NCFE Level 3

Certificate in Cyber Security Principles

(603/5762/9)

Unit 1:

Understand cyber security principles

WORKBOOK

Name:

Tutor:

ncfe. endorsed

Unit 1:

Understand cyber security principles

Contents

Section 1:

Understand cyber security

1.1 The concepts of cyber security

Cyber security includes a large number of basic concepts. Here, we will review a few of the most common.

Security: In the field of IT, security refers to the protection of computer systems and networks from breaches, damage and theft of information. Cyber security is the protection of internet-connected systems such as hardware, software and data from cyber threats. Security includes everything from fences and security passes to network security and anti-malware software.

Identity: In cyber security, identity has to do with managing access to resources in order to keep systems and data secure. A big part of cyber security systems involves verifying users' identities before they are granted access to workplace systems and information.

Confidentiality: The purpose of confidentiality is to ensure that data is protected by preventing the unauthorised disclosure of information. This includes aspects such as only giving access to information to those with legitimate authorisation. There are a number of measures that are used to assist with confidentiality, including multi-factor authentication, strong passwords, encryption, segregation of data, and assigning appropriate user privilege levels.

Integrity: This is the principle that a cyber security system, and professional, should work to ensure the accuracy, trustworthiness and validity of information. It is important to put effective measures in place to prohibit the alteration or theft of data by unauthorised individuals or processes.

Some of the measures that are used to prevent unwanted modifications, and to ensure that information can be restored if altered, include making regular backups and putting in place effective access privileges, version controls and input validation. Ways that data integrity can be affected include through human error, lack of encryption systems and the theft or physical compromise of a device.

Availability: This refers to the principle that information should be accessible to authorised personnel as and when it is needed. Availability relies on proper and effective maintenance and security of hardware, software, equipment and communication channels that are used to store and process information.

Methods used to protect organisations from loss of availability include performing regular updates, installing DDoS protection, having redundant systems, firewall and proxy servers in place, and ensuring adequate bandwidths and the use of access controls. In the event of a security breach/attack, steps for maintaining availability should be included in the organisation's Incident Response plan.

Threat: A cyber security threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks, malware, etc.

Cyber threats can come from within an organisation or from unknown threat actors from outside an organisation. Threat actors can include individuals such as criminals, hackers and disgruntled insiders, or other organisations, governments and even natural disasters. Some common types of cyber threat include:

- malware
- spyware
- phishing attacks
- distributed denial of service (DDoS) attacks
- ransomware
- zero-day exploits
- advanced persistent threats
- Trojans
- wiper attacks
- intellectual property theft

Vulnerability: In cyber security, a vulnerability is a weakness that can be exploited by cyber criminals to gain unauthorised access to a computer system. After exploiting a vulnerability, a cyber attack can run malicious code, install malware or steal sensitive data.

Vulnerabilities can be exploited by a variety of methods including SQL injection, buffer overflows, cross-site scripting (XSS) and open-source exploit kits that look for known vulnerabilities and security weaknesses in web applications.

Risk: Cyber risk, or cyber security risk, is the potential exposure to loss or harm from an organisation's information or communications systems. A cyber attack, such as from malware, is a type of risk. However, cyber security risk also includes theft of intellectual property, productivity losses, risk of being fined by regulatory bodies and reputational harm.

Hazard: A cyber security hazard is anything that could lead to a breach or theft of data. Hazards can include the type of organisation, how it operates online, where it's located, and the access it provides employees, business partners and customers. For example, having an online application database could be a hazard if it risks exposing customers' personal information. The organisation would then need to decide if this is an acceptable hazard, or if the risk from this hazard needs to be mitigated.

Stretch and challenge

For each of the categories above, write out a definition or explanation in 140 characters or less.

1.2 The importance of cyber security

Cyber security is essential for protecting all types of data from theft and damage. This includes sensitive data, personally identifiable information (information that could be used to identify a specific individual), health information, intellectual property, financial data, and governmental and industry information.

Without an effective cyber security programme, an organisation cannot defend itself against data breaches and theft of data, making it a tempting target for cyber criminals.

The increasing use of the internet for banking and business, along with the growth of cloud services and the Internet of Things, means that it is becoming even more important to integrate cyber security into all computing systems and networks. At the same time, cyber criminals are becoming more sophisticated and better organised. This means that a simple firewall and some antivirus software are no longer enough to protect organisations (and individuals) from cyber crime.

On top of this, cyber crime is constantly changing and evolving to adapt to security measures. So, cyber security must also constantly change and evolve in order to stay one step ahead of the criminals.

Organisations of all sizes also need to be informed about their duties under regulations such as the GDPR, and how to meet these. In addition to making cyber crime more common, the growth of the internet also means that ordinary people are better informed about security breaches at large organisations. This means that a breach can now cause irreversible reputational damage to the organisations involved.

Did you know?

According to a study by the UK government, in March 2021, four out of every ten UK businesses (39%) and a quarter of charities (26%) reported either a cyber security breach or an attack in the previous 12 months.

Among organisations that suffered from breaches or attacks, around a quarter experienced them at least once a week. The most common types were phishing attacks (around 81% of organisations reported these), followed by impersonation (around 25%).

The study also found that one in five of the organisations that suffered from a cyber attack ended up losing money, data or other assets, while one-third reported having to spend time and money responding to the breach, or lost business because of it. The mean cost of a cyber security breach to organisations was estimated at £8,460.

