

## Unit 1 – Cyber security & Cyber threats

### 1 Understand the range and variety of cyber threats

#### 1.1 Basic nature of cyber threats

**Cyber threat** is a potential attack coming from computers with malicious intentions of stealing personal information, passwords, bank details, IP addresses (locations). Those threats are done through the internet, using different techniques and methods which are constantly improving and approached differently every day.

The nature of a cyber threat can vary from a phishing email that tries to trick a target into thinking that their bank account was compromised, leading to financial loss, - all the way to massive corporations with large cyber security teams being infected with ransomware like the case of Colonial Pipeline, an American fuel company which was attacked with a ransomware in May of 2021 by a cyber criminal team called DarkSide and caused the company to lose \$4.4 million and caused fuel shortages.

**Malware** - This is one of the most common ways a cyber-attack can happen. It involves the users downloading and installing a piece of software which is supposedly safe into the computer, then giving it access to all the information that is stored in that computer: from the programs installed all the way to personal information, bank details, important documents, which can then be stolen by the attacker.

**Ransomware** - Used for both individuals and companies but mainly companies. When the malicious software gets its way into a computer, it can directly infect all the other machines that are in the same network with a virus that encrypts all information stored in that machine which makes it inaccessible by the users unless they have the key. The key is only obtainable if the ransom is paid

**Cyber security** is required to defend cyber threats. It is a very advanced knowledge field that is very looked for in the job industry. However, no matter how good the cybersecurity is, hackers will try to find vulnerabilities in anything.

## 1.2 Most common threats

Cyber-criminals have a very large variety of methods to penetrate into individuals' and even large companies' systems for malicious purposes, here are some of the most common ones, listed in order of the damage it can do.

- Ransomware
- DDoS
- DoS
- Social engineering
- Malware
- Spyware
- Trojan
- Man in the middle
- Phishing

## 1.3 I can describe the key aspects of threats faced by individuals.

Malware is one of the most common threat to individuals as most internet users have little knowledge about internet safety therefore, they are easy targets. When an individual is infected with the malware, depending on what type of malware it is and the purpose of it, it can lead to minor damage like old passwords being leaked to severe damage like personal information and passwords stolen and even financial losses which can affect the individual to a personal level.

My experience with this threat was a devastating experience. I didn't have the knowledge required to protect myself from the threats which caused in personal account theft and ultimately financial loss. It happened when I have downloaded what I thought was a safe piece of software from an unknown source. The software was what's called a trojan horse where it disguises itself as a wanted software, but when it is completely installed on the machine, it receives full control over the computer, leaving the user unable to control their own personal computer whilst the virus steals all the personal information including browser credentials and session tokens which are the personal emails and passwords stored locally, with session tokens, the attacker can infiltrate into an account without the need of any password, even bypassing the 2FA (two factor authenticator) protocol. In my case, the trojan also included a software to turn my machine into a crypto currency mining machine. I tried using safe mode which allowed me to boot up the computer into windows. I have noticed that the system is extremely slow, so I checked the task manager which allows me to see all processes as well as how much processing power they are using. It showed that the GPU process was at 100% utilisation and CPU was higher than it should be, around 40%-100%. I knew that it was highly unlikely to manually try to get rid of the virus and I knew that antiviruses won't either. The only solution I could think of was a complete re installation of the operating system so any harmful files that might be hidden inside the computer will be deleted. Since this

happened, I was more careful of the sources where I download software from and only download from known sources.

The main and most direct feature of threats to individuals is **financial loss**, however there are many more aspects to the features of threats that are different from person to person and are caused by different threats:

**reputation damage** - depending on the threat, the reputation of an individual can be damaged. This can be a weak point for the targets as no one wants to have their reputation ruined. The attackers are using this fact in their favour, creating their attack strategy around it. For example, an individual receives an email from the same email address as their, mentioning the fact that they have been recorded during intimate actions and that the recordings will be published online to their friends and family if the individual doesn't pay the attacker. The attacker also refers to old passwords that have been breached online for stronger evidence that the account really has been compromised. In reality, the account was not hacked into, and no recordings have been made. This kind of threat is called sextortion scam, it is very common and has a high success rate.

#### 1.4 I can explain the main features of threats to companies. I can describe the key characteristics of threats to companies

Because the fact that a company generally has a lot more personal information involved, it will be a high priority target for cyber criminals. The safety of their client's personal data is a top priority for companies as the risks of it being stolen could cause immense damages to both the companies and the users. The company could get fines for being unable to protect the personal data of the users, reputation of the company be ruined causing less customers/users, therefore less money. However, because the personal data is so valuable, and the fact that big companies like Microsoft have hundreds of millions of users, causes hackers worldwide to try to hack into their system and steal as much data as possible, that data can then be sold on dark web for huge amounts of money.

