Faculty of Science and Technology

A multi-method approach of comparing the role advancing technology has played on both the evolution of cybercrime, and the policing strategies used to combat it.

A dissertation submitted as part of the requirement for the

BSc Forensic Science

Kelsie India Makepeace

4546055

15th June 2017

Abstract

Cybercrime has gained rapid attention in the UK in recent years, with the proliferation of technology use, particularly the internet, allowing for the evolution of cybercrime to occur alongside advancing technology. With increased ways to commit both computer-enabled and computer-dependant crimes being created, the rates if illicit cyber activity has increased to the extent of certain attacks gaining media attention worldwide. This paper will explore existing literature, as well as conducting archival research and survey research to explore in details the ways in which technological developments have altered aspects of cybercrimes and government and police strategies that are in place to combat it. This dissertation was designed to understand how these relevancies can be analysed to decipher if the strategies in place are effective in all aspects of the aim.

Acknowledgements

I would like to express my appreciation to all of the academic staff at Bournemouth University who assisted me through this project. In particular, I would like to thank Paul Kneller, my project supervisor whom has been a constant source of support and enthusiasm not just during the course of my dissertation writing but rather the whole four years of my degree. I would also like to give my thanks to both Michael Jones and Christopher Richardson, for providing me with both knowledge and guidance within the realms of computer science that I had yet to encounter, despite either not being my assigned supervisor.

I would also like to thank each and every member of my family and friendship circle for the constant motivation and encouragement that they have provided me with during this process. In particular I would like to thank my mum, for always teaching me to ‘walk like a man’.

Contents

Chapter 1 Introduction

1.1 Defining cybercrime

Synder (2001) states that any definition of cybercrime ought to begin with the internet, simply because the latter is the necessary platform for the former to exist. Moreover, it can be further explained that the internet should be viewed as a set of social practices because it takes the form that it does depending on the ways and purposes for which people use it; This is how the internet provides the crucial electronically generated environment in which cybercrime takes place. For example, Millhorn (2007) notes that if the internet could not be used for online shopping, then there would be no opportunities for credit card crimes such as those that can be seen in *R v Raphael Gray (2001),* which involved the hacker known as 'Curador' (Goodman & Brenner, 2002). In addition, it is only because of the fact that the internet is used as a communication tool that the 'Love Bug' worm, released by Onel de Guzman in 2000, was able to spread using email systems as a method (Bell, 2002).

In essence, Castell's (2002) describes the internet as a network of networks that links computers together, which allows for information to be exchanged between all nodes (e.g individual computers) within it. The origin of this network can be traced back to the Advanced Research Projects Agency Network (ARPANET), a system used by the US military in the 1960's. Further networks, such as the UK's Joint Academic Network (JANET), and the US's National Science Foundation Network (NFSNET), were established and could all be connected together to form the network of networks mentioned earlier. In 1990, the US released the ARPANET to civilian control which was the main impetus for the creation of the internet as we know it today (Majid, 2013). In the same year, a software called the World Wide Web (www) was developed, and Internet Service Providers (ISPs) worked together with browsers that were created (such as Microsoft's Internet Explorer in 1994) which allowed for the internet to be accessed via personal computers. Subsequently, the use of the internet in society has grown rapidly since it's commercialisation in the mid-1990s.

Year	Internet Users	Percentage of Population
1995	44,866,595	0.69%
1996	77,585,866	1.28%
1997	120,922,212	1.97%
1998	188,507,628	3.08%
1999	281,537,652	4.60%
2000	414,794,957	6.80%
2001	502,292,245	8.10%
2002	665,065,014	10.60%
2003	781,435,983	12.30%
2004	913,327,771	14.20%
2005	1,030,101,289	15.80%
2006	1,162,916,818	17.60%
2007	1,373,226,988	20.60%
2008	1,575,067,520	23.30%
2009	1,766,403,814	25.80%
2010	2,023,202,974	29.20%
2011	2,231,957,359	31.80%
2012	2,494,736,248	35.10%
2013	2,728,428,107	38.00%
2014	2,956,385,569	40.70%
2015	3,185,996,155	43.40%
2016	3,424,971,237	46.10%

Table 1: Worldwide internet use statistics from 1995-2016 (as of July 1st), with integrated bar chart. Data source: (InternetLiveStats, 2016).

1.2 Aims and Objectives

This dissertation possesses three objectives, which via all three being completed aim to enable to driving aim of this study to be accomplished. The first objective of the study is to evaluate how advancing technology has affected cybercrimes in all aspects, including the types of illicit activities cyber criminals are performing, how they are conducting these crimes and the success rates of attacks. Objective two of the study is to consider how UK police forces and other national law enforcement agencies have adapted their methods and approaches to combatting cybercrimes, with particular reference being assigned to police

structure and cyber unit budgets. In addition, the final objective of this study is evaluate the general amount of cyber security and crime knowledge in society, taking public perceptions into consideration alongside this. With these objectives being met, the main aim of the project will be to use all information provided by the objectives to ascertain whether the combined efforts the UK strategy is making towards combatting cybercrimes are keeping pace with the demand of the problem.

Chapter 2 Methodology

Cresswell (2014) states that research can be defined as a way of approaching the collection, interpretation and analysis of data, with a methodical process being used to enquire about or to increase knowledge of the chosen subject (Collis & Hussey, 2009). Two different types of data can be acquired from research; primary data is collected from an original source, whereas secondary is the interpretation of sources that already exist (Dantzker, et al., 2016).

The term ‘methodical process’ is used to describe the particular way in which the research is conducted, with Trochim (2002) emphasising the importance of the application of the most applicable method in the success off the project. The three traditional methods of research are quantitative (numerical data), qualitative (textural) or the mixed methods approach (a combination of the two) (Williams, 2007).

This chapter will detail both the process for which the research strategy was determined, as well as the specific methods used for data collection and analysis in order to most appropriately meet the aims and objectives outlined.

2.1 The research onion

Saunders et al. (2007) developed the research onion technique for formulating an effective strategy, which illustrates the stages that should be covered during this process. The basis of the technique is defined by the layer feature of an onion (see figure 1), with each additional layer being a more detailed stage of the research. First of all, the research philosophy must be determined, which leads to the appropriate research approach being

adopted. The research strategy is then considered, with the time horizon being identified in the next step. The final step represents the process of the actual data collection.

