may be set up to identify future market opportunities. This will be done through a planned process that involves assigned roles and duties. Formal teams may work very efficiently, but there may be fewer opportunities for creativity and to introduce new ideas.

Informal groups tend to be less planned. The lack of formal structure may mean that personalities play a larger part in how work is accomplished. Informal groups may be very creative and innovative, but can sometimes fail to make progress because it may be difficult for them to make decisions.

Knowledge Activity 8: Think about a time when you worked in a team and were impacted by poor team dynamics. What were some of the consequences and how might they have been prevented?

Find Out More: Research how team dynamics work in formal and informal settings.

Team working versus working alone

Please read the following as it will help you to answer question 24.

Good teamwork skills can be critical for success in both professional and personal ventures. There will be times where you will have to work with someone else to achieve a goal. When this happens, it is important that you have the skills needed to work effectively with others.

Some benefits of working with others:

- Group members compensate for each other's weaknesses and share broad perspectives
- Greater opportunity to learn from others
- Make it easier to share ideas and brainstorm, so there is a greater opportunity for creativity and innovation
- Workloads and large tasks can be shared, often making them go faster
- Opportunity to improve communication skills and develop better relations and networking with colleagues

Some benefits of working alone:

- Fewer distractions
- Greater efficiency
- No conflicts or personality clashes
- No need to share responsibility
- Fewer meetings and other events that can decrease productivity
- More control over how and when you work and over project management

Ways in which team members can work together to make use of individual strengths

Please read the following as it will help you to answer question 25.

Within a team setting, it is still important that team members work to their own strengths. It is the bringing together of these individual strengths which makes a team successful.

Individuals who know their strengths tend to create more effective teams.

When team members value each other's strengths, they more effectively relate to one another, avoid potential conflicts, boost group working and create positive discussions.

Here are some ways that team members can make use of individual strengths:

- Discuss the strengths and weaknesses of individual team members, so that all team members can help each other and work to their strengths
- Plan projects around the individual strengths of each team member
- Pair up team members who are strong in one area with members who are weaker in that area, so the weaker member can learn new skills
- Analyse project performance to identify the strengths and weaknesses of each team member
- Team members who are strong in one area can offer training in that area

Solving team conflicts

Please read the following as it will help you to answer question 26.

Conflict is pretty much inevitable when you work with others.

This is because everyone has different views, and sometimes those differences escalate to conflict. How you handle that conflict determines whether it works to the team's advantage, or ends up damaging the team.

Conflict isn't necessarily a bad thing. Healthy and constructive differences are often a part of teamwork. Conflict can arise when people have varying views, experiences, skills, and opinions. Team members should be aware of these differences and not let them lead to full-blown arguments.

Here are some steps that can help resolve conflict effectively:

- **Acknowledge the conflict** – The conflict has to be recognised before it can be managed and resolved. Usually people ignore the first signs of conflict, perhaps because they hope it will just resolves itself. If you are concerned about conflict in the team, discuss it with the other members. Once the team recognises the issue, it will become easier to resolve.
- **Discuss the impact** – As a team, discuss the impact of the conflict on team dynamics and performance. When everyone understands the damage conflict is having on the team and the project, people may be more willing to work towards resolving the issue.
- **Agree to a cooperative process** – Everyone involved needs to work together to resolve the conflict. This may mean setting aside individual opinions or ideas for the time being and returning to them later, once things have cooled down.
- **Agree to communicate** – The most important thing is for communication to remain open. Active listening is an important tool for having constructive conversations, as it helps everyone to understand where the other person is coming from.

Sometimes team members simply need to have their problems heard and discussed by the rest of the team. By looking at the argument together, the team can move forward in agreement.

Resolving conflict when it does arise in a quick and efficient fashion helps maintain a strong and healthy team environment. Remaining open to differing beliefs and ideas is vital, and learning to view conflicts from a co-worker's perspective will help you become a more effective team member.

