BELGIUM CAMPUS

ETHICS

ETH271

BELGIUM CAMPUS
iTversity

CYBERCRIME PREVALENCE

Which countries do you think have the highest/lowest rate of malware infection?

Countries with highest rate of infected computers		Countries with lowest rate of infected computers	
Country	Rate	Country	Rate
Sudan	70%	Japan	6%
Bangladesh	64%	Germany	9%
Iraq	62%	Switzerland	10%
Rwanda	57%	Luxembourg	10%
Nepal	56%	Denmark	11%

Surfshark's cybercrime report for 2021 showed that South Africa had 52 cybercrime victims per one million internet users, with other countries showing even more alarming numbers. The top-ranking country was the UK, with a whopping 4,783 victims per one million users – followed by the US (1,494/1m), Canada (174/1m), Australia (102/1m) and Greece (72/1m).

The FBI's major cybercrime cases

CYBERCRIMES

What kind of crimes can be committed in the world of IT?

Cybercrime is the biggest form of crime in the world at the moment, even surpassing drug trafficking and illegal arms dealing.
This is expected to worsen as the world becomes more digitally inclined, with the World Economic Forum Global Risk Report 2022 noting that cybersecurity failures have increased by 12.4% since the start of the Covid-19 pandemic.

As a result, the report ranked cybercrime among the top 10 global risks for the future, listing it above infectious diseases, stagflation, and human environmental damage – estimating that cybercrime will cost the world $10.5 trillion (R192 trillion) annually by 2025.

A FIRM IS A VICTIM OF INTERNET CRIME. WHAT SHOULD IT DO?

Internet crime can appear in various forms. It invariably has a negative impact on the company itself but often also has a negative impact on the customers or clients.

A Pursue persecution of the criminals at all costs

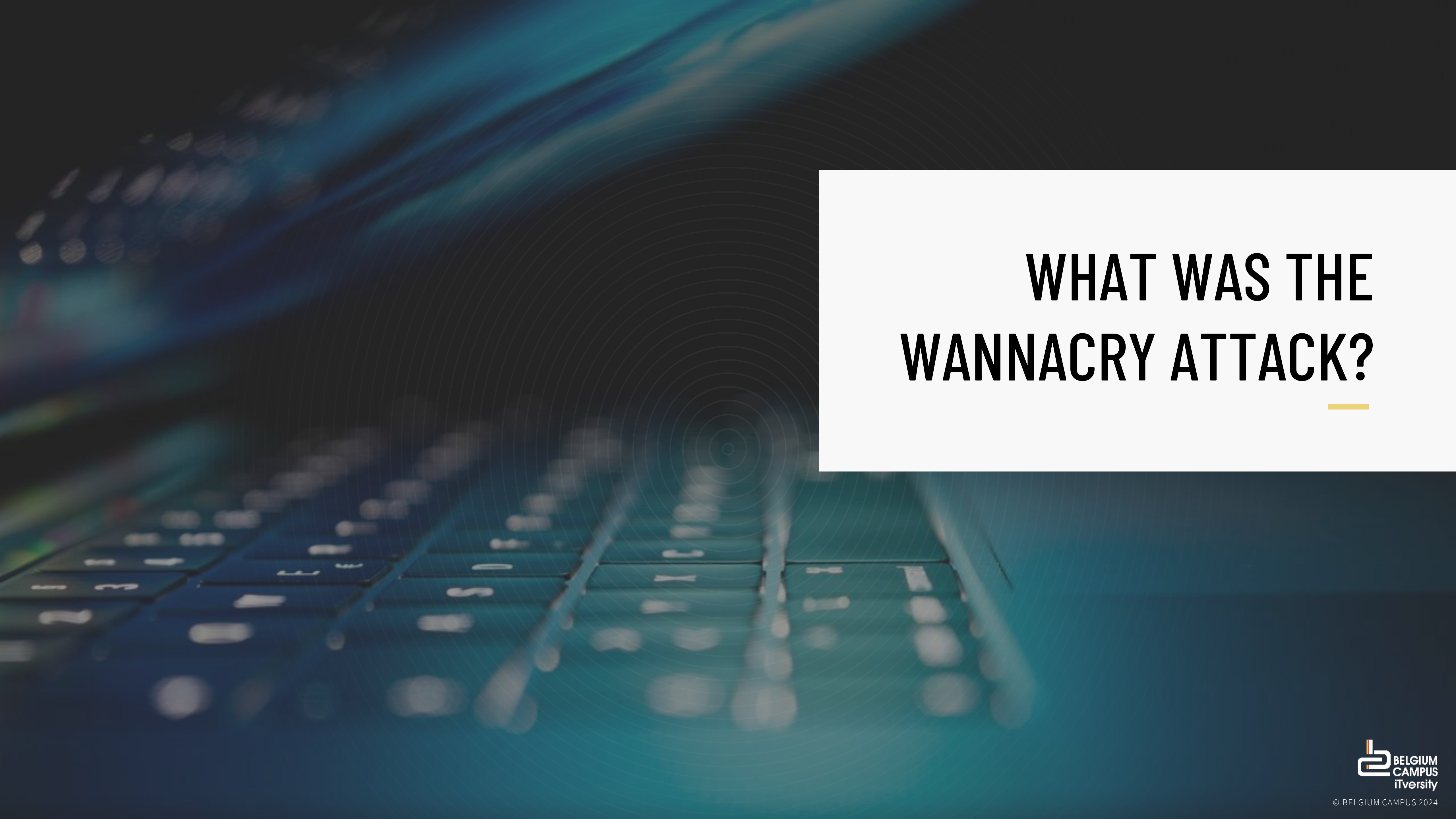
B Maintain a low profile to avoid negative publicity.