The survey also found the following actions had been taken by organisations:

- 43% of businesses and 29% of charities had taken out some form of cyber insurance.
- 34% of businesses and 32% of charities had conducted a cyber security risk assessment.
- 20% of businesses and 14% of charities had conducted staff testing, such as mock phishing exercises.
- 15% of businesses and 12% of charities had carried out cyber security vulnerability audits.

1.3 The consequences and implications of inadequate cyber security

A successful cyber attack can cause major damage to an organisation or individual. It can lead to a loss of revenue, as well as the time and money spent on fixing the problem, and can also cause a loss of trust and even regulatory fines.

The possible consequences of an attack can also include the loss of:

- Sensitive data: this can be sold on for money or used by competitors.
- Personally identifiable information: this includes information that can be used to identify specific individuals for attacks such as spear phishing.
- Protected health information: this is often the target of cyber blackmailers.
- Personal information: this includes information such as birthdates and addresses that can be used in phishing attacks.
- Intellectual property: this can be sold on for money or used by competitors.
- Industrial information systems: detailed information on this can be used to launch more sophisticated and damaging attacks.

Loss of any or all of these types of data can have economic, reputational and legal consequences.

Economic costs of cyber attacks

Financial gain is the main goal for most cyber criminals. All of the types of data mentioned above can be sold on to other thieves, used in phishing attacks or used to steal money directly from individuals and organisations. Cyber attacks often result in substantial financial loss arising from:

- theft of proprietary information and intellectual property, such as formulas, which can be sold to competitors
- theft of financial information (e.g. bank details or payment card details) which can be used in financial crimes
- disruption to trading (such as the inability to carry out transactions online) which can cause loss of revenue
- loss of business or contracts from reputational damage

Businesses that suffer a cyber breach will also have costs associated with repairing the affected systems, networks and devices. These costs can include the time taken to repair the damage, money spent on repairing the damage or on investing in security testing and anti-malware software, etc., and money lost while the systems are offline.

Reputational damage

Trust is an important element of consumer relationships. Cyber attacks can damage an organisation's reputation and erode the trust that customers or clients have in the organisation. This, in turn, could potentially lead to:

- loss of customers
- loss of sales
- a reduction in profits

Reputational damage can also impact on an organisation's suppliers, or affect relationships between organisations and their partners, investors and other third parties, such as government bodies. This damage to reputation and goodwill can be more damaging than the actual data loss itself.

Legal consequences of cyber breaches

Data protection and privacy laws require organisations to manage the security of all personal data that they hold. If this data is accidentally or deliberately compromised, and the organisation had failed to use appropriate security measures, they may face fines and other types of regulatory sanctions.

There may also be other ways that a cyber security attack can have legal consequences. There is the risk that a hacker might obtain sensitive information such as bank account or credit cards details. There are open markets for such information on the 'Dark Web'. If others access such sensitive information, the organisation might find its banking or credit card facilities withdrawn or in breach of privacy laws. A third party might also file a lawsuit against an organisation if they have themselves incurred a loss.

Case study

The accountant for a small hotel, the Rendezvous Inn, began to receive insufficient fund notifications from the hotel's bank when he tried to pay the hotel's monthly bills. The accountant notified the CEO, who conducted a review of the accounting records and found a serious problem.

A few weeks earlier, the CEO had clicked on a link in an email that they thought was from HMRC. It wasn't. When they clicked the link and entered their credentials, cyber criminals captured the CEO's login information. This gave them full access to the CEO's business and personal details, including banking information. The criminals quickly emptied the hotel's bank account of more than £1 million and accessed the hotel's computer system, stealing the details of people who had stayed there in the past.

What might be some of the consequences of this attack for the hotel?

Section 2:

Understand core terminology and key aspects of cyber security

2.1 Define core terminology used in cyber security

As with any area of study or career, there is a lot of specialised terminology used in cyber security. We will review some of the core terminology.

Malicious software

This is an umbrella term that describes all types of malicious software designed to steal data or damage software and systems. Some common types of malicious software include: viruses, Trojans, worms and ransomware.

Cloud computing

Cloud computing involves the delivery of computing services – including servers, storage, databases, networking, software, analytics, and intelligence – on demand over the internet ('the cloud'). When organisations or individuals use the cloud, they are using the computing provider's servers as opposed to servers located on the organisation's own premises.

There are three main models of cloud computing – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). IaaS offers infrastructure of virtual servers, network, operating systems and data storage drives. It removes the need for keeping hardware in the office, which makes it ideal for small and medium sized organisations. PaaS is where organisations can develop and run their own applications using the infrastructure and software framework provided by cloud computing providers. SaaS involves using software over the internet. Organisations or individuals pay using subscription or a pay-per-use model.

Software

Software includes all of the instructions that tell a computer what to do. It is the entire set of programs, procedures, and routines associated with the operation of a computer system. The operating system is the most important software that runs on a computer. It manages the computer's memory and processes, as well as all of its software and hardware.

Domain

A domain is a group of computers, printers and devices that are interconnected and governed as a whole. For example, a work computer is usually part of a domain at a workplace.

Exploit

This is a broad term that describes any malicious application or script that can be used to take advantage of a computer's vulnerability.

Breach

This is the act of successfully exploiting a vulnerability in a computer or device, to gain access to its files, data and network.

Firewall

Firewalls are software or hardware that work as a filtration system for data before it enters your computer or network. Firewalls scan packets of data for malicious code or viruses that have already been identified as a threat. Suspicious data packets are flagged as a security risk and prevented from entering the network or computer.