Knowledge Activity 9: Think about a time when you have been in conflict with someone else. How could you have resolved the conflict in a constructive way?

Importance of reviewing work activities

Please read the following as it will help you to answer question 27.

Reviewing is the process of going back over the work that has been completed and ensuring it is still fit for purpose and meets the objectives set out at the start.

This process allows team members to identify whether tasks are on track and whether key targets have been met.

It also allows the team to identify what has gone well and what could be improved.

Reviewing is vital in ensuring the best quality work is produced within the timescales set.

Reviewing helps ensure that everyone is working to the same common goal. Work can sometimes veer off-track, and a regular review helps ensure everyone is moving towards the correct end point.

Sometimes a task may be allocated to someone who may not be the most effective. A review of work tasks helps ensure the right people are chosen and work is reallocated when not.

The use of interpersonal skills for working in cyber security

Please read the following as it will help you to answer question 28.

We all use interpersonal skills every day. Interpersonal skills describe how we communicate or interact with other people.

Lots of skills can be defined as interpersonal, including our awareness of ourselves and others; caring about others; collaborating and working with others; having clear communications; conflict management and resolution skills.

Employers often actively look for applicants who can work collaboratively, communicate effectively and have positive relationships with customers and co-workers.

Even if you have a very technical job, such as an IT role, you will need to interact with colleagues or clients regularly, often providing complicated information or having to listen carefully to requirements. Having excellent IT skills on your CV won't necessarily be enough to get you the job.

IT professionals need to be able to interact successfully with others, as well as manage projects and teams.

Some key interpersonal skills

1. Work Ethic – Having a strong work ethic is viewed favourably by many organisations. This can be split into three distinct aspects:

- Professionalism – This incorporates everything from how you present yourself to your appearance and how you treat others.
- Respect – All workplaces will require you to work under pressure at some time or another, and being able to remain calm and respectful under pressure is vital.
- Dependability – Employers and team members need to know they can count on you. This includes being on time, being prepared and delivering the work when you say you will.

2. Verbal communication skills – Being able to have clear conversations with other staff, managers and customers is essential to being an effective worker. This could include being a good listener, carrying out excellent presentations to customers, or working with other team members effectively.

3. Questioning - Knowing when to ask questions, and what questions are important to ask is an important interpersonal skill. You should not be afraid to ask questions, but you should also make sure that you are asking in an effective way, so that you receive the answers you need.

4. Giving information - Working effectively with others will often include a willingness to help out team members and clients with answers to questions or practical help. This will create a spirit of collaboration.

6. Clarifying - This includes not being afraid to ask for clarification, as well as being willing to give clarification when asked for it. This may also include showing someone how to do something.

7. Giving and receiving feedback – Being open to feedback can help you develop both personally and professionally. View all feedback as a chance to learn. When giving feedback, it is important to focus on being constructive rather than negative.

8. Listening – Failure to listen properly can have disastrous consequences, from failing to follow through on a manager's instructions to not completing a customer's request.

Active listening signals to others that you are taking what they say seriously and are willing to learn from them. It includes giving non-verbal signals, such as nodding and maintaining eye contact. This will build trust as the people you are collaborating with will feel heard.

9. Collaboration – Working collaboratively increases productivity and helps deliver better outcomes. Being able to collaborate, particularly in challenging situations, is a real positive for employers and yourself. It shows a clear, positive attitude and an enthusiasm for team working.

10. Conflict management – This is an important skill, especially for those looking at leadership roles.

This includes being able to put your views across, or defend the views of others, in a professional and respectful way.

11. Positive attitude – Showing positivity, even in difficult situations, is important.

It is best not to say anything negative about your current or past employer or colleagues even if you feel strongly about it.

Employees with a positive attitude also tend to treat others positively, which creates a more harmonious and friendly working environment.

12. Putting across your own views clearly and appropriately – How you come across to others can speak volumes. Demonstrating kindness and courtesy is a great way of developing long lasting relationships with colleagues and managers.