C Inform its affected customers and stakeholders.

D Take some other action.

INTERNET CRIME IS A COMPLEX ISSUE. LOOK AT THESE QUESTIONS:

1. How much effort and money should be spent to protect against computer crime? How safe is safe enough?
2. If a company realizes it has produced software with defects that open the user up to attacks, what should it do?
3. What should be done if recommended security safeguards make business more difficult for customers and employees, resulting in a loss of profit/sales?



WHAT WAS THE WANNACRY ATTACK?

ZERO-DAY ATTACKS

How many days has the vendor been aware of the vulnerability? Zero.

A zero-day attack is aimed at a vulnerability the developer is not aware of.

If another party like the government or a criminal detects the vulnerability, it is still a zero-day vulnerability until the developer is aware of it.

ZERO-DAY ATTACKS

What if Google detects a vulnerability in a foreign power? Should they let the US government know? Research the coordinated US/Israeli governments' attack on Iran's nuclear program.

ZERO-DAY ATTACKS

In ethics there is an **equivalence principle**. It states that actively doing harm is just as bad as not acting to prevent harm.

This means that not reporting these vulnerabilities is just as bad as exploiting them yourself.

TYPES OF ATTACKS

There are many types of computer exploits or attacks. New varieties are being invented all the time. Here we will look at some of the more common attacks.

01

Zero-day attacks

These take place before the developer has been able to patch it. Mobile phones have increasingly become a target.

02

Worms, viruses, trojans etc.

These are well-known attacks that have been around for quite some time. Typically, these are what anti-virus software protect against.

03

Ransomware

An attack that locks up a computer and requires users to pay an amount/fine to receive an unlock key. It is often downloaded automatically when a user visits an infected website.

TYPES OF ATTACKS

There are many types of computer exploits or attacks. New varieties are being invented all the time. Here we will look at some of the more common attacks.

04

DDoS attacks

Distributed denial-of-service attacks flood a server with demands for data and other small tasks. It’s not a direct attack but causes the server to crash.

05

Rootkits

A rootkit is a set of programs that enables its user to gain administrator-level access to a computer without the end user’s consent or knowledge. They are difficult to discover since the OS currently running cannot be trusted.

06

Phishing

The act of fraudulently using email to try and get the recipient to reveal personal data. Legitimate looking emails are sent urging the recipient to, typically, avoid some negative consequence or receive a reward.

Should spam be seen as a cybercrime?

Spam is legal but has certain conditions. It needs to comply with privacy laws.

BELGIUM CAMPUS iTversity

TYPES OF PERPETRATORS

There are many types of computer exploits or attacks. New varieties are being invented all the time. The people committing these acts do so for a variety of reasons.

Hackers and crackers

Hackers test the limitations of a system our of intellectual curiosity while crackers cause problems or steal data.

Malicious insiders

Fraud or security risks from inside the company. This often involves collusion between an employee and an outsider.

Industrial spies

Using illegal means to obtain trade secrets from competitors.

TYPES OF PERPETRATORS

There are many types of computer exploits or attacks. New varieties are being invented all the time. The people committing these acts do so for a variety of reasons.

Cybercriminals

Committing various forms of computer fraud – stealing and selling credit card numbers, personal identities, etc. Motivated by the potential for monetary gain.

Hacktivists and cyberterrorists

Hacking that is done to achieve a political or social goal. A cyberterrorist launches computer-based attacks against other computers or networks in an attempt to intimidate or coerce them.

WHY ARE COMPUTER INCIDENTS SO PREVALENT?

INCREASED COMPLEXITY

Networks, computers, operating systems, applications, web sites, switches, routers – the more components, the more entry points there are.