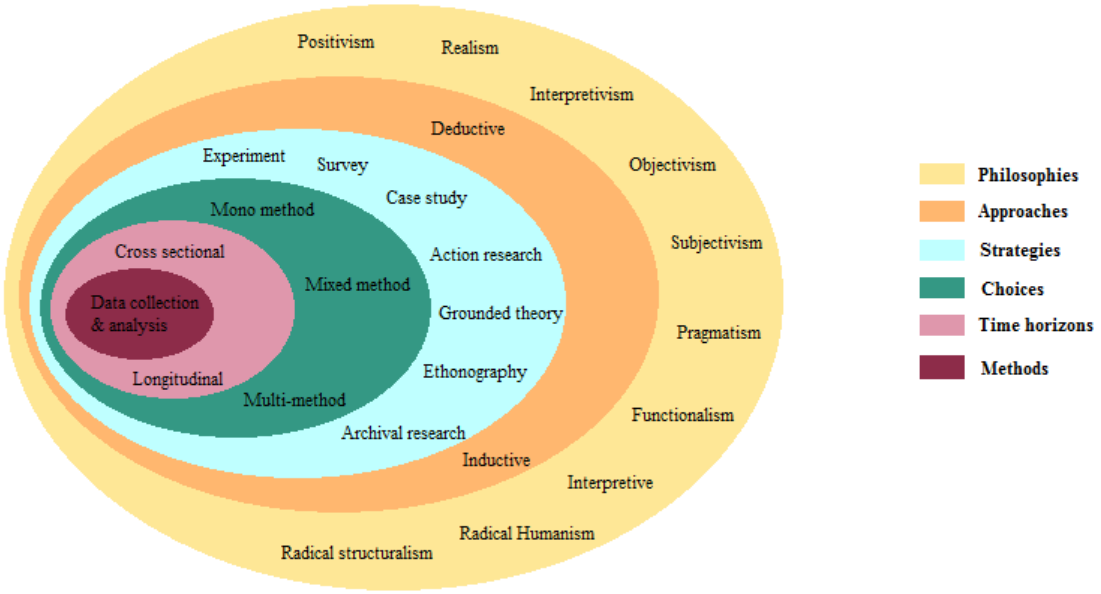


Figure 1: The research onion (Scott, 2015).

2.1.1 Research Philosophy

The first stage of defining the research philosophy for a project provides the justification for how and why the research will be undertaken (Flick, 2011), by outlining the knowledge of the subject being investigated (Bryman, 2012). Therefore, philosophies differ depending on the goals of the research, and how best these goals can be accomplished (May, 2011). Subsequently, to determine the accurate philosophy for this study, the aim and objectives were considered, and the philosophy of acknowledging and developing existing knowledge, called epistemology, was deemed the most appropriate. Furthermore, particular attention was drawn to objective 3, as the this objective required information to be gathered on both the knowledge and perceptions that UK citizens possess towards cybercrime relations, and therefore a possible method of data collection could be through primary data in the form of a survey. Holden and Lynch (2014) state that positivism is the side of epistemology that is most associated with using quantitative methods involving surveys, questionnaires and simulations, thus a positivism philosophy was undertaken.

2.1.2 Approach

There are two main approaches, either inductive or deductive, that can influence a research strategy (Essays, 2013). Silverman (2013) denotes that the latter approach develops a hypothesis upon existing knowledge, and then uses a primary research technique to question this knowledge. Therefore, the deductive approach is most suitable for situations where a study aims to test whether the observed phenomena fits the expectations outlined in already existing research (Wiles, 2011). Moreover, in order to assess whether or not the relevant research that explores the objectives of this study already exists, an initial desk based study in the form of a literature review (see chapter 2), was conducted in accordance with the subjects.

The first step was the collate all of the literature, in the form of books, book sections, journal articles and reports regarding cybercrime in terms of its growth, public perception and policing methods, and their views on these topic areas. The literature was obtained using Google Scholar, Bournemouth University Library Catalogue (both on-campus and e-resources) and Research Gate (including full text requests). The relevant literature was scoped by using suitable key words and phrases to gather as many desirable results as possible; a breakdown of the search terms used can be found in appendix 4.

With the literature review resulting in a suitable amount of secondary research, the literature was interpreted to determine the views of the topics already available, in order for the primary research of this study to allow for comparison. By doing this, the deductive approach allowed for a general knowledge base that is already established to be tested against the primary research gained from this study (Kothari, 2004).

2.1.3 Strategy

Saunders et al. (2007) states that the research strategy is the factor that concerns how the researcher will carry out the study. For example, this could be via a survey/questionnaire, a literature review, an experiment, or an action/case study, depending on what is the most applicable. With the literature review already outlined in chapter 3.1.2 to meet objective 1, objectives 2 and 3 were considered in terms of their suitability to a method.

In order to meet objective 2, it was necessary to gather existing relevant materials on how the UK police forces have adapted aspects of their policing strategies to effectively combat the growing rates of cybercrime. Therefore, an archival research strategy was conducted from existing materials via making a Freedom of Information request to each of the 43 police forces in the UK, under the guidelines set out in Freedom of Information Act 2000. The requests were sent out using the website What Do They Know (www.whatdotheknow.com) (2008), specifically asking them to disclose the yearly budget that has been allocated to their cybercrime unit (if the force in question possesses one) from 2006 – present, using Oppenheim's (2000) theory that simple questions yield more responses in mind. A complete copy of the request text can be found in appendix 6.

Secondly objective 3, as previously mentioned, required survey based quantitative research to gain illustrative and objective knowledge, in regards to two types of UK citizens; those who do not work within a cybercrime capacity, and those who do. Thus, two self-completing and internet based surveys were designed, using SurveyMonkey (www.surveymonkey.com) as a platform.

2.1.4 Choices

The next stage in the research onion is to establish whether the study is a mono method (one research approach), a mixed method (uses both quantitative and qualitative data for a single dataset), or a multi-method (combined methods creating multiple datasets) (Feilzer, 2010). This study comprises of a literature review, an archival research strategy and two survey research strategies, each producing a specific dataset to be combined for analysis. Thus, this study denotes a mutli-method choice.