Knowledge Activity 10: Choose five of the interpersonal skills listed here and give examples of each one.

Examples of when interpersonal skills are used in cyber security

Please read the following as it will help you to answer question 29.

Verbal and non-verbal communication skills

As an IT employee, you often have to explain technical processes in clear, easy-to-understand terms to customers and colleagues. Many of these people may not have the same level of technical knowledge as yourself. You may also need to promote security practices to diverse audiences. All these activities require verbal and written communication.

Having good written and verbal communication skills will make this much easier. Focus on how to explain your ideas both clearly and concisely – without adding un-needed descriptions or jargon words.

Collaboration

Solving security problems doesn't happen in a vacuum, and it is likely that you won't always have all the answers. There will be many situations, such as an urgent malware attack or the need to develop an entire security system, when you will need to work with others in a team. For example, the problem or task may be too large for one person to manage alone, or you may not have all the skills needed to tackle it. In this case, you will need to be able to collaborate with others and work in a team to solve the problem.

Questioning

The field of cyber security is always changing, as new threats and new solutions come along. This means that you will always be learning new things in your work. It is important to remember that you may not have all the answers, and you should be willing to ask questions and seek advice from those with more experience.

The same is true for helping others by giving information. As an IT expert, clients and co-workers will look to you for help and information. A willingness to help others is an important interpersonal skill.

A detail-oriented work ethic

Steve Jobs once said, "Details matter; it's worth waiting to get it right." He once left an urgent voicemail on a Sunday morning for Vic Gundotra, Google senior vice president. The second O in Google's logo on the iPhone was the incorrect shade of yellow, and Jobs wanted it fixed immediately.

In cybersecurity, the wrong logo colour may not be your responsibility, but many other small details might be. You will need to be detail-oriented to find the root of a data breach or analyse thousands of logs after an attack. Sometimes, you will have to do these things while working fast under pressure.

Listening

In cyber security, listening is an important part of paying attention. For example, using active listening can help you to understand why someone may be likely to click on a link in an email, and can help you to analyse problems and search for solutions.

Giving information

Technology is always changing, and cyber criminals are always adapting and coming up with new ways of breaking into systems. Because of this, as a cyber security expert, it is very important that you are always learning new things. There will be many times when you will rely on someone else to give you information, and so it is very important that you are also willing to give out information that can help others.

Respecting others' opinions and views

In cyber security, you never know where a good solution to a problem will come from. So, it is important to always listen to and respect the opinions of others.

Giving and receiving feedback

This is an excellent way to learn what areas you need to learn more and to help others to improve their knowledge as well. As we said above, cyber security professionals are always learning, so it is important for them to be aware of what they do not know.

Clarifying

Any time you are working in a technical field like cyber security, there will be times when you will need clarification or to have something explained in more detail. The same is true for those you work with. Many of your colleagues will not be knowledgeable about technical subjects, so you will need to clarify things for them so they can understand.

Putting across your own views clearly and appropriately

You will often be working with managers, clients and colleagues. This makes it important to put across your own views in a way that is appropriate and which other people can understand – no matter what their level of technical knowledge and experience. One way to do this is to always treat others with respect.

Working with others within an organisation to support cyber security

Please read the following as it will help you to answer question 30.

Effective cybersecurity requires that every individual, and every part of the organisation, actively participates.

Effective IT departments can establish excellent policies and processes. But it takes only one mistake to give a cyber criminal the opening needed to cause a potentially disastrous breach.

Clicking on links in phishing emails, opening attachments from unknown senders, using weak passwords – these are just some examples of how individual team members' actions can create vulnerabilities.

Educating employees and then regularly reviewing their individual responsibility can go a long way towards reducing the organisation's risk.

True cybersecurity teamwork requires that every individual within the organization be responsible for ensuring they understand and follow the procedures set out by the cybersecurity team. All individuals and all groups need to work together as a team. This includes not just working with the members of your team, but also with other teams, sections or departments. In order to avoid problems when working with other teams, it will be important for you to find different ways of communicating, to suit different people. For example, you may need to simplify technical information for some people.

