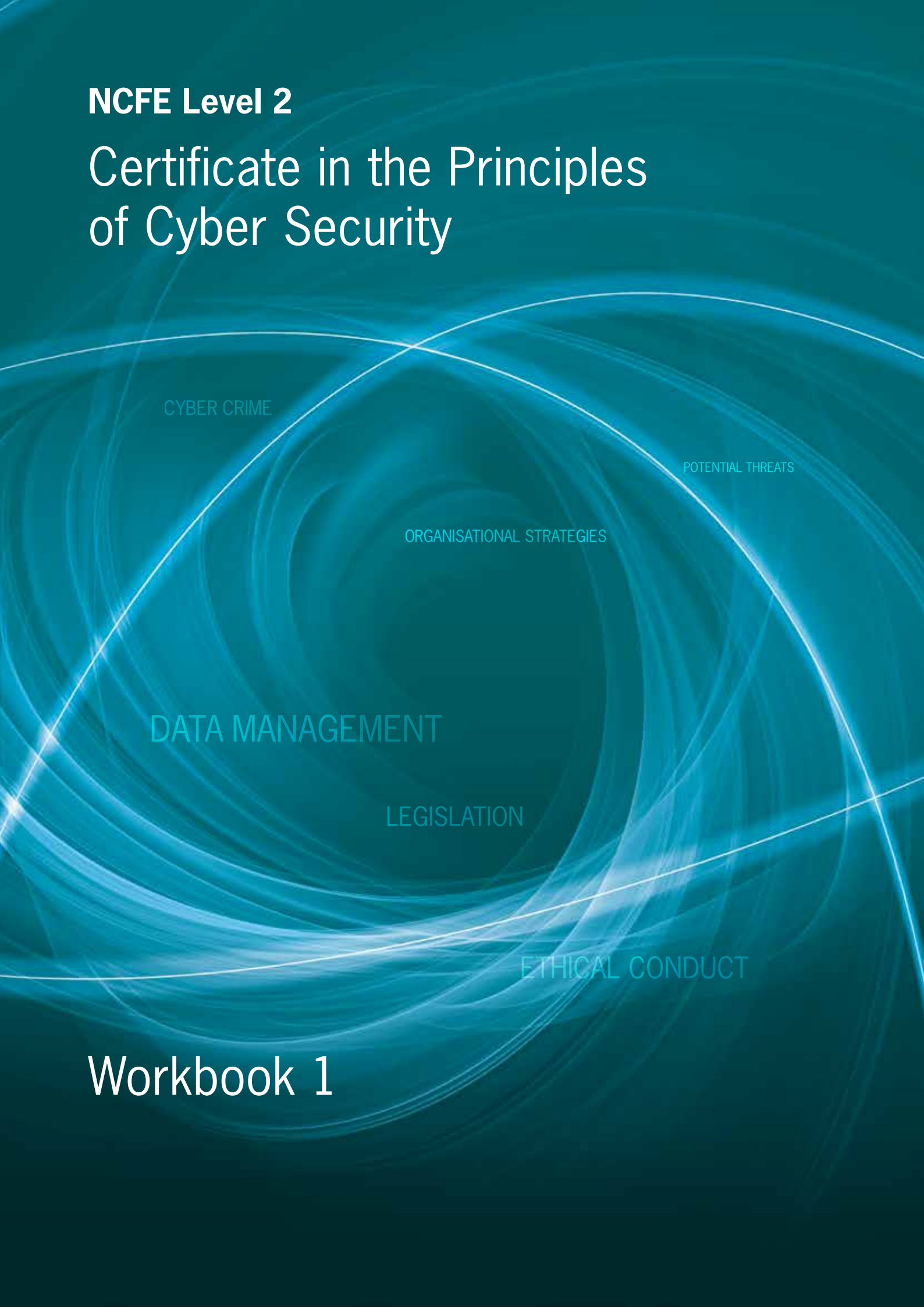
NCFE Level 2

Certificate in the Principles of Cyber Security



Workbook 1

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 1

Workbook Contents

In this workbook you will learn about the roles and issues relating to Cyber Security. You will gain an understanding of cyber security and the impact that cyber crime can have on individuals, businesses, and nations. You will develop an understanding of the motivations of cyber crime and where potential threats can come from. You will also investigate various job functions in the sector and identify the key skill requirements.

Contents

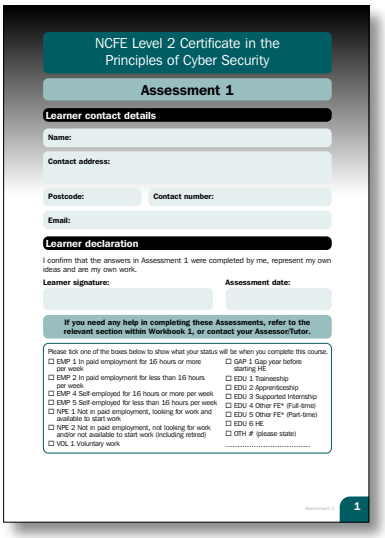
This workbook contains four sections:		Page
Section 1:	Introduction to cyber security	4
Section 2:	Understand industry terminology used in cyber security	37
Section 3:	Understand legal and ethical aspects of cyber security	64
Section 4:	Extension activities	90

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 1

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 1

Learner contact details

Name:

Contact address:

Postcode:

Contact number:

Email:

Learner declaration

I confirm that the answers in Assessment 1 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 1, 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)

.....

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 cyber security and the impact that cyber crime can have on individuals, businesses and nations. You will understand the motivations and reasons as to why cyber crime can occur and where potential threats can originate from. Finally, you will understand how attacks can be both targeted and untargeted.

What is 'cyber crime'?

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

Cyber crime can be classed as any criminal activity which involves a computer, networked device or a network. Most cyber crimes are undertaken in order to generate profit for the people behind the attacks – the cybercriminals.

The majority of cyber crimes are carried out against computers or devices such as printers and routers directly. Cybercriminals also use computers or networks to spread malware (software designed to damage or gain unauthorised access to a computer system), images and illegal information.

Cyber crime can be carried out by individuals or small groups. However, recently there have been a significant number of attacks carried out by highly organised criminal groups. These groups usually include skilled software developers and others with relevant expertise. One reason that cyber crime is difficult to stop is that cybercriminals are able to carry out attacks from anywhere in the world.

Types of cybercrime

There are many different types of cyber crime, and most cyber crimes are carried out with the expectation of making substantial amounts of money for the people carrying out the attacks.

For legal purposes, there are three broad types of cyber crime:

- Cyber Dependent Crimes, where criminals use digital systems to attack digital targets. These include attacks on computer systems to disrupt IT infrastructure, and stealing data over a network using malware. The purpose of the data theft is usually to commit further crime.
- Cyber Enabled Crimes, which are 'existing' crimes, such as fraud, extortion and identity theft, that have been transformed by the use of the Internet. In many cases, the use of the Internet allows these crimes to be carried out on a very large scale.
- The use of the Internet to enable crimes such as drug dealing, people smuggling and other 'real world' types of crime.

Did you know?

The first person convicted of a cyber crime was Ian Murphy, aka 'Captain Zap', who was convicted in 1981 of hacking into the AT&T telephone network and changing the internal clock to charge off-hour rates at peak times. He was sentenced to 1,000 hours of community service and 2.5 years of probation. He was the inspiration for the 1992 movie *Sneakers*.

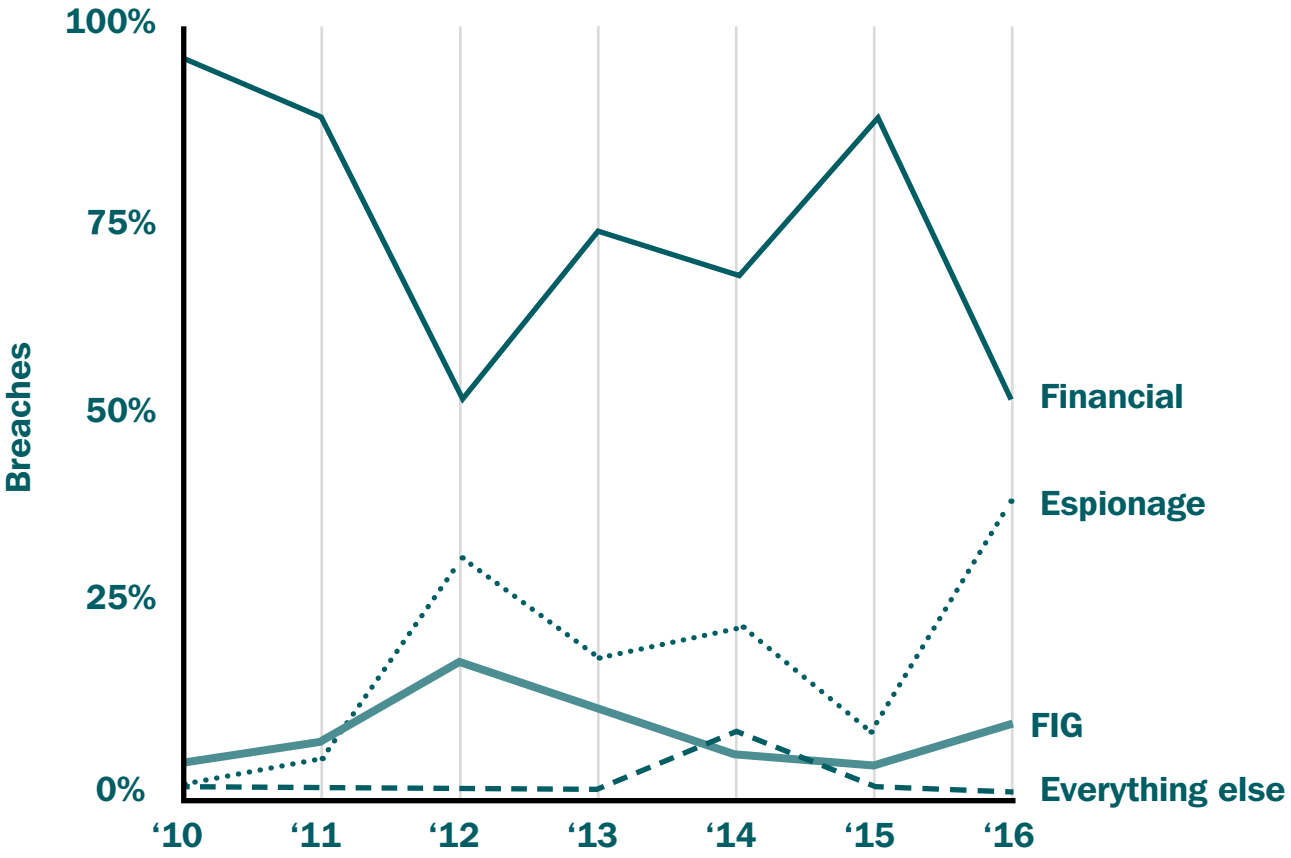
Motives behind cyber crime

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

Cyber crime has increased greatly, partly because committing crimes online makes it easy for the criminals to hide their identity and location, which can be anywhere in the world that has an Internet connection. This makes it challenging for police and other law enforcement agencies to locate them, but to further complicate this, different countries have different laws and bringing cyber criminals to justice often involves cooperation between countries.

The key motivations for cyber criminals are money and information. According to a Verizon Enterprise report, around 93% of attacks are motivated by reasons related to financial motivation and corporate or government espionage (spying). Another less frequent but broader set of motives is often categorised as 'FIG' (Fun, Ideology, and Grudges).

The graph below shows the main motives for cyber criminals between 2010 and 2016.



Source: **https://www.vircom.com**

Some motives for cyber crime include:

Money

This can be the motive for many types of attacks and data theft. The cyber criminal will make money either by stealing from the victim directly, or by selling stolen data in underground marketplaces.

Competition

Gaining access to a business competitor's data can be very valuable. Many attacks are aimed at stealing IP (Intellectual Property) such as blueprints, designs for new technology or research. However, competitors also carry out attacks for blackmail, to gain the upper hand in a specific market or to create bad PR for a competitor.

Organisations that have intellectual property at the core of their business, such as pharmaceuticals, high tech manufacturing, mining or utility companies, are especially vulnerable to attacks from competitors.

Political motivation

In recent years, cyber crime has also been used for political reasons. This may take the form of actions such as attempting to manipulate elections, inserting malware or 'spyware' (software that allows a user to gain information from another computer by transferring data secretly from their hard drive) into government systems or hacking the personal accounts of government members to learn information.

Personal reasons

There are a wide range of personal reasons why people may attempt cyber crime. Some criminals just enjoy the challenge of finding and exploiting weaknesses in systems and software. Other people may do it for ideological reasons, for revenge or to expose sensitive information which they think is of interest to the public.

Did you know?

The cost of cyber crime in the UK is estimated to be around £27bn per year. A significant proportion of this cost comes from the theft of IP from UK businesses, which is estimated at £9.2bn per year. Worst-case scenarios, however, put the real impact of cyber crime much higher.

Source: **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf**

Examples of cyber crime attacks:

WannaCry virus attack, 2017

The WannaCry ransomware attack was a global attack where users' files were held hostage, and a Bitcoin ransom was demanded for their return.

Cybercriminals took advantage of a weakness in the Microsoft Windows operating system to gain entry to as many as 300,000 computers in 150 countries.

Thousands of NHS hospitals and surgeries across the UK were affected. The attack on the NHS was stopped by a 22-year-old former hacker turned cyber security expert who managed to find the 'kill switch' in the code and slow down the attack.

The attack was estimated to have cost the NHS £92 million, with global costs from the attack at around £5 billion.

A patch that could have stopped the attack had been released by Microsoft about two months earlier, but many users never downloaded it.