2.1.5 Time horizons

The time horizon for a project is subjective to the intended completion date for the study (Saunders, et al., 2007), which can be either cross sectional or longitudinal (Bryman, 2012). Longitudinal is concerned with data collection that is repeated over a certain amount of time, most often used to examine change (Goddard & Melville, 2004). In

comparison, cross sectional is used when a time has already been established, due to the study of a specific phenomenon at a certain time. Therefore, due to this study aiming to analyse current aspects of cybercrime, the time horizon is cross sectional.

2.1.6 Data collection and analysis

Data collection for the Freedom of Information requests was conducted via a manual interpretation of the individual responses received. The relevant budget numerical amounts in the textual responses were sourced, collected and collated into one data table using the Microsoft Excel programme.

Moreover, both of the survey responses were exported from the SurveyMonkey site into an Excel document using the numerical data conversion tool. Following this, the data was exported into the IBM SPSS Statistics 23.0, in order for appropriate statistical analysis to be performed (Field, 2013).

2.2 Survey design

Surveys allow for the participants to report their knowledge, opinions or attitudes to a topic, resulting in relevant data being gathered for the study (Teddlie & Tashakkori, 2009). Identical questions in a predetermined order are presented to each participant to ensure reliable results. In order to increase the validity of the survey, the questions should not share any bias or personal opinions of the researcher and thus the questions should be worded in an unambiguous way without any leading questions used.

The first survey conducted, titled ‘Cybercrime: A Survey of Public Knowledge and Perceptions’, had the objective of indicating current public knowledge and perceptions on subjects that surround cybercrime. The survey consisted of close-ended multiple choice questions that used a scale system of ‘strongly disagree’ (1) to ‘strongly agree’ (5). The sampling method used was the non-probability convenience technique, whereby the target population was anyone, over the age of 16, who had access to the internet. Because of this factor, social media was used as a marketing tool, which achieved 142 responses over the

course of 4 days. The number of respondents exceeded the initial target of 100, ensuring a substantial amount of data was obtained for an effective, well-founded conclusion to be drawn. Furthermore, Gideon (2012) denotes that adding an incentive for people to complete surveys increases response rate, thus for every survey completed I donated 10p to Meningitis Now (appendix 7 shows receipt of final donation made).

Furthermore, the second survey titled 'Cybercrime: A Survey on Expert Opinion', was structurally similar to the previous with the same close-ended question traits and scale system, however the objective differed in the sense that it aimed to extract opinions on relevant matters from specifically chosen people who work within cybercrime matters in some capacity. Subsequently, the non-probability purposive sampling method was used whereby 8 participants where handpicked depending on their occupation. A range of relevant occupations in the relevant field was deemed desirable, and therefore staff members from the following organisations were selected:

- Daniel Masters – Officer at National Crime Agency
- Christopher Richardson – Head of Cyber Security Unit Bournemouth University
- Michael Jones – Digital Forensics at Bournemouth University
- Isabel McQueen – Fraud Analyst at JP Morgan
- Peter O'Doherty – Detective Superintendent at City of London Police
- Tracy Alexander – Head of Forensic Services at City of London Police
- Dominic Plummer – Security Analyst at Royal Bank of Scotland
- Benjamin Twomey - Policy Officer for the West Midlands Crime Commissioner

Chapter 3 Literature Review

In order to meet the aims and objectives of this study, this literature review intends to expand on key areas of importance to provide valuable research in the field of forensic computing. Three different areas will be focused on, with an in depth comparison made of the different views of authors concerned with the topic. The first key discussion topic will delve into how the ever advancing technology that is used in society has been leveraged by cyber criminals, allowing them to commit both dependant and enabled computer crimes. Secondly, the focus will move onto how both policing and investigative bodies within the

UK have changed their strategies and methods of combat in order to meet the demands of the increase in these types of crimes. Thirdly, literature will be studied to question as to whether the typical amount of cyber security knowledge the average UK citizen possesses suffices in terms of their protection against potential attacks, as well whether or not a typical member of a policing authority understands aspects of cyber enough to effectively police it. The first area is being explored with the aim of understanding how aspects of cybercrimes have changed in accordance with what is considered the 'digital era' (Spiller, 2002), considering particularly the way in which it has affected methods of attack and public perceptions of cybercrimes. Furthermore, strategies of combat will be discussed in regards to economic factor's and penalties of crimes; particular attention will be assigned to the 'defend, deter, develop' strategy outlined in National Cyber Security Strategy 2016 (Gummer, 2016). Finally, there is a need for an understanding of the level of knowledge a person who is in no way professionally involved in computer science typically possesses, and whether or not this correlates to a higher risk of being victim to a cybercrime. To conclude the literature review, any of what can be referred to as 'gaps in the literature' will be highlighted in order to define the necessity of this research project and justify the aims and objectives in place.

3.1 Modern day cybercrime

Since the mid 1990's, the internet has become an integrated part of everyday life for many people worldwide; those living in the western industrialised world are particularly prone to internet usage. Castell (2002) argues that what seems to be a constantly evolving digital era is transforming the spheres of leisure, work, consumption, business and politics within society. Similarly, Webster (2003) states that we are now in the midst of an industrial revolution, one that is changing the way in which our society works in a manner known as the 'information age'. However, though the wide use of the internet creates new opportunities, these opportunities are tempered by fears that the internet can also jeopardise the security of the activities that rely on it, but Britz (2004) argues that our understanding of this lack of security can be simultaneously both informed and obscured during both political and media discussions. Gibson (1984) first coined the term 'cyberspace' as the realm of computerised interactions, which offers new opportunities to all members of society who have access to it, including those with criminal or deviant

motives. Furthermore, Majid (2013) summarises these statements by denoting that the development of the internet, and other related communication technologies, seems to cause an array to both individual and collective safety, economic prosperity, political liberty and social order.

3.1.1 Online environments

Grabrosky (2001) suggests that, as mentioned earlier, it is the social practices that members of society engage in in online environments that create distinctive opportunities for cybercrime offending; this is known as 'opportunity structures' (Newman & Clark, 2003). As well as for social uses, the internet is increasingly being used by businesses as a means to completing their activities that can involve research and development, production, distribution, marketing and sales; thus creating a wide range of criminal opportunities in not just social but business sectors also (Jackson, 2000).