By putting protective filters in place around your network and devices, firewalls can help to prevent a number of different security risks, including backdoors (a hidden way to access and exploit a system); macros (scripts that applications can run to streamline a series of complicated procedures into one executable rule); remote logins; spam; and viruses.

There are several different ways security firewalls can monitor and regulate network traffic. These methods can include:

- Packet filtering: This runs incoming packets against a group of filters. These remove the packets that match certain identified threats and allow the others through to their intended destination.
- Proxy service: These function as go-betweens to prevent direct connections between the customer device and the incoming packets.
- Stateful inspection: This type of firewall examines a variety of elements of each data packet and compares them to a database of trusted information. The elements include source and destination IP addresses, ports, and applications. The information on incoming data packets must match the trusted information in order to be allowed through the firewall.

Encryption

This is the process of encoding data to prevent theft by ensuring the data can only be accessed with a secret encryption 'key' – a collection of algorithms that scramble and unscramble data back to a readable format.

There are two types of encryption systems: symmetric encryption and asymmetric encryption. Symmetric encryption uses a single password to encrypt and decrypt data, while asymmetric encryption uses two keys for encryption and decryption. These are: a public key, which is shared among users and encrypts the data, and a private key, which is not shared and which decrypts the data.

Bring Your Own Device (BYOD)

This refers to a policy used by many organisations where employees are allowed to use their personal devices at work. A BYOD policy sets limitations and restrictions on whether or not a particular phone or laptop can be connected over the corporate network, and may also involve installing firewalls on personal devices.

Denial of Service (DoS) attack

A denial-of-service (DoS) attack occurs when users are unable to access information systems, devices, or other network resources due to the actions of a cyber threat actor. DoS attacks, for example, can stop people accessing company resources, such as their websites. DoS attacks can cost an organisation both time and money while their resources and services are inaccessible, and they can damage an organisation's reputation.

Distributed Denial of Service (DDoS) attack

A distributed denial-of-service (DDoS) attack occurs when multiple computers are operating together to attack one target. DDoS attackers often use a botnet, a group of hijacked internet connected devices, to launch attacks. DDoS attacks are used predominantly against websites and file storage, taking away the ability to access various resources. DDoS attacks can cost an organisation considerable time and money to restore services, and an attack may occur over days or even weeks.

Penetration testing (pen testing)

This is a way of evaluating security using the same tools and techniques as hackers, with the aim of discovering vulnerabilities and evaluating security flaws. There are a number of different types of pen test. These include:

- External network penetration test: This involves an ethical hacker trying to break into an organisation's network across the internet. It is done off-site (as a hacker would be), using controlled and agreed ethical hacking techniques to accurately simulate a targeted attack from malicious parties on your network.
- Internal network penetration test: This simulates either the actions a hacker might take after gaining access to a network, or the actions of a malicious actor, such as a disgruntled employee, with access to the system. The end target is ultimately the same as an external penetration test (above), but the starting point assumes a degree of network access already.
- Web application penetration test: This looks for any security issues that might have arisen as a result of insecure development, design or coding, and identifies potential vulnerabilities to websites and web applications, including CRM, extranets and internally developed programmes, which could lead to exposure of data.

Research task - Terminology

In addition to the terms mentioned above, research some other common terms used in cyber security and write a short definition for each one.

2.2 Explain the terms good actors and bad actors

While most people are familiar with the idea of a hacker as the 'bad guy', there are actually a number of different types of hacker, including many that are involved in the security industry. The terms 'good actor' and 'bad actor' are often used to distinguish between someone who breaks into computers or systems in order to cause damage or steal information (bad actor) and someone who breaks into computers or systems in order to test them.

Here we take a look at some of the different categories of both good and bad actors.

Bad actors

These are people whose goal is to cause damage or steal data. There are many different types of bad actors, and they all have somewhat different motivations.

Black hats – these are the stereotypical 'hackers' portrayed in movies and TV as sitting in a dark room hammering away on a keyboard. While some black hat hackers act on their own, trying to exploit cyber security vulnerabilities, they can also work as hackers-for-hire. These people often advertise their services on the Dark Web.

Script kiddies – 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.

Hacktivist – hacktivists are actors who are politically, socially, or ideologically motivated, and target victims for publicity or to effect change, which can result in high profile operations. Some well-known examples are groups like Anonymous or WikiLeaks, whose members use their computer skills to access networks with a political or social agenda in mind.

These ideological bad actors typically target state and local governments, leaking insider information to the press or seeking to interfere with processes they disagree with (the cyber equivalent of a street protest or sit-in). But they have also gone after corporations, drug dealers and individual paedophiles. In addition to shutting down sites, they might alter them, or they might hack into private or confidential documents to make them public.

Organised crime – this includes both traditional organised crime groups, like the mafia, who have added cyber crime to their other criminal activities, as well as newer types of organised crime groups, who may engage exclusively in cyber crime. These criminals may target individuals and companies for direct financial gain, or may use hackers to aid them in other types of crime.

For example, in a case in Brussels, a Dutch-Turkish organised crime group importing heroin from South America hacked into the port of Antwerp and manipulated the unique nine-digit PIN numbers that every seagoing container is allotted. Using this, they were able to digitally mark those containers carrying the cocaine as having been customs cleared.

Insider threats – these actors are people who are already in an organisation. They may include disgruntled employees, or contractors making mistakes. This type of bad actor can be especially dangerous, as they are less likely to trigger red flags or to cause alerts until it is too late.

Good actors

These are people who hack into computer systems or networks, but with good intentions. They include the following types.

