BTEC DIT

Component 3 Effective Digital practices

B1

Learning Aim B: Cyber Security: Threats to data

Knowledge and Assessment Organiser

Student name: .....

What are the threats to data and why do they happen?

Contents

Exam question command words

Command verbs	Definition
Describe	To give an account of something, such as steps in a process or characteristics of something. The response should be developed as they are often linked, but do not need to include a justification or reason.
Discuss	Identify the issue/situation/problem/argument that is being assessed in the question. Explore all aspects of an issue/situation/problem/argument etc. by reasoning or argument.
Draw	Produce an annotated process either in the form of an information flow or data flow diagram
Evaluate	Review information then bring it together to form a conclusion, drawing on evidence, including strengths, weaknesses, alternative actions, relevant data or information. Come to a supported judgement of a subject's qualities and relation to its context.
Explain	An explanation that requires a justification/exemplification of a point. The answer must contain some element of reasoning/justification.
Give/State/Name	Require recall of one or more pieces of information.
Identify	Usually requires some key information to be selected from a given stimulus/resource.
Annotate the diagram to explain how ...	Label the diagram and provide an explanation for each identification.
Assess	Give careful consideration to all the factors or events that apply and identify which are the most important or relevant. Make a judgement on the importance of something, and come to a conclusion where needed.

Key terms

Intellectual Property – is an idea that you invented that belongs to you, for example, an image that is copyrighted.

Ransomware – is a form of **malware**, usually systems, occurring when users open malicious email attachments.

Malware – is a malicious form of software that is transferred to, and then executed on a user's machine to damage or disrupt the system or allow unauthorised access to data.

Did you know…?

In 2015, the United States Chamber of Commerce published a study that estimated that the global cost of cyberattacks on organisations could be as much as $1 trillion.

What are the threats to data and why do they happen?

Why are systems attacked?

What is a hacker?

What are external threats?

What are internal threats?

What is the impact on security?

Why are systems attacked?

There are many reasons why systems are attacked, and they are not always for financial gain. Sometimes attacks are purely for making mischief or due to a personal vendetta.

When we look at the reason why a system has been attacked, the most common factors are included below.

- **Fun/challenge –** Some attackers gain unauthorised access to systems for the purpose of amusement or challenge. Attacking a system for this purpose can allow individuals to gain experience for future cyber-attacks, overcome personal goals of 'beating' an organisation's cybersecurity measures, or in some cases, allow them to gain kudos from their peers or a community.
- **Industrial espionage –** Cyber-attacks may be perpetrated on specific targets for stealing unique sensitive information from a rival business (quite often intellectual property). This data can then be used to aid those carrying out the attack to be one step ahead of the rival, such as releasing a proprietary product before the original organisation can.
- **Financial gain –** More often than not, an attack will be motivated by money as the end goal, even if it is not immediately obvious. This could be through:
    - ***Direct gain***, where the attacker directly steals money/information during the attack which will lead to profit.
    - ***Indirect gain,*** for example, extortion, where attackers may use ransomware, or denial of service attacks in order to threaten an organisation into paying them to end the attack.
- **Personal attack –** On occasion, the motivation for attacks can be personal, for example, an individual may be targeted based on their beliefs/opinions, or organisations may receive attacks from employees who feel they have been mistreated.
- **Disruption –** Attacks may occur with the primary purpose of disrupting an organisation's service. This may be to benefit financially, or in business, but is often for personal, political, or social reasons. Common forms of attacks that cause disruption include denial of service attacks and website defacement.
- **Data/information theft –** Attacks may occur for the purpose of stealing data. More often than not, this is customer, personal or financial data stored by the company. Stolen data can then be used by

the attackers for identity and bank fraud purposes, such as purchasing items using the customer's credit card details.

Task 1

Below are **six** cyber attack scenarios.

(a) For **each** scenario, write the most likely motivation for the cyber attack.

(b) In **each** scenario, underline the reason for your choice of motivation.