The biggest threat to companies is a ransomware attack. When a computer in a company is infected with ransomware, it will spread to the entirety of the network and infect all the computers and even file servers that are connected to the network. It will then encrypt all the information stored on both computers and servers. The only way to recover the data is by paying the ransom, which by itself is not guarantee that will recover the data. The payment is most of the times done through cryptocurrency as the blockchain makes it safe for the attackers to not be tracked.

Examples:

##### **NHS patient data stolen in cyber attack**

Recently, on 3rd June 2024, NHS confirmed almost 400GB worth of its patient private data managed by pathology testing organization Synnovis was stolen in a ransomware attack, however NHS said that there is no evidence supporting that the stolen data has been published online.

The responsible for this cyber incident was a Russian cyber-criminal group called Qilin. They are known for cyber-attacking through ransomware. They were detected by Trend Micro in 2022 August in the act of promoting ransomware called Agenda.

How did it happen?

How did a company such as NHS fail to secure their important data? The truth is that it doesn't matter how secure a company is, if the attackers are dedicated, they will keep trying and searching for any vulnerabilities until they find one and make the most use of it. In this case Qilin (attackers) infiltrated into the NHS computer systems located in London and encrypted a big part of important patient personal information, meaning that the information is now locked up and hidden making it inaccessible by NHS, however, the information could be recovered if an amount of money is paid, if

not, the information will be permanently deleted from their systems, and be published on dark web for money.

Because of these attacks, NHS lost its credibility and 'safe' reputation.

This attack could be prevented by a stronger cyber security team



### **EasyJet Data breach 2020**

In early 2020 an airline company named EasyJet suffered a data breach where around 9 million customers personal information were stolen and approximately 2000 customer's credit card's detail was accessed and stolen. The data breach happened due to a vulnerability in the EasyJet's online booking system.

#### **Impacts:**

Financial loss – EasyJet faced fines of £18 million from the Information Commissioner's Office under GDPR rules, along with cost related to security updates and compensation for affected customers.

Reputation – Customers trust was severely damaged, with many questionings EasyJet's ability to secure their personal data. The airline faced a public backlash, further damaging its reputation.

Operational impact – EasyJet had to enhance its security infrastructure, conduct audits, and invest in additional cyber defences.

Legal issues – The Ico investigation resulted in heavy fines, and EasyJet also faced legal claims from affected customers.

#### **1. How should EasyJet have responded to mitigate reputational damage?**

The Cyber-attack resulted in EasyJet's reputation being ruined. The first thing that EasyJet should've done is to apologize to its customers and communicate that any affected customers will be compensated. This would not completely mitigate the reputational damage of the company; however, it would be significantly better than just ignoring and moving over.

2. What steps could EasyJet have taken to prevent this breach from happening in the first place

EasyJet should've had a better cyber security team in order to be protected from the cyber-attack. A white hat hacker should've been assigned to try to find vulnerabilities, therefore fix them with updates. This would benefit the company not only because it's safer to cyber-attacks, but it would also benefit the customers, as they are assured their safety, this could bring more customers, therefore more profit for the company.

3. How do GDPR regulations influence the financial consequences of cyberattacks?

The financial consequences of the cyberattacks to EasyJet is significant as the company was fined £18 million, also had to compensate any affected customers which could be thousands of £. Furthermore the reputation damage could indirectly cause financial loss as customers will stop using their services due to meaning less profit

### **British Airways Data Breach**

In 2018, British Airways suffered a data breach that compromised the personal and financial information of over **400,000** customers. The breach occurred through a '**man in the middle**' method, when hackers redirected users from the official British Airways websites to a clone page where all the personal information that would be inputted by the user that would normally be encrypted, it would instead go directly to the attackers and then sold for profit.

#### **Impacts:**

Financial loss – British Airways was initially fined £183 million by UK's Information Commissioner's Office but the amount was reduced to £20 million after a review. A lot of money was also lost due to lawsuits from the customers, compensation requests, and indirectly due to reputation damage as people are less likely to continue using a company's services if its security is not as safe as it should be.

Reputation – After British Airways data breach happened, a reputation loss would be inevitable, and in this scenario, it was very negative for the company as they would not only expect less customers, but also less investors which mean further financial loss. In fact, the value of a share became 4 times less than it used to be, and with thousands of shares owned, the amount lost for both the company and investors is very significant.

Cybersecurity - British Airways were now forced to improve and invest in a better and larger cyber-security team to prevent any other cyber-attacks happening.  
Meaning

## Sources:

<https://www.bbc.co.uk/news/articles/c9777v4m8zdo#:~:text=NHS%20confirms%20patient%20data%20stolen%20in%20cyber%20attack&text=Qilin%2C%20a%20Russian%20cyber%2Dcriminal,to%20extort%20money%20from%20Synnovis.>

[https://en.wikipedia.org/wiki/Qilin\\_\(cybercrime\\_group\)#:~:text=Qilin%20is%20a%20Russian%2Dspeaking,Agenda%2C%20which%20affiliates%20could%20tailor.](https://en.wikipedia.org/wiki/Qilin_(cybercrime_group)#:~:text=Qilin%20is%20a%20Russian%2Dspeaking,Agenda%2C%20which%20affiliates%20could%20tailor.)