One billion user accounts stolen from Yahoo, 2013

In one of the largest cases of data theft in history, Yahoo had information from all of its three billion user accounts stolen.

Personal information including names, phone numbers, passwords and email addresses were taken from the Internet giant.

Yahoo claimed at the time that no bank details were taken, and only released information about the breach in 2017.

It was the second time Yahoo had suffered a major breach, after the accounts of nearly 500 million users were accessed in 2014.

Who carries out cyber crime?

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

Threat actors

Definition of a threat actor

In cyber security, a threat actor is a broad term for any individual or group of individuals that attempts to conduct malicious activities against individuals or enterprises, whether intentionally or unintentionally.

Threat actors can be internal or external to the organisation being targeted.

Threat actors with the technical skills to target and breach security networks often fall into the category of hackers, but the term threat actor is broad and also includes security incidents initiated through negligence, mistake or social media.

Types of threat actors:

- Individual – This can include both insider and outsider actors. Individual cybercriminals may be motivated by gain or revenge. Some are employees who may carry out cyber crime intentionally, or unintentially through negligence, accident or incompetence.
- Outside actors – Individuals acting alone, for either money or revenge. These are a much smaller threat than organised crime as they usually lack the resources for mounting wide-spread attacks.
- Inside actor – These are people who already have access to sensitive data or processes from their work. They may be acting out of desire for money or revenge, or they may simply be careless or negligent. Insiders are less likely to trigger red flags or to cause alerts until it is too late.
- Organised crime – These are often highly sophisticated organisations who are motivated by profit. They usually target data that has a high value on the dark web, such as banking information, and also engage in ransomware attacks. These organisations may be quite large and will invest in technology and automation to improve their reach and scope.
- Company – These may target other organisations, attempting to steal business secrets in order to gain a market advantage.

- Nation – Actors sponsored by nation-states tend to be sophisticated and well-funded. They may carry out large-scale attacks or advanced persistent threats – stealthy attacks whose purpose is to gain long-term access to sensitive data. They may be motivated by gain, but are more usually motivated by national security, gaining IP data, political espionage, or attempts to influence the political process.
- Hacktivist – Hacktivists are politically, socially, or ideologically motivated and target victims for publicity or to effect change, and often plan high profile operations.
- Script kiddie – These are actors who lack skills to write their own code, so they rely on scripts they have acquired from other sources. They may be motivated by peer competition, mischief or for gain, and their attacks are not very sophisticated, often being limited to defacing websites or launching denial-of-service attacks (DoS). These are attacks meant to shut down a machine. DoS attacks work by flooding the target with traffic, often from computers that have been 'hijacked' using malware.
- A hacker is any skilled computer user that uses their technical knowledge to overcome a problem. While 'hacker' can refer to any computer programmer, the term is most often used to refer to someone who uses their technical knowledge to access 'secure' systems and networks.

Did you know?

In the UK, it is estimated that around 88 percent of businesses have suffered some form of data breach in the past 12 months, with a small business being hacked every 19 seconds on average.

Globally, cyber attacks are occurring constantly. In 2020, more than 267 major public institutions were breached by cyber attacks that included:

- a cyber attack on Norway's parliament
- an infiltration of Canada's Justice Department
- a malware infection of Chile's Banco Estado
- hacking of servers belonging to Chinese tech giant Alibaba
- malware infecting India's National Informatics Centre
- ransomware attacks on Newcastle University, Argentina's border agency, Pakistan's largest power utility K-Electric, Spanish bank SegurCaixa Adeslas, Clark County School District, French container line CMA CGM
- data breaches of the Belarus Ministry of Internal Affairs, University of Tasmania, and Australia's Department of Foreign Affairs and Trade

Source: **https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019**

Knowledge Activity 1: Describe the following types of threat actor and the danger they represent to individuals and companies:

- individual
- company
- nation
- hacker
- hacktivist

External and insider threats

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

Cyber threats may be internal or external. An external threat may be much trickier to identify as it comes from someone that does not have authorised access to the data and has no formal relationship to the company. These threats could be from someone who is actively trying to carry out a cyber attack on the company or it could have been triggered accidentally from someone who saw an opportunity, perhaps by finding or stealing a company computer or mobile phone. Threats coming from outside the company always aim to cause disruption and damage. They are carried out for the purposes of stealing data, for financial gain, or to disrupt the operation of the company.

Internal or insider threats are likely to come from someone who works at the organisation and has access to sensitive corporate data as part of their day-to-day duties. This could be someone working within the company, or who works for subcontractors, external IT support engineers or consultants. Insiders have a much greater advantage in being able to carry out cyber attacks because they already have access.

Recent cases highlight that many insider threats come from unhappy or disgruntled employees, such as someone who was informed they will be made redundant. These people may not carry out the attacks themselves, but may pass on or sell security or other inside information to those who will carry out the attack.

The reasons people carry out cyber attacks

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

We have already seen that almost any business or organisation can be a target for a cyber attack, so it follows that there are many reasons for these attacks. The most common reason is financial gain, but there may be a host of other motivations. Attacks on different industries tend to have different motivations.

Motivations for outsider/external attacks

Cyber attacks against businesses are often deliberate and are usually motivated by financial gain. However, other motivations may include:

- Making a social or political point – e.g. hacktivism.
- Espionage – such as spying on competitors to gain unfair advantage.
- Intellectual challenge – so-called ‘white hat’ hacking.

Attacks on healthcare providers may be designed to collect medical and personal data that can then be sold on. Stolen medical information can sometimes also be used to gain unauthorised entry to some medical programmes or to obtain prescription drugs for personal use or to sell for profit.

Attacks on food service, accommodation and retail establishments are most often done to collect customer payment information, such as credit card numbers and addresses, which can then be used to make unauthorised purchases and for identity theft. Similarly, attacks on financial services can glean sensitive banking and credit card information.

Public administration bodies are often victims of data breaches where thieves try to steal confidential government records to sell to foreign entities. They may also be made by hackers who want to make a political statement.

Hacktivists are another source of external threat. These people often want to make a political or social statement, or to demonstrate their expertise and earn 'bragging rights'.

Motivations for insider/internal attacks

Many insider attacks are also carried out for financial gain. For example, around 26% of internal hackers are based in systems administration. These employees have access to sensitive data and information and they may sell this data on to external sources. Other internal attacks may be motivated by a desire for revenge or to seek retribution for a slight or because they feel undervalued by their employer.

Technically proficient employees may use their systems access to open back doors into computer systems (a back door is any method that allows users or hackers to get around normal security measures to gain access to a computer system, network or software) or leave programmes on the network to steal information or wreak havoc. They may even sell access to these backdoors.

However, the largest number of internal attackers are actually people who have accidentally and unknowingly downloaded malware or leaked information accidentally. Many of these errors take place because an organisation is using outdated software, has failed to install needed updates and patches, or hasn't invested in raising awareness among its employees. Social engineering attacks are also common. In this case, the employee has unwittingly given out a password or other information and does not know they are part of an attack. Social engineering attacks, like phishing, are also common.

Other insider attacks may be done for different types of personal gain. For example, in 2020, two former eBay employees pleaded guilty to a cyber stalking campaign against a Massachusetts couple whose online newsletter was seen as critical of the e-commerce company.

Example 1

An office administrator who stole almost £600,000 from her employers in order to fund her online gambling addiction was jailed for three years at the Crown Court in Londonderry.

Tracey Curran, 44, pleaded guilty to six charges of unlawfully taking the money from the Bank Of Ireland and American Express credit card accounts belonging to her employer.

Source: **https://www.belfasttelegraph.co.uk/news/northern-ireland/woman-who-stole-600k-from-employers-to-feed-gambling-addiction-jailed-for-three-years-38850876.html**

Example 2

The 2013 breach of American retailer Target is an example of a breach caused by employees acting unknowingly. Someone at a partner company opened an email infected with malware and poor internal controls allowed criminals to then gain access to Target. On top of this, many of Target's own staff were using weak or even default passwords, and storing login credentials on servers where the hackers could access them. The company was also using outdated software with inadequate patching, creating more security holes.

Untargeted and targeted attacks

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

Untargeted cyber attacks

In untargeted attacks, attackers indiscriminately target as many devices, services or users as possible. They are not targeting a specific individual or business. To do this, attackers use techniques that take advantage of the open nature of the Internet. This type of attack includes techniques like:

- **Phishing** – sending emails to random people asking for personal information (such as bank details) or encouraging people to visit a fake website.
- **Water holing** – setting up a fake website or redirecting people from a real website to order to collect personal information.
- **Ransomware** – a type of malware that encrypts a victim's files to make them inaccessible. The attacker then demands a ransom from the victim, usually to be paid in crypto-currency, to restore access to the data upon payment.
- **Scanning** – attacking large parts of the Internet at random.

Targeted cyber attacks

In a targeted attack, a particular industry, organisation or person is singled out for attack. The attackers might spend months laying the groundwork for the attack. This type of attack is often more damaging than an untargeted attack because it has been specifically directed at a particular target. Targeted attacks may include:

- **Spear-phishing** – sending emails to particular individuals which contain an attachment with malicious software, or a link that downloads malware.
- **Deploying a botnet** – a botnet connects together a number of Internet-connected devices, each of which is running one or more bots – a type of malware, without the owners' knowledge. Botnets can be used to steal data, send spam, and allow the attacker to access the device and its connection.
- **Subverting the supply chain** – equipment or software being delivered to the organisation is implanted with malware.

Differences between targeted and untargeted attacks

Untargeted attacks are far more common than targeted attacks, for two primary reasons. First, untargeted attacks are easier to carry out. Instead of trying to find out how to access a specific system, hackers simply create a generic email with malicious content such as an attachment or link. They will then send this out to every email address they have access to. Depending on the form of malware that was used, the goal of the attack might be extortion from ransomware, installing keyloggers to track user credentials, or the installation of spyware. Since they are not targeting a specific person or audience, the content in the email is kept very vague. For instance, it may be a fake tracking link for a recent 'purchase'.

Did you know?

According to the Crime Survey for England and Wales, there were 3.7 million reported incidents of fraud where individuals were targeted for credit card, identity and cyber fraud in 2019-2020.

The report said that, "Fraud has the potential to disrupt society in multiple ways, by psychologically impacting individuals, undermining the viability of businesses, putting pressure on public services, fuelling organised crime and funding terrorism."

Source: **https://www.ons.gov.uk/**

Did you know?

One type of cyber fraud common at Christmas is for criminals to pose as well-known delivery companies, and send emails saying they have not been able to deliver goods and asking for a fee to rearrange delivery. The email will contain a link to a fake website that will ask unsuspecting victims to enter their bank details or other personal information.

This type of scam takes advantage of the fact that people receive a lot of packages and gifts at Christmas, so they often enter the information without really thinking about it.

Knowledge Activity 2: List some of the differences between targeted and untargeted attacks.

What is a cyber crime vulnerability?

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

A vulnerability is an oversight by an individual or a flaw or weakness in a system or network that could be exploited by a threat actor to cause damage, or allow an attacker to manipulate the system in some way.

Individuals, organisations and nations all have different, but often overlapping, areas of vulnerability.

Vulnerabilities faced by individuals

In terms of cyber security, one of the biggest vulnerabilities is people themselves. Lack of IT knowledge or lack of training can lead to people becoming an easy target for threat actors. The opening of emails and files which contain malware have led to numerous cyber security incidents in recent years, such as the 'WannaCry' malware attack on the NHS in 2017, which also affected computers in a further 149 countries. Individuals may also not have the latest security patches on their computers. Because fraudsters are coming up with new scams all the time, it can be very difficult for individuals to keep up with the latest types of attack and protect themselves.

The Internet of Things (IoT), a system of interconnected devices is another area of risk. The IoT encompasses many 'smart' devices, such as Wi-Fi capable refrigerators, printers, manufacturing robots, webcams and cars. The issue with these devices is that they can be hijacked to carry out further attacks. Worryingly, many businesses do not even realise just how many IoT devices they have on their networks – meaning that they have unprotected vulnerabilities that they are not aware of.

These devices could represent a massive opportunity to attackers and a massive risk for businesses.

Example

The iKettle, made by UK company Smarter, allows users to turn their kettles on and off using a smartphone app – to avoid wasting valuable seconds waiting for the water to heat.

However, a UK security firm has found that the kettles can be used as an entry point for hackers, allowing them to take over a home Wi-Fi network. Specifically, it is possible for hackers to gain access to users' wireless network key, which in turn can give them access to the network.

Vulnerabilities faced by businesses and organisations

For any organisation, there are a number of cybersecurity threats and network vulnerabilities that malicious actors can exploit. These include:

Flaws – These are vulnerabilities in software and applications that include coding errors. A market has grown in software flaws, with detailed information on some fetching hundreds of thousands of pounds. These may also include zero-day vulnerabilities, which are software vulnerabilities where there is no patch yet in place to fix it.

Network vulnerabilities – These result from insecure operating systems and network architecture. This type of vulnerability includes flaws in servers and hosts, misconfigured wireless network access points and firewalls, and flaws in network protocols.

Features – Common features may be those intended to improve the user's experience, help diagnose problems or improve management, which can also be exploited by an attacker. For example, JavaScript, which is widely used to develop dynamic web content, can be used by attackers to divert the user's browser to a malicious website, and for hiding malicious code.

User error – This is by far the most common vulnerability for all types of companies. Common issues include:

- Having weak login credentials, e.g. choosing a common or easily guessed password.
- Leaving laptops or mobile phones unattended in a public place.
- Opening email attachments from an unknown sender.
- Leaving passwords in the open, such as on sticky notes.
- Giving all employees access to everything, or having too many people with administrator access.
- Exposure to social engineering/phishing attacks.
- Lack of effective employee training.
- Not updating systems and antivirus software.