The first scenario has been done for you

	Scenario	Motivation
1	Gigaclean is a large international vacuum cleaner company which has many patents on their technology worth millions of pounds. An employee working for a competitor manages to gain access to Gigaclean's file server and obtains important documents showing future vacuum designs.	Industrial espionage
2	A teenager, Noah, has an argument with Alfie who attends the same school. Noah knows one of Alfie's friends, who knows the password to his Facebook account. He uses the password to post inappropriate messages to his friends as if he is Alfie.	
3	A hacker manages to gain access to an ecommerce website's server. They obtain 3000 names and credit card details. Before the website can fix the problem, the hacker manages to sell the card details for £10,000.	
4	Jaxon has been programming since age 10. Already, at age 15, he is able to program in three languages and has his own website. He mainly uses Linux and the command line. He wants to take his skills to the next level and decides to break into his parent's home computer. He doesn't damage or steal anything whilst there.	
5	A programmer creates a virus which infects thousands of computers. Once infected, the virus encrypts everything on the computer's hard disk. The virus then shows the user that they have a choice: they can either lose everything on their computer or pay a ransom of 0.1 bitcoin to decrypt the data (worth around £1000 at the time of the attack).	
6	Kevin has started working with the hacking group Anonymous. He starts a denial of service attack on a major online organisation which the group disagree with. The media organisation distributes huge quantities of video data and their servers cannot cope with the attack. The server goes offline resulting in millions of pounds of losses for the company.	

Task 2

Visit the following websites to determine the motive for the attack and the type of attack committed.

https://cyberstartupobservatory.com/cyber-attack-a-modern-day-horror-story/

What was the reason for the attacks?

What have you read in the story to determine your reason? Do not just write that it states the hacker type in the story. There are other points that will determine your answer.

Name the cyber attack (e.g. ransomware, DDOS, malware

https://www.bbc.co.uk/news/technology-57946117

What was the reason for the attacks?

What have you read in the story to determine your reason? Do not just write that it states the hacker type in the story. There are other points that will determine your answer.

Name the cyber attack (e.g. ransomware, DDOS, malware

1. Open the link below.
2. Read the different news stories about cyber attacks.
3. Summarise the reason for the attacks.
4. What points can you take from the stories to determine the motive for the attack?

https://www.bbc.co.uk/news/uk-england-devon-46757849

What was the reason for the attacks?

What have you read in the story to determine your reason? Do not just write that it states the hacker type in the story. There are other points that will determine your answer.

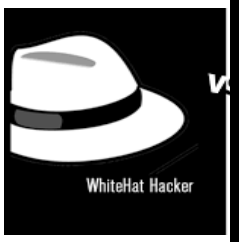
What are external threats

What is a hacker?

A hacker is a person who gets access to a computer system without permission.
They can use this access to:

- make the computer run different programs such as a virus or a botnet
- steal information
- damage files by corrupting or deleting them
- A hacker who misuses computers is known as a **'black hat'** hacker.

A white hat hacker



A white hat hacker is an independent computer security specialist who is authorised by an organisation to test its system for security weaknesses.

A grey hat hacker

Is an independent computer security specialist who may discover vulnerabilities in an organisation. They may sometimes break laws or ethical standards but do not hack for personal gain

External threats

Social engineering

Social engineering allows attackers to gain access to a system without using technical hacking techniques; instead, using human psychology and social techniques in order to manipulate individuals into handing over private information.

Social engineering doesn't even need to involve technology at all and can be done face-to-face, by letter or over the phone.

- **Phishing** – This usually takes place via an email or phone service and involves an electronic message being sent to an individual containing some form of request (often to click a link, or return information). The attacker usually pretends to be a legitimate business. The goal is to either get the victim to reveal information, such as login or bank details, or to infect their device with a virus that will allow for data to be stolen later.
- **Shoulder surfing** – Shoulder surfing is the process of observing an individual in a physical location in order to obtain information, for example looking over someone's shoulder. This technique can be used to gain information such as pin numbers or password.

Malware threats

Malware stands for malicious software and covers a variety of computer programs that perform attacks on a system. We most commonly know of the term "virus" but this is in fact just one type of malware.

- **Virus** – A malicious program which is used to harm the operation of a computer system, such as by deleting files. As the name suggests, viruses spread from computer to computer, attached to a legitimate piece of software or file.
- **Worms** – Similar to viruses, except they do not require the need to attach themselves to programs/files. Instead, once on your system, it copies itself and spreads on its own via an internet/network connection.
- **Botnet** – A number of connected computers co-ordinated together to carry out an often-repetitive task. Any computer can become a botnet if exposed to a form of malicious code. If your computer is added to a botnet, it can then be used as part of a 'web' or 'network' of computers to carry out an attack (i.e. a DDOS attack).
- **Rootkit** – A type of malware that hides on your computer and allows a malicious user to remotely access and control it. They could then change security settings to gain access later, install malware to steal data and much more.
- **Trojan** – Where malicious code is disguised as a legitimate piece of software but contains a harmful payload. Users will download & install the program thinking it will provide a legitimate function but behind the scenes it is causing damage, such as installing keyloggers, adding you to a botnet or deleting data.