1.5 I can summarise the variety of threats for an audience.

There are many threats for any audience, from young internet users to older internet users which are not familiar with the internet and are easiest targets for the attackers. It is as easy as clicking on a fake download button and installing a wrong program and the computer is infected with malware. Phishing is also commonly used for audience with little internet knowledge thus it has a relatively high success rate. However.

The main threats for these users are:

**Phishing** – This method is very common and old. The method is made up of 3 steps:

### 1.Baiting

The first step consists of the attacker sending an email pretending to be a known company for social media online banking or other stating that your account vulnerable and that you need to take action to prevent your account from being compromised.

### 2.Hooking

The said email will most of the time contain a link to a clone website to the corresponding company that has the user to think that they need to reset the password by introducing their email and password. Those details are then sent directly to the attacker's database where they can take full control of the account

### 3.Harvesting

After the attacker gathered full control over the victims' account, it can then be used for a multitude of malicious activities like stealing money from the account, using the identity for further spreading malware and advertising scams.

There are also threats for expert internet users and even large companies. In those situations, a phishing email will not be enough to cause damage, however cyber criminals have developed methods that are more likely to cause damage:

**Distributed denial of service** attacks are meant to overwhelm a company server through intense traffic to the server. If their website or services and even database are stored on that server, it will become slower and slower until it won't be usable anymore. Anyone that wants to access the company's website will not be able to.

### **How does DDoS work?**

There must be a team of cyber criminals behind a DDoS attack that already have access to a botnet. **A botnet** is a network of hacked computers around the world (thousands) that the hackers have access to using malware. When a DDoS attack is initiated, the botnet will simultaneously send requests to the server and because of the volume of the requests at the same time, the server will overload and cause all services to be unavailable

### **Impacts of DDoS attacks**

The implications of a DDoS attack on a company are financial loss. Because the services will be down for an unknown amount of time, which will cause revenue loss, reputation damage and overall damage to the structure of the systems.



## 2 Analyse and detail the types of threat currently in operation

### 2.1 I can describe the motivations of people behind threats.

**Financial** - The motivations of people behind the threats are mainly financial reasons. Most threats involve in either stealing the personal information of people then selling it on black market for significant profit or encrypting people's files making them inaccessible unless a ransom is paid. The ransom's amount is usually around \$800.000 and it is not guaranteed that paying it will recover the files or that it will not be shared online

This list shows the average ransomware damage cost globally.

2015 - \$325 million

2017 - \$5 billion

2021 - \$20 billion

2024 - \$ 42 billion

It is expected to hit \$75.5 billion by 2026.

**Political** - Other reasons are political reasons which can significantly affect the outcome of events at a national level in the cyber criminal's benefit. For example, recently in 2024 the United States presidential election was influenced by groups of cyber criminals from Russia and China who used a collection of fake identities obtained through hacking to spread misinformation and propaganda. The voting system was attempted to be hacked and exploited by searching for vulnerabilities. Artificial Intelligence was also used for media and fake news. All these actions were made to influence the ultimate result of the election, and in this case the hackers wanted Donald Trump to win the election, the exact reason for this is not known but we can theorise it was about the geopolitical alignment and how Trump showed suspicion of the NATO alliance, which is directly against Russia and east Asia.

**Pure passion** – This can be individuals that are passionate of coding and programming and simply want to develop their skills or test them. Because of the age of this category, it is common that gaming might be implicated in their hobbies. Cheating in videogames will be a challenge for those who are interested in hacking as it can ease the process that is required for rewards or recognition. This is perfect use of reverse-engineering the game code for your benefit, meaning that you access the already made code, study it, and modify it.

### The Gateway

The Getaway, as the name suggest, are the suspects that even if they are caught, they get away with little to no punishment, as they are using the fact that they are

underage in their favour. They will most likely get away with cyber-crime, even though it is. Getaways are not a big threat most of the time as their hacking skills are usually basic or below average, however, there are some exceptions; individuals that are passionate about computers from young age and improve their skills day by day and manage to reach significant potential. However, that potential is sometimes used for negative things instead of positive. One example of that is an Australian teenager named Dylan Wheeler, which was accused of stealing \$100M worth of intellectual property. He was actively being searched but he could not be found. 3 years later and he was still not found, he decided to play safe and get away from Australia before he gets caught, but that would be a real challenge for him as he would have to surrender his personal information, therefore be arrested, however, that did not happen. 'It was quite scary that I was able to leave', says Mr. Wheeler. He was able to bypass even the Australian border control system,

Source: <https://cybersecurityventures.com/ransomware-report-2021/>

<https://www.abc.net.au/news/2015-11-27/teenage-hacker-dylan-wheeler-accused-of-hacking-us-army-flees/6977106>

2.2 I can analyse the main threats in terms of the mechanisms they use. Along the time, cyber criminals have created a multitude of ways to do malicious things through cyber threats, which can be split into categories of the methods they use:

DDoS / DoS (distributed denial of service / denial of service)

SQL injections.