White hat hackers – these are also known 'ethical hackers' and include people who are paid employees or contractors working for companies as security specialists. White hat hackers are typically looking to break a system or application in order to better secure it. They use the same methods of hacking as black hats, but with permission from the owner of the system, which makes the process completely legal.

Ethical hackers will work for the organisation to try and find any vulnerabilities before they can be used for malicious purposes. White hat hackers may perform penetration testing, test in-place security systems and perform vulnerability assessments for companies. There are even courses, training, conferences and certifications for ethical hacking.

Grey hat hackers – a grey hat hacker lives somewhere in the middle between black hats and white hats. Grey hat hackers will often look for vulnerabilities in a system without the owner's permission or knowledge.

Grey hat hacking is sometimes done in the 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 hack to help fix the exploit. Companies will often reward them just like they would a white hat. If a hacker is rewarded well enough for reporting a vulnerability rather than exploiting it, they are more likely to do so.

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.

Certified penetration tester – penetration testing is a form of white hat hacking, where cyber security specialists are paid to break into an organisation's systems and test their cyber defences. There are a number of different certification programmes for penetration testers. In the UK, the National Cyber Security Centre (NCSC) recommends that organisations use pen testers and companies which are part of the CHECK scheme. Companies providing CHECK services use staff who hold one of the NCSC approved qualifications, from CREST, Tiger Scheme or the Cyber Scheme.

Reflective question

What are some of the differences between good actors and bad actors?

2.3 Distinguish typical behaviours of good actors and bad actors

Good actors and bad actors usually have the same sets of skills and use the same techniques. They can be distinguished by their reasons for doing what they do. In fact, some actors may move between the groups, or may be considered both a good actor and a bad actor. For example, is a hacker working for their own government to break into the files of a different government a good actor or a bad actor? If a group like Anonymous hacks files to expose a paedophile or corporate crime, are they good actors or bad actors? What if they expose the addresses of government agents who are then killed?

Many of the people who use the cyber crime markets on the Dark Web are bad actors looking for hacking tools or a place to sell information they have stolen. But many others are actually good actors who are trying to learn more about the latest types of hacking software or whether their organisation is going to be targeted.

As you can see, there are not always clear answers to who is a good actor and who is a bad actor, or clear ways to tell between them.

One way to distinguish between a good actor and a bad actor is that many good actors have certification in ethical hacking from a recognised organisation or certification body, such as CREST, Tiger Scheme or the Cyber Scheme. However, in the end, the best way to tell between good and bad actors is to learn about their motivations.

Reflective question

Suppose you met someone who said they were an active hacker. What kinds of questions could you ask them to find out if they were a good actor or a bad actor?

2.4 Explain the motivations of good actors and bad actors

There are a wide variety of motivations for both good actors and bad actors.

For bad actors, the primary motivation is usually for personal or financial gain. This can come from ransomware, cyber blackmail (where information is stolen and then a payment is organised to prevent it being made public), selling on data and information that they have gathered, or using stolen data to launch other types of attack.

Some bad actors, such as script kiddies, may also be motivated by the thrill of gaining access to organisations or government departments, or by trying to build a reputation for themselves among other hackers. Hacktivists usually have a political motivation, such as exposing what they see as corruption, unearthing government secrets or disrupting the operation of organisations that they do not like.

Hackers working for governments may also have political motivations, as well as getting paid for their work. Some hackers are engaged in terrorism and hope to cause damage and disruption to government or civil organisations and institutions, in order to sow confusion and fear.

Good actors may share some of the same motivations – for example, the thrill of hacking into organisations, earning a reputation for their hacking skill and the challenge of being better than, or defeating the plans of, a black hat hacker.

Of course, money is also a common motivation for an ethical hacker, only instead of stealing it, the ethical hacker earns money through their work. Highly skilled ethical hackers may find themselves in great demand, and may be able to demand a much higher fee as a result, and the desire to earn a reputation may motivate them to innovate in their work.

Some ethical hackers are also motivated by wanting to improve things or their personal ethics – such as the belief that black hat hacking is wrong, or a desire to make the internet safer for ordinary people.

Stretch and challenge - Good actors vs bad actors

Put a tick in each column that is a common motivation for each type of actor. The first one has been done for you.

	Money	Make internet safer	Thrills	Terrorism	Earn a Reputation	Revenge	Espionage	Politics
Script kiddie	✓	☐	✓	☐	✓	☐	☐	☐
Organised crime/Black hat	☐	☐	☐	☐	☐	☐	☐	☐
Pen tester/ White hat	☐	☐	☐	☐	☐	☐	☐	☐
Foreign government	☐	☐	☐	☐	☐	☐	☐	☐
Hacktivist	☐	☐	☐	☐	☐	☐	☐	☐
Insider	☐	☐	☐	☐	☐	☐	☐	☐

2.5 Identify key sectors that are most vulnerable to a cyber attack

Anyone and any sector is vulnerable to a cyber attack. However, some sectors are more vulnerable than others. This may be because they hold a great deal of personal data or valuable information, or because they tend to have less secure systems. Here are some of the key sectors that are most vulnerable to a cyber attack.

Financial institutions

These are particularly vulnerable to cyber attacks and data breaches because hackers can gain access to financial information such as credit card and bank account numbers, which they can use to steal money from accounts. Cyber threats facing banks and other financial organisations include everything from malware to highly targeted attacks from organised criminals and state-sponsored actors.