Furthermore, Turkle (1995) depicts that another aspect of cyberspace that enables illicit activity is the ability to manipulate and reinvent ones identity, giving individuals a method to adopt a virtual persona to interact with individuals who may not have chosen to interact with them if they were aware of their real life identities. In early stages of commercial internet use, this was often seen in cases of cyber grooming, normally via the use of internet chat rooms. However, the means to commit these cybercrimes can be more diversely approached in modern society by the use of popular social media sites such as Facebook, Twitter, Snapchat and Instagram, as well as common mobile phone/tablet applications such as Tinder and Grindr; this is often referred to as 'catfishing' (Smith, et al., 2017).

Similarly, Shields (1996) states a further aspect of cybercrime exists in the global nature of the internet making it a de-territorial phenomenon, thus offences can cross national boundaries. Therefore, this renders individuals vulnerable to potential cyber criminals who can reach their victims instantaneously, with the usual barrier of physical distance not being present. Though agencies such as the International Police Organization (INTERPOL), created in 1923, attempt to strengthen the methods of transnational policing, Bowling and Foster (2002) argue that this generally only applies to cases of suspected organised crimes of a larger scale.

Majid (2013) concludes from the above that it is the social-interactional features of the cyberspace environment that makes illicit activity accessible, with it being primarily the non-existence of space – time barriers, multiple device connectivity and the anonymity of online identities that allow for deviant activities to readily occur. These difficulties are exacerbated by the reality that cybercrimes all share the common feature of the cyberspace in which they take place, but can be a wide range of illegal activities within this area.

3.1.2 Evolution of cybercrime

Shinder and Cross (2008) inform that it was scientifically inclined students who first came enamoured with computers, with the first group of computer hackers being students at the Massachusetts Institute of Technology (MIT) in 1961, who went by the name of Tech Model Railroad Club. Mitnick and Simon (2011) highlight the importance of the creation of email and File Transfer Protocol (FTP) in the increase of cybercrimes, with Orman (2003) supporting this by stating that one of the first worms (a self-replicating programme) called the Morris worm, which was spread via email, was instrumental in the public perception of the security of computers. Further advancements in technology have allowed for criminal activity, such as Zimmerman's (1995) Pretty Good Privacy (PGP) encryption programme allowing for cybercrime evidence to be hidden online, as well as the first cyber bank creation called First Virtual in 1994, resulting in a vast amount of new opportunities for cyber criminals such as the buying and selling of illegal substances (Crede, 1995).

It has been a common understanding that the existence of technology presents threats to its users since before the birth of the digital era; Snow (1971) made the following comment –

"Technology is a queer thing. It brings you great gifts with one hand, and stabs you in the back with the other".

This quote allows for the understanding that technology has always shown signs of its potential to be exploited for criminal purposes. However, Clough (2015) argues that modern day cybercrimes differ from earlier cases in the sense that they most often illustrate features such as being organised, transnational, technologically sophisticated and financially motivated; an example of which can be seen in *United States of America v. Viktor Pleshchuk, Sergei Tsurikov, Hacker 3, Oleg Covelin, Igor Grudijev, Ronald Tsoi,*

Evelin Tsoi, and Mihhail Jevgenov, (2009), where the defendants successfully hacked into a computer network of RBS Worldpay, resulting in a loss of approximately $9.4million (Smith, 2015). Furthermore, a crime such as this is made possible by the current ubiquity of digital technology in modern society. Clough (2015) states that there is a maxim that all crimes, cyber or traditional, follow opportunity, and evidence of this can be seen by the fact that almost all technological advances have been accompanied by a corresponding niche that results in its exploitation for illicit activities. For example, the development of digital cameras allowed for the digital sharing of photographs, a platform for which child pornographers can use to commit such crimes. In addition, online fraud would not be possible without the processes of electronic banking and online shopping. The use of social networking sites and other electronic communication techniques ensures the possibility of cyberstalking, grooming, bullying and harassing. And finally, the quick and simple method with which digital media can be shared to various devices has caused a huge increase in copyright infringement.

Before the creation of the modern day internet cybercrimes, there were reports as early as the 1960's of computer related crimes such as computer manipulation, sabotage, espionage and illegal use of systems (Sieber, 1998). However, as technology started to continuously evolve new generations of cybercrimes were identified, with three main categories being outlined by Wall (2007). Wall states that the first emergence of cybercrimes were those of a traditional crime nature, but which were facilitated through the use of cyberspace; an example of this is cyber fraud. Secondly, the development of crimes across different networks became a type of cybercrime with the growth of offences such as hacking increasing in rates. Finally, the creation of a crime that wholly depends on the technology being used, such as botnets, was established. Additionally, Smith (2010) denotes that the motivations of the offenders has evolved, changing from curiosity and skill showing motives to those of a more organised and financially motivated nature.

Increased connectivity of computer networks not only magnifies current deviant activity concerns, but also gives rise to new problems. For example, Morris (2004) suggests that the increase of broadband use means that more users are leaving devices constantly connected to the internet, thus increasing their chances of external attack as it allows for more time for hackers to guess passwords or discover what Transmission Control Protocol/User Datagram Protocol ports may be open. Moreover, the development of increased connectivity speeds may be desirable to the user for improved internet

performance, but it also results in the ability for a hacker to access files quickly. Morris also denotes that peer-to-peer technology has allowed for more varied types of malware and Denial of Service (DoS) attacks. Also, the International Telecommunication Union (2005) suggests that the convergence of telecommunications has changed mobile phones into essentially mini networked computers, with the increase of 'Internet of Things' (IoT) items allowing for more devices to be potentially subject to a cybercrime.

Cohen and Felson (1979) state that the three factors that are considered necessary for the process of a predatory crime according to the 'routine active theory' (motivated offenders, suitable opportunities and absence of capable guardians), can all been seen when translated to an online environment. The Office for National Statistics (ONS) (2016) report states that 99% of households with children in the UK are connected to the internet, compared to 95% in 2012, which gives evidence to the second factor of opportunity. This increase in internet use means that more vulnerable children can be subject to cybercrimes.