Man in the middle.

Phishing.

The way that the most common threats operate are by exploiting the structure of the internet, the hardware inside the computers and even the humans themselves.

**Malware** - One of the most common cyber-threat, malware, works by convincing the victim into downloading the malicious software, by appearing to be a known official program that is safe. Other methods of infection with malware are:

External devices – devices as small and as innocent as a regular USB type C cable can be enough to infect a computer. It only needs to be plugged in, and the malware will be immediately installed in the machine.

Vulnerabilities in software – hackers will search for vulnerabilities in software, but most of the times the developer will fix the vulnerabilities before they are exploited. However, if an individual won't update the software, then the vulnerabilities are still exploitable by the hackers, and this is another way that hackers infect computers with malware.

After the malware is installed on the machine, the attacker will have full control over the computer, they can then further infect the network that the computer is connected to, steal all the data that is stored on it or use it for crypto currency mining.

**Social engineering** – rather than trying to penetrate systems through hacking, social engineering focuses on the human's psychology and manipulation. It might not sound as dangerous as no one would ever tell their passwords to anyone, but because social engineering focuses on human vulnerabilities rather than technical vulnerabilities, they will find a way to accomplish their target, whatever it might be.

Example:

### **2020 X event**

In 2020 of July, X (formerly Twitter) was targeted by a team of social engineers with the intention of gaining full control over the accounts of some of the most influential and popular images on the platform like Apple, Elon Musk, Jeff Bezos, and promoting cryptocurrency scams using these accounts, as they are credible by most people.

The social engineers started by using typical methods of calling the employees and pretending to be part of the IT staff. The employees were sent to a clone log in page which is meant to trick users into thinking that they are logging in the real X, however when the credentials were inputted, they were directly sent to the attackers. This allowed them to have access to admin tools which are powerful and must only be used by highest level X employees.

With access to admin tools, the attackers took over the mentioned images accounts and started posting advertisements to cryptocurrency scams. Causing a value of bitcoin worth \$100,000 to be lost from people all around the world. This also caused reputation damage to X's image.

2.3 I can describe how the features of threats make them operate.

**Social engineering** - One of the main methods used by cyber criminals to penetrate large companies is through social engineering. By directly interacting with employees and exploiting their lack of experience, they are able to gather their login information by pretending to be someone else from their company. As unrealistic as this sounds, this method is the reason of a very good proportion of successful cyber-attacks.

**Malware** - Malware is the most common cyber threat on the internet. It can include any piece of malicious software from simple viruses that can easily be detected by an antivirus, to deadly software that locks the user out of their own computer and gather full control over it, only a full factory reset or re installation of the operating system being able to get rid of the virus. Malware can make its way in anyone's personal computers by multiple different ways, some of them are as easy as clicking on a fake download button, but others consist in more advanced techniques which are mastered by cyber criminals. They are able to hack into systems because they understand how they function. This needs very advanced knowledge of the backbone of computers and how they operate.

**SQL injection** – This type of cyber threat consists in the attacker modifying the target's web application system's database queries through injecting the malicious sql code, the code will then automatically search for vulnerabilities, then, by exploiting it, the attackers get access to the database. More specifically, they look for code that directly interacts with the database security field like login forms then modifies it which makes bypassing it easy, giving them full access to the database.

2.4 I can describe how attacks on companies are designed to work.

Attackers are continuously trying to find new ways and vulnerabilities to penetrate large companies' security systems. Most of the times, attackers make use of the structure of the computer's hardware to try to find vulnerabilities. This consists in **scanning a website** for open logical ports, any opened port being a vulnerability that the attackers could exploit.

Theres no specific way which attacks are designed to work which makes it extremely hard to prevent them. Most of the times, the attackers will first need to penetrate into the system network before being able further advance in the attack. Example:

### **Target Data breach**

In 2013 Target suffered a data-breach exposing personal information of 70 million individuals including the card details of 40 million.

How did it happen?

The attackers have tricked a third-party vendor (HVAC) employee into giving their credentials, because target and HVAC were linked, they have used them to infiltrate inside the Target's network to install malware directly inside the point-of-sale system which is used for the sales, because of that, all payments information go through this system therefore the malware gathered the information of 40 million debit/credit cards.

Studying the attackers and thinking like them is a good way of preventing them. This is where white hats come into play.