Charities – Suffering a data breach is serious for any organisation. Yet for charities, whose success is built upon their reputations and the goodwill of supporters, the loss of any sensitive information can be devastating. Charities often hold sensitive information, such as names, addresses and payment details, and may spend less on training and IT infrastructure.

International organisations and multi-national organisations – In addition to all of the vulnerabilities listed above, these may also be vulnerable to being targeted by government-sponsored hackers trying to keep tabs on the organisation, or hacktivists looking to publicise their own views.

Vulnerabilities faced by nations

The risk of cyber attacks on governments is very high, and growing, as hackers develop more sophisticated tools. Many of the attacks faced by governments are not orchestrated for money, but for information or control – making the stakes for governments very high. This so-called 'cyber warfare' may be conducted for a variety of reasons, often to extract information, for money, to test vulnerabilities to a 'hard' attack, disrupt the economy, create national trauma or insecurity, or to engage in social engineering, such as influencing an election.

Threat actors who target nations are often well-financed and have support from a particular nation.

One area of vulnerability for nations is that systems for different departments are often linked together, allowing attackers to gain access to sensitive systems by attacking ones that are less well-protected. Because governments tend to have large and unwieldy bureaucracy, this can also make them slow to adopt the latest cyber defences or to upgrade outdated systems.

Governments also have a huge number of employees and people with access to various systems, making them vulnerable to the same type of techniques used against individuals and companies.

Case Study – hackable cardiac devices

In 2020, it was reported that Implantable cardiac devices made by St Jude Medical were found to have vulnerabilities that could be exploited by hackers.

Devices such as pacemakers and defibrillators had a transmitter that read the device's data and shared it remotely with a physician. This transmitter had vulnerabilities which could allow hackers to gain access to the devices and interfere with their functions, such as using up the battery or giving incorrect pacing or shocks.

Find Out More: Research some common cyber crime vulnerabilities. List some of the vulnerabilities faced by each of the following:

- individuals
- charities
- nations
- international organisations
- multi-national organisations

Potential impacts of cyber crime

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

According to some estimates, by 2025, cyber crime will cost the world more than $5 trillion each year. This will have a significant impact on jobs, research and development, economic growth and investment.

As cyber crime increases, the costs to prevent it also increase. The damage is not limited to finances. There is also a high cost to intangible assets like brand reputation and customer goodwill.

Let's now look at how cyber crime impacts individuals, businesses and nations.

Individuals

Individuals can be severely impacted by cyber crime, not only financially, as attacks may clear out bank accounts and impact credit ratings, but also psychologically. Individuals can end up feeling depressed, embarrassed, shamed or confused following the attack. Individuals may not understand why they have been attacked, and embarrassed that they have let something like this happen to them. Recovering from an attack may also be time consuming and involve setting up new accounts or speaking to a wide range of authorities.

Organisations

There are obvious financial implications faced by any organisation which has been attacked, potentially including a fall in stock price, regulatory fines and reduced profits. Organisations may lose key data or research to competitors resulting in huge costs and a loss of competitive advantage. Reputational impacts can include a loss of key staff, damaged relationships with customers and intense media scrutiny. Customers may not feel safe shopping with the organisation and so stop visiting their websites.

Companies now have to rethink how they collect and store information to ensure that sensitive information isn't vulnerable. Many organisations have stopped storing customers' financial and personal information, such as credit card numbers, home addresses and birth dates.

Cyber crime is also a rapidly growing threat to the charity sector. In the next two years, one in every six large charities will suffer from cyber crime. Many other charities will be the victim of cyber attacks without knowing about it. A charity is four times more likely to discover cyber crime through internal IT controls or by staff raising concerns than all other external sources combined.

Some larger charities believe they experience several thousand attempted cyber attacks every week.

Multi-organisational

A multi-organisation enterprise is where different organisations work together collaboratively to deliver complex products or service systems. For example, the NHS is made up of a number of different organisations (GP surgeries, hospitals, clinics, etc.) that all work together to deliver health care.

For large organisations such as the NHS, their size makes them a high profile target. Digital Health Intelligence has reported that more than 50% of NHS trusts now have electronic patient record systems which hold vast amounts of sensitive personal data.

What is the impact for organisations such as the NHS? It is predominantly financial loss, for example, extortion using ransomware or theft of data such as staff or user bank account details.

An international organisation is one that has branches, or conducts business, in different countries. International organisations face an even greater risk of cyber attack, as it may be necessary to work across borders, or to co-ordinate many different parts of the organisation, in order to fight the attacks. International organisations may also need to adhere to different types of laws, so they may also be at risk of larger fines and legal consequences if there is a breach.

Nations

As we have seen, nations are facing a huge increase in cyber espionage, including damage to infrastructure and key services. There is also evidence in some places of election tampering and other types of large-scale social engineering, reducing trust in governments and making it harder for them to act. State secrets, personal data on citizens, blueprints to military technology and political manipulation are all key areas in which cyber criminals are attempting to gain access. The impact of cyber attacks on states can be catastrophic, and cyber criminals have attempted to gain access to nuclear power plants, and vital facilities such as dams and electricity supplies.

Importance of cyber security

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

What is cyber security?

Cyber security is the practice of securing devices, networks, systems and any other digital infrastructure from malicious attacks. The best strategy, whether for individuals, companies or governments, is to have in place a strong security system that includes multiple layers of protection. This could include firewalls, antivirus software, anti-spyware software and password management tools.

The importance of cyber security for individuals

On an individual level, poor cyber security can lead to financial loss, identity theft and even personal safety risks. The best ways to prevent this are to exercise caution, use anti-virus software on all devices, always use strong passwords and never open or respond to suspicious emails.

Mobile phones are at serious risk of cyber attacks. To safeguard phones, users can install tools that lock the phone or enact multi-factor passwords in the event of a loss. To combat mobile apps that do not protect against viruses or that leak personal information, it is important to install cyber security tools that will alert or block suspicious activity.

Using public Wi-Fi is another risk for individuals. To secure against man-in-the-middle attacks, where communication is intercepted by a third party, cyber security experts suggest using the most up-to-date software and avoiding password-protected sites that contain personal information. One way to guard against a cyber attack on public Wi-Fi is to use a virtual private network (VPN). These create a secure network, where all data sent over a Wi-Fi connection is encrypted.

The importance of cyber security for businesses

Most businesses rely on computer systems to operate. A breach of their systems could result in substantial financial, as well as reputational, loss. In addition, GDPR and other data protection laws mean that organisations can suffer from regulatory fines or sanctions as a result of cyber crimes. This is particularly true for international businesses, who must make sure they meet the laws in all of the countries in which they operate.

Example

In 2020, British Airways was fined $26 million by the ICO for an issue that occurred in 2018, where the airline's systems were breached, resulting in hackers getting their hands on names, addresses and payment card details of 400,000 BA customers. According to the ICO, BA had failed to put in place sufficient security measures to protect their systems, networks and data. In fact, at the time of the breach, BA were not even using multi-factor authentication.

It is vitally important that businesses invest in training, tools, and technology to reduce the risk of cyber crime. These should include tools that monitor third-party risk and vendor risk, and continuously scan for data exposure and leaks. All organisations should also have robust policies and procedures in place, as well as training programmes, so that all staff know how to guard against data leaks and common social engineering scams.

Multi-organisational businesses – these include organisations like the NHS. These need to ensure that cyber security is applied uniformly across the entire enterprise – any gaps could allow threat actors to gain access to the entire system.

Charities – organisations like charities, who may have overlooked this type of threat in the past, are now finding cyber security of vital importance. In the UK, 22% of charities experienced a data breach in 2019, and a fifth of these reported weekly attacks.

International organisations – cyber security is vital for international organisations, which face all of the threats mentioned here, but also need to make sure that they co-ordinate their cyber security with the parts of the organisation in other countries. Some threats, technology and laws may be particular to a specific country, so international organisations may also need to hire experts in each country where they operate.

The importance of cyber security for nations

Here, the risk is often both more nebulous and more high stake. Concrete risks include attacks on infrastructure and defence systems, and theft of data which can lead to financial loss. Less concrete but equally important risks are those which impact on public safety, governmental reputation, the overall economy and international relations.

To combat these risks, all countries should develop a robust national cyber security strategy which should include:

- a national cyber security agency
- a national Critical Infrastructure Protection program
- a national incident response and recovery plan
- clear laws relating to cyber crimes
- cyber security education and training

Knowledge Activity 3: List the steps you would take to guard against cyber threats, as an individual, a business and a nation.

Individual:
Business:
Nation:

Importance of reporting issues promptly

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

For individuals, data breaches or cyber attacks should be reported immediately, so that relevant organisations, such as banks, can act quickly to stop the theft and hopefully return the money. In fact, any delay in reporting a financial loss from a data breach will often result in the permanent loss of money.

For businesses and government employees, however, reporting data breaches is a legal requirement. The GDPR introduced a duty on all organisations to report certain types of data breaches to the relevant supervisory authority. Failing to do so can result in heavy fines and penalties, and an investigation by the Information Commissioner's Office (ICO).

Although the EU GDPR no longer applies to UK residents' personal data, the Data Protection Act 2018 enacted the EU GDPR's requirements in UK law, meaning that UK organisations must still comply with its requirements.

The law requires all breaches of personal data, such as customer information, whether they are accidental or the result of cyber crime, to be reported within 72 hours of being made aware of the breach. However, not all breaches need to be reported, only those which "pose a risk to the rights and freedoms of natural living persons". This usually includes the possibility of affected individuals facing economic or social damage (such as discrimination), reputational damage or financial losses.

Aside from the legal requirements, notification can help others avoid similar risks, and may help the police to track down the criminals.

Notification also helps other organisations prepare for similar attacks. Criminals often reuse successful techniques, whether it's a particular scam method or a network vulnerability, and publicly announcing this threat allows organisations to address the issue.

Example

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data

Example

The ICO would need to be notified of the theft of any customer data because the data could be used to commit identity fraud or theft from individuals.

Example

A hospital suffers a breach that results in an accidental disclosure of patient records. There is likely to be a significant impact on the affected individuals because of the sensitivity of the data and their confidential medical details becoming known to others. This is likely to result in a high risk to their rights and freedoms, so the ICO would need to be informed about the breach.

The role of key organisations in the cyber security industry

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

NCSC (National Centre for Cyber Security)

The role of the NCSC is to help to make the UK a safe place to live and work online. Launched in October 2016, the NCSC is headquartered in London and brings together expertise from other UK and European organisations. It carries out its main role by supporting critical organisations in the wider public sector, industry, and business, as well as the general public.

More specifically, the NCSC:

- Understands cyber security, and distils this knowledge into practical guidance that they make available to all.
- Responds to cyber security incidents to reduce the harm they cause to organisations and the wider UK.
- Uses industry and academic expertise to support and grow the UK's cyber security capability.
- Reduces risks to the UK by securing public and private sector networks.

GCHQ (Government Communications Headquarters)

The Government Communications Headquarters, better known as GCHQ, is a world-leading intelligence, cyber and security agency with a mission to keep the UK safe.

The agency employs highly skilled people who use cutting-edge technology, technical skills and wide-ranging partnerships to identify, analyse and disrupt threats.

The priorities of GCHQ are set by the UK's National Security Strategy and the decisions of the National Security Council, chaired by the Prime Minister, as well as the Joint Intelligence Committee.

The three key mission areas of GCHQ are:

- Counter Terrorism – Stopping terrorist attacks in the UK and against our interests overseas.
- Cyber Security – Making the UK the safest place to live and do business online.
- Strategic Advantage – Managing the threats from hostile states, promoting the UK's prosperity and shaping the international environment.

ICO (Information Commissioner's Office)

The ICO is an independent body established to uphold information rights.

The role of the ICO is to uphold information rights in the public interest. More specifically, the agency's role is "to ensure that personal information is kept secure and safe."

The ICO is responsible for ensuring organisations follow the requirements of the following three pieces of legislation. We will look at these in more detail later in the workbook.

- Data Protection Act
- General Data Protection Regulation
- Freedom of Information Act

Scotland

Scotland has its own Information Commissioner. The Scottish Information Commissioner and the UK Information Commissioner's Office (ICO) have separate roles and responsibilities.

In general, the Scottish Information Commissioner is responsible for the freedom of information compliance of all public authorities in Scotland, while the ICO is responsible for Data Protection rights for the whole of the UK, including Scotland.

The ICO is also responsible for freedom of information compliance for public authorities in England, Wales, and Northern Ireland, and for any agencies that operate in both Scotland and another part of the UK.

The ICO also has regulatory power under the Freedom of Information Act for UK public authorities based in Scotland. These include:

- BBC Scotland (in relation to its public functions)
- The Northern Lighthouse Board

Example of action taken by the ICO

In 2018, the ICO fined ride sharing company Uber £385,000 for failing to protect customers' personal information during a cyber attack.

According to an ICO press release, "A series of avoidable data security flaws allowed the personal details of around 2.7 million UK customers to be accessed and downloaded by attackers from a cloud-based storage system operated by Uber's US parent company. This included full names, email addresses and phone numbers.

The records of almost 82,000 drivers based in the UK – which included details of journeys made and how much they were paid – were also taken during the incident, in October and November 2016.

The ICO investigation found 'credential stuffing', a process by which compromised username and password pairs are injected into websites until they are matched to an existing account, was used to gain access to Uber's data storage.

However, the customers and drivers affected were not told about the incident for more than a year. Instead, Uber paid the attackers responsible $100,000 to destroy the data they had downloaded."

General job functions carried out by cyber security professionals

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

Cyber security professionals have a wide range of responsibilities, but their main role is to protect electronic data from being compromised. As a cyber security professional, you can expect to safeguard an organisation's files and network, install firewalls, create security plans and monitor activity.

