

University Of Essex

Principles of Digital Forensics and Cyber Law January 2022

Unit 6 – Mid-Module Assignment 1: Presentation

Introduction:

Today, more than sixty per cent of the world's total people have internet access. About half of the internet users are below the age of 25 years, and many are less than 18 years. The high risk and challenge about the internet are that it is entirely open worldwide with minimal rules in big countries.

In many parts of the world, the internet is already blocked by censorship, an act implemented by regimes seeking to maintain their power over the population.

Picture an internet cafe. These are places where internet users can sit for free and use internet access for their purposes. They are mainly used for social interaction such as chatting, sharing music, movies and TV shows, online magazines, and also in virtual business settings.

However, in many of the world's most populated countries, this need is not always fulfilled. In fact, there are two main ways governments block their populations from connecting to the internet.

Firstly, often referred to as 'proxies', or Internet Service Providers (ISPs) block access to the internet through the pipes that carry the relevant internet traffic. In the future, with all the fast internet growth, it will become hard to control cybercrime, and of course, any crime that does not include electronic evidence.

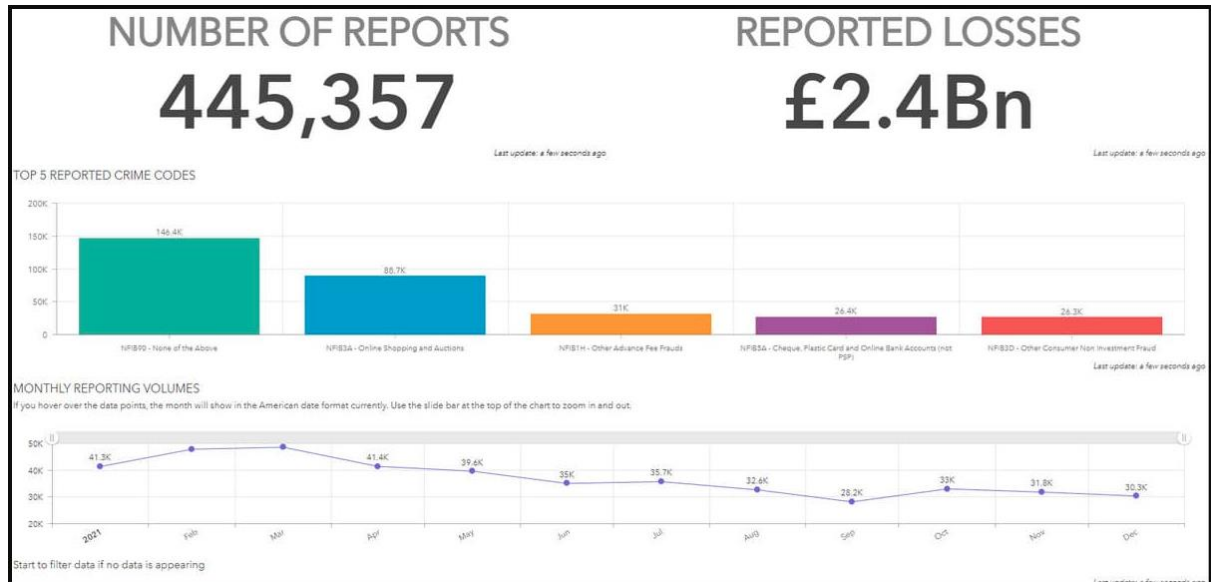
The country chosen and reason:

In this assignment, the United Kingdom has been chosen as an example of the cybercrime case study.

The UK is one of the most critical financial business countries globally, and most of the prominent organizations have employees in the UK. Furthermore, most UK houses have internet access, and most people have mobile with GSM data connectivity. As a result, physical, cyber and psychological threats exist for individuals, businesses and national security. The UK is vulnerable and targeted from anywhere globally because of the borderless nature of cybercrime. The UK government has labelled any cyber threat as a tier-one threat in its National Security Strategy, and it is one of the highest priorities for action.