Healthcare

Healthcare and medical organisations store electronic healthcare records, which contain large amounts of personal information, such as addresses and financial details. On top of this, because of their size, many healthcare institutions are not well equipped to fend off attacks or are slow to act once an attack is taking place.

Did you know? - The WannaCry virus

The WannaCry virus was a ransomware attack that affected thousands of computers, including many belonging to Britain's NHS. Like other types of crypto-ransomware, WannaCry works by encrypting data and holding it hostage, promising to return it only if a ransom is paid.

WannaCry was launched in 2017 and targeted computers using Microsoft Windows as an operating system. The cyber criminals took advantage of a backdoor in the Windows operating system to gain access.

Microsoft had released a security patch which protected users' systems against this exploit almost two months before the WannaCry attack began, but many of the organisations affected had not updated their operating systems and were left vulnerable.

Around a third of NHS hospital trusts were affected by the attack, which caused a disruption in NHS services. It was estimated to cost the NHS a whopping £92 million after 19,000 appointments were canceled as a result of the attack.

As the ransomware spread beyond Europe, computer systems in 150 countries were affected. It is estimated this cyber crime caused $4 billion in losses across the globe. It also appears that the criminals had no way to track ransom payments to specific computers, so even those who paid did not get their files back.

Educational institutions

This is another sector that stores a lot of personal information, including names, addresses and billing information, as well as academic research. Some institutions, especially primary and secondary schools, are seen as an easy target because they tend to have less focus and budget for security. They often rely on a few common security solutions, such as firewalls and antivirus software.

Educational institutions also have a lot of users who spend a lot of time on the internet. Younger students especially are not always aware of the best ways to stay secure.

In addition, very few educational systems are watching the use of their network – most are focused on their security perimeter (for example, keeping malware out) rather than checking to see whether someone has already breached their security.

Retailers

Retailers are especially vulnerable to breaches because they collect data through a variety of sources, such as point of sale machines, tap to pay terminals, beacon terminals and online. Protecting massive amounts of data across different information systems can be quite challenging for retailers. It also means that cyber criminals can target retailers both remotely and at their operating locations, such as stores and warehouses.

Another vulnerability for retailers is their high turnover of staff and the use of seasonal workers, which makes them more vulnerable to insider attacks. For example, in 2014, a disgruntled employee of UK supermarket chain Morrisons used a portable storage device to copy the personal information of thousands of staff online. This was then sent anonymously to a local paper in Yorkshire. The leak was timed to take place just hours after the chief executive had boasted that Morrisons' new IT systems would help increase profits. The embarrassment sent shares down 12 percent.

Government

Governments, including local, state and federal government, are popular targets for cyber criminals, especially those supported by other countries who may be interested in cyber-espionage. Although governments tend to spend a lot of money and resources on cyber security, the sheer number of attacks means they are still vulnerable.

Insider attacks are also a source of vulnerability for government organisations. Many also use in-house IT professionals, who may get regularly rotated into unrelated jobs or different departments, leaving a new team to essentially start over.

Manufacturing

This is a sector that has paid less attention to cyber security until recently, and so may be more vulnerable to attack than better-protected industries. Manufacturers are vulnerable from actors who are looking to steal intellectual property or to insert ransomware, but also from criminals who could shut down a plant's operations or start making equipment produce faulty products without the knowledge of managers.

On top of this, many manufacturers are small businesses that may not be prepared for an attack. This increases the likelihood that the manufacturer will have a longer period of downtime if they are attacked, and this can affect their business and reputation.

As more and more products include electronic components, manufacturing could become more vulnerable from attackers looking to insert vulnerabilities in products at their manufacture. For example, inserting faulty software into smart cars and other Internet of Things devices.

Utilities

The infrastructure that includes utilities and refineries is another sector that is vulnerable to attacks from terrorists and foreign governments seeking to damage infrastructure and sow fear and disorder. As analog controls are replaced with digital systems, these systems have become more vulnerable to cyber attack.

The power grid consists of many interoperable systems, including power generation stations, transmission lines, distribution lines and energy markets. These many interacting systems provide numerous entry points an attacker could exploit. In addition, the growth of smart meters, which collect data about end-point usage and feed it back to centralised information processing hubs to be analysed, could also offer entry points for cyber criminals trying to steal personal information. Because these meters are often physically unprotected at the consumer end-point, they are vulnerable to tampering. All of this makes utilities more vulnerable.

Stretch and challenge - Vulnerabilities and potential impact

Fill in the chart with the vulnerabilities and potential impact of a cyber attack on these sectors.

	Vulnerabilities	Potential impact
Financial institutions		
Healthcare		
Educational institutions		
Retailers		
Government		
Manufacturing		
Utilities		

2.6 Compare the motivations for a cyber attack in key sectors

In all sectors, the major motivation for cyber attacks is financial gain. There are many ways cyber criminals can gain financially. The most obvious, and common, ways are by stealing money directly, for example, by gaining access to bank accounts; using ransomware to encrypt files and then demanding ransom; or by tricking people and organisations to send them money, for example, by posing as a friend or a trusted supplier.

Some cyber criminals may also be working for a fee, or may be working for pay for a foreign government.

Attacks on businesses such as retailers and manufacturers may be motivated by industrial espionage – gaining intellectual property or learning proprietary information that can help a competitor.

Revenge is another common motivation, especially for insider attacks. The insider may be a disgruntled employee looking to embarrass their employer.