Responsibilities of the cyber security professional

New security threats pop up all the time, and IT security professionals need to stay up to date with the latest tactics employed by hackers. In addition to the high-level responsibilities already mentioned, some specific duties include:

- Set and implement user access controls and identity access management systems.
- Monitor network and application performance to identify any irregular activity.
- Perform regular audits to ensure security practices are compliant with government regulations.
- Use endpoint detection and prevention tools to thwart malicious hacks.
- Set up patch management systems that update applications automatically.
- Implement comprehensive vulnerability management systems across all assets, both on-premises and in the cloud.
- Work with IT teams to set up a shared disaster recovery/business continuity plan.
- Work with HR and/or team leads to educate employees on how to identify suspicious activity.

Hacking

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

What is a hacker?

The basic definition of a hacker is someone who uses a computer system to gain illegal access to another system. There are different types of hacker, and they are not all interested in the same thing.

Three types of hackers

Black hat

A black hat hacker is what people usually think of as the traditional 'hacker'. They have malicious intent and are looking to break into and exploit vulnerable systems. Most hacks that you see in the news are a result of black hat hackers.

White hat

A white hat hacker is what is known as an ethical hacker. They act to protect businesses and support them against black hat hackers. They are often hired by companies and organisations, and may help install effective protections, find vulnerabilities and provide solutions for them. They typically have authorisation to do what they are doing and there is even a qualification for them – Certified Ethical Hacker – from the EC Council.

Grey hat

A grey hat hacker lives somewhere in the middle. Generally speaking, they are breaking laws and violating ethics, but their intent isn't usually malicious. Usually, grey hat hackers will not exploit the vulnerabilities they find. However, this type of hacking is still considered illegal because the hacker did not receive permission from the owner prior to attempting to attack the system.

Grey hat hacking is sometimes done in the name of public interest, although quite commonly, if a grey hat identifies a flaw and points it out to a company, the company will want to work with the hacker to help fix the breach. Companies will often reward them just like they would a white hat.

However, the difference between grey hat hackers and white hat hackers is that, if the company decides to ignore a grey hat hacker, the hacker is not bound by ethical hacking rules or an employment contract. They could decide instead to exploit the flaw themselves or sell and share the knowledge online for other hackers to take advantage of.

Did you know?

A white hat hacker

Charlie Miller is considered one of the best white hat hackers in the world. He has a PhD in Mathematics and has worked as a hacker for the National Security Agency.

He has also won the annual PWN2OWN hacking contest – the 'Super Bowl of hacking' – four times. In the 2009 contest, he broke into a Macintosh in less than 10 seconds. He hacked the first Android phone on the day it was released, and was the first person to hack the iPhone remotely by sending an SMS message.

His demonstration of how he could remotely take over any Fiat Chrysler to control the radio, brakes, transmission and steering led to a recall of 1.4 million vehicles.

Knowledge Activity 4: List the different types of hacker and what they do.

Key skills for cyber security specialists

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

Key skills:

- Strong IT and digital skills and knowledge of hardware, software and networking systems – the exact systems used will vary from employer to employer, but you should have a good basic knowledge that you can build on.
- Communication – being able to communicate what issues you have found and how to fix them, in a way that anyone can understand, is very important in any positions.
- Analytical skills – cyber security requires the ability to think through a problem and work out solutions in a logical manner.
- Team working – many issues will be too large for one person to manage, so it is important that you are able to work effectively in a team, and that you can not only get along with others in the team, but can help others and be willing to learn.
- Project management – cyber security often involves organising large projects, and being able to create a plan to tackle these effectively and in a timely manner is a vital skill.
- Problem solving – cyber security is all about finding problems and then working out how to solve them. This requires the ability to think logically, and also the mindset of not wanting to give up until the problem is solved.

With the pace of development in IT security, you will also need ongoing training and certification in new skills. Cyber security professionals need to continue learning new technology skills to be able to resolve new security issues.

Knowledge Activity 5: Choose two of the key skills required for a cyber security specialist and describe a situation where you would need to use each of those skills.

Summary

In this section, you have learned about:

- motivations for cyber crime
- different types of threat actors
- external and internal threats
- targeted and untargeted attacks
- cyber crime vulnerabilities of individuals, businesses, and nations
- the impact and importance of cyber crimes on individuals, businesses, and nations
- key organisations and job functions in cyber security
- what hacking is, and different types of hackers
- some of the key skills required for a cyber security professional

Section 2: Understand industry terminology used in cyber security

In this section, you will gain an understanding of basic cyber security terminology and be able to define certain common terms in relation to cyber security. You will be able to describe the differences between LAN and WAN and understand how terms like vulnerable, attack, protection and risk are applied to cyber security. Finally, you will be able to describe organisational strategies in relation to cyber security.

Key terminology used within cyber security

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

Hardware

Hardware refers to the physical parts of a computer, server and related devices. Internal hardware can include motherboards, hard drives, CPU, power supply, GPU and RAM. External hardware can include monitors, keyboards, camera, touchpad, mice, printers, and scanners. Internal hardware is often referred to as components, while external hardware devices are referred to as peripherals. Together, they are all computer hardware.

Software

Software is the instructions that tell a computer what to do. Software includes the entire set of programs, procedures and routines associated with the operation of a computer or network.

There are two main types of software – system software and application software. System software includes the operating system and controls a computer's internal functioning, as well as peripherals like monitors, printers and storage devices.

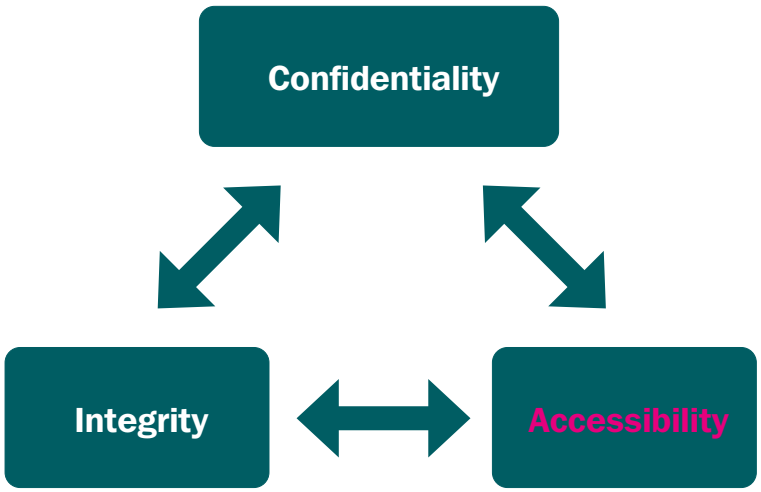
Application software tells the computer to execute commands and includes programs that process data, such as word processors, spreadsheets, database management, inventory and payroll programs.

Network software is used to coordinate communication between the computers linked in a network.

Application software may be stored in an internal or external memory device, such as a hard drive. When the program is in use, the computer reads it from the storage device and temporarily places the instructions in random access memory (RAM). This is called 'running' or 'executing' a program. System software that is permanently stored in the computer's memory using read-only (ROM) technology is called firmware, or 'hard software'.

Data management

In cyber security, data management refers to the process of protecting data from unauthorised access and data corruption. Managing data securely includes three components: confidentiality, integrity and availability.



Confidentiality is about privacy and ensuring information is only accessible to those with a proven reason to see it.

Integrity is about making sure that information stored in a database is consistent and un-modified. Systems need to be designed to reduce the chance of human error when information is input and managed, and to make sure that the flow of information does not result in loss or alteration.

Availability is about information being available when it's needed. System design must include appropriate access controls and checks so that the information in the system has consistency and accuracy, can be trusted as correct and can be relied on when providing information to the user.

Section 2: Understand industry terminology used in cyber security

Networking in cyber security

A computer network is when two or more computers or virtual resources (such as the cloud) are connected to each other in order to share resources (such as printers), exchange files, or allow electronic communication. Computers may be networked together physically, using cables, or may be connected wirelessly. Three common types of networks are:

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)

LAN – Local Area Network

A Local Area Network (LAN) is a private network that connects computers and devices within a small area like a home, an office or a building. LANs enable a number of computers to share a variety of resources like hardware (e.g. printers, scanners, network storage devices), software (e.g. application programs) and data.

MAN – Metropolitan Area Network

A metropolitan area network (MAN) is a computer network that connects computers within a metropolitan area; this could be a single large city, multiple cities and towns, or over a large area with multiple buildings. A MAN is larger than a local area network (LAN) but smaller than a wide area network (WAN).

WAN – Wide Area Network

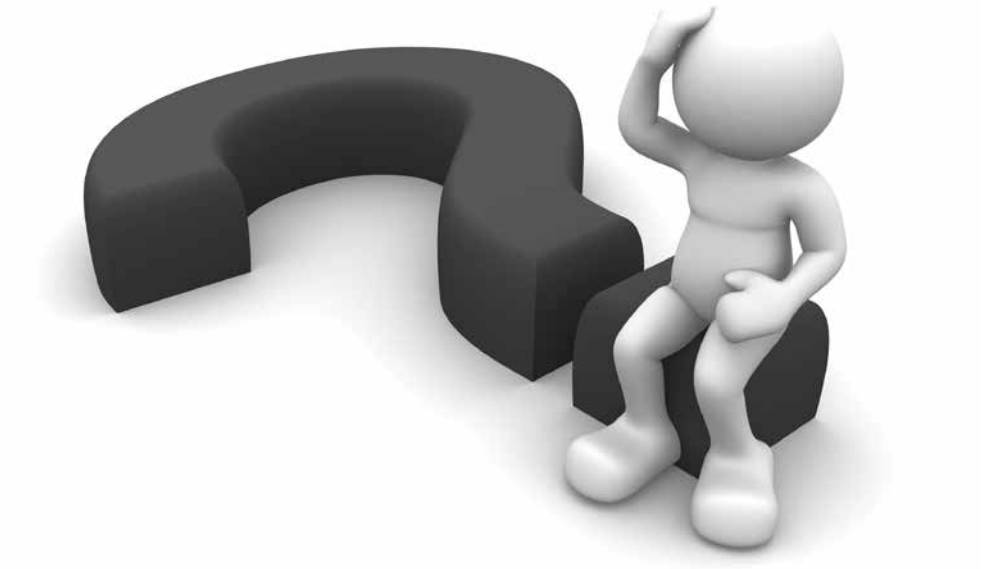
A wide area network (WAN) is a network that exists over a large geographical area, and connects different smaller networks, including local area networks (LANs) and metro area networks (MANs). It allows computers and users in one location can communicate with computers and users in other locations. A WAN is essentially a network of networks. The Internet is an example of a WAN.

Section 2: Understand industry terminology used in cyber security

Did you know?

In the early days of networking, the first webcam was deployed at a Cambridge University computer lab. Its sole purpose was to monitor a particular coffee maker so that lab users could avoid wasted trips to an empty coffee pot.

Knowledge Activity 6: In your own words, write the definitions of hardware, software, data management and networking.



Differences between a LAN and a WAN

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

The main difference between a LAN and a WAN is that a LAN connects local devices to each other, while a WAN connects LANs to each other, usually across multiple locations spread over large distances. A WAN may be limited to one corporation or organisation, or it may be accessible to the public, like the Internet. Some of the advantages and disadvantages include:

A LAN is used because:

- Computer resources like hard-disks, DVD-ROM, and printers can share local area networks which reduces the cost of hardware purchases.
- You can use the same software over the entire network instead of purchasing the licensed software for each client in the network.
- Data of all network users can be stored on a single server hard disk.
- It is easy to transfer data and messages over networked computers.
- Managing data from one location improves security.
- LAN users can share a single Internet connection.

Drawbacks to using a LAN:

- The LAN administrator can check the data files of every LAN user, which reduces privacy.
- A LAN network can reduce costs by sharing computer resources. However, the initial cost of installing Local Area Networks may be high.
- Unauthorised users can access critical data of the company in case LAN admin is not able to secure a centralised data repository.
- A LAN needs constant administration as there may be issues related to software setup and hardware failures.

A WAN is used because:

- It covers a larger geographical area, which helps facilities located far apart to communicate more easily.
- It can include devices like mobile phones, laptops, tablets, computers, gaming consoles, etc.
- It allows software and resources to be shared by connecting with various workstations.
- Information and files can be shared over a larger area.

Drawbacks to using a WAN:

- The initial set up cost of a WAN network is high.
- It can be difficult or expensive to maintain a WAN network as you need skilled technicians and network administrators.
- It can take more time to resolve issues because of the involvement of different types of technologies.
- It offers lower security compared to other types of networks.

Cyber security terms

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

Vulnerability

A vulnerability is a flaw or weakness in a system or network that could be exploited by a threat actor to cause damage, or allow an attacker to manipulate the system in some way.

Cyber risk

This is defined as "the potential of loss or harm related to technical infrastructure or the use of technology within an organisation."

Cyber attack

This occurs when cybercriminals try to gain illegal access to electronic data stored on a computer or a network. The intent might be to inflict reputational damage or harm to a business or person, or the theft of valuable data. Cyber attacks can target individuals, groups, organisations or governments.

Protection

While IT security protects both physical and digital data, cyber security protects the digital data on your networks, computers and devices from unauthorised access, attack and destruction. Cyber security includes both network security and computer security.

Recovery

This describes the steps taken to recover from a cyber attack. The exact steps will depend on the type of attack, but recovery may include determining what was lost, reinstalling software and data from backups, finding and eliminating viruses and malware, investing in new software to block attacks, developing new procedures to prevent attacks and changing passwords.

A cyber or cyber security threat

This is an act that seeks to damage or steal data and disrupt digital life in general. They can be against individuals, businesses or nations. Cyber attacks include threats like computer viruses, data breaches, and Denial of Service (DoS) attacks.