The UK has a robust digital economy, high levels of educational attainment among its inhabitants, and an impressive history in science and technology innovation. Government research suggests that the UK has the highest percentage of GDP involved in the digital economy in Europe, and that between 2003 and 2013 its digital industries grew two and a half times as fast as the whole economy (House of commons 2016). (Saunders, 2017)

In all world countries, cybercrime is becoming a national-scale issue. Cybercrime had cost the UK economy about £2.4bn in 2021, and it is likely to be growing. Cybercrime poses a critical problem as attackers can easily access and relative anonymity provided by ICTs while also lowering the risk of being caught in crimes that are straightforward to conduct.



(Comparitech Limited, 2022)

Cybercrime case study:

R v Rogers [2014] EWCA Crim 1680 has been chosen as an example of the cybercrime case study.

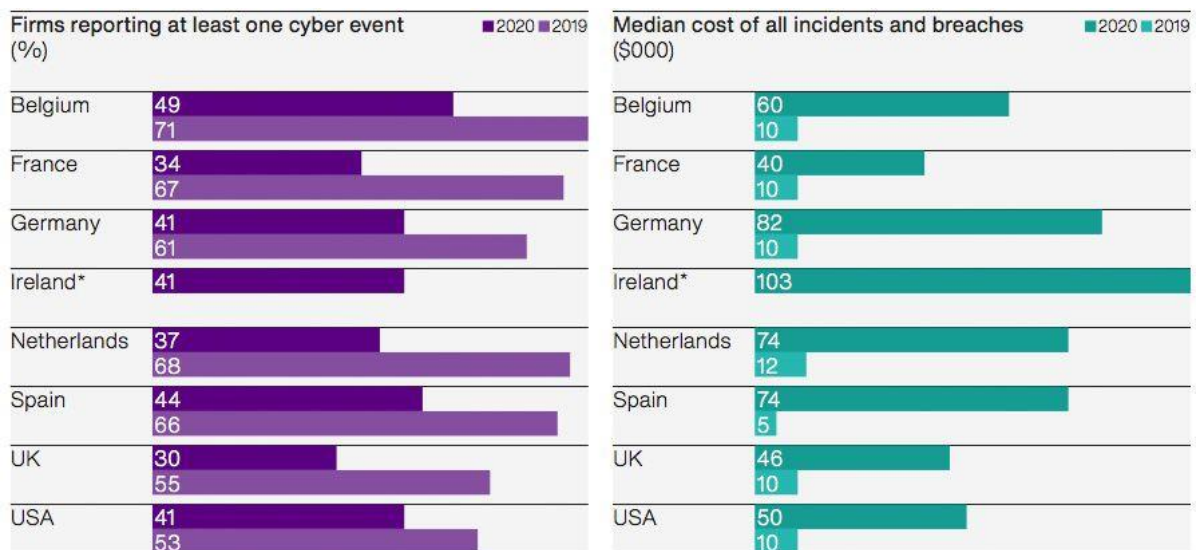


(Europol, 2019)

Reasons about this cybercrime to be chosen are:

- 1- Technological connectivity has been used in this cybercrime.
- 2- Covered under Europol cybercrimes types like the cyber dependent as computers used on it, and cyber-enabled crime facilitated by internet and electronic technologies.
- 3- It is international cybercrime as several countries like the UK, Spain, and Turkey have been used, and INTERPOL has been asked to help.
- 4- This cybercrime is a legal challenge as perpetrators were located in several countries, and they used Turkey as a non-European country with differences in the cybercrime law. Also, using different countries is a big challenge due to the differences in criminal procedures and data protection.
- 5- This cybercrime had personal information as the data of victims like bank accounts can harm them.
- 6- This cybercrime has happened in several countries, so there were operational challenges. As not always, the countries have correct laws and agreements to communicate and investigate each other.