Teamwork and communication can ensure cyber threats are identified quickly and potential issues can be acted upon.

The purpose of written communications in cyber security

Please read the following as it will help you to answer question 31.

As a cyber crime specialist, writing reports is an important part of your role. These may be viewed by your manager or by clients, and may even be used by the police, legal authorities, and perhaps even as evidence in a court of law, depending on the circumstance. Therefore, it is important that they are written clearly, efficiently and professionally. Communicating effectively in writing is essential in the IT industry. Within cyber security, there are numerous different types of written communication used. It is vitally important that the written communication is of a high standard, clear, detailed and fit for purpose.

Common types of written communications include a wide range of reports and fault logs. Reports specific to the cyber security profesison include:

- vulnerability reports
- penetration testing reports
- incident reports
- internal policy documents specific to to cyber security

The potential audience for the written communications used

Please read the following as it will help you to answer question 32.

Knowing or anticipating who will be reading what you have written is key to effective written communication.

The first question to ask is, “Who am I writing this for?” The answer to this question may not always be obvious.

In an IT role you may produce written communication for a wide range of people including;

- line managers
- senior management
- team members
- external clients or suppliers
- all staff

Within the workplace, it is important to use the correct tone, language and level for your audience. For example, an annual report written on behalf of a large corporate organisation would be extremely professional in terms of its writing style, as it is read by investors. However, an email to a colleague notifying them of when you will install new software on their computer can be short and more informal.

As an IT professional, you also need to be aware of the level of information you need to provide. For example, not everyone will be able to understand complex technical details - you will need to know when to simplify your language and when you can use technical jargon. For example, explaining the inner workings of the security systems may be an information overload for someone requesting a password reset.

For an IT professional, it is important that the level of language used is relevant to the audience. The IT industry has always contained a lot of terminology and abbreviations, and whilst this may make a lot of sense to other IT professionals, non IT experts may struggle to understand the concepts if the language is not adapted to meet their needs. To get a clear message across, always make sure the level of language meets the needs of the audience.

In an IT role, you will have a wide range of audiences and will need to adapt your writing for each.

Typical Audiences could be:

Audience	Language	Level of IT language
Colleagues in your IT department	Usually Informal	You can use technical language.
Colleagues in other departments	Informal / Formal depending on reason	Use limited jargon and offer clear explanations
Line managers	Formal	This will vary by manager, but try to keep language clear and concise.
Clients	Formal	Use clear and concise explanation, but technical terms are usually ok.
Suppliers	Formal	Technical terms and jargon is fine and often expected.
Government bodies / agencies	Formal	This varies by agency, do not assume a high level of knowledge and check first.
Other IT professionals in other organisations	Informal / Formal depending on reason	Technical language and jargon is expected.
Visitors to the organisation	Formal	Explain terms clearly and simply.

Knowledge Activity 11: Imagine that you are writing a report for each of the following: line manager, senior manager, team member, all staff. What types of information and language would you include in each case?

The type of information that may be included in written communication

Please read the following as it will help you to answer question 33.

Vulnerability reports

The purpose of a vulnerability assesment is to review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends solutions, if needed.

The vulnerability report sets out the key findings of the vulnerability assessment. It details the organisations IT assets, security flaws, and the overall risk with regards cyber security.

Vulnerability reports are often reviewed by senior management teams and it is important that they are written clearly and set out the details of any problems and recommended solutions in a clear and understandable way.

Penetration testing report

A penetration test report details the finding of the penetration test, a simulated cyber attack against a computer system which checks for exploitable vulnerabilities.

An effective penetration testing report should include an executive summary, a detailed report, and the raw data from the tests. The executive summary should be a very brief overview of the major findings, of around two pages in length. The detailed report will include a comprehensive list of the findings and proposed solutions. The final section of the report usually includes the technical details and raw output from each of the tools used in the tests.