- Denial of Service (DoS) – A Denial of Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attackers accomplish this by flooding the target with traffic, or by sending it information that triggers a crash. The DoS attack might crash a website or deprive legitimate users, such as employees, account holders or the public, of access to the service or resource.
- Distributed Denial of Service (DDoS) – A DDoS attack occurs when attackers synchronise a DoS attack using multiple systems. However, with a DDoS attack, instead of being attacked from one location, the target is attacked from many locations at once. The distribution allows the attacker to make a more disruptive attack, and makes the attack more difficult to track down and stop.
- Botnet – A Bot is a type of software application or script that performs tasks on command, allowing an attacker to take remote control of an affected computer or device. A collection of computers infected with Bots is called a 'botnet', and is controlled by the hacker or 'bot-herder'. Botnets are commonly used in DDoS attacks.
- Trojan – A Trojan is a type of malicious code or software that looks like a real piece of software but can then be used take control of your computer. A Trojan is generally designed to disrupt operations, to steal data or to damage a network or system.

- Ransomware – A form of malware that deliberately prevents you from accessing files on your computer, holding your data hostage. They normally work by encrypting files and requesting that a ransom be paid in order to have them decrypted or recovered.
- Spyware – This is a type of malware that infiltrates your computing device, stealing your data and any sensitive information. Spyware may gather personal information such as your bank account log in details or passwords to email accounts.
- Virus – This is a software program that is loaded onto a user's computer without the user's knowledge, and performs malicious actions. These range from deleting files to potentially destroying hardware.

Malware

This is a broad term that describes all forms of malicious software designed to wreak havoc on a computer. Common types of malware include:

- viruses
- trojans
- worms
- ransomware

Section 2: Understand industry terminology used in cyber security

Did you know?

Powerful botnets have been responsible for some of the largest, most devastating cyber attacks. Examples include:

- The 2014 Hong Kong Attack – Political unrest in Hong Kong was the target of the largest DDoS attack in history up to that point, when several large botnets joined forces against pro-democracy websites in the country. Some have accused the Chinese government of this attack, but the actual perpetrator remains unknown.
- The 2016 Mirai Attack – Named after a popular anime series, Mirai was a botnet consisting of more than 100,000 computers. The Botnet was behind a massive DDoS attack that left much of the Internet inaccessible on the U.S. east coast. This was also the first major botnet to infect IoT devices, and may have infected more than 600,000 devices. Perhaps most surprising of all was that the botnet was created by a group of college kids looking to gain an edge in Minecraft.
- The 2018 3ve ('Eve') attack – This was a global, complex group of online fraud operations. Around 1.7 million computers were infected with bots that created up to 12 billion fake ad views a day – charging companies for ads that were never seen. A White Hat alliance dismantled the botnet, resulting in the first-ever indictment and arrest of the perpetrators of this type of ad fraud.

Knowledge Activity 7: Describe what is meant by DoS, DDoS, Botnet, Trojan, Ransomware and Virus.

Organisational strategies

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

An organisational strategy is the sum of the actions a company intends to take to keep its IT infrastructure secure. To keep its systems secure, an organisation (usually large in size) may build two separate functions which work together to meet the organisational strategy. These functions are the Security Operations Centre (SOC) and the Network Operations Centre (NOC).

SOC

A Security Operations Centre (SOC) is a central function within an organisation employing people, processes, and technology to continuously monitor and improve an organisation's security, while preventing, detecting, analysing, and responding to cyber security incidents. An SOC acts like a central command post, taking in information from across an organisation's IT infrastructure. The SOC then decides how security events will be managed and acted upon.

The key aims of an SOC are:

- To detect and respond to threats, keeping the information held on systems and networks secure.
- To respond better to threats by learning about the exisiting and potential threats. The threats from cybercriminals are constantly evolving and the SOC must keep up to date with these threats and adapt the organisation's security.
- To identify negligent or criminal behaviours. This could be from either internal or external threats.
- To improve business intelligence about user behaviours to shape and prioritise the use of new technologies. For example, do key cards keep getting lost? Should the organisation look at finger print scanners instead?

NOC

A network operations centre (NOC) is a centralised location where IT support technicians can supervise, monitor and maintain client networks.

These centres may not necessarily be on site, and operations are often carried out by external suppliers. Their role is to ensure 24/7 uptime for all parts of the network.

NOC services

An NOC is a central point for software distribution and updating, performance monitoring, coordination with other networks, network troubleshooting and router and domain name management. Almost anything related to the network falls under the responsibility of the NOC. Key tasks include:

- performance reporting and improvement recommendations
- firewall and intrusion prevention system monitoring and management
- network discovery and assessments
- optimisation and quality of service reporting
- patch management and whitelisting
- backup and storage management
- email management services
- voice and video traffic management
- antivirus scanning and remediation
- shared threat analysis
- policy enforcement
- application software installations, troubleshooting and updating

What is the difference between an NOC and an SOC?

Both the NOC and SOC serve critical functions – to identify, investigate and resolve issues. While the NOC is focused on network performance and availability, the SOC consists of tools and employees who monitor, detect and analyse an organisation's full security health every minute of every day.

Knowledge Activity 8: Why is it important to have both an NOC and an SOC?

Current and emerging challenges in cyber security

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

The cyber security landscape is constantly changing as it tries to keep pace with the vast amount of cyber attacks. Here, we discuss the key challenges facing cyber security professionals, as well as some emerging threats which organisations and professionals are working hard to protect against.

Current challenges in cyber security

Phishing attacks

Phishing is a cyber attack that usually uses email as a weapon. The goal of attackers is to trick the email recipient into believing that the message is from a trusted source, and to either click on or download an attachment, or navigate to a fake site and enter their personal details. This is one of the oldest types of cyber attacks, dating back to the 1990s, and is still one of the most widespread. It is also becoming more sophisticated, with attackers using off-the-shelf tools and templates that very closely mimic real sources, like banks and government institutions. Nearly a third of all data breaches involve phishing.

Ransomware

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom, usually paid in Bitcoin or another cyber currency, in order to restore access to the data. Ransomware is often downloaded in email attachments that appear to come from a trusted source – a form of phishing. Once the malware is downloaded, it can take over the victim's computer. Some types of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users.

Increased data privacy regulation

Europe's GDPR law, which was launched in 2016, and the UK Data Protection Act 2018 and UK GDPR, which apply provisions of the GDPR to the UK, set out the key principles, rights and obligations for most processing of personal data in the UK. Companies operating in both the UK and the EU may need to comply with both the UK GDPR and the EU GDPR.

These laws give individuals more power over their data and enhance the responsibility of organisations in protecting the data they collect and use, including responsibility for data breaches. There are tough penalties for those companies and organisations that don't comply. For example, in 2020 British Airways was fined $26 million for a data breach that occurred in September 2018, and Marriott International was fined £18.4 million for a data breach between 2014 and 2018.

Cyber attacks on mobile devices

Recent research from RSA insurance found that in 2018, 80% of fraudulent transactions originated from mobile devices. As mobile devices increasingly touch every aspect of our personal and professional lives, they have become the focus for phishing, malware and other types of attacks. As many people now use their phones to conduct online banking, this makes mobile devices even more attractive to threat actors.

Emerging challenges in cyber security

IoT ransomware

The Internet of Things is made up of devices which are connected to the Internet and to each other. For example, home appliances, lighting and security cameras. Hackers can use these devices as a gateway to access more sensitive information within the network, as well as information in the devices themselves. Hackers are increasingly targeting IoT devices, especially those that control other devices, for ransomware attacks. Some hackers also aim to 'brick' the appliance or device with Brickerbots – rendering it useless.

For example, in 2019, a 14-year-old developed a piece of ransomware called Silex, which targeted IoT devices, for no apparent motive other than to cause financial loss. Silex works by destroying an IoT device's storage, dropping firewall rules, and removing network configuration, ultimately causing the device to stop functioning.

The Dark Web

Websites like Wikipedia, Google, Amazon, YouTube, and Facebook are only a small part of the Internet. Beyond these 'visible' websites are others that are not readily available to the general public. That is where the Dark Web and the Deep Web can be found.

The Dark Web is a general term for a collection of websites on encrypted networks with hidden IP addresses – all of which give users strong anonymity. Because they are not indexed by traditional search engines, they can only be accessed with special anonymity browsers.

The Dark Web isn't just for criminals. There are also legitimate reasons for using the Dark Web. In past years, it has gained popularity as a safe haven for whistle-blowers, activists, journalists, and others who need to share sensitive information, but can't do so out in the open for fear of political persecution or retribution by their government or employer.

Police and intelligence agencies also monitor the Dark Web to keep tabs on terror groups and cybercriminals. Additionally, corporate IT departments frequently crawl the Dark Web in search of stolen data and compromised accounts, and individuals may use it to look for signs of identity theft.

In many circles, the Dark Web has become synonymous with the Internet. It now plays host to a number of media organisations involved in investigative journalism, such as ProPublica and Intercept. WikiLeaks – the website that publishes classified official materials – and similar sites, also have a home on the Dark Web. Even Facebook maintains a presence there in order to make itself accessible in countries where it is censored by the government.

Cloud services

A cloud service is an Internet service made available to users on demand instead of from a cloud computing provider's servers. Cloud vulnerability will be one of the biggest cyber security challenges in the future as businesses are increasingly using cloud applications and storing sensitive data related to their employees and business operations on the cloud. This makes a tempting target for malicious hackers. Data breach, misconfiguration, insecure interfaces and APIs, account hijacking, malicious insider threats, and DDoS attacks are among the top cloud security threats that firms will be facing.

On top of this, cloud companies like Google and Amazon which store data belonging to other companies will be open to large-scale hacking and deep cyber intrusions like the 2016-2017 Cloud Hopper attack that accessed data stored on six major cloud service providers. Access management is one of the most common cloud computing security risks, because it is a key point of attack for hackers.

Deepfakes

Deepfakes are fake videos or audio recordings that look and sound just like the real thing. Once requiring the expertise and skills of Hollywood special effects studios or intelligence agencies like the CIA, today anyone can download deepfake software and create convincing fake videos in their spare time.

A key purpose of deepfakes is to create misinformation and fake news to undermine trust.

As well as all the ethical issues, fake news can also have a damaging effect on hardware too.

In the business world, AI-generated fake videos or audio recordings can be used to impersonate CEOs, steal millions from enterprises, spread incorrect and misleading information about companies that can affect their stock price and interrupt business operations.

In the future, deepfakes are expected to evolve into a sophisticated type of forgery, making it a huge cyber security threat.

AI-enhanced cyberthreats

This is related to deepfakes. AI and machine learning have disrupted every industry and are finding their way into the business mainstream. However, AI is also a boon for cybercriminals, who are developing ways to use AI to create malicious software that can adapt to evade those who are trying to eliminate it.

Hackers could integrate fuzzing techniques – the process of sending intentionally invalid data in the hopes of triggering an error condition or fault – with AI to create an automated tool that detects system vulnerabilities.

Example

In March 2019, the CEO of a UK energy provider received a phone call from someone who sounded exactly like his boss. The call was so convincing that the CEO ended up transferring $243,000 to a Hungarian supplier. But this was really a bank account that belonged to a scammer and the ‘boss’ was a deepfake that used AI to mimic the boss’s voice.

Section 2: Understand industry terminology used in cyber security

Did you know?

Full Fact is the UK's independent fact checking charity.

They are a team of independent fact checkers and campaigners who find, expose and counter the harm done by fake news.

www.fullfact.org

Knowledge Activity 9: Conduct research to find real world examples of a cyber attack that used a current technique, and an emerging technique for committing cyber crime.

Understanding social engineering

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

Social engineering is an attack that involves manipulating people into breaking normal security procedures in order to gain access to systems, networks or physical locations, usually for financial gain.

The criminals who carry out social engineering exploit the one weakness that is found in every person and organisation: human psychology. Usually using phone calls, emails and text messages, these attackers trick people into handing over access to sensitive information.

There are several common attack types that social engineers use to target their victims. These include phishing, spear phishing, vishing, and smishing.

Criminals use social engineering tactics because it is usually easier to exploit people's willingness to trust someone than it is to discover ways to hack software. For example, it is much easier to fool someone into giving out their password than it is to hack their password.

Security is all about knowing who and what to trust. It is important to know when and when not to take a person at their word, and when the person you are communicating with is who they say they are.

It doesn't matter how many locks, alarm systems, floodlights, fences with barbed wire, and armed security personnel you have; if you trust the person at the gate who says they are delivering pizzas and let them in without first checking to see if they are legitimate, you are completely exposed to whatever risk they represent. The same is true for cyber security. It doesn't matter how much anti-virus software you have if you then tell someone on the phone your password details.

Example

Real world spear phishing attack

One of the biggest social engineering attacks was perpetrated by a threat actor named Evaldas Rimasauskas against two of the world's biggest companies: Google and Facebook. Rimasauskas and his team set up a fake company – pretending to be a real computer manufacturer that worked with Google and Facebook, as well as bank accounts in the fake company's name.

The scammers then sent phishing emails to specific Google and Facebook employees, invoicing them for goods and services that the real company had genuinely provided – but directing them to deposit money into the fake accounts. Between 2013 and 2015, Rimasauskas and his associates cheated the two tech giants out of over $100 million.

Benefits of using social engineering for cyber criminals

Please read the following as it will help you to answer questions 22a and 22b.

Phishing is a low-investment, low-risk, high-reward strategy for cybercriminals. Some of the techniques used don't even rely on people being particularly gullible, and can snare almost anyone. For example, pharming is a type of social engineering where the cyber criminal redirects web traffic from legitimate sites to malicious clones that can be indistinguishable from the real site. Users think they are on a real site, and put in their personal information or payment details without realising they are on a fake site.