The below charts can show us the difference for cybercrime events and costs between some European countries:



(Consultancy EY, 2020)

The description and explanation of the chosen cybercrime:

(UNODC, 2014) The four appellants (Bradley David Rogers, Colin Martin Samuels, Geraldine French, and Mark Julian Bell) were charged and convicted for their roles in two advance fee frauds. Both frauds were operated by Muldoon (not included in the appeal), who pled guilty to charges of conspiracy to defraud and was sentenced to 7 years and 5 months' imprisonment. Muldoon employed UK nationals at call centres in Spain or Turkey in either an advance fee fraud scheme that involved debt elimination or an advance fee fraud scheme that involved escort services.

This company promoted escort services and debt abstraction as well as ads in the local newspapers. People in the UK responded to these advertisements, and they have paid advance money to get the company services, and they have been allocated for a specific date to get the fake service. Once the customers paid the fees, they discovered that no other dates were made available; this is one kind of fraud scheme used by employees at call centres who cold-call people on a list of those purchased from data providers. The other type involves promising customers debt elimination services costing them money upfront but not delivering any service whatsoever after taking payment.

This cybercrime covered by three crime types:

- 1- Cybercrime: computer-related actions for people and financial gaining, including fraud-ing and electronic evidence.
- 2- Money laundering: transfer money between different countries to avoid government tracking them and translate part of the money to properties to get them back as clean money.
- 3- Participation as an organized criminal group.

The countries involved in this cybercrime are:

- United Kingdom.
- Turkey.
- Spain.

How UK dealt with cybercrime:

Apart from Rogers, the defendants were convicted of a conspiracy to defraud and received prison sentences. Following his extradition from Spain, Roger was also convicted for converting criminal property contrary to section 327(1)(c) Proceeds of Crime Act 2002 (POCA) and sentenced to two years and ten months imprisonment. (Allen & Overy LLP, 2015)

Rogers appealed his case to the Court of Appeal, but they ruled that England had jurisdiction to try Rogers and dismiss the appeal. Two bases for their decision were: 1- provisions under POCA. 2- In the case of modern principles, jurisdiction is derived from previous cases.

The appeal argues that he had been wrongfully accused because the Crown Court lacked jurisdiction over him since he lived in Spain and committed no part of this crime within Britain's borders.

Parliament created the converting and transferring criminal property, concealing, converting, disguising with section 327(1) POCA. Parliament typically presumes that it does not intend to punish conduct outside the UK when enacting a statute.

As soon as the money was obtained through any fraud and reached a UK bank account, it became criminal property. That continued when it transferred to Rogers' Spanish bank account.

The costs of this crime:

This cybercrime was a sophisticated fraud that operated professionally over time. The frauded money amount was more than five million and seven hundred thousand pounds, this money have been taken from the customers by those in charge. Some were vulnerable and easy to deceive.

Mr Muldoon was the principal beneficiary. He got about two millions pound in financial gains. Mr Bell has been received about fifty-seven thousand pounds.

Rogers was in charge of a significant amount of money. This money has been transferred to one account in Spain ,and he was the owner of it. The money received about £715,000.00 from small tranches to avoid anti-money laundering requirements. Roger gave Muldoon the privilege to access one account for him, and large sums of money were taken out of it.

French worker was working as an accountant reporting to Muldoon. The woman tried to keep the money transfers below the anti-money laundering levels. They have paid about £274,000 on her Capital One card. (BAILII, 2014)

Identify issues concerning crime investigation:

1- After examining the investigator from Crown's financial, they found that the money had been transferred from the UK banks to Spain bank accounts.

2- The emails between the French women and Allpay company.