The penetration test report will be read be people with some technical skills and understanding, such as IT managers, security experts, and network administrators, so it can be written in more technical language.

Incident report

Many organisations record cyber security incidents in some form of database, ranging from ticketing systems to excel spreadsheets or in-house software.

The cyber security incident database will contain details of any incidents that are investigated by the security team. Each incident will have information about when it was created and closed, who the investigator was, incident information and impact, etc.

For most incidents, these reports tend to be quite short, so they should be written in a very clear and concise way.

Internal policy documents

Internal policy documents relate to the day-to-day administration of an organisations' internal policies, procedures and rules. For example, a cyber security professional may have responsibility for writing a policy document on how employees should report or respond to a suspected phishing attempt. Other types of internal policy documents might include a company email use policy or an IT use policy.

These documents are often read by all employees, including those without a high level of technical knowledge, so they need to be clear, easily read, and provide the right level of information to those who are reading them.

The elements that support effective written communications

Please read the following as it will help you to answer question 34.

While written communication skills share many of the same features as verbal communication skills, there are some important differences. Where verbal communication uses body language and tone of voice to express meaning and tone, written communication relies on grammar, punctuation and word choice. Developing effective written communication skills requires practice and attention to detail.

In professional settings, great written communication skills are made up of a number of key elements. These include:

- Having a clear purpose
- Having a clear message
- Information should be accurate
- The correct use of spelling, grammar and punctuation
- Layout (use of headings, section numbers, bullet points etc)
- An attention to detail
- Using the right tone of voice for the intended audience

Clear purpose

Having a clear purpose helps your reader understand what you are saying or, at least, understand enough to know what questions they need to ask for further clarification. Writing in simple language and using shorter sentences can convey information with clarity.

Example: "We are implementing a new email policy to ensure that all employees can confidently rely on our email systems. See the details of the new policy below. If you have any questions, you may direct them to the head of IT."

In this example, the writer sets out the goal of the message right away, then mentions the reason for the policy change and provides simple instructions to follow for further clarification.

Clear message

It is important that your audience can easily understand what you are saying. Make sure that your writing does not contain a lot of ambiguous or confusing statements and that it is clear what you are saying or asking for. One way to do this is to keep sentences and paragraphs short, and to use bullet points.

Accuracy

This is especially important in cyber security, where you may be dealing with very important or complicated issues that can have legal consequences. Check your statements for accuracy and make sure that any opinions are clearly labelled as opinions (for example, by writing, “In my opinion …”). It is also easier to be accurate if you keep your sentences short and clear. Try to avoid embellishing factual statements with too much jargon.

Attention to detail

This is vital in every aspect of cyber security, including written communications. In your reports, break problems down into smaller components and write about these individually. Attention to detail also includes elements such as making sure you have checked your spelling, double-checking any facts and figures used, and addressing your writing to the correct audience. It is very easy to get into trouble by sending emails to the wrong address, or by hitting “reply all”.

Correct use of spelling, grammar and punctuation

Don’t assume that a spellcheck has caught every error – always read over your written communications before you send them. For longer, or formal reports, it can also be helpful to have a colleague look over it and make sure it reads well. Sloppy spelling, grammar and punctuation can make you look unprofessional and change the meaning of your words to something you have not intended.

Tone of voice

This refers to the language that you use, the writer’s attitude toward the reader and the subject of the message.

When writing, it is important to adjust your tone according to the circumstances. For example, in more formal types of communication, you need to know when to be direct, assertive, conversational, encouraging or apologetic, depending on the situation.

To set the right tone for your work-related writing, you should first ask yourself:

- What is the purpose of this document? Why am I writing it?
- Who is my reader, and what do they need to learn from my writing?

For most business messages, it is safest to use a more formal tone, a tone that is confident, courteous, and sincere. Your writing should always use non-discriminatory language, and write at an appropriate level of difficulty for the audience.