- **Ransomware** – Refers to a piece of malicious software that infects computer systems & will secretly encrypt local files. It will then ask for some sort of fee, or other demand, to unlock & decrypt the data.
- **Spyware** – Gains access to the system and works in the background to monitor a user's actions (keylogging for a password, downloading files etc.). This information is then commonly used for further attacks or as part of identity/bank fraud.

Other external threats

- **Unauthorised access/hacking** – Where an individual gains access to a system without the permission of the system owner/administrator. Hacking doesn't necessarily involve any clever technical skills & often is as a result of the social engineering techniques we've looked at previously. There are two main types of hacking:
    - *White hat hacking* – performed by security professionals to find exploits in a system for the purpose of implementing a cybersecurity solution.
    - *Black hat hacking* – gaining access to the system without the permission of its owner.
- **Denial of service attacks** – Where servers are flooded with traffic to overwhelm resources, making it unbearably slow, or completely unusable. The primary goal is usually to disrupt a service.
- **Pharming** – This misdirects users to a fraudulent/fake website without the individual's knowledge. Domain name poisoning is a form of pharming which modifies the domain name system table in a server to re-direct users entering in legitimate information (e.g. they could type google.com but it takes them to a spoofed site).
- **'Man-in-the-middle' attacks** – A form of attack where an individual with malicious intent inserts themselves into the middle of a communication between two parties. An example might be setting up a fake WiFi access point that people connect to. Anything transmitted on this connection could be intercepted by the attacker who creates the access point.

Task 1

Have a go at this memory matching game. Can you match the image of the external threat to its description in less than 3 minutes?

https://interacty.me/projects/f273286e933fe0c4

Task 2

For each of the scenarios given below, tick which hacking techniques have been used. Underline the part(s) in the scenario that support(s) your choice(s). The first scenario has been completed as an example

	Scenario	Virus	Worm	Trojan	Ransomware	Spyware	Rootkit	Botnet	Denial of Service
1	Tyler goes to a website that says that it will supply cracked software that doesn't need a licence. After installing the software, the user is pleased as it works as expected. They notice later that many adverts display on their computer.			✓		✓			
2	Leila clicked on a file in an email attachment. Today when she turned on her computer, it said that all her files are now encrypted. She has been given 24 hours to pay one bitcoin to unencrypt the files.								
3	ILOVEYOU infected 10% of the worlds computers in 2000. On clicking an email attachment, it sent itself to all other contacts in the email address book. It is estimated that $10 billion of damage was done by ILOVEYOU.								
4	In 2016 a major IT service provider, Dyn, was disrupted by a cyber attack. This caused the websites AirBnB, Netflix, PayPal, Visa and Amazon to be disrupted. The attack started by gaining control over Internet of Things (IoT) devices such as cameras, printers, TVs and baby monitors. These devices were all then told to target Dyn's servers with unnecessary requests.								
5	CopyCat is malware that affects the Android operating system. It infected 14 million devices in 2016. The software spreads by popular apps that have been rebuilt to contain malicious code. These are delivered via 3rd party websites. Once installed, the malware managed to gain full root access to the device.								

Task 3

Open the following link: https://www.bbc.co.uk/sport/football/55094962

What are **three** key points of the story?

1. _____

2. _____

3. _____

b) What was the motive for the cyber-attack?

What are internal attacks?

Internal threats refer to vulnerabilities which come from within the organisation itself. In most cases, this is employees who look to damage an organisation's systems and/or data.

Not all internal threats are purposeful though. Through trickery or human error employees can sometimes accidentally expose or harm data.

To learn the difference between deliberate and accidental internal threats, it's important to learn some of the key internal threats that are posed to organisations.

The types of internal threats fall under the following:

1. Deliberate threats, such as stealing/leaking information & overriding security controls.
2. Accidental threats, such as unintentional disclosure of data, using portable storage, internet downloads & visiting untrustworthy sites.

Deliberate Internal Threats

This is a threat which is purposefully conducted by an individual within the organisation with malicious intent in mind. This is often as a result of perceived mistreatment by employees or perhaps even being fired.