### **White, grey and black hats:**

**White hats** - To prevent possible threats to the company, the cyber security chief information security officer (CISO) may employ professionals which will make unannounced simulated attacks on the cyber-security team which purpose is to check for vulnerabilities. These professionals are known as **white hats**. White hats are first party hackers that are meant to improve the cyber security abilities through simulating attacks. This is the only scenario where hacking is allowed and legal.

**Gray hats** – These are a combination of ethical and unethical hackers as it refers to hackers that act illegally, but on good purposes like finding vulnerabilities on systems then reporting them to the owner.

**Black hats** – These are the unethical hackers that exploits vulnerabilities for malicious purposes bases on their motivation which can be financial, social or other. Most hackers

Aspect	White hat	Gray hat	Black hat
Ethics	Ethical	Mixed	unethical
intention	Improve system	Improve system	Damage, harm
Law	Legal	Illegal	Illegal
example	Simulated attack	Unapproved attack	Ransomware attackers

### 2.5 I can describe threats in terms of their hierarchy of damage.

Cyber threats are classified on a scale according to the amount of damage it can do. The scale is standard in industry. Common Vulnerability Scoring System (CVSS).

The calculator works by selecting different factors that are linked to the specific scenario. The algorithm then calculates the damage possible by the vulnerability score on a scale of 0 to 10:

The calculator requires 8 factors which describes the vulnerability to a system.  
The factors are the following:

Score	Security
0.0	Non
0-3.9	low
4.0-6.9	Medium
7.0-10	High/critical

AV: Network

Attack Vector

AV: Local

AV: Adjacent

AV: Network

AV: Physical

1.

The attack vector suggests the state of how the attack can initiate: through internet, local adjacent or physical, meaning it can happen from the internet or locally only, or from sources which have access to the system

PR: None

Privileges Required

PR: None

PR: Low

PR: High

2.

States what level of privilege is required in order to initiate the threat lower is worse as less people will have high level privilege therefore less possibility of it happening

S: Unchanged

Scope

S: Unchanged

S: Changed

3.

states whether or not the scope is changed or not changed. will be the same or will differ. If only one person is potentially a threat, or different persons.

I: High

Integrity Impact

I: None

I: Low

I: High

4.

states the impact or effects on a successful threat on the integrity of the system.

AC: Low

Attack Complexity

AC: Low

AC: High

5.

states the difficulty level of the threat. higher is safer as less people will be able to successfully initiate one.

UI: None

User Interaction

UI: Required

UI: None

6. States whether user interaction is needed or not.

C: High

Confidentiality Impact

C: None

C: Low

C: High

7. High means the attacker would have full control over the impacted systems while none means that no data will be accessible in case of an attack.

A: High

Availability Impact

A: None

A: Low

A: High

8. states how much a successfully exploited vulnerability would affect the accessibility of a system.

After selecting the correct values, the calculator will give the base score on a scale of 1 to 10, 1 being low risk and 10 being very high risk.

AV: Network

AC: Low

PR: Low

UI: None

S: Unchanged

C: High


I: None

A: None

Base Score:

6.5

After inputting the factors, the website calculated that the base score of the vulnerability was 6.5, which is applicable for the 'medium' category, meaning that it is dangerous and the potential damage is high risk, but not the highest risk possible.

AV: Network ▼	AC: High ▼	Base Score:  <h1>8.0</h1> 
PR: High ▼	UI: None ▼	
S: Changed ▼	C: High ▼	
I: High ▼	A: High ▼	

After I've changed some factors, the base score increased significantly. This suggests that this case **needs more attention** than the previous one as it fits in the **high/critical** category of the CVSS. In this case, a company will allocate more cyber security power to eliminate any potential vulnerabilities being found and exploited. The damage it can do is far more significant than what the previous one was able to do. However, not all attention must be on this vulnerability, because if the other is left defenceless it will be able to penetrate the systems and cause damage.