As soon as one scam is detected by authorities, new scams can be easily thought up, many of which respond to rapidly-changing world events. When vaccinations for the coronavirus first became available in the UK, scammers sent out phishing emails within days, pretending to be from the NHS, and directing people to enter their personal details on a cloned website in order to be scheduled for a shot.

Social media is also an easy place to gather information, especially as people often let their guard down while on social sites. For example, angler phishing uses spoof customer service accounts on social media to get people to divulge personal details. Fear is another strong motivator. Scareware takes the form of a pop-up that warns that your security software is out of date or that malicious content has been detected on your machine – fooling victims into visiting malicious websites or buying worthless or non-existent products.

Because these attacks rely on human error, many people are too embarrassed by them to report them, or when they do, the money stolen may be refunded by banks, giving police little incentive to pursue the thieves.

Example

In July 2020, Twitter lost control of 130 Twitter accounts, including those of Barack Obama, Joe Biden, and Kanye West. The hackers downloaded the data of high-profile users and used this to access their direct messages. They then made tweets requesting donations to a Bitcoin wallet. Within just a few minutes – even before Twitter could remove the tweets – the scammers had earned around $110,000 in Bitcoin from more than 320 transactions.

The vishing attack may have begun when Twitter employees were somehow tricked into revealing account credentials that allowed access to the compromised accounts. After the hack, the FBI launched an investigation into Twitter's security procedures.

Open source information

Please read the following as it will help you to answer questions 23a and 23b.

Open source information may be defined as information which is publicly available and which anyone can lawfully obtain by request, purchase, or review. A lot of open source information is easily obtainable by criminals.

This information comes from a variety of sources, including the social media pages of a company and its staff, websites and google searches. These can be a goldmine of information, revealing details such as the names of key staff, design of ID badges, layout of the buildings and software used on internal systems. Many attackers will claim to be from someone in IT or senior management as a way of gaining access to the organisation. This type of information can be readily found on platforms such as LinkedIn or by looking at the company's 'about us' webpage.

Often, seemingly innocent information shared through social networks and blogs can be used to develop highly convincing social engineering campaigns, which in turn are used to trick well-meaning users into handing over key information like passwords.

This is why using open source intelligence for security purposes is so important – it gives an organisation an opportunity to find and fix weaknesses in an organisation's network and remove any sensitive information before a threat actor uses the same tools and techniques to exploit them.

Information a cyber criminal could obtain through open sources

Please read the following as it will help you to answer questions 24a, 24b and 24c.

All you need to do is consider how you use social media in order to realise that there is likely to be a huge amount of open source information already available about you. This could include information about your job history, education, hobbies, birthdates, family, and more. All of this information could help threat actors to tailor their phishing attacks.

Gathering open source information does not require hacking into systems or using private credentials to access data. Much of this information can be obtained by Googling for a person's name, accessing their social media accounts or through a phone call, perhaps while pretending to be a government worker.

Company webpages can also be a good source of information on employee names, emails and job descriptions. Information like a person's address and what they paid for their house are easily found on legitimate websites. Just having access to someone's Facebook profile can show you information on their friends, relationship, personal interests, and family photos.

And there are many techniques for easily finding out more about someone online. For example, typing filetype:PDF "john" "doe" into Google could result in John Doe's resume – complete with contact information and employment history. And because most companies use a standard email format (e.g. first initial.last name@company.com), once you know the work email address of one employee, you know them all.

If the person or organisation owns a website you can grab information about it, revealing the operating system being used, software version, personal contact info, and more. There are any number of free-to-use resources out there that will help people gather open source information.

Knowledge Activity 10: Conduct research to find real world examples of a cyber attack that used open source information, and that demonstrates the type of information a cyber criminal could obtain.

Social engineering techniques

Please read the following as it will help you to answer questions 25a, 25b, 26a and 26b.

Phishing

Phishing is a very well-known way to grab information from an unwitting victim. Whilst it has been around for a while, it remains quite successful. The attacker typically sends an email or text to the target, seeking information that might help with a more significant crime. There are a huge number of different ways to conduct phishing attacks, including sending emails purporting to be from senior members of staff, targeting high-profile indviduals like senior management or CEO (this is a type of phishing called 'whaling'), rewriting unattended browser tabs with malware so the user thinks they are on a real site, when really they are on a fake site (this is called tabnabbing), etc.

Example

An attacker might send emails that appear to come from a source trusted by the would-be victims. That source might be a bank, for instance, asking email recipients to click on a link to log in to their accounts. Those who click on the link, though, are taken to a fake website that, like the email, appears to be the real site. If they log in at that fake site, they're essentially handing over their login credentials and giving the attacker access to their bank accounts.

In another form of phishing, known as spear phishing, the fraudster tries to target or 'spear' a specific person. The attacker will use social media to identify the name and email of, for example, a human resources person within a particular company.

The attacker then sends the HR person an email that appears to come from a high-level company executive. Some recent cases involved an email request for employee payroll data, which includes names, home addresses, and National Insurance numbers. If the attacker is successful, the victim will unwittingly hand over information that could be used to steal the identities of dozens or even thousands of people.

Did you know?

One of the simplest – and often most successful – social engineering techniques is to simply pretend to be your victim. In 2016, a hacker found out the email address of a U.S. Department of Justice employee and used it to impersonate the employee. He managed to convince the help desk to hand over an access token for the DoJ intranet by saying it was his first week on the job and he didn't know how anything worked.

Email hacking and contact spamming

It's in our nature to pay attention to messages from people we know. Some criminals try to take advantage of this by taking over email accounts and then sending out lots of emails spamming account contact lists. People are more likely to open emails from people they know, allowing scammers to gain access to insert malware or to pretend to be the sender and ask for money or information.

Example

If your friend sends you an email with the subject, “Check out this site I found, it’s totally cool,” you might not think twice before opening it. By taking over someone’s email account, a fraudster can make those on the contact list believe they’re receiving an email from someone they know. The primary objectives include spreading malware and tricking people out of their data.

Quid pro quo

This scam involves an exchange – I give you this, and you give me that. Fraudsters make the victim believe it’s a fair exchange, but that’s far from the case, as the cheat always comes out on top.

Example

A scammer calls a target, pretending to be an IT support technician. The victim is persuaded to hand over the login credentials to their computer, thinking they’re receiving technical support. Instead, the scammer takes control of the victim’s computer, uploads malware or steals personal information from the computer.

A recent and prolific recent example was the ‘Microsoft tech support scam’. In this social engineering fraud, a fake representative calls victims, spoofing the caller ID so it looks like the phone call really is coming from the software giant.

The scammer walks the victim through the process of installing applications that allow remote access to your computer. Or, the scammer may initiate contact by displaying fake pop-up messages on your screen that trick you into calling a fraudulent ‘support’ hotline.

With both scams, the goal is to get victims to pay, in the form of a one-time fee or subscription, to fix the problem.

Vishing

Vishing is the voice version of phishing. 'V' stands for voice, but otherwise, the scam is the same. One type of vishing attack involves sending recorded messages telling recipients their bank accounts have been compromised. Victims are then prompted to enter their details using their phone's keypad, giving the scammers access to their accounts.

Smishing

Smishing is any kind of phishing that involves a text message. Smishing is effective because people tend to be more likely to trust a text message than an email. Most people are aware of the security risks involved with clicking on links in emails. This is less true when it comes to text messages.

The scammer will send text messages that purport to be from legitimate entities. This is often used in combination with other techniques to bypass 2FA (two-factor authentication). They might also direct victims to malicious websites on their phones, where malware may be downloaded. Another technique is to say that if the victim doesn't enter their personal information they will be charged for use of a service.

Knowledge Activity 11: Conduct an audit of your social media use to identify ways in which you might be open to a social engineering attack.

Look through your social media accounts (including sites like Instagram, Facebook, LinkedIn, etc) and Google yourself and note down what types of information about yourself are easily obtainable. This could include personal contact information, date of birth, place of birth, etc., employment and education, history, information about your family and friends, sites and news organisations that you subscribe to, online sites you shop at frequently, political opinions, etc.

Write down some of the ways that this information might be used in a social engineering attack.

Summary

In this section, you have learned about:

- different terms related to cyber security
- the differences between LAN and WAN
- organisational strategies in cyber security
- current and emerging challenges in cyber security
- how social engineering attacks work and the types of information that cyber criminals can gain
- how cyber criminals take advantage of open sources of information

Section 3: Understand legal and ethical aspects of cyber security

In this section, you will learn about some of the key legislation related to cyber security, and how it is used to protect individuals, organisations and nations.

Key UK legislation relating to cyber security

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

The UK has a number of different pieces of key legislation which cover various aspects of cyber security:

- The Computer Misuse Act 1990
- The Data Protection Act 2018 / GDPR
- Official Secrets Act 1989
- The Privacy and Electronic Communications Regulations 2003

Computer Misuse Act 1990

The Computer Misuse Act 1990 protects personal data held by organisations from unauthorised access and modification. The four clauses cover a range of offences including hacking, computer fraud, blackmail and viruses.

The act makes the following illegal:

1. Unauthorised access to computer material. This refers to entering a computer system without permission (hacking).
2. Unauthorised access to computer materials with intent to commit a further crime. This refers to entering a computer system to steal data or destroy a device or network (such as planting a virus).
3. Unauthorised modification of data. This refers to modifying or deleting data, and also covers the introduction of malware or spyware onto a computer (electronic vandalism and theft of information).
4. Making, supplying or obtaining anything which can be used in computer misuse offences.

Failure to comply with the Computer Misuse Act can lead to fines and potentially imprisonment.

The Computer Misuse Act was first proposed when computers were a rarity in public life, and as a result, it used a fairly narrow definition of what was considered a malicious act. The rise of the digital age since the Act's passage has led to the insertion of a number of new sections.

In 2015, the Computer Misuse Act was amended to create a new offence of unauthorised acts causing serious damage; to bring the EU Directive on Attacks against Information Systems into UK law; and to clarify the protections for law enforcement if they break into a computer in the course of a criminal investigation.

The new offence of unauthorised acts causing serious damage was made partly to increase the penalties for the kinds of attack that might by classed as cyber terrorism.

The changes made in regard to the EU Directive on Attacks Against Information Systems focused on making it easier to prosecute cyber criminals who were using the UK as a base (even if they weren't physically located in the UK) as well as to allow the police and Crown Prosecution Service to pursue and prosecute UK residents for cyber crimes committed abroad.

The final provision was more controversial. Civil rights groups have argued that it gives an exemption under the law to police and spy agencies.

Data Protection Act 1998

In the 1990s, as more organisations began using digital technology to store and process personal information, there was a growing danger this information could be misused. The Data Protection Act of 1998 was designed to tackle this issue.

Data stored electronically is vulnerable as it is very easy to copy it to a removable drive or to email or transfer it via the Internet. Individuals who had data stored had several concerns:

- Who could access this information?
- How accurate was the information?
- Could it be easily copied?
- Was it possible to store information about a person without that individual's knowledge or permission?

The Data Protection Act 1998 aimed to safeguard information held about an individual classified as personal (e.g. name, address, financial details) or sensitive (e.g. ethnicity, political opinion, religion). The act ensures data stored is processed fairly and lawfully. For example, there are strict rules as to who can access and alter health records. Regular checks are made to ensure that the rules of the Data Protection Act are being followed.

Principles of the Data Protection Act 1998:

1. Data must be collected and used fairly and inside the law.
2. Data must only be held and used for the reasons given to the Information Commissioner.
3. Data can only be used for registered purposes. You cannot give it away or sell it unless this was stated initially. For example, a school could not sell pupils' data to a book or uniform supplier without permission.
4. The data held must be acceptable, appropriate and not beyond what is necessary when compared with the purpose for which the data is held.
5. Data must be accurate and be kept up to date. For example, making sure contact numbers are current.
6. Data must not be kept longer than is necessary. This rule means that it would be wrong to keep information about past customers longer than a few years at most.
7. Data must be kept safe and secure – for example, personal data should not be left open to be viewed by just anyone.
8. Data may not be transferred outside of the European Economic Area unless the country where the data is being sent has similar data protection laws. This part of the Data Protection Act has led to some countries passing compatible laws to allow computer data centres to be located in their jurisdiction.

Under the Data Protection Act 2018 (DPA), individuals have the right to find out what information the government and other organisations have on file. These include the right to:

- be informed about how your data is being used
- access personal data
- have incorrect data updated
- have data erased
- stop or restrict the processing of your data
- data portability (allowing you to access and reuse your data for different services)
- object to how your data is processed in certain circumstances

The DPA 2018 updated and replaced the Data Protection Act 1998. It was amended again on 01 January 2021, to reflect the UK's status outside the EU.

The amended DPA sits alongside and supplements the UK GDPR – for example, by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas, such as national security and defence, and sets out the Information Commissioner's functions and powers.

The law applies to anyone using information about people for any business or other non-household purpose and applies to most businesses and organisations, whatever their size. It does not apply to anyone using information for personal, family or household purposes – such as personal social media activity, private letters and emails, or use of your own household gadgets. For law enforcement and national security organisations, the updated DPA sets out the regulations for processing personal data.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation or GDPR came into effect in 2018. Essentially, it is an EU regulation that's designed to further strengthen data protection for everyone in the public, private and third sector, giving more control to individuals over how their data is used.

Some of the key privacy and data protection requirements of the GDPR include:

- Requiring the consent of subjects for data processing.
- Anonymising collected data to protect privacy.
- Providing data breach notifications.
- Safely handling the transfer of data across borders.
- Requiring certain companies to appoint a data protection officer to oversee GDPR compliance.

In effect, the GDPR set a basic level of standards for all companies and organisations that handle the data of EU citizens.