Some examples of deliberate internal threats include:

- **Intentional stealing or leaking of information** – Individuals who have access to sensitive information may feel the need to copy, delete, or leak it. Other than feeling mistreated by the organisation, this could be done for financial gain, perhaps by leaking data to a competitor. There are also cases of this for whistleblowing, where an individual purposefully leaks sensitive data that the company is holding, to reveal illegal or unethical practices.
- **Users overriding security controls** – Some individuals within an organisation are given access to a majority of the company's files, data, and software so as to be able to complete their job on a day-to-day basis. They may decide to alter the settings/configuration of security software protecting the company (such as firewalls and antiviruses) to allow a third-party attacker to gain access to the system.

Accidental Internal Threats

Not all internal threats are as a result of malicious intent. Simple mistakes by individuals within a business can actually have devastating consequences for an organisation.

Some examples of accidental internal threats include:

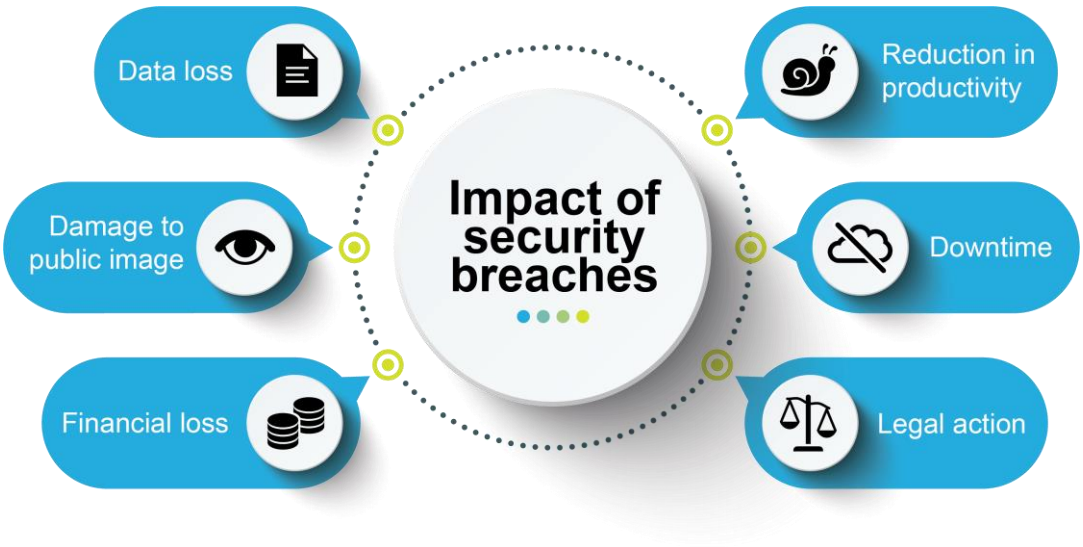
- **Unintentional disclosure of data** – On occasion, data is disclosed to someone outside of the company, without the individual knowing of any wrongdoing. For example, phishing, where an employee may relay sensitive information over phone or email to an individual, posing as a fellow employee or manager.
- **Use of portable storage devices** – Portable devices, such as memory sticks & portable hard-drives, are more often than not harmless when brought in to the workplace. We often use these to transfer data between computers. However, this can lead to accidentally introducing malware to a business system from outside, potentially by transferring an infected file.
- **Downloads from the internet** – Downloads from the internet can often contain malware which can infect the company's system. An employee may innocently open an email attachment or download a file from the web that secretly contains malware and causes huge damage to the data on a computer system.
- **Visiting untrustworthy websites** – Similar to downloading from the internet, employees may visit websites that are not reputable and pose a risk to their computer or the wider network. Just by visiting the site they could be infected by malware, or the site could be used to trick an employee into revealing confidential information.

Did you know…?

You can visit https://haveibeenpwned.com/ to find out if your email address has been compromised in a data breach.