USER EXPECTATIONS

Users share login details since they believe the internet to be more secure than it is. In professional situations, authentication can happen too fast.

BYOD

Employees bringing their own laptops or phones onto the company network can be risky.

BELGIUM CAMPUS iTversity

WHY ARE COMPUTER INCIDENTS SO PREVALENT?

WHICH APP OR WEBSITE WOULD YOU STILL USE, EVEN IF IT WERE NOT 100% SECURE?

HOW DOES TODAY'S TECHNOLOGY COMPARE WITH TECHNOLOGY FROM 2008?

HOW PROFICIENT ARE YOUR PARENTS/GRANDPARENTS AT USING TECHNOLOGY, THEIR PHONES, OR THE INTERNET?

WHY ARE COMPUTER INCIDENTS SO PREVALENT?

SOFTWARE RELIANCE

Certain applications are so widely used that, even with vulnerabilities, they will still be used.

EXPANDING AND CHANGING

Technology is developing so fast that, in the rush to stay up to date, security checks can be done too quickly.

GENERATION GAPS

The huge boost in IT occurred over the past 30 years. This leads to large numbers of people being either computer illiterate or very proficient.

THE LAW

Why is it so difficult to stop sites like PirateBay?

INTERPOL'S AFRICAN CYBERTHREAT ASSESSMENT REPORT

What are the main points raised by this report?

BELGIUM CAMPUS iTversity

WHAT SHOULD BE INCLUDED IN A LAW TO COMBAT CYBERCRIME?

South Africa has a new cybercrime law. What is the extent of cybercrimes in South Africa?

CYBERCRIME

THE SOUTH AFRICAN CYBERCRIME LAW

The South African Cybercrime Act was signed into effect in December 2021. On the right you will find some of the areas this law addresses.

1 Unlawful access

2 Unlawful interception of data

3 Unlawful acts in respect of software or hardware tools

4 Unlawful interference with data or computer program

5 Unlawful interference with a computer data storage medium or computer system

6 Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device

7 Theft of incorporeal property

CYBERCRIME

THE SOUTH AFRICAN CYBERCRIME LAW

The South African Cybercrime Act was signed into effect in December 2021. On the right you will find some of the areas this law addresses.