Urbas and Choo (2008) note that both technological change and social interaction are the cause of the evolution of digital crime, with the Bipartisan Policy Center (2014) report suggesting that for these reasons the internet's vulnerabilities are overtaking the global ability to be secure.

Shinder and Cross (2008) imply that as the convenience and performance of technological devices improves, the security of the software is often compromised. Casey (2011) stated that cybercriminals have been able to exploit technologies used in modern day such as wireless networks, mobile computing and remote access, Java, Hypertext Markup Language (HTML), instant messaging and e-commerce systems. Contrastingly, Gast (2005) argues that 802.11 wireless networks do provide authentication and encryption security measures, but these can possess flaws that still allow for programmes to break them. For example, mobile phones often use Wi-Fi Protected Access (WPA) or Wireless Equivalent Privacy (WEP) to secure their data, however programmes such as Aircrack-ng can recover both WEP and WPA keys by capturing pockets of data.

3.1.3 Media coverage

Studies show that media coverage of computer related crime has increased in correlation with computer crime rates, and both direct and non-direct effects can be seen as a result of this. For example, Dowland et al. (1999) surveyed UK newspapers over a 30 month period and found that, on average, stories surrounding computer crimes featured around twice a week. Contrastingly, Jewkes (2015) stated that in today's society, with the numerous ways that news articles can be read (for example, newspapers, internet sites, the radio, and mobile phone applications), it is common to come across a story relating to cybercrime every day, with Wykes and Harcus (2013) suggesting that the media has been instrumental in heightening public fears of cybercrime because of this. Similarly, popular fiction films have also caused public awareness of the possible threats that cyber usage entails (Webber & Vass, 2010), with Yar (2014) denoting that such media is increasingly portraying a 'cyber-dystophian' outlook, thus the social effects of emerging technologies being characterised negatively. Goode and Ben-Yehuda (1994), state that this direct effect can be seen throughout history when not only technological change, but also social and economic changes, are accompanied by higher cultural anxieties when concerning familiar daily activities. Moreover, Thomas and Loader (2000) suggest that this is due to internet technologies causing social transformations that make the future appear 'less secure' and 'unpredictable', and Critcher (2003) states that subsequently the media fuels a view that these new technologies present a threat to society.

3.2 UK policing strategies

3.2.1 Organisational structure

Broadhurst (2006) highlights the necessity that continued attention is paid nationally, internationally and regionally to the risks associated with digital and information technologies, as well as stating that a fully global response to such issues is yet to be established and that efforts to secure cyberspace have so far been reactive as opposed to proactive. In addition, Broadhurst also suggests that effective cybercrime policing requires

complete cooperation between polices forces, relevant government agencies and private institutions.

Since the increased rates of cybercrimes being committed in society, two new treaty instruments were established on an international level in attempt tackle the issue. Hopkins (2003) describes the first of these instruments, the Council of Europe's Cybercrime Convention, as having global significance and an essential for cross border law enforcement. Secondly, the United Nations Convention against transnational organised crime (2005) incorporates illegal cyber activity that is global in scope. To argue the necessity of international cooperation such as this, Csonka (2005) outlines "that the fight against cybercrime is either a global one or it makes no sense".

In the UK specifically, the National Cyber Crime Unit (NCCU) (2017), which is part of the National Crime Agency, leads the UK's policing against cybercrime. The NCCU works closely with the Regional Organised Crime Units (ROCUs), the MPCCU (Metropolitan Police Cyber Crime Unit), and partners within industry, government and international law enforcement. Within the common law tradition, O'Connor (2012) argues that local police forces work with the investigative agencies named above for smaller scale cybercrimes.

3.2.2 Changes in legislation

Although Mcknight (1973) notes the first legal punishments for computer crime occurred in 1970, Goodman and Brenner (2002) argue that the limited daily role of computers in society meant that these crimes generally fit into categories such as theft of telecommunication services. They further state that it was the proliferation of networking of computers and the increase of personal use that created the necessity for specific computer and cybercrime laws.

Graceful (2016) highlights the major legislation changes that have thus occurred due to technological advances, stating that the most relevant act is the Computer and Misuse Act 1990, which brings in the following three offences:

1) Unauthorised access to computer material.

2) Unauthorised access with intent to commit or facilitate commission of further offences.

3) Unauthorised modification of computer material.

Furthermore, this act has been amended by the Police and Justice Act 2006, as well as the Serious Crime Act 2015, which illustrates the necessity for the law to be amended as the related technology advances. For example, section 3ZA of the Computer Misuse Act 1990 incorporates serious damage as a separate offence, in order to effectively assign appropriate legal sanctions for the more common modern day serious and organised cybercrimes. Similarly, the creation of Denial-of-Service attacks resulted in the Police and Justice Act 2006 amending the Computer Misuse Act to include "Unauthorised acts with intent to impair operations of a computer". In addition, section 43 of the act was amended to ensure that a crime is still committed if a United Kingdom (UK) national commits an offence whilst outside of the UK so long as the offence is illegal in that country too. This change was made due to the increasing transnational crimes being committed through cyberspace. These changes clearly show how advancing technology has influenced current legislation.

Furthermore, Edwards et al. (2010) highlights the difference sentences that each of these offences carries; offences that come under section 1 and 3A carry a potential sentence of up to two years imprisonment, whereas section 2 and section 3 carry a possible five years and ten years respectively. Moreover, the recent addition of section 3ZA holds the longest possible imprisonment sentence of life.

Another essential point that is made by Bryant (2014) is in reference to what is known as cyber terrorism, with section (1)(2)(e) denoting that a disruption of a computer/electronic system, which action would fit into the legal guidance of the term 'terrorism', can be prosecuted as a cyber terrorism offence under UK Terrorism Act 2000. Gable (2010) states that attacks on computer networks such as these are often done for causes that concern political, religious or ideological factors, and often target networks concerned with essential services such as hospitals, air control, water supplies and financial systems. For example, Industrial Control Systems (ICS) are used to monitor critical infrastructures of such networks (Clapper, 2013). Wilson (2005) expands on this by noting that as technology is used more and more for systems such as these, the number of cyberattacks

targeting them is increasing. As Wilson (2014) denotes, an example of an attack such as this can be seen in the 'Stuxnet' worm, which specifically targeted control equipment at an Iranian uranium storage facility.