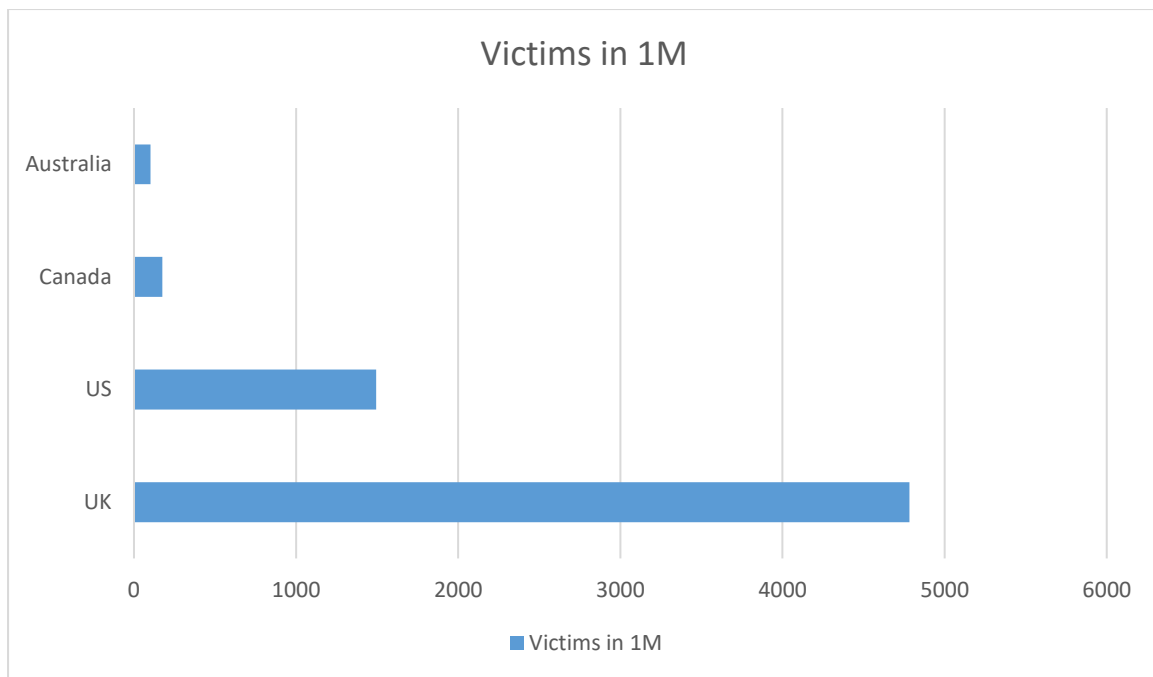
### 3 Evaluate the impact of threats on various individuals and organisations.

3.1 I can evaluate the impact on the economy of cyber threats. Cyber threats are known for causing big financial damages to not only individuals, but also companies and even governments. Only one cyber-attack is enough to cause immense financial and reputation loss to a company, or even completely ruin one with no chance of recovery. Annually, it is estimated that cybercrime causes damages of up to £27 billion in the UK only.

According to Independent.co.uk, UK has the most victims in cyber crime

Source: <https://www.independent.co.uk/advisor/vpn/cybercrime-statistics>





Data breaches are one of the dangerous cases for a company as it causes the biggest financial and reputation loss and potential lawsuits, fines and compensation for the damage for everyone that has been affected.

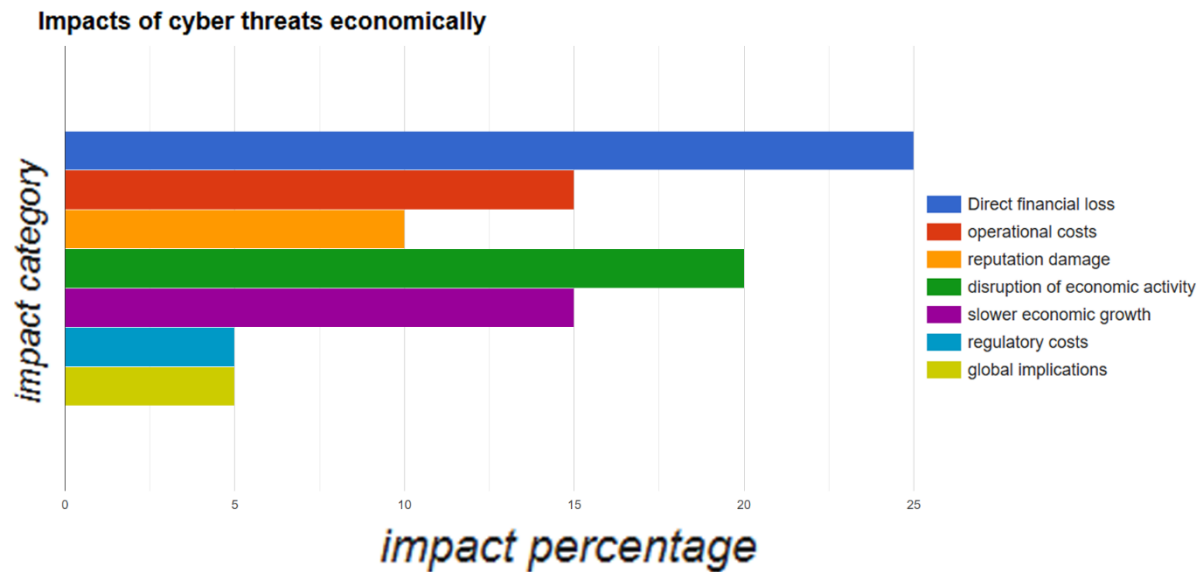
An example of that is the Equifax data breach case in 2017 where around **147 million** people's personal information were exposed including credit card numbers, addresses and social security numbers. Both clients and the company suffered financial damages, however, in the end the company agreed to pay for all the damage caused to its clients which was around **\$425 million**. Furthermore, the company suffered a significant drop in market capitalization after the incident. In total the company suffered a financial damage of at least **\$700 million**.