8 **Cyber fraud**

using data/software to misrepresent yourself

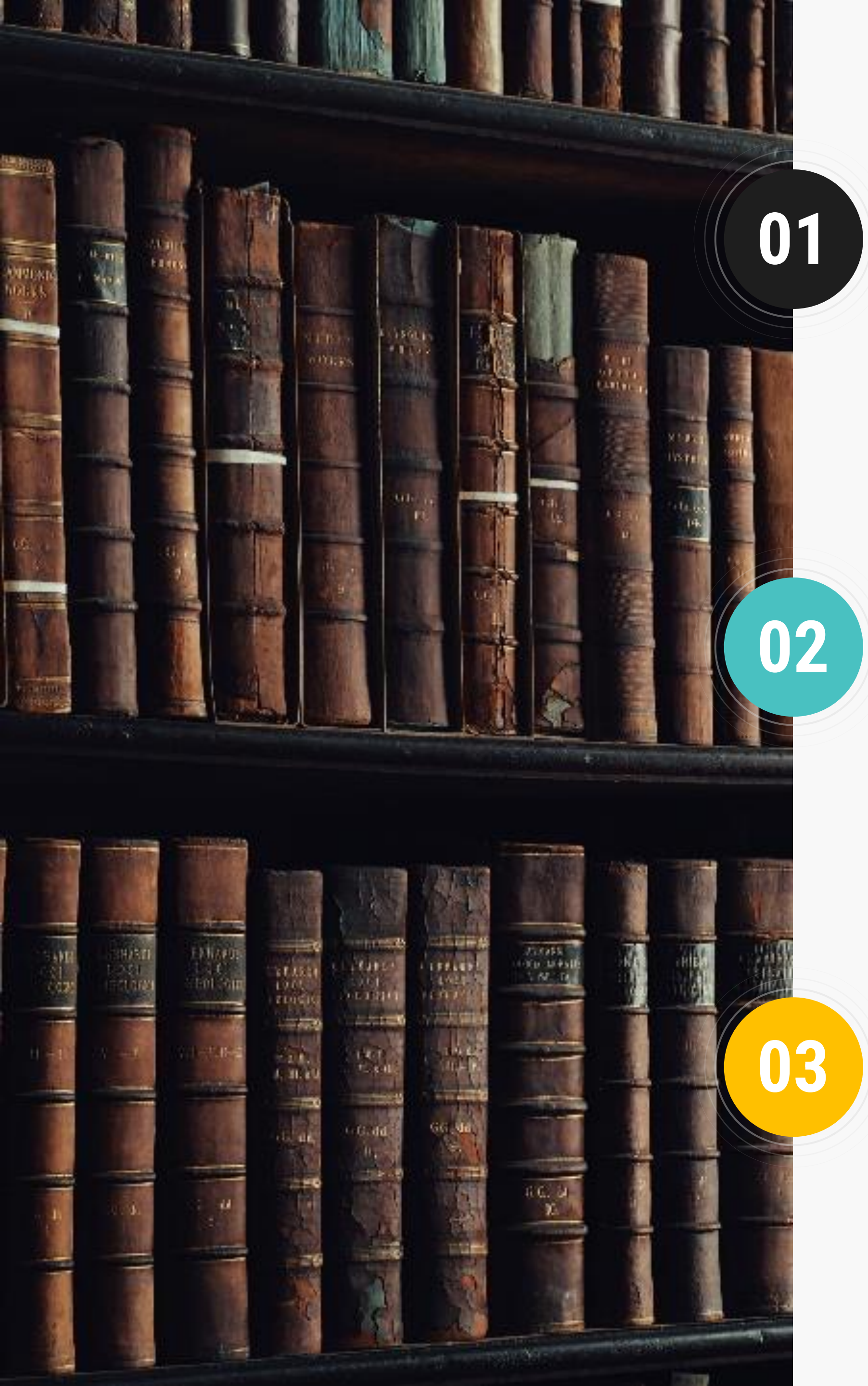
9 **Cyber forgery**

using false data/software (usually with the intention to commit fraud)

10 **Cyber extortion**

using illegal data/software to gain an advantage or to force someone else to do something.

RISK ASSESSMENT STEPS



01

PRIORITISE

Identify the assets related to the company’s primary business goals. Which IT assets are you most concerned about?