Some general guidelines to keep in mind when considering what kind of tone to use include:

- Be confident.
- Be courteous and sincere.
- Use appropriate emphasis and subordination.
- Use non-discriminatory language (for example, don't use words like 'manmade' or assume your reader is a man.)
- Stress the benefits for the reader.
- Write at an appropriate level of difficulty.

Layout

This is most important when you are writing longer documents. A huge mass of text can be very off-putting to readers. In order to engage readers and keep their interest, break up your text with headings and sub-heading, section numbers, bullet points and other organising features. Make sure you choose a font and size that is simple and easy to read. Overly ornate fonts or very large font sizes do not look professional. When in doubt, keep it simple and use frequent headings and subheadings to organise your work.

Did you know?

Small errors, big payout

Even small errors can have big consequences.

In 2014, three truck drivers sued their employer for four years' worth of overtime pay, based on a misplaced comma.

The law involved required time-and-a-half pay for each hour worked after 40 hours, but it set out exemptions for: The canning, processing, preserving, freezing, drying, marketing, storing, packing for shipment or distribution of:

(1) Agricultural produce;

(2) Meat and fish products; and

(3) Perishable foods.

The problem was that it was not clear what followed the last comma in the first sentence: "packing for shipment or distribution of." A court ruled that it was not clear whether the law exempted just the distribution of the three categories, or if it exempted packing for the shipment or distribution of those categories. Had there been a comma after "shipment," the meaning would have been clear.

The missing comma cost the company $5 million in overtime pay.

Source: **https://www.nytimes.com/2018/02/09/us/oxford-comma-maine.html**

Summary

In this section, you have learned about:

- Team dynamics and working with others
- Ways to resolve conflict in a team
- Different types of interpersonal skills and how they are used in cyber security
- Different types of written communication used in cyber security
- How to create effective written communication

Section 4: Extension activities

Further your knowledge and understanding of the topics in this workbook by completing the following extension activities.

Extension Activity 1: Research different types of malicious software or attacks that are not discussed in this workbook.

Extension Activity 2: Research some different ways of removing malicious software from computers and networks.

Extension Activity 3: Research some of the best practice methods of maintaining cyber security.

Extension Activity 4: Research ways of creating a user access control system using Cloud software.

Extension Activity 5: Research some of the different elements of team dynamics.

Extension Activity 6: Research the most important interpersonal (soft) skills needed for cyber security professionals.

Extension Activity 7: Research some examples of the most common grammar and punctuation errors.

Well done!

You have now completed Workbook 2 and should attempt the assessments. If you require any help or guidance, please contact your Assessor/Tutor.

Please use this page for additional notes

Disclaimer

Every effort has been made to ensure that the information contained within this learning material is accurate and reflects current best practice. All information provided should be used as guidance only, and adapted to reflect local practices and individual working environment protocols.

All legislation is correct at the time of printing, but is liable to change (please ensure when referencing legislation that you are working from the most recent edition/amendment).

Neither Learning Curve Group (LCG); nor their authors, publishers or distributors accept any responsibility for any loss, damage or injury (whether direct, indirect, incidental or consequential) howsoever arising in connection with the use of the information in this learning material.

NCFE is a trading name of NCFE (registered company number 02896700) and NCFE; Council for Awards in Care, Health and Education; and NNEB are registered trademarks owned by NCFE. NCFE has exercised reasonable care and skill in endorsing this resource, and makes no representation, express or implied, with regard to the continued accuracy of the information contained in this resource. NCFE does not accept any legal responsibility or liability for any errors or omissions from the resource or the consequences thereof.

If you have any queries, feedback or need further information, please contact:

Learning Curve Group
1-10 Dunelm Rise
Durham Gate
Spennymoor, DL16 6FS
info@learningcurvegroup.co.uk
www.learningcurvegroup.co.uk

This resource has been endorsed by national Awarding Organisation, NCFE. This means that NCFE has reviewed it and agreed that it meets the necessary endorsement criteria.