Some attackers, especially those who attack government departments, may be motivated by idealism. These hacktivists may want to expose government corruption or they may believe that all government is evil and want to cause damage to the reputation of a government or its systems. Governments are also often attacked by foreign agents and governments. These may be looking to steal state secrets, or to learn how to control or affect different systems, such as utilities, in order to launch an attack, or in the event of war.

Those who attack governments may also be motivated by the thrill and challenge of seeing whether they can break into well-protected systems. These people may be looking to increase their standing or credibility in the hacker community, or as a way to demonstrate their skills to potential employers – either legal or illegal ones.

Reflective question - Motivations

Which motivations do you think are most important in the following areas?

Government	
Retail	
Education	
Manufacturing	
Utilities	
Healthcare	
Financial institutions	

2.7 Consider how an actor may carry out a cyber attack

Many attacks, regardless of whether they are targeted or un-targeted, or the type of tool being used, have a number of stages in common. In addition, many attacks consist of repeated stages as the attacker probes an organisation's defences for weaknesses. The steps involved in a cyber attack are often referred to as the Cyber Kill Chain.

The general steps may include:

Reconnaissance/survey: This stage involves investigating and analysing available information about the target in order to identify potential vulnerabilities. It can include harvesting information such as email addresses, employee information, types of systems used, etc. Attackers will use open source information such as LinkedIn and Facebook, domain name management/search services, and social media. They will employ commodity toolkits and techniques, and standard network scanning tools to collect and assess any information about an organisation's computers, security systems and personnel.

Weaponisation: Once a vulnerability is found, or an approach is decided on, the attacker needs to decide how to exploit it. This could involve creating software to take advantage of the vulnerability or purchasing ready-made software.

Delivery/intrusion: The software is delivered to the victim. This may include strategies such as sending an email containing a link to a malicious website or an attachment which contains malicious code; giving an infected USB stick away at a trade fair; or creating a false website in the hope that a user will visit.

Exploitation/breach: Once the virus or malware is inserted into the victim's system, it is activated or exploited. This may occur automatically or it may need an action by the attacker. Once in, attackers can install additional tools, modify security certificates and create new script files, etc. If attackers need more privileges on a system to get access to more data and permissions, they may escalate their privileges. The malware may also install an access point, a backdoor for the attacker.

Anti-forensics/command and control: In this stage, the malware gives the attacker access in the network/system. Once in, the attacker may lay false trails, compromise data, overwrite data with false timestamps (timestomping) and clear logs to conceal their presence and avoid detection.

Actions on objective: Once the attacker gains persistent access, they finally take action to fulfil their purpose, such as encryption for ransom, data theft or destruction, making changes for their own benefit (e.g. creating payments into a bank account they control), or disrupting normal business operations.

After achieving their objectives, many attackers will then exit, carefully removing any evidence of their presence. They could also create an access route for future visits. Some attackers will want to seriously damage your system or make as much 'noise' as possible to advertise their success.

Did you know? - Case Study

A large UK company's internal network was attacked through their externally managed corporate website. The attackers gained access through the company's network service provider, which contained a known vulnerability. They used software designed to exploit that vulnerability, which was purchased on the Dark Web.

Survey stage: As part of their survey of the victim's network and services, the attackers discovered that the corporate website was hosted by a service provider whose systems contained a known vulnerability.

Weaponisation: The attackers exploited the vulnerability they found to add a specialised exploit delivery script to the corporate website. The script compared the IP addresses of the website's visitors against the IP range used by the company.

Delivery stage: The attackers then infected a number of computers within the company by downloading malware to visitors' computers within a directory that allowed file execution.

More than 300 computers were infected during the delivery stage with remote access malware.

Exploitation: The malware then delivered network information to domains owned by the attackers.

Anti-forensics/command and control: Once in the system, the attackers installed further tools and were consolidating their position and identified high value users.

Detection and repair: While the breach was successful, it was detected using network security monitoring. The organisation had an incident response plan in place, which made it possible to investigate the incident using system and network logs, plus forensic examinations of many computers.

To remove the infection, the computers had to be returned to a known uninfected state using backups made before the infection. To prevent further attacks through the same route, the contract terms with the website provider needed to be renegotiated, to ensure they had similar security standards to the targeted organisation.

Section 3:

Understand security by design principles

3.1 Describe the term security by design

Security by design describes a system or product that has been designed from the ground up to emphasise security, rather than trying to tack security features onto an existing system. It involves building security into hardware and software from the beginning, rather than waiting until something goes wrong, or trying to bolt on security systems after the system or network is in use.

Security by design is not a set plan or standard; it is more of a mindset or philosophy. It includes:

- Building security into products from the beginning.
- Security should treat the root cause of a problem, not just its symptoms.
- Security as a continuous process.
- Security should work reliably and should constantly evolve to meet and defeat the latest threats.
- Security should not require highly technical understanding or non-obvious behaviour from the users.

Reflective question

Does security by design sound like a good idea? Why or why not?

3.2 Explore the principles of security by design

The National Cyber Security Centre (NCSC) has set out some of the principles that should be considered when designing security systems. These include the following:

Establish the context

This means that, before you can create a secure system design, you need to have a good understanding of what the system will be used for, what is needed to operate it, and what is an acceptable level of risk.

Gain a clear understanding of the type of system you want – before designing a security system, the first step is to have a clear understanding of the purpose of the system. This includes knowing which data, connections, people, and other systems will be required for it to operate. It also includes determining what impacts you are not willing to accept – for example, you might decide that it is vital for systems to be available to users at all times, or that it is crucial that attackers cannot undermine the safety controls of an industrial control system.