02

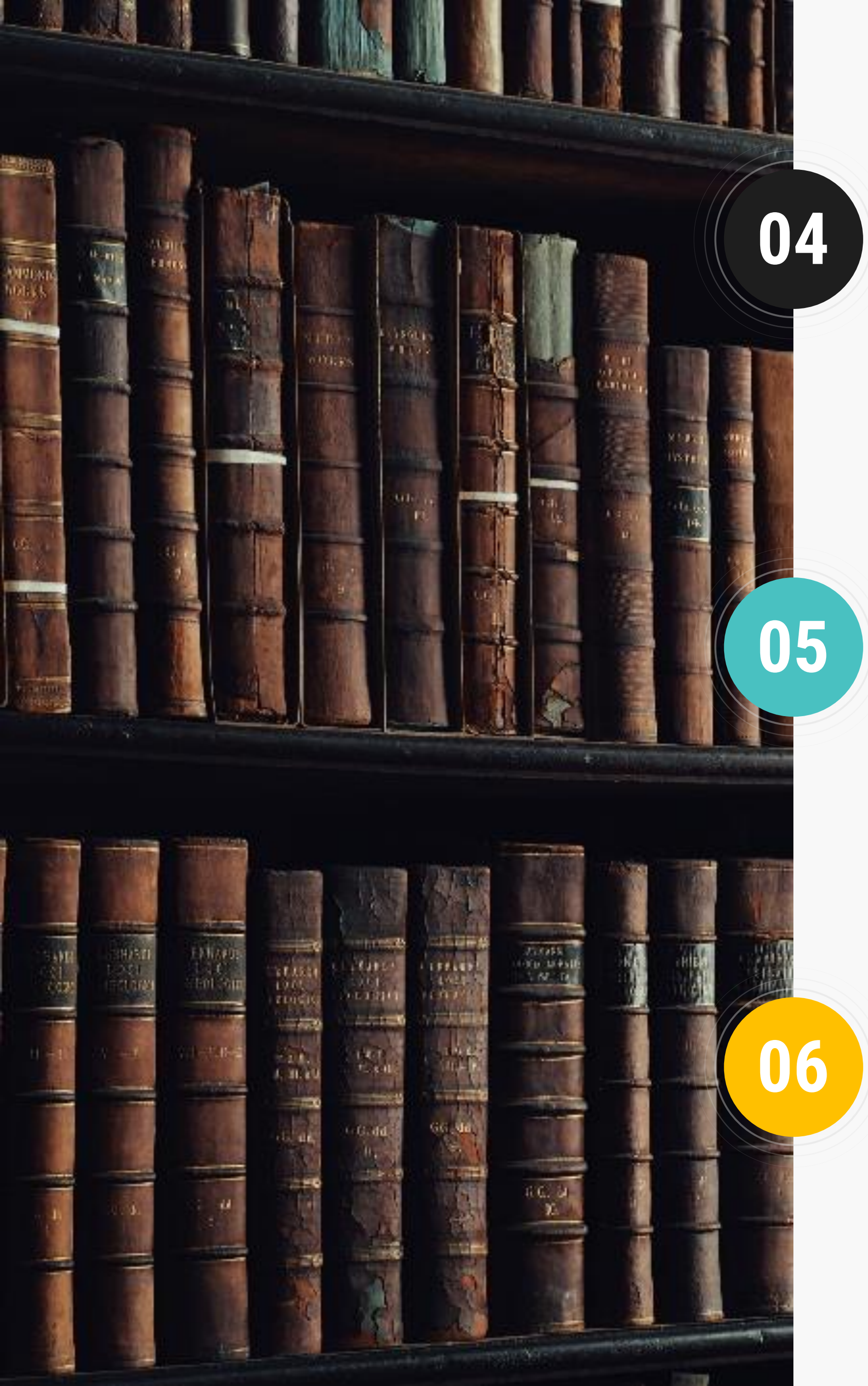
IDENTIFY

Identify the risks or threats that could occur, such as insider fraud of DDoS attacks.

03

ASSESS

What is the likelihood of each threat. Which potential threat would be more likely to occur?



RISK ASSESSMENT STEPS

04

IMPACT

How would an attack affect the continuity of the organisation?

05

MITIGATE

What counter-measures or preventative steps can be taken to lessen the impact of an IT attack?

06

IMPLEMENT

If financially and practically feasible, decide to implement the measures.

CASE STUDY - DISCUSSION

In 2012 powerful DDoS attacks were directed at the Web servers of several major US banks. These attack directed 65Gbps of data at each server – the network equivalent of a category 5 hurricane – effectively disabling the server. What is concerning is that the banks were not able to fend off the attack. The attackers simply stopped on their own to avoid detection. Should they communicate this to their customers? If so, how should they approach this?

CYBERCRIME PREVALENCE

Which countries do you think have the highest/lowest rate of malware infection?

Countries with highest rate of infected computers		Countries with lowest rate of infected computers	
Country	Rate	Country	Rate
Sudan	70%	Japan	6%
Bangladesh	64%	Germany	9%
Iraq	62%	Switzerland	10%
Rwanda	57%	Luxembourg	10%
Nepal	56%	Denmark	11%

Surfshark’s cybercrime report for 2021 showed that South Africa had 52 cybercrime victims per one million internet users, with other countries showing even more alarming numbers. The top-ranking country was the UK, with a whopping 4,783 victims per one million users – followed by the US (1,494/1m), Canada (174/1m), Australia (102/1m) and Greece (72/1m).

The FBI’s major cybercrime cases

BELGIUM CAMPUS iTversity

CYBERCRIMES

What kind of crimes can be committed in the world of IT?

Cybercrime is the biggest form of crime in the world at the moment, even surpassing drug trafficking and illegal arms dealing.
This is expected to worsen as the world becomes more digitally inclined, with the World Economic Forum Global Risk Report 2022 noting that cybersecurity failures have increased by 12.4% since the start of the Covid-19 pandemic.

As a result, the report ranked cybercrime among the top 10 global risks for the future, listing it above infectious diseases, stagflation, and human environmental damage – estimating that cybercrime will cost the world $10.5 trillion (R192 trillion) annually by 2025.

A FIRM IS A VICTIM OF INTERNET CRIME. WHAT SHOULD IT DO?

Internet crime can appear in various forms. It invariably has a negative impact on the company itself but often also has a negative impact on the customers or clients.

A Pursue persecution of the criminals at all costs

B Maintain a low profile to avoid negative publicity.

C Inform its affected customers and stakeholders.

D Take some other action.

INTERNET CRIME IS A COMPLEX ISSUE. LOOK AT THESE QUESTIONS:

1. How much effort and money should be spent to protect against computer crime? How safe is safe enough?
2. If a company realizes it has produced software with defects that open the user up to attacks, what should it do?
3. What should be done if recommended security safeguards make business more difficult for customers and employees, resulting in a loss of profit/sales?

WHAT WAS THE WANNACRY ATTACK?

ZERO-DAY ATTACKS

How many days has the vendor been aware of the vulnerability? Zero.

A zero-day attack is aimed at a vulnerability the developer is not aware of.

If another party like the government or a criminal detects the vulnerability, it is still a zero-day vulnerability until the developer is aware of it.

ZERO-DAY ATTACKS

What if Google detects a vulnerability in a foreign power? Should they let the US government know? Research the coordinated US/Israeli governments' attack on Iran's nuclear program.