Examination of public and social perception:

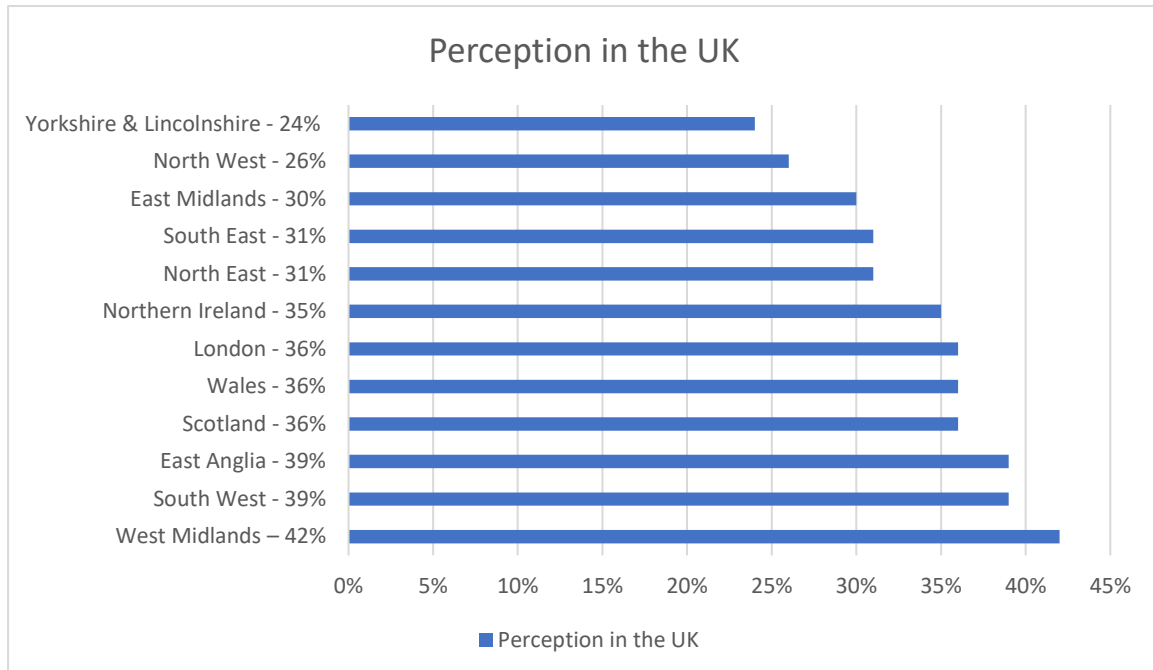
This cyber threat has caused a great deal of public tension, which motivated national and international bodies to make cybersecurity their top priority.

Despite public concern being fuelled by the increased number of cyberattacks, and the adverse financial and psychological impacts that come with it, there is a lack of research on policing economic cybercrime through expert police officers' perspectives.

The UK PM [Theresa May] was fond of saying that crime is falling, but, as people can see, crime has moved online, and until now, the official statistics have not shown that. Her complacent claims do not read well alongside these worrying increases in violent crime, sexual crime and homicide. (Theguardian, 2016)


To help the government plan for future budgeting and workforce development, they must form the ability requirement of law enforcement. Government officials also need access to the data about victims from organisations such as the bank accounts defrauded and the devices infection rates to make plans appropriately. Resource planning also requires an assessment of offender volumes over time, which will vary depending on circumstances like recidivism levels or other factors that could affect criminal behaviour.

Avast with the support from the University of Birmingham, has researched the cybercrime perception, and they have found that the level of perception in the UK is deficient:



(PR Newswire Europe Limited, 2021)

The feedback and comments from the people on the social websites show how people can deal with cybercrime. Year after year, people learn and distinguish between false and accurate information.

**RobHardy** 21 Jul 2016 10:26 2 ↑

I have, but never bothered to report it, just took it as a lesson in failed common sense, but I suppose thats what too many people do. I also apparently had my name and address used for the registration of a website for the sale of counterfeit goods. There is a lot of toughening up to be done in the way we regulate the setting up of businesses in this country.

Report

(The Guardian, 2016)



PzjnnAQXWmcDCZbX 21 Jul 2016 10:27

21 ↑

You can no longer laugh off online abuse.

If someone kept sending you text messages from different numbers, or calling your house phone from different numbers, sending you abusive letters by snail mail, would you accept it?

Being online and using social media are the norm for the majority, especially the young. Whether you think that is right or wrong is irrelevant, this is the reality in 2016.