Impact of security breach

Think of an example for each of the security impacts



- **Data loss** – This could either be due to data theft, or data which has been deleted/corrupted as a result of a malicious payload (e.g. virus).
- **Damage to public image** – Attacks may cause customers to view an organisation more negatively, and indirectly cause loss of customers, public panic, or create a political statement.
- **Financial loss** – Business may lose money such as from the theft of banking details, a loss in profit after the attack as a result of damage to the public image, data loss, and industrial espionage to name a few examples.
- **Reduction in productivity** – Attacks such as data theft (so employees cannot access the data they need to carry out their job), and denial of service attacks, prevent a business from performing their daily operations.
- **Downtime** – An attack may cause the system to fail, and go down completely, often as a result of a malicious payload being so disruptive that the service must be shut down manually, or due to an attack which takes the servers offline directly.
- **Legal action** – Organisations are legally obliged to ensure that individuals' data is secure and not misused. If data is harmed during an attack, then the organisation may be liable to huge fines under the Data Protection Act (2018).

Task 1

Ex-Apple Employee Accused of Stealing Self-Driving Car IP

Read the article on the link below on how an ex-employee of Apple was accused of stealing technical data files about Apple self – driving car.

https://digitalguardian.com/blog/ex-apple-employee-accused-stealing-self-driving-car-ip

Answer the questions below determine the type of threat and the impact on the employee and Apple.

Was the type of threat deliberate or accidental?

Using information from pages 14 and 15 decide what type of threat best fits with this story. Identify the threat with an explanation for your choice.

What was allegedly stolen?

How did Xiaolang Zhang obtain access to the material? Think about the role and responsibility that he was given.

Did Apple have any security measures in place? Briefly discuss those.

Use the information on page 16 to discuss the security breach on Apple.

Task 2

Complete the Trivia quiz on internal threats and the types of security breach.

https://interacty.me/projects/92114add62ae2f7c

Exam questions practice

Q1.

A doctor's surgery provides medical care for people in the local area. The surgery uses Information Technology to collect, store and process patient data.

A patient data breach would impact on the surgery.

One possible impact is damage to the surgery's public image.

Give **two other** possible impacts to the surgery.

(2)

1 .....

2 .....

(Total for question = 2 marks)

Chocawoca is a confectionary manufacturer that makes high quality sweets and chocolates that they sell in their shops and online.

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

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

(4)

1 .....

.....

.....

.....

2 .....

.....

.....

.....

B1: Exam Questions

Clare is a designer for a games development company.

She works from home and in public places such as cafés, train stations and airports.

Clare uses her laptop to prepare designs.

Clare has recently been a victim of phishing.

Describe **one** way that this could have happened.

(2)

Answer: Claire may been a victim of phishing by clicking on a link on the email she received.

The example has some good bits but is far from being great. Why?

Hint

Describe question ask you to give an account of something. You are not expected to give a reason although the points you make might be linked!

Andrea owns an indoor trampoline park.

Customers can pay for their visit to the park on the park's website. However, the current website is not secure.

Give **two** potential threats to the customer of paying through a website.

(2)

1 .....

.....

2 .....

.....

Clare is a designer for a games development company.

She works from home and in public places such as cafés, train stations and airports.

Clare uses her laptop to prepare designs.

Clare's laptop has been infected with a virus.

Explain **two** ways Clare's laptop could have been infected with a virus.

(4)

1 .....

.....

.....

.....

2 .....

.....

.....

.....

Q1

Question Number	Answer	Additional Guidance	Mark
	Any two from the following: • Personal information can be stolen (1) • Customers identification can be used for other purposes (1) • Payment details can be replicated (1) Accept any other appropriate response		2

Q2

Question Number	Answer	Additional Guidance	Mark
	An explanation such as: • Clare could have shared portable storage devices with colleagues/other people (1) that hadn't been checked using up to date anti-virus software (1) • Clare used an unencrypted Wi-Fi network (1) which allowed a hacker to install a virus on her laptop (1) • Clare downloaded files from the internet (1) where she used sources from a site that was not genuine/a trusted organisation that contained a viruses (1) • Clare could have downloaded an email attachment (1) which ran a malicious program (1). Accept any other appropriate response	• Award one mark for an identification and one mark for a linked justification Identification and justification may be reversed. Do not accept just hacking on its own	4

Articles for Wider Reading and Flipped Learning

Subscribe and watch the YouTube clip on Cyber security.

https://www.youtube.com/watch?v=jGBdmHvNXfs&list=PLmyUnKEeJk-6gijRiVKEfcvZhwcj6LWpo&index=5

Threats to data - Know it all Ninja

Read through the topics on **THREATS TO DATA.** Remember to complete the on-line quiz to gain house points!

https://www.knowitallninja.com/