ZERO-DAY ATTACKS

In ethics there is an **equivalence principle**. It states that actively doing harm is just as bad as not acting to prevent harm.
This means that not reporting these vulnerabilities is just as bad as exploiting them yourself.

TYPES OF ATTACKS

There are many types of computer exploits or attacks. New varieties are being invented all the time. Here we will look at some of the more common attacks.

01

Zero-day attacks

These take place before the developer has been able to patch it. Mobile phones have increasingly become a target.

02

Worms, viruses, trojans etc.

These are well-known attacks that have been around for quite some time. Typically, these are what anti-virus software protect against.

03

Ransomware

An attack that locks up a computer and requires users to pay an amount/fine to receive an unlock key. It is often downloaded automatically when a user visits an infected website.

TYPES OF ATTACKS

There are many types of computer exploits or attacks. New varieties are being invented all the time. Here we will look at some of the more common attacks.

04

DDoS attacks

Distributed denial-of-service attacks flood a server with demands for data and other small tasks. It’s not a direct attack but causes the server to crash.

05

Rootkits

A rootkit is a set of programs that enables its user to gain administrator-level access to a computer without the end user’s consent or knowledge. They are difficult to discover since the OS currently running cannot be trusted.

06

Phishing

The act of fraudulently using email to try and get the recipient to reveal personal data. Legitimate looking emails are sent urging the recipient to, typically, avoid some negative consequence or receive a reward.

Should spam be seen as a cybercrime?

Spam is legal but has certain conditions. It needs to comply with privacy laws.

TYPES OF PERPETRATORS

There are many types of computer exploits or attacks. New varieties are being invented all the time. The people committing these acts do so for a variety of reasons.

Hackers and crackers

Hackers test the limitations of a system our of intellectual curiosity while crackers cause problems or steal data.

Malicious insiders

Fraud or security risks from inside the company. This often involves collusion between an employee and an outsider.

Industrial spies

Using illegal means to obtain trade secrets from competitors.

TYPES OF PERPETRATORS

There are many types of computer exploits or attacks. New varieties are being invented all the time. The people committing these acts do so for a variety of reasons.

Cybercriminals

Committing various forms of computer fraud – stealing and selling credit card numbers, personal identities, etc. Motivated by the potential for monetary gain.

Hacktivists and cyberterrorists

Hacking that is done to achieve a political or social goal. A cyberterrorist launches computer-based attacks against other computers or networks in an attempt to intimidate or coerce them.

WHY ARE COMPUTER INCIDENTS SO PREVALENT?

INCREASED COMPLEXITY

Networks, computers, operating systems, applications, web sites, switches, routers – the more components, the more entry points there are.

USER EXPECTATIONS

Users share login details since they believe the internet to be more secure than it is. In professional situations, authentication can happen too fast.

BYOD

Employees bringing their own laptops or phones onto the company network can be risky.

WHY ARE COMPUTER INCIDENTS SO PREVALENT?

WHICH APP OR WEBSITE WOULD YOU STILL USE, EVEN IF IT WERE NOT 100% SECURE?

HOW DOES TODAY’S TECHNOLOGY COMPARE WITH TECHNOLOGY FROM 2008?

HOW PROFICIENT ARE YOUR PARENTS/GRANDPARENTS AT USING TECHNOLOGY, THEIR PHONES, OR THE INTERNET?

WHY ARE COMPUTER INCIDENTS SO PREVALENT?

SOFTWARE RELIANCE

Certain applications are so widely used that, even with vulnerabilities, they will still be used.

EXPANDING AND CHANGING

Technology is developing so fast that, in the rush to stay up to date, security checks can be done too quickly.

GENERATION GAPS

The huge boost in IT occurred over the past 30 years. This leads to large numbers of people being either computer illiterate or very proficient.

BELGIUM CAMPUS iTversity

THE LAW

Why is it so difficult to stop sites like PirateBay?

BELGIUM CAMPUS iTversity

INTERPOL’S AFRICAN CYBERTHREAT ASSESSMENT REPORT

What are the main points raised by this report?

WHAT SHOULD BE INCLUDED IN A LAW TO COMBAT CYBERCRIME?

South Africa has a new cybercrime law. What is the extent of cybercrimes in South Africa?

CYBERCRIME

THE SOUTH AFRICAN CYBERCRIME LAW

The South African Cybercrime Act was signed into effect in December 2021. On the right you will find some of the areas this law addresses.

1. Unlawful access
2. Unlawful interception of data
3. Unlawful acts in respect of software or hardware tools
4. Unlawful interference with data or computer program
5. Unlawful interference with a computer data storage medium or computer system
6. Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device
7. Theft of incorporeal property

CYBERCRIME

THE SOUTH AFRICAN CYBERCRIME LAW

The South African Cybercrime Act was signed into effect in December 2021. On the right you will find some of the areas this law addresses.