In the UK, the GDPR was brought into domestic law through the amended version of the DPA (2018) and the UK GDPR (2021). Post-Brexit, the main principles, rights and obligations of the GDPR remain the same. However, there are some new rules for the transfer of personal data between the UK and the EEA.

The GDPR requires that businesses keep personal data secure and only permit third parties access to the personal data if there are sufficient guarantees regarding security. Businesses must put in place safeguards that include physical measures (e.g. firewalls, anti-virus programs, perimeter scanning tools) and organisational measures (e.g. policies and procedures related to cyber security). Businesses are required to protect against unauthorised or unlawful use of personal data and against its loss, destruction and damage.

Failing to implement appropriate security measures to safeguard personal data can result in large fines (up to £20 million or 4% of annual global turnover, whichever is greater). Enforcement action can be taken even when there has been no cyber attack or data breach.

Any company that markets goods or services to EU residents, regardless of where it is located, is subject to the GDPR regulations. As a result, the GDPR also affects global data protection requirements.

The Privacy and Electronic Communications Regulations 2003

This directive works with the GDPR and sets out more specific privacy rights on electronic communications. It recognises that widespread public access to digital mobile networks and the Internet not only creates new opportunities for businesses and users, but also new risks to their privacy. It is mainly focused on the stopping of spam calls and unwanted marketing communications.

There are specific rules on:

- marketing calls, emails, texts and faxes
- cookies (and similar technologies)
- keeping communications services secure
- customer privacy such as the telephone directory listings

What is the Official Secrets Act?

The Official Secrets Acts 1911-1989 are four legal documents protecting the UK against espionage and the leaking of sensitive government information.

Offences covered by the acts include spying and sabotage, as well as the disclosure of sensitive information by employees and ex-employees of the security services. The penalty for breaching the Official Secrets Act is a maximum jail term of 14 years if the crime relates to spying or sabotage, and a maximum jail term of two years for offences under the 1989 Act.

In Scotland, the Scotland Act 1998 provides that members of the Scottish Executive and junior Scottish Ministers are to be considered as Crown servants for the purposes of the Official Secrets Act 1989. It also provides that people supplying goods or services for the purpose of office holders of the Scottish Administration are government contractors for the purposes of the 1989 Act.

Who has to sign it?

Employees and ex-employees of the security services, civil servants, law enforcement officers, judges, members of the armed forces and government contractors are among those subject to the Official Secrets Acts.

Even those who have not signed the act are bound by it, and government employees are usually informed they are subject to it in their contracts.

Did you know?

An Information Commissioner's Office (ICO) document describes how the ICO fined CRDNN Limited with the maximum £500,000 fine for making more than 193 million automated nuisance calls.

The company was raided by the ICO in March 2018, and computer equipment and documents were seized for further analysis of their nuisance call operation.

The subsequent ICO investigation revealed that CRDNN Limited was making nearly 1.6 million calls per day about window scrappage, debt management, window, conservatory and boiler sales between 1 June and 1 October 2018.

According to the ICO, "Some of the calls potentially put people's safety at risk as they were made to Network Rail's Banavie Control Centre, and clogged up the line for drivers and pedestrians at unmanned level crossings, who were calling to check it was safe to cross the rails.

The calls were all made from so-called 'spoofed' numbers, which meant that people who received the calls could not identify who was making them. The company broke the law by not gaining consent from the phone owners to make those calls and by not providing a valid opt out.

CRDNN Limited came to the attention of the ICO when more than 3,000 complaints were made about the nuisance calls."

Find Out More: Complete the table for each of the four acts, considering how they apply to individuals, businesses and nations.

Legislation	Who it protects (individual, business, or nation)	How it protects
The Computer Misuse Act 1990		
The Data Protection Act 2018		
Official Secrets Act 1989		
The Privacy and Electronic Communications Regulations 2003		

Ways to protect stored data

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

All the way through this workbook we have looked at the importance of keeping data secure; now we will look at it from an IT system point of view.

Measures that can be taken to keep data secure include:

- Making regular backups of files. If the worse was to happen, a recently saved copy of the data could be used to bring all the systems back with minimal impact.
- Protecting yourself and your organisation against viruses by running anti-virus software.
- Using a system of secure passwords so that access to data is restricted.
- Only allowing authorised staff access to data storage systems.
- Turning terminals off at night and locking them down with passwords.
- Using data encryption techniques to code data so that it makes no apparent sense if intercepted.

Back up early and often

The single most important step in protecting data from loss is to back it up regularly.

Individuals can use the backup utility built into Windows and Apple operating systems to perform basic backups and even set this up to be performed automatically.

There are also numerous third-party backup programs that offer more sophisticated options for individuals and businesses. Whatever program you use, it's important to store a copy of the backup offsite or in the cloud, in case of a disaster that can destroy an organisation's servers or other physical backups.

Password protection

For an organisation, all of the laptops, computers, tablets and smartphones in use will contain a lot of business-critical data, such as personal information on customers, and proprietary information. It is essential that this data is available only to authorised users.

Passwords, when set up correctly, are a free, easy and effective way to prevent unauthorised access. Some factors to consider include:

- Organisations should have a policy in place that requires everyone to use strong passwords.
- Passwords should not be left on notes by the device.
- Consider using a cloud-based password safe/vault.
- Strong passwords consist of a random string of letters (both capitals and lower case), numbers and symbols. A series of random words is easier to remember, but they must be truly random.
- Passwords should be changed regularly.
- Never use the same password twice – use a unique password for every service, and don't swap backwards and forwards between old and new passwords if a service demands that you input a brand-new password.
- Passwords should not be shorter than 12 to 14 characters in length.

Did you know?

World Password Day occurs each year on the first Thursday of May. There's no better time than the present for organisations to assess cyber-hygiene best practices for keeping data and devices secure from cyber threats.

The use of anti-malicious software

Anti-virus or anti-malware secures data by protecting against many types of malware, including all types of viruses, as well as rootkits, ransomware and spyware. Anti-malware software can be installed on an individual computer, server or mobile device.

There are many types of anti-malicious software. The exact type you use will depend on the system you use and the level of security you need.

Performing operating system updates

Many malware attacks take advantage of software vulnerabilities in common applications, like operating systems and browsers. These are programs that require regular updates to remain safe and stable.

Operating system updates are some of the most essential steps you can take when it comes to protecting your information. In addition to making security fixes, software updates can also include new or enhanced features, allow compatibility with different devices or applications, improve the stability of your software and remove outdated features. You can schedule regular, automatic updates.

Share vs. file level security

These are different types of permission for accessing networks and files. Share permissions manage access to folders shared over a network. For example, they allow everyone on a project to access the documents used in that project. They don't apply to users who log on locally, so any documents kept on an individual computer are not shared.

There are three types of share permissions – Full Control, Change and Read:

- Read – users can see what is in the file or folder, but cannot make changes.
- Change – users can read files, and can also add files, change the data in files, and delete files – but not folders.
- Full Control – users can do everything in both Read and Change, and they can also change permissions and delete folders.

File or NTFS permissions determine the action users can take for a folder or file both across the network and locally. Unlike share permissions, NTFS permissions offer several other permissions besides Full Control, Change, and Read that can be set for groups or individually. Here you can change who has visibility of folders and who can access the specific folder by putting specific users into groups.

For example, senior managers may have full access to folders containing the company accounts across the network; however, you would not want the office administrator or receptionist to have access to these key documents unless authorised. To do this, the senior management team would be assigned access as a group through the NTFS permissions, whereas all other groups would be denied access.

Encryption

File and disk encryption is an important and necessary way to protect data stored on a computer or network.

Disk encryption doesn't completely protect a computer. Hackers can still access the computer over an insecure network connection, or infect the computer with malware. However, encrypting a computer's files or the entire hard disk greatly reduces the risk of data theft.

Encryption works like a form of digital cryptography. It uses mathematical algorithms to scramble messages, so that only individuals who have the digital key are able to decrypt and access the messages. Encrypted files can often be seen in a file listing, but they cannot be accessed and read without the key.

Many operating systems have built-in encryption.

For example, Windows supports an encryption system called the Encrypting File System (EFS). You can use this built-in certificate-based encryption method to protect individual files and folders stored on Windows machines. Encrypting a file or folder is as easy as checking a box.

There are many products available that will allow you to encrypt an entire disk, for example, by locking down the entire contents of a disk drive/partition. Data is automatically encrypted when it's written to the hard disk and automatically decrypted before being viewed.

Disk encryption products can also be used to encrypt removable USB drives, flash drives, etc. Some allow creation of a master password along with secondary passwords that allows you to give partial access to other users. There are two main methods of encryption: symmetric encryption and asymmetric encryption.

Knowledge Activity 12: Think about the passwords that you use for your data. How secure are they? Write down some ways that you could make them more secure.

How to encrypt information

Please read the following as it will help you to answer questions 29 and 30.

The encrypting of data is vitally important as a measure to protect files. Two common encryption types are:

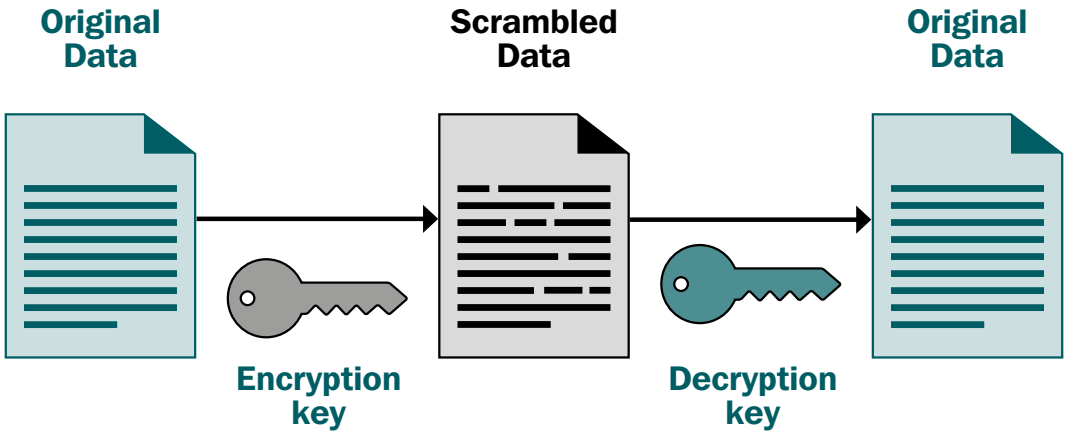
- symmetric encryption (also called secret key encryption)
- asymmetric encryption (also called public key encryption

The basic difference between these two types of encryption is that symmetric encryption uses one key for both encryption and decryption, and asymmetric encryption uses a public key for encryption and a private key for decryption.

Let's explore each of these encryption methods separately to understand their differences better.

Symmetric encryption

In symmetric-key encryption, each computer has a secret key that it can use to encrypt information before it is sent to another computer, where it is decoded. It is like a secret code that both computers must know in order to decrypt the information. The code provides the key to decoding the message.



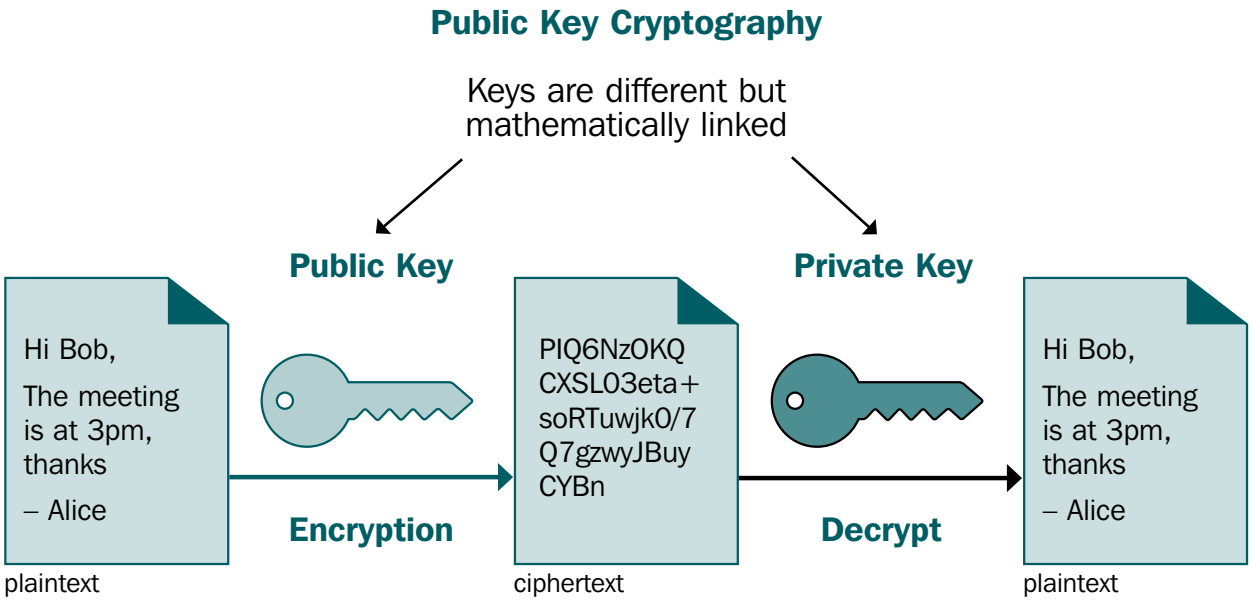
The standard used for encryption is called the Advanced Encryption Standard (AES). This uses 128-, 192- or 256-bit keys. A 128-bit key, for instance, can have more than 300,000,000,000,000,000,000,000,000,000,000,000 key combinations, making it time consuming to break this type of encryption using brute force techniques (trying every combination).