Ransomware attacks are in the list of the most impactful damages that a company can experience because hackers are asking for money to get access to a key to decrypt the files, and that request can sometimes be in the millions level.

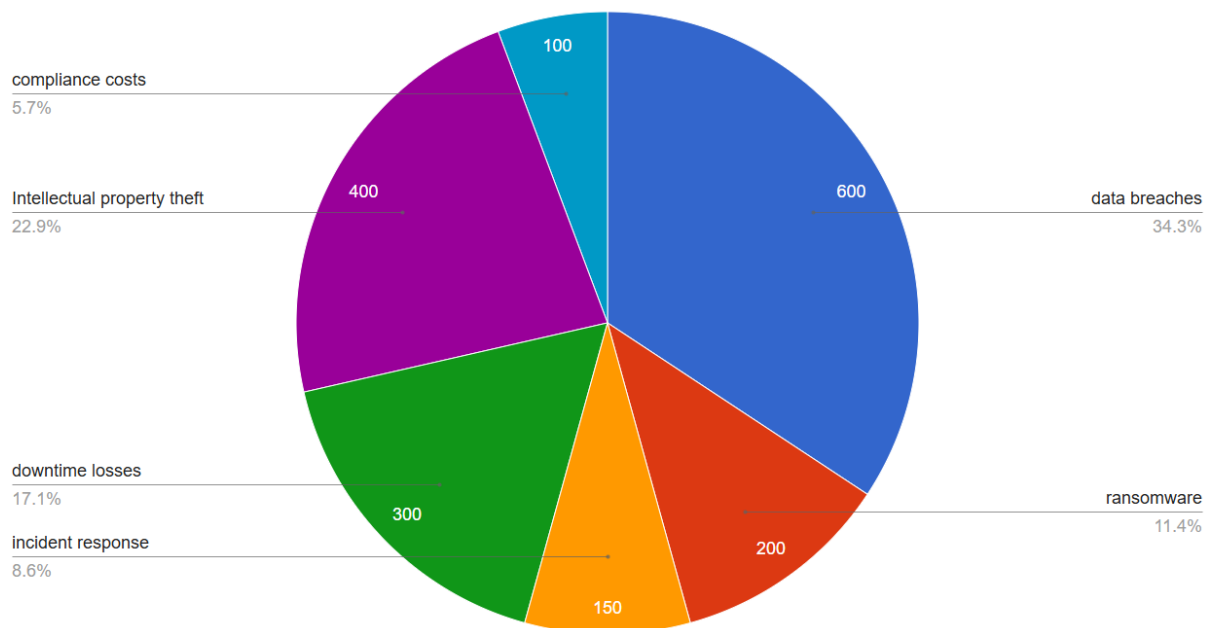
For example, in 2017 Maersk, a logistics company, suffered a ransomware attack by NotPetya. The attack was successful because the attackers have found a vulnerability in the Microsoft Windows operating system which allowed them to penetrate inside of the Maersk's network. All the files were encrypted which left some systems unable to operate.

It is now known what exact amount the ransom was, but Maersk later reported that around **\$300 million were lost** because of the whole event. This includes the ransom itself, as well as the operations, services, booking systems and shipping.

The following graphs shows the global economic damages due to cyber threats. This one shows how more factors including reputation damage, global implications and operational costs contribute to the overall damage being so high



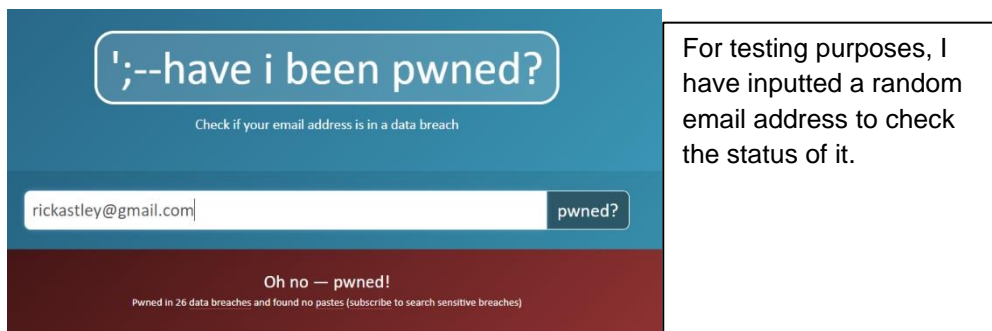
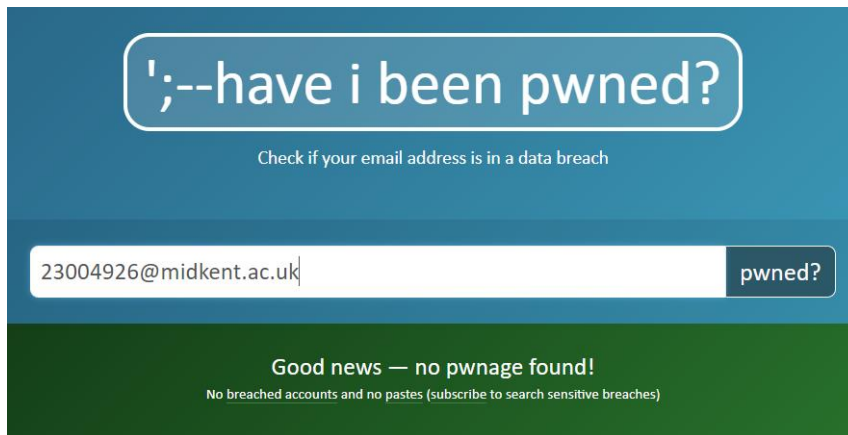
**Distribution of economic impacts from cyber threats**