8 **Cyber fraud**

using data/software to misrepresent yourself

9 **Cyber forgery**

using false data/software (usually with the intention to commit fraud)

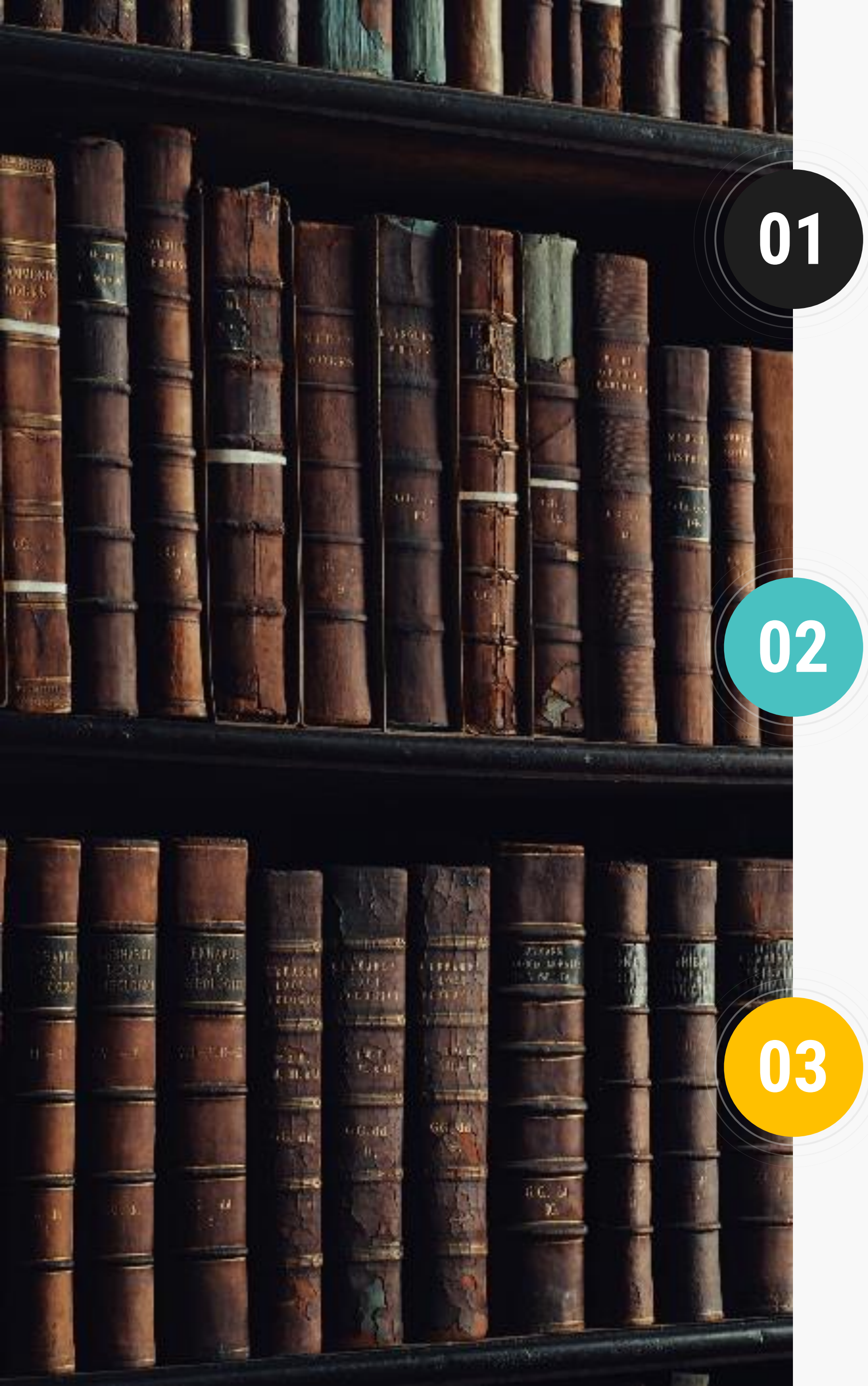
10 **Cyber extortion**

using illegal data/software to gain an advantage or to force someone else to do something.

DETERMINING VULNERABILITY

At what stage of growth should a company become wary of software vulnerabilities?

RISK ASSESSMENT STEPS



01

PRIORITISE

Identify the assets related to the company’s primary business goals. Which IT assets are you most concerned about?