3.2.3 Challenges within policing

Technological developments result in serious challenges for the law and the criminal justice system, often due to the adaptation needed from crimes that take place in the terrestrial world to crimes which scenes are of a virtual nature. Clough (2012) states it is factors that illicit activities over the internet allow for, such as anonymity, deception and disguise, that result in difficult questions being posed to criminologists when concerning cybercrime. Furthermore, a United Nations (2013) report suggests that where tradition crime is most often regarded as having a territorial jurisdiction, cybercrimes challenge that paradigm because communication can be achieved over the internet as easily to an overseas recipient to someone that lives on your street. Therefore, a world, quite literally, of opportunities has been created for offenders; this presents new challenges to law enforcement and to the harmonisation of society. This means that offenders can target many victims at any one time, with King et al. (2009) expressing that unsolicited emails (spam) are the most common version of this cybercrime with email addresses being harvested from public websites.

Bocij and Mcfarlane (2004) argue that one of the more challenging aspects of cybercrime is the faceless nature of the internet. Not only can true identity be hidden online, technological resources have been development to hide location information as well as this. For example, proxy servers act as an intermediary between a computer and the servers it is connected to through the internet, allowing for users to route a command through a proxy server rather than their individual computer. Similarly, software such as the Tor browser, an anonymizing network based on the onion routing concept, can be used to protect the Internet Protocol (IP) address of an individual node in a network; Chaabane et al. (2010) argues that this enables anonymous access of both the Deep and Dark webs for internet users, a platform of which cybercrime is highly associated.

Additionally, another policing factor that poses a challenge is when a nation exists with no relevant laws on a cybercrime that is committed, it can serve as a safe haven for offenders as they can operate with a lower risk of legal sanction (Brenner, 2008). Holt et al. (2015) link this challenge with the previously mentioned ILOVEYOU virus spread by Onel de Guzman in 2000. Because at the time no laws were in place against writing malware in the Philippines, prosecution could not occur.

Moreover, the evolution of cybercrime had a corresponding element of a new type of evidence that could be used in a court of law, digital forensics. Wiles and Reyes (2007) state that the volatile nature of electronic data which is the main source of digital forensics requires specific forensic techniques to effectively retrieve, preserve and keep valid. Seizure of digital forensic evidence can include hardware, software, peripheral storage devices, and information in binary and printed form (Brown, 2015), which Clancy (2011) argues that this makes in incumbentfor investigators to be sufficiently aware of the appropriateness of acquiring data *in situ.*

To summarise, Brown (2015) highlights the primary challenges and barriers presented by cybercrime for the administration of criminal justice, which can be seen in the table below:

Category	**Description**
Identification	- Attributing ownership to electronically stored information - Identifying the individuals in control of electronic devices - Expediently locating information amongst large data sets - Tracing criminal activity when data anonymization has been used
Access	- Acquiring data when strong encryption, open source privacy tools, and anti-forensics technologies are used on devices - Obtaining authorisation for online inspection and collection of data, particularly when the target host is a cloud service provider with a base of operations outside the jurisdiction of local authorities
Wellbeing	- Exposure to obscene material may create mental health issues for staff involved in investigation

	- Staff welfare may be overlooked when non-technical managers are appointed to higher positions without experience overseeing cybercrime inquiries
Liability	- Unintended damage to information systems or devices may expose law enforcement agencies to civil litigation - Disclosure of private, confidential, or legally privileged information may lead to criminal or civil legal proceedings
Retrieval and retention	- Ephemeral sources of digital information which is not collected from live systems during warrant activity may weaken a case in the eyes of the court, or lead to miscarriages of justice
Admissibility and fairness	- Chain-of-custody documentation which is incomplete or inaccurate may result in digital forensic evidence being deemed inadmissible - If law enforcement are unable to attest to the reliability or authenticity of the evidence it may thwart the efforts of legal counsel to introduce that material as evidence in court
Human Capital	- Analysts who are not qualified to operate technical equipment or extract data from information systems may contaminate evidence - Agencies without sufficient expertise will undermine the ability of prosecutors to introduce expert evidence that explains the technical underpinnings and relevance of material before the court
Technical resources and funding	- Police who are not equipped with specialised tools for extracting information, or furnished with sufficient computational power to expediently process data, may miss critical evidence during analysis in the laboratory or while performing triage in the field
Training	- Police officers, prosecutors, and members of the judiciary that are not provided with ongoing training which is focused on modes of criminal offending, diplomatic channels of cooperation, foreign mechanisms of justice, sovereignty issues, emerging sources of electronic information, and

	communication technologies more generally, will be manifestly ill-equipped to manage cybercrime cases
Underreporting and uncertainty	- Public misconceptions about the capacity of police to target cybercrime offending contributes to the problem of underreporting - Gaps in legislation, and administrative delays owing to judicial uncertainty about the nature of cybercrime offending, may prevent investigators from obtaining requisite legal authority to intercept electronic data
Cooperation	- Private sector entities that are slow in responding to requests for assistance or from police, or are generally dismissive of collaborative initiatives with law enforcement agencies, create barriers to cybercrime investigations, prosecutions, and digital forensics interrogations - Strict and formal international mechanisms of cooperation may impede the agility of police investigations which target cybercrime offending originating outside national borders
Legal frameworks and due process	- Legislative provisions which are not harmonised among members of the international community may create safe jurisdictions for cybercrime offending, and possible conflicts of law

Table 1: An overview of the challenges that the policing of cybercrimes can be subject to (Brown, 2015).

3.2.4 National Cyber Security Strategy 2016-2021

The latest National Cyber Security Strategy (NCSS) (2016) is set out to invest a total of £1.9billion over the five year period with the aim of making the UK 'capable and resilient' in the ever advancing digital era, and states that in order to achieve this cyber skills need to reach into every profession. The quote from the report reads 'previous approaches have not achieved the scale and pace of change required to stay ahead of the fast moving threat', denoting that the strategy has been created in regards to offenders leveraging technology at a faster pace than those attempting to combat the offences.