You should document the risks you are willing to take and ensure that all people involved in designing the system are familiar with them, so they can make well-informed decisions.

Understand the threat model for your system – you can use threat modelling techniques, such as attack trees, to help you discover the ways in which an attacker could realise their goals. Your design should also consider what level of capability an attacker would need to be successful, and whether your aim is to defend, detect, or recover, along with any useful time-bound goals. Once you understand these items, you can design security controls to counter those types of attacks.

Understand the role of suppliers in system security – if your organisation will be using outside suppliers to build and operate a system, then it is very important that they understand all of your security requirements.

Understand the system end-to-end – the system designers should understand how information and/or communication will flow through the system, taking into account every possible point where data could be stored, manipulated or rendered. This should include the following areas:

- devices used to access data
- third-party services, e.g. outsourced support suppliers and hosting providers
- network-security devices, e.g. web-browsing proxies and other network-monitoring devices
- where copies of your data are stored
- communications over insecure networks

Be clear about how you manage security risks – this involves where design decisions require you to balance security, usability and cost. You should consider all the costs of not using a particular security procedure, such as reputational damage or regulatory fines, as well as the financial cost of doing it.

Ensure everyone involved knows their responsibilities – everyone involved in designing and operating a system should be suitably qualified or experienced, know what their role is, and what decisions they are allowed to make on their own, as well as decisions they need approval for.

Make compromise difficult

An important part of designing an IT system with a security by design mindset is to use techniques which make it harder for attackers to compromise your data or systems. Here are a few principles for this.

Validate that all externally input data is safe or make it safe. Any data from an external source could have been crafted to attack your system. This can be done by:

- Transformation – it is not possible to reliably check for malicious code in complex file formats like PDFs or word-processing documents, so these files should be transformed into a safer format to disable any malicious content.
- Validation – this involves checking that the structure and content of data or files are as expected and will not have any unintended effects.
- Render safe – if validation and transformation are not possible, or won't provide confidence that the content is safe, then rendering the content in a disposable environment, such as a non-persistent virtual environment or remote desktop may be an option.

Reduce the attack surface

This refers to reducing the number of places where hackers can get in. You can take a number of steps to do this, including:

- Remove all default configurations and features that aren't required, such as user accounts, passwords, scripts and demo capabilities.
- Only use trustworthy vendors or service providers with formal certifications and audit reports.
- Protect privileged users such as managers from targeted attacks such as spear phishing emails or watering hole attacks. Design the system so that privileged users have a separate management infrastructure. This means they will not be able to view email, or browse the web, from the same account or device that they use to perform their privileged actions.
- Prefer tried and tested approaches. Where possible, build onto popular and well-tested software frameworks and libraries, and those with a community of developers actively searching out and fixing vulnerabilities.
- Make sure all sensitive or privileged actions are individually authorised and accounted for.
- Design the system for easy maintenance, such as patching. Frequent small updates are less risky than infrequent large ones. Design the system so you don't need to have outages in order to apply updates.
- Make it easy for administrators to manage access control.
- Make it easy for users to maintain security. Many security breaches occur because users have developed workarounds for system inadequacies. Limiting issues will make it easier for users to stick with the security procedures.

Make disruption difficult

For many organisation, having the system go down due to an attack can be expensive and difficult to recover from. To prevent this 'down time', system developers can consider the following points:

- Ensure the system is resilient to both attack and failure, for example by having standby systems, alternative routes, and data backups.
- Design for scalability. Make sure the system can be easily scaled up to handle increased load, without having to take it offline.
- Identify potential bottlenecks – for example, periods of high capacity or denial of service attacks. Use openly available tools, such as Netflix's Chaos Monkey, to test how your system will perform under high load or when components fail.
- Identify issues with third parties. Many organisations rely upon third party services, such as telecommunication links, hosting, authentication or system administration services. Make sure you know the impact on your operations if these fail and have a plan in place for minimising disruption if this occurs.

Make breach detection easier

No matter what precautions you take, there is always the chance that the system will be compromised by a new or unknown attack. To give yourself the best chance of spotting these attacks, use the following guidelines when developing the system.

- Collect all relevant security events and logs. This will make it easier to perform root cause analysis in event of a failure and will ensure that an attacker will not be able to cover their tracks.
- Design simple communication flows between components. This can simplify security analysis and enable you to identify when something is not right. Configure your monitoring tools to detect these indicators and automatically raise alerts.
- Watch for attempts by compromised components to contact their command and control infrastructure.
- Make monitoring independent of the system being monitored. This ensures that if the system being monitored is compromised, the attacker will not know that the breach has been detected.
- Make it difficult for attackers to detect security configurations through external testing. This makes it more difficult for an attacker to map out your defences.
- Know how your systems normally operate so that unexpected behaviour can be more easily recognised. This can include monitoring network load, storage I/O and transaction activity, to help you understand when your system is behaving abnormally.

Reduce the impact of an attack

Design systems so that they naturally minimise the severity of any breach. Some ways to achieve this include:

- Use a zoned or segmented network approach. This helps to contain the attack to the segment that has been breached and helps to protect the most sensitive or valuable data.
- Remove unnecessary functionality. If functionality exists, then it can be abused by unauthorised users in event of a compromise. Reduce this risk by removing unnecessary functionality. This also reduces the time and cost of maintaining software you don't need, simplifies the system and makes monitoring easier.
- Avoid creating a 'management bypass', where management communications have weaker security controls than in the systems being managed.
- Make it easy to recover following a compromise. Design the system architecture so that if there is a compromise, you can quickly rebuild to a clean system.
- Anonymise data when it's exported to reporting tools. This will reduce the number of places that a high impact breach could occur.
- Avoid unnecessary caches of data, as these are likely to be less well protected than the main data storage. A data-fading policy can be used so that records are purged as soon as possible after access has finished. This ensures that a minimum amount of data is stored in the cache.