02

IDENTIFY

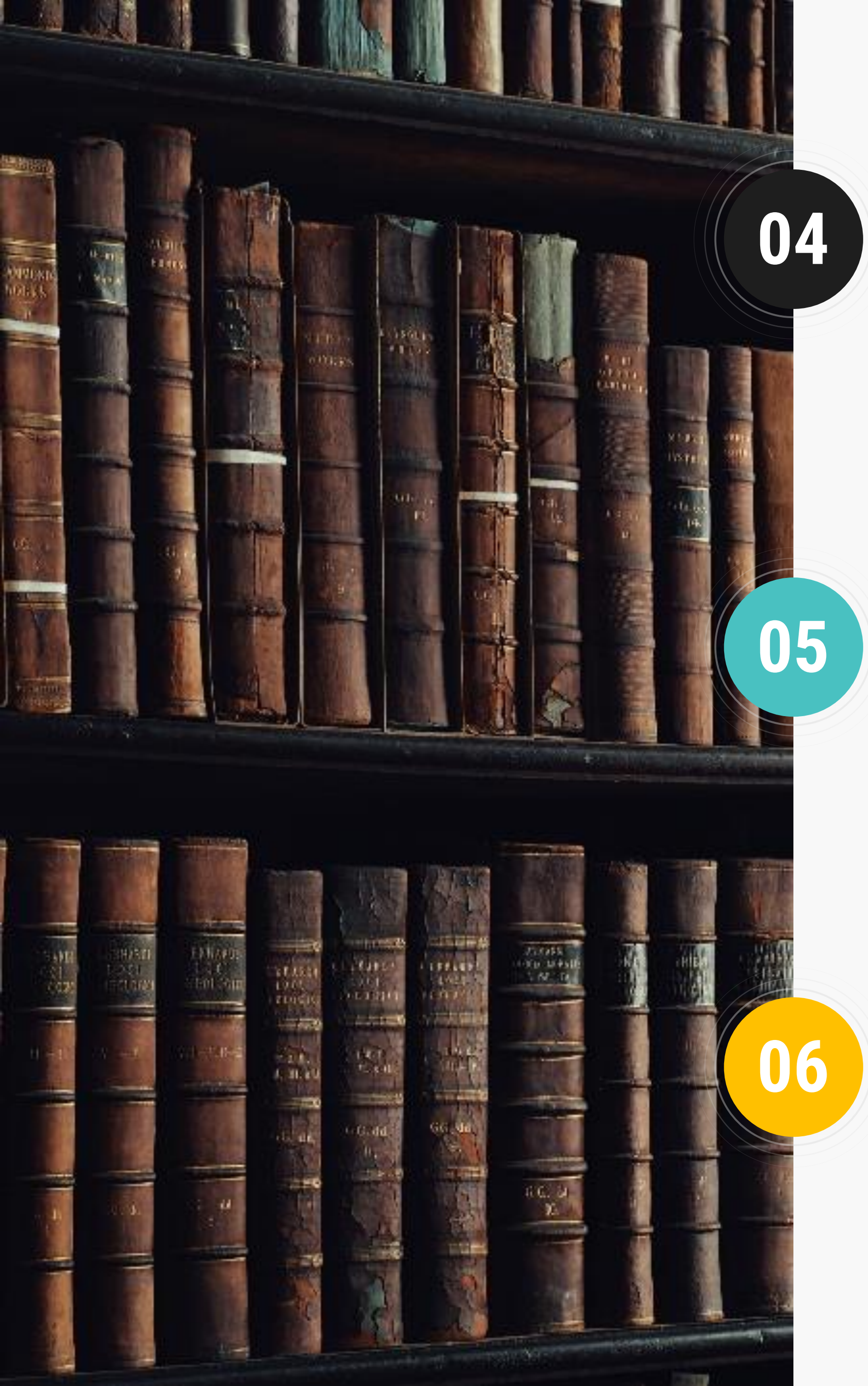
Identify the risks or threats that could occur, such as insider fraud of DDoS attacks.

03

ASSESS

What is the likelihood of each threat. Which potential threat would be more likely to occur?

BELGIUM CAMPUS iTversity



RISK ASSESSMENT STEPS

04

IMPACT

How would an attack affect the continuity of the organisation?

05

MITIGATE

What counter-measures or preventative steps can be taken to lessen the impact of an IT attack?

06

IMPLEMENT

If financially and practically feasible, decide to implement the measures.

CASE STUDY - DISCUSSION

In 2012 powerful DDoS attacks were directed at the Web servers of several major US banks. These attack directed 65Gbps of data at each server – the network equivalent of a category 5 hurricane – effectively disabling the server. What is concerning is that the banks were not able to fend off the attack. The attackers simply stopped on their own to avoid detection. Should they communicate this to their customers? If so, how should they approach this?