The first aim set out in the NCSS is to defend the country against cybercrimes in terms of the protection of networks and responses to incidents. Secondly, an aim of deterring criminals from targeting the UK for a cyber-attack, by showing the ability to detect and prosecute offenders, is set out. Finally, an aim to develop expertise in the cyber security industry, from the 'self-sustaining pipeline of talent' available, is expressed with the need for this to ensure national safety. Furthermore, the strategy emphasises the importance of deepening links with international partners for collective safety, with reference to the European Union, United Nations and the North Atlantic Treaty Organization.

The strategy has resulted in the opening of the National Cyber Security Centre (NCSC), hiring over 700 people to take the authority of the UK's cyber security environment. The opening of this centre is said to be in accordance with the new comprehensive approach to tackling cybercrime, as opposed to the previous market based approach, which Kesan et al. (2017) argued did not produce the required scale of change.

The NCSS states that the aims in place put a higher focus on larger scale cybercrimes, with justification of this being in statistics such as internet banking fraud rising by 64% in 2015, demonstrating that businesses and high net-worth customers are increasingly being targeted by digital crimes (HMG, 2016). Similarly, the strategy outlines that, in general, the UK is not sufficiently cyber aware, allowing for both personal and work-place risk. For example, the Cyber Security Breaches Survey (2017) states that only 58% of businesses sought advice or training on any cyber security matters in 2016, despite each using the internet as a platform for communication. As well as basic cyber knowledge, the strategy denotes specialist cyber skills and capabilities need to be possessed by more individuals in society, stating that this skills gap represents a national vulnerability.

3.3 Cyber security knowledge

"We live in a society exquisitely dependent on science and technology, in which hardly anyone knows anything about science and technology" – Dr Carl Sagan (2006).

The quote above depicts what can be seen to be a popular opinion amongst relevant literature; there is a cyber skills shortage within society, law enforcement and the IT

industry in general. Macdonald (2015) explores this point further, by stating that most police forces, enterprises and other members of the UK public lack the required skills to both protect against and tackle the ever expanding world of cybercrime.

3.3.1 UK law enforcement

PA Consulting (2014) carried out a survey that explored police intelligence analysts in regards to cybercrime, finding various statistics that imply a corresponding agreement to the lack of cyber skills statement made above. First of all, the report found that only 30% of interviewees, all possessing roles within the 43 police forces in the UK, felt they had access to the skills and technology needed to fight cybercrime effectively by being sufficiently equipped to conduct digital investigations; a lack of adequate cybersecurity training was frequently cited in the reasoning's. Similarly, when questioned as to their extent of cyber knowledge, only 5% of respondents answered with the category 'considerate knowledge'. However, the College of Policing (2014) argues that it has recognised this need within policing, and therefore introduced a mainstream officer cyber awareness training course. Despite this, the PA Consulting report denoted that due to economic reasons the course was not available to every officer in a force, thus resulting in only those who are considered more likely to be involved in a cybercrime investigation partaking in it, with other officers still left with a lack of cyber knowledge.

Furthermore, as well as investigating officers, cybercrime analysis requires experienced data scientists with both skills and experience that allow them to exploit big data. However, a recent study by Fisher (2016) shows that 70% of enterprises outsource some of their cyber security personnel, leading to high calibre cyber skilled individuals having the option of private sector roles, as opposed to a most likely lower wage (due to budget cuts and austerity) in a UK police force. Therefore, the UK is presented with the challenge of recruiting and retaining trained specialists into roles within policing cybercrime.

3.3.2 UK industries

Franke and Brynielsson (2014) imply that the growing rates of cybercriminal activity has shed light on the importance of cyber intelligence in industry, with Davies and Patel (2016) agreeing with this statement and adding that organisations that use information technology need to assess whether they understand the risks that are associated with online activity, as well as vulnerabilities in their own infrastructures.

Morgan (2016) shares the statistic of a minimum of 1.6 billion online data breaches being made in 2016, which resulted in average losses of £36,000 to businesses that were subject to them (Klahr, et al., 2017). Furthermore, 65% of large organisations reported an information security breach in 2016, with 25% of these stating that they experienced one every month of the year. These statistics show a clear need for a change in cyber security techniques employed by the effected companies.

The NCSS (2016) states that all organisations are responsible for the security of their networks being suitably safe, highlighting the importance for them to keep pace with evolving technological threats. It is suggested that they do this by investing in both relevant technology and staff members, in order to maintain a level of cyber security proportionate to the risk. A study by Ben-Asher & Gonzalez (2015) explored as to whether cyber security knowledge had an effect on detecting potential illicit cyber activities in the work place, with the results strongly indicating that the more cyber security knowledge the individual possessed, the higher the chance of correct detection of malicious events and decreased chance of classifying benign events as malicious. Ben-Asher & Gonzalez conclude their findings by conveying at least basic information and network security knowledge is necessary for each end user in a business environment for intrusion detection to occur more prominently.

These factors that contribute to the successes of cybercrimes are addressed in the NCSS, with the solutions being suggested in terms of how industry can strengthen its basic cyber security knowledge (HMG, 2016). First of all, the report states that almost all cyber-attacks have been successful due to a contributing human factor, stating that thus they intend to invest in government employees to ensure each person has at least basic awareness of cyber security, as well as hiring those of cyber expertise to manage potential risk effectively; the government suggests that all businesses should follow this employee

strategy. Moreover, the Cyber Security Breaches Survey (Morgan, 2016) informs the NCSS that approximately 70% of cyber-attacks in 2016 were deployed using viruses or malware, education for which is included in the Government's Cyber Essentials scheme available to UK industries, and therefore if this scheme had been enforced by the different companies affected by attacks, it could have allowed for the employee to detect the threat, thus preventing the offence.

In addition, the government is attempting to tackle the issue by reducing the ability of our adversaries to conduct the illicit activity, by employing a 'secure by default' aspect to software and hardware that is installed during the manufacturing process, allowing for maximum security of a product or service automatically. As well as this, they are investing in technologies such as Trusted Platform Modules (TPM) and Fast Identity Online (FIDO), which are innovative authentication mechanisms (Kinney, 2006), to test on behalf of companies their security features.