No-one should have to accept online harassment or hate speech, no matter how much you sneer and dismiss it as "over-sensitive snowflakes", etc.

[Report](#)

(The Guardian, 2016)



laguerre

August 4, 2021

[Share](#) [Flag](#)

There's a difference between cyber attacks on businesses, and phishing scams on individuals, and the necessary actions are different. In a phishing scam, the solution is mental - learn not to fall for apparent tempting stories. In a cyber-attack on a poorly defended system, the solution is technological - finding the right help to make the system more robust. I didn't really get this distinction from the article.

[Reply](#)

3 👍 0 💬

(Independent UK, 2021)

Conclusion:

The low number of prosecutions for cybercrimes is not evidenced that they do not exist. Cybercrimes undoubtedly happen, but the way people look at them is wrong. Digital realism is the reality of what a cybercrime looks like online; it is paradoxically different from the mythology surrounding it, which predicts its unrealistic nature in other ways.

The truth is that cybercrime's science fiction roots and media distortion have caused the problem. Without reliable information, we can not understand it at all.

References:

- Saunders, J., 2017. Tackling cybercrime—the UK response. *Journal of cyber policy*, 2(1), pp.4-15.
<https://www.tandfonline.com/doi/abs/10.1080/23738871.2017.1293117>. [Accessed: 27 February 2022].
- Comparitech Limited (2022) UK cyber security and cyber crime statistics (2022). <https://www.comparitech.com/blog/information-security/uk-cyber-security-statistics/#:~:text=2021%20losses%20to%20fraud%20and,%C2%A32.4%20billion%20in%202021>. [Accessed 28 February 2022].
- Europol (2019) common challenges in combating cybercrime,
<https://www.europol.europa.eu/publications-events/publications/common-challenges-in-combating-cybercrime> [Accessed 04 March 2022].
- Consultancy EY (2020) Cost of cybercrime per incident jumps six-fold to €50,000. <https://www.consultancy.eu/news/4409/cost-of-cybercrime-per-incident-jumps-six-fold-to-50000>. [Accessed 04 March 2022].
- UNODC (2014) Sharing Electronic Resources and Laws on Crime, R v Rogers [2014 EWCA Crim 1680. https://sherloc.unodc.org/cld/case-law-doc/cybercrimetype/gbr/2014/r_v_rogers_2014_ewca_crim_1680.html. [Accessed 25 February 2022].
- Allen & Overy LLP (2015) Money laundering offences apply to conduct occurring entirely outside the UK. <https://www.allenoverly.com/en-gb/global/news-and-insights/publications/money-laundering-offences-apply-to-conduct-occurring-entirely-outside-the-uk>. [Accessed 01 March 2022].
- BAILII (2014) England and Wales Court of Appeal (Criminal Division) Decisions, Rogers & Ors, R v [2014] EWCA Crim 1680 (01 August 2014). <http://www.bailii.org/ew/cases/EWCA/Crim/2014/1680.html>. [Accessed 26 February 2022].
- PR Newswire Europe Limited (2021) Which UK region has been hit the hardest by cybercrime?, URL: <https://www.prnewswire.co.uk/news-releases/which-uk-region-has-been-hit-the-hardest-by-cybercrime--886680933.html>
- The Guardian (2016), Crime, Cybercrime figures prompt police call for awareness campaign. <https://www.theguardian.com/uk-news/2016/jul/21/crime-rate-online-offences-cybercrime-ons-figures#comments>. [Accessed 01 March 2022]
- Independent UK (2021) Cybercrime can be incredibly traumatic so why don't victims get more help?, <https://www.independent.co.uk/voices/cybercrime-attacks-psychological-trauma-b1895775.html#comments-area>. [Accessed 01 March 2022].
- PR Newswire Europe Limited (2021) Which UK region has been hit the hardest by cybercrime?, <https://www.prnewswire.co.uk/news-releases/which-uk-region-has-been-hit-the-hardest-by-cybercrime--886680933.html>. [Accessed 02 March 2022]