Stretch and challenge - Security by design

Imagine that you are developing a cyber security system for PaperCorp. PaperCorp runs a plant that produces PaperX, a new type of paper that is used by many large corporations. It is created from volatile raw products using a continuous chemical process. In order to supply its customers, PaperCorp must protect its network, information systems and production technology from cyber attacks.

The process for producing PaperX involves a number of steps and PaperCorp's IT system has two critical requirements:

- They need to keep the local environment safe from release of the chemicals used to make PaperX.
- The product must remain available for customers in order for PaperCorp to continue as a profitable company.

Think about a cyber security system for PaperCorp. What principles would you include?

3.3 The consequences of not considering cyber security during the design phase

Unless cyber security has been considered during the design phase, the organisation will be left to take a reactive approach to attacks. This means that they will need to deal with each attack as or after it occurs, rather than preventing the attacks in the first place.

The risk is that an attack may cause damage before it is caught, and the organisation may not have a plan in place to minimise this damage or recover from it quickly. In fact, most businesses only consider cyber security after it's already too late, rather than building security into new systems from the beginning. This is inefficient, because it prevents the creation of really effective systems.

Another consequence is that the lack of confidence in an organisation's cyber security can cause organisations to be more timid and afraid of innovation. For example, they may not adopt Artificial Intelligence tools that could improve their business because they are worried about security.

Reflective question

Look back at the section on the principles of security by design and this section. What are the consequences of not considering cyber security during the design phase?

3.4 The advantages and disadvantages of security by design

There are a number of benefits of a security by design mindset. One benefit is that it is much cheaper to solve security issues at the beginning, before they have caused damage. For many organisations, security is added to existing systems and may be designed more around ticking off items on compliance checklists, rather than being based on calculations of business risk. If security is built in from the beginning, this offers a greater ability to tailor the security systems to the particular needs of the organisation.

There may also be fewer time and budget constraints in building security in at the beginning of a project, when more time can be spent to develop the most suitable security system, and where the costs of the security system can be budgeted in from the beginning.

One drawback of security by design is that the upfront costs are higher, as the system may be more complex and require more expertise to design. It may also take longer to build this way, as organisations will first need to spend time considering exactly what they need.

There is also the chance that a system designed when an organisation is first established will no longer be suitable if the organisation grows or changes a great deal. However, this can be prevented by making sure that the system can be adapted without needing to be taken offline.

Research task - Security by design

Examine a cyber system that you are familiar with, such as at work, school or even at home. What might be the advantages and disadvantages of using security by design when this system was set up?

Summary

We began this Unit by looking at some basic concepts of cyber security, including:

- security
- identity
- confidentiality
- integrity
- availability
- threat
- vulnerability
- risk
- hazard

This was followed by a discussion of the importance of cyber security and some of the consequences and implications of having inadequate cyber security, including the unauthorised access to and distribution or loss of sensitive data, personally identifiable information, protected health information, personal information, intellectual property and industry information systems.

In the next section, we discussed terminology, including core terminology such as:

- malicious software
- distributed denial of service (DDoS)
- cloud
- software
- domain
- exploit
- breach
- firewall
- encryption
- Bring Your Own Device (BYOD)
- penetration testing (pen testing)

We then moved on to good and bad actors, such as ex-employees, black hats, script kiddies, hacktivists, white hats, grey hats and certified penetration testers. We discussed some of the typical behaviours and motivations of good actors and bad actors including money, thrills, terrorism, earning a reputation, politics, espionage, revenge and altruism.

Key sectors that are most vulnerable to a cyber attack were identified, such as financial institutions, healthcare, education, government, utilities, retail and manufacturing. We discussed how motivations for a cyber attack can vary depending on the sector. Lastly, we examined some of the stages used to carry out cyber attacks, including:

- reconnaissance/survey
- weaponisation
- delivery/intrusion
- exploitation/breach
- anti-forensics/command and control
- actions on objective

In the last section, we developed an understanding of security by design. This included a look at the National Cyber Security Centre principles that should be considered when designing security systems, including:

- establishing the context
- making compromise difficult
- reducing the attack surface
- making disruption difficult
- making breach detection easier
- reducing the impact of an attack

We also discussed some of the consequences of not considering cyber security during the design phase, such as the risk that an attack may cause damage before it is caught, and the damage this can cause to an organisation. Finally, we explored the advantages and disadvantages of security by design, including cost and time implications.

Further reading

Hacking: A Beginners' Guide to Computer Hacking, Basic Security, And Penetration Testing. John Slavio

Computer Networking Hacking: Ultimate Guide To Ethical Hacking, Wireless Network, Cybersecurity With Practical Penetration Test On Kali Linux And System Security Practices. Ramon Base

Learning Malware Analysis: Explore the Concepts, Tools, and Techniques to Analyze and Investigate Windows Malware; Monnappa K A; Packt Publishing (2018)

Cybersecurity: An Essential Guide to Computer and Cyber Security for Beginners, Including Ethical Hacking, Risk Assessment, Social Engineering, Attack and Defense Strategies, and Cyberwarfare. Lester Evans

2600: The Hacker Quarterly

https://www.2600.com/Magazine/DigitalEditions

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