3.2 I can determine the level of threat to my home environment. By using third party apps, I can analyse my home network and scan for vulnerabilities and open ports for each device connected to the network. In my case, ports 135, 139 and 445 are open for my personal computer, however, this is not a risk as these ports do not offer access to any important action or information.

Using [Have I Been Pwned: Check if your email has been compromised in a data breach](#) I am able to check if an email address has been found on a breach by scanning known data bases for the inputted email address.

I have inputted my college email address to check and I was immediately provided with the answer that the email address was not found in a data breach.

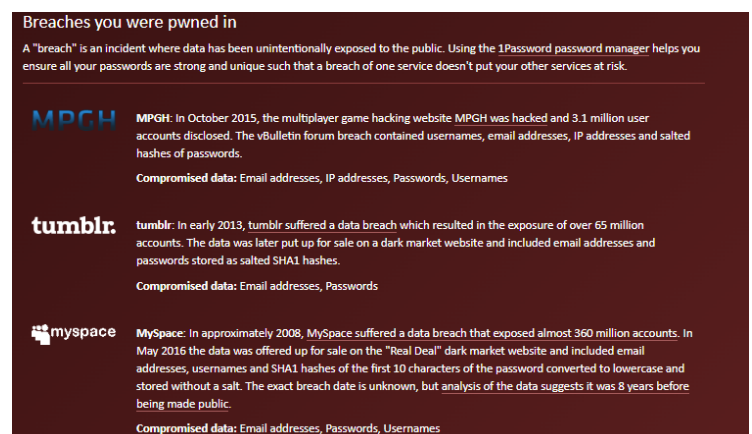


If an email address is found on a data breach it will mention that, as well as all the breaches that the address was found in.







These are just 3 of the 26 breaches that the email address was found.

If this happens, it is recommended to immediately change the password, enable 2 factor authentication and also use different passwords for each platform that the email address is used for as log in.

Using a different third-party app called Fing, I am able to check all the devices connected to the same network.



6 devices of 10 1 min ago


	LER 192.168.1.73	Asus VIVOBOK X509FA_X509FA	>
	XBOXONE 192.168.1.81	Microsoft Xbox One	>
	Generic 192.168.1.108	-	>
	Generic 192.168.1.148	-	>
	OnePlus 8 192.168.1.176	OnePlus 8	>
	BT HomeHub6DX 192.168.1.254	BT Home Hub 6DX	▶


Further more I can manage each device with a variety of actions provided by the app


MODEL


HOME HUB 6DX


Manage this device

















One option is find open ports which is useful if you want to find vulnerabilities in the network or devices

### 3.3 I can determine the threat to a website in a safe and controlled environment.

It is possible to easily determine if a website is vulnerable or not by scanning for open ports. However, doing that irresponsibly and without permission is prohibited and can lead to fines. For testing purposes, we are allowed to target some websites which we do not need permission for.

Scanning a website consists in going through all logical ports and checking if they are either opened, closed or filtered. The ports are virtual channels for specific internet traffic.

As we can see from the screenshot below, a quick scan of a website which allows scanning the ports, shows that ports 80 and 443 are open which mean a hacker could infiltrate and take control of those ports, which would give them access to all the information traveling through that port.

We can also see most ports are filtered, meaning that the ports are locked up to unwanted traffic, but available for safe traffic. There are also closed ports which completely blocks any traffic from accessing it.

```
65.61.137.117

Quick Nmap Scan

Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-06 20:48 UTC
Nmap scan report for 65.61.137.117
Host is up (0.019s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    filtered  telnet
80/tcp    open      http
110/tcp   filtered  pop3
143/tcp   filtered  imap
443/tcp   open      https
3389/tcp   filtered  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
```