This encryption method is best suited for encrypting files and drives. Because the key is often derived from a password, one weak spot with symmetric-key encryption is that it is only as strong as the password itself.

Asymmetric encryption

Unlike symmetric-key encryption, asymmetric-key encryption uses two different keys at the same time – a public key and a private key. This type of encryption is commonly used for sending information between two devices.

Public-key encryption uses two different keys at once – a combination of a private key and a public key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it.



To decrypt an encrypted message, a receiving computer must use the public key, provided by the originating computer, and its own private key. Although a message sent from one computer to another won't be secure, since the public key used for encryption is published and available to anyone, it can't be read without the private key.

The key pair is based on very long prime numbers. This makes the system extremely secure, because there is essentially an infinite number of prime numbers available, meaning there are nearly infinite possibilities for keys. One very popular public-key encryption program is Pretty Good Privacy (PGP), which allows almost anything to be encrypted.

In order to use public-key encryption on a large scale, such as with a Web server, a different method is used – digital certificates. A digital certificate is basically a unique piece of code, or a very large number, that is authorised by an independent source known as a certificate authority. The certificate authority is a middleman that both computers trust.

The certificate confirms that each computer is in fact who it says it is, and then provides the public keys of each computer to the other.

The Secure Sockets Layer (SSL) is an Internet security protocol that makes use of a certificate and public-key encryption. It is part of a larger security protocol known as Transport Layer Security (TLS).

In your browser, you can tell when you are using a secure protocol because the 'http' in the address line is replaced with 'https', and a small padlock will appear in the status bar at the bottom of the browser window.

Once your browser requests a secure page and adds the 's' onto 'http', it will send out the public key and the certificate, and check that the certificate is valid and comes from a trusted party, and that the certificate belongs with the site from which it's coming.

Advantages and disadvantages of encryption techniques:

- Symmetric encryption is faster to run because the keys used are much shorter than those used in asymmetric cryptography. This allows symmetric encryption to handle a greater volume of data in a given time.
- Symmetric encryption is the preferred method for encrypting long messages or large files because it will not place a heavy load on processors, memory capacity or the batteries of portable devices.
- In symmetric encryption, the key needs to be transmitted between the communicating devices and it can be intercepted.
- Asymmetric encryption is more secure, because it uses two different keys.
- Asymmetric encryption is slower and takes more processing power and energy.
- In asymmetric encryption, once your private key is identified by an attacker, then all of your messages can be accessed.

Movement of data

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

Data in transit vs data at rest

Data in transit refers to data that is moving from one location to another, such as across the Internet or through a private network.

Data protection in transit is the protection of this data while it's travelling from network to network or being transferred from a local storage device to a cloud storage device – wherever data is moving, effective data protection measures for data in transit are critical, as data is often considered less secure while in motion.

Data at rest refers to data that is not moving from device to device or network to network, such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way. Protecting data at rest involves securing inactive data stored on a device or network. While data at rest may be less vulnerable than data in transit, it can also be a more valuable target than data in motion.

In either case, protecting sensitive data both in transit and at rest is important, as attackers find increasingly innovative ways to compromise systems and steal data.

The role of encryption in data protection in transit and at rest

Data can be exposed to attacks both in transit and at rest and requires protection at both times. There are a number of approaches to protecting data in transit and at rest. For example, encryption is a popular tool for securing data both in transit and at rest.

Best practices for data protection in transit and at rest

While data in transit and data at rest may have slightly different risk profiles, the risk lies primarily in the sensitivity and value of your data; attackers will attempt to gain access to valuable data in whichever state is easiest to breach. That's why a proactive approach is the safest and most effective way to protect sensitive data.

Security checks made by an organisation before releasing information

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

Data sharing usually means disclosing personal data to third parties outside of the organisation.

In the UK, organisations have to be extremely careful with how they share and distribute personal information.

Organisations are usually very familiar with protecting personal information they hold themselves, but establishing appropriate security in respect of shared information usually presents new challenges.

Before sharing information an organisation should:

- Review what personal data your organisation receives from other organisations, making sure you know where it came from.
- Review what personal data your organisation shares with other organisations, making sure you know who has access to it and what it will be used for.

These two areas are what an organisation would call a due diligence check. This means ensuring that all key security checks are complete before handing over personal information.

An organisation should also assess whether and how to share any data that is particularly sensitive.

Due diligence also involves identifying who has access to information that other organisations have shared with your organisation. You should avoid giving anyone access to shared information they do not need to carry out their job.

There should be robust security policies and procedures in place, and all staff members in the organisation who are involved in the sharing of information should be aware of these policies and procedures.

For both parties, it is good practice to have a data sharing agreement in place. This will set out the purpose of the data sharing, cover what is to happen to the data at each stage, set standards of data management and help all the parties to be clear about their roles. This will help you to demonstrate your accountability under the GDPR.

Example - Bounty UK fined £400,000 for sharing personal data unlawfully

In 2019, the Information Commissioner's Office (ICO) fined Bounty (UK) Limited £400,000 for illegally sharing personal information belonging to more than 14 million people.

According to the ICO, an investigation found that "Bounty, a pregnancy and parenting club, collected personal information for the purpose of membership registration through its website and mobile app, merchandise pack claim cards and directly from new mothers at hospital bedsides.

But the company also operated as a data broking service until 30 April 2018, supplying data to third parties for the purpose of electronic direct marketing.

Bounty breached the Data Protection Act 1998 by sharing personal information with a number of organisations without being fully clear with people that it might do so.

The company shared approximately 34.4 million records between June 2017 and April 2018 with credit reference and marketing agencies, including Acxiom, Equifax, Indicia and Sky.

These organisations represented the four largest recipients out of a total of 39 organisations which Bounty confirmed it shared personal data with.

The personal information shared was not only of potentially vulnerable new mothers or mothers-to-be, but also of very young children, and included the birth date and sex of the children."

Steve Eckersley, ICO's Director of Investigations, said:

"*The number of personal records and people affected in this case is unprecedented in the history of the ICO's investigations into data broking industry and organisations linked to this.*

"*Bounty were not open or transparent to the millions of people that their personal data may be passed on to such large number of organisations. Any consent given by these people was clearly not informed. Bounty's actions appear to have been motivated by financial gain, given that data sharing was an integral part of their business model at the time.*

"*Such careless data sharing is likely to have caused distress to many people, since they did not know that their personal information was being shared multiple times with so many organisations, including information about their pregnancy status and their children.*"

Knowledge Activity 13: Imagine that you are working for an organisation which collects personal data about a large number of customers. What policies and procedures would you put into place to safeguard that information?

Ethical conduct in cyber security

Please read the following as it will help you to answer questions 33 and 34.

What are ethics in digital technology?

Ethics are "a system of principles and customs that affect how people lead their lives". Although we do not have to follow these principles or ethics, it is generally in the best interests of everyone that we do.

Ethics are different to legislation or laws that legally dictate what is right and wrong. Ethics are more about society's opinions about what is right and wrong.

When we think about ethics in digital technology, we are considering how society treats the use of digital technology and the development of hardware and software.

For example, should a company be allowed to sell your search history to third parties? Should an employer be allowed to access your social media history? How should you conduct yourself when online?

Section 3: Understand legal and ethical aspects of cyber security

Because cyber security professionals are responsible for keeping data, computer systems and networks safe, they are also protecting the lives, livelihoods and happiness of those who depend upon them. For example, if you are a cyber security professional responsible for securing a hospital's network and critical data, you are also involved in protecting sick patients, even though you are not a health care worker. Patients' privacy and health are in your hands.

This means that ethical issues are at the core of cyber security practices. Given the increasing complexity and difficulty of securing data, the ethical responsibility that falls on cyber security professionals is growing.

Examples of ethical conduct in cyber security

Following company IT policy

Organisational IT policies are written to ensure that personal customer and company information is protected, and that there is a balance between work efficiency and risk.

Some basic organisational IT policies could include:

- Not visiting harmful sites from work devices.
- Not connecting personal devices to the organisation's WiFi.
- Not accessing company servers from personal devices.

Not following these types of IT policies could leave companies and customers exposed to loss of information, hacking, and financial penalties.

Maintaining confidentiality

In the course of their job, cyber security professionals often have access to confidential information, including personal information about employees, customers and clients, and information about the organisation they work for. It is very important that they keep this information confidential, both to protect the people and organisations involved, and to protect the reputation of their employer.

Adherence to applicable laws

Cyber security professionals in the UK have both an ethical and a legal duty to adhere to various types of legislation, such as the GDPR. Failure to do so can have a negative effect on their employer, and on those whose information was compromised.

Promoting information security

Effective security awareness training is essential in order to identify and respond appropriately to the growing range of cyber security threats. All employees, at every level of the organisation, should receive training to ensure they have the skills required to identify an attack. Cyber security awareness training should be engaging and informative, to ensure that staff understand what is required of them and the importance of their role in safeguarding the organisation's sensitive data.

Security awareness training should:

- Educate staff on the cyber threats faced.
- Raise awareness of the sensitivity of data on systems.
- Ensure procedures are followed correctly.
- Provide information on how to avoid phishing emails and other scam tactics.
- Reduce the number of data breaches.
- Build a culture of enhanced security compliance.

Organisations have an ethical duty to provide this training in order to protect their employees, clients and customers from data breaches.

Refraining from conflicts of interest

A conflict of interest arises when a person owes a duty, or believes they owe a duty, to two competing interests. For example, if a cyber professional is asked by an employer to grant someone access privileges that they think are inappropriate, or that place security at risk. In this case, the cyber security professional may feel they have a duty to both the employer and to those whose information may be at risk. This is an ethical conflict of interest.

It is not always possible to avoid conflicts of interest, but all organisations should have a policy in place that sets out what should be done in the case of a conflict of interest. The policy should clearly set out what a conflict of interest is, what steps should be taken, when a conflict must be reported, and who is responsible for making a decision.

Unethical conduct within cyber security

Cyber security professionals are often in a position to engage in different types of unethical conduct. Some of this may seem, at the time, like something that will not cause any damage – such as looking up the credit score of a friend at their request – but which is still clearly unethical behaviour and violates a professional duty of cyber security practice. Some common types of unethical behaviour include:

- Sabotage – damaging equipment or files.
- Misusing or disclosing confidential information – looking up confidential information without a legal reason, selling or giving confidential information to others, or manipulating information.
- Using information maliciously – this could include to get revenge or to damage the reputation of a business or a person, posting confidential information on social media, or simply discussing confidential information with fellow employees who do not have access to that information.

It is not always completely clear what types of behaviour are unethical. For example, if your organisation is slow to report a data breach, at what point is the delay unethical? A week? A year? Or, how does your organisation respond to a request from a law-enforcement agency to weaken your organisation's encryption practices or to decrypt specific devices? This is why it is important that all organisations have a clear policy regarding ethical and unethical conduct and who is responsible for making decisions.

Did you know?

A British man was sent to prison for two years after he wiped out his ex-employer's business-critical data in cloud storage, according to a report by the Thames Valley Police.

The report describes how Steffan Needham, of Bury, Greater Manchester, worked as an IT consultant at a digital marketing and software agency called Voova for four weeks in early 2016. After he was sacked for poor performance, he used a former coworker's Amazon Web Services (AWS) account to access 23 AWS servers, where he deleted data related to Voova's customers.

The rampage cost the company £500,000 in lost contracts, causing it to let a number of employees go. The data was never reconstituted. The case is a good example of the need for effective data protection and recovery strategies.

Knowledge Activity 14: Read the following case study and answer the questions about it.

Case study: In 2015, Mattel released its WiFi-enabled Hello Barbie doll. The doll's microphone was able to record what a child said to the doll, sending it by WiFi to a third party for audio language processing. The doll would then offer the child an appropriate natural language response. Because the conversations were stored in the cloud, parents could monitor the child's conversations with the doll and even share the audio clips of their children's conversations online.

However, security professionals soon discovered that they were able to hack into the doll, giving them access to the doll's system information, account information, stored audio files, the ability to override security features to turn on the microphone, and even give them direct access to the doll's microphone. Security researchers argued that there had not been enough analysis of the security risks of the doll before it was put on sale. The doll was discontinued.

1. What ethical duties did the manufacturer have to parents who bought this doll? Did they meet those ethical duties?

2. Did the hackers act ethically or unethically in hacking into the system and pointing out its flaws?

3. What are the potential benefits and harms of a toy like this? Could a toy like this have benefits that would be significant enough to justify the risks of harm you have identified?

4. Did the manufacturer have an especially strong ethical duty to offer cyber security protections for users of their product? Did they fulfil that duty?

Summary

In this section, you have learned about:

- some of the key legislation related to cyber security and how it protects individuals, businesses, and nations
- ways of protecting stored data
- advantages and disadvantages of different data encryption techniques
- types of security checks that might be undertaken before releasing information
- what constitutes ethical and unethical conduct in cyber security

Section 4: Extension activities

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

Introduction to cyber security

Extension Activity 1: Research the different job functions and job positions that exist in cyber security.

Section 4: Extension activities

Extension Activity 2: Research ways that the NCSC, GCHQ and ICO prevent cyber attacks.

Understand terminology used in cyber security

Extension Activity 3: Research some different types of hardware, software and applications used in cyber security.

Section 4: Extension activities

Extension Activity 4: Research different types of cyber attack not covered in this workbook.

Understand legal and ethical aspects of cyber security

Extension Activity 5: Research different ways of maintaining data confidentiality and security not covered in this workbook.

Section 4: Extension activities

Extension Activity 6: Conduct further research on some of the ethical issues in cyber security.

Well done!

You have now completed Workbook 1 and should attempt the assessments. If you require any help or guidance, please contact your Assessor/Tutor.

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.

NCFE ENDORSED

LCG-PCS (603/5853/1)

PC2B.4.23