3.3.3 Public perception and knowledge

Macdonald (2015) denotes that the cyber security skills gap is a 'societal challenge', and argues that the strategy to fill in the gap should start within school education, with the need for businesses to train and develop staff, as well as training for law enforcement, coming after in importance. Fisher (2016) also states the importance of tackling education for generation Z members of society (currently the nation's 16-18 year olds), because it would mean targeting 'digital natives' who have grown up using the internet and digital medias. Furthermore, the previously mentioned PA Consulting Cybercrime Survey (2014) states 90% of the generation Z community use social media, which emphasises the risk of them being subject to potential cyber-attacks. On the other hand, Khanna (2017), argues that growing up in what is considered the 'digital era' has been highlighted in literature as a positive for the younger generation, especially when considering their potential with online capabilities. However, research conducted by Kaspersky Labs (2016) shows that although technical capabilities might be present, only 27% of the younger generation (under-25s) have considered a career in cybersecurity. Similarly, the research showed that 17% would choose to use their cyber skills only for fun, 16% would use them for secretive activities and 11% for financial gain. Therefore, this denotes that the idea of a career encompassing

cyber skills for policing is not popular enough with the younger generation to fill the specialist cyber skill gap.

The UK government has put various schemes in place in order to promote cybersecurity education. First of all, the 'Post-16 Skills Plan' was introduced, offering a digitally focused apprenticeship as an option for placement (HMG-DBIS, 2016). Secondly, the NCSS (2016) has stated it will establish an 'extra-curricular' programme for talented 14-18 year olds, as well as continuing its CyberFirst initiative which identifies young talent within national security. Furthermore, a new institution called National College of Cybersecurity plans to teach select 15-17 year olds a curriculum that is 40% devoted to cyber security.

However, Kritzinger et al. (2017) argues that the current education schemes in place, although attempting to address the skill shortage, do not address the risk of school learners being victims of cybercrimes. Currently, the only aspect of cyber security education that features in mandatory school education in the UK is a visit from the Government's 'Cyber Aware' (formerly Cyber Streetwise) team, who normally host a day of educational activities on the topic (Furnell & Moore, 2014). Therefore, although the UK has cyber security education offerings from primary to postgraduate level (HMG-DE, 2013), it does not incorporate any mandatory learning, resulting in literature such as Kritzinger et al. expressing concerns that basic cybercrime knowledge for school learners is not being met.

3.4 Gaps in the literature

Currently, there are more mobile phones in the world than people and 40% of the world's population has access to the internet (HMG-DE, 2013); statistics such as these emphasise the importance of a rigorous, thorough and all-encompassing nationwide strategy for combatting ongoing cybercrimes. In order to do this, the NCSS (2016) states that the government will provide both individuals and organisations in the UK access to 'the information, education, and tools that they need to protect themselves'. However, although a vast array of changes can clearly be seen with how the UK is combatting cybercrime, the literature above calls upon certain aspects that imply a flawed paradigm to the NCSS statement above. With much literature analysing these individual governmental and law enforcement changes, highlighting the successes and flaws along the way, no literature

explores whether the combined provisions that have been made, and are still being made, make a genuine attempt at leveraging advancing technology to combat cybercrime in order to meet the current demand in UK protection.

Chapter 4 Results and Analysis

4.1 Freedom of Information requests

	Yearly Budget (£)				
Police Force	**2006 - 2007**	**2007 - 2008**	**2008 - 2009**	**2009 - 2010**	**2010 - 2011**
Leicestershire					
West Yorkshire					
Cumbria					£256,036
Bedfordshire	£166,382	£197,651	£234,600	£11,100	£55,600
Dyfed-Powys	£105,232	£150,689	£165,026	£194,044	£216,505
Norfolk & Suffolk					
South Wales		£360,203	£508,773	£439,832	£432,763
South Wales ROCU					
Dorset					
Gwent			£324,721		£280,568
Surrey					
North Yorkshire					
Merseyside					
North Wales		£238,105	£385,284	£401,354	£367,242
Northamptonshire					
Metropolitan Police					
Greater Manchester					

	Yearly Budget (£)					
Police Force	**2011 - 2012**	**2012 - 2013**	**2013 - 2014**	**2014 - 2015**	**2015 - 2016**	**2016 - 2017**
Leicestershire						£1,326,174
West Yorkshire				£29,520	£291,088	£483,671
Cumbria	£245,029	£266,111	£306,911	£433,814	£440,511	£512,585
Bedfordshire	£67,400	£542,700	£575,800	£689,200	£1,044,400	£1,320,100
Dyfed-Powys	£261,753	£230,100	£241,017	£218,354	£446,700	£572,850
Norfolk & Suffolk					£368,001	£707,540
South Wales	£372,688	£408,892	£422,722	£432,585	£435,454	£438,781
South Wales ROCU			£198,000	£188,900	£313,333	£360,000
Dorset					£236,200	£239,416
Gwent	£374,554	£367,385	£378,565	£362,446	£814,710	£893,336
Surrey				£142,474	£189,542	£211,517

North Yorkshire					£225,000	£225,000
Merseyside					£3,179,000	£2,482,000
North Wales	£387,286	£398,457	£446,082	£533,073	£656,257	£621,878
Northamptonshire		£403,754	£468,526	£536,025	£763,015	£755,049
Metropolitan Police			£2,700,000	£1,950,000	£1,950,000	£1,950,000
Greater Manchester						£221,004

Table 2: Budget for cybercrime unit of UK police forces yearly from 2006-2011

Out of the 43 requests made to police forces in the UK, 43 responded and 17 gave details of budget amount for their cybercrime departments, for the time scale requested (2006-present). Only two police forces possessed a dedicated cyber unit in 2006, with a steady increase of cyber units being added yearly from then onwards (1-2 on average). 2014-2015 saw the largest amount of new cyber units with a total of 4 police forces acquiring them. Some police forces, such as North Wales and Dyfed-Powys, show a fairly steady yearly increase in budget totals (never exceeding £250,000), whereas other police forces show larger increases over time, such as Bedfordshire's total increase since the unit opened being £1,153,718. Merseyside currently holds the largest cyber unit budget of £2,482,000.

As well as budget information, 10 of the responses included information such as the breakdown of costs for the cyber unit, as well as structural information. A common trend in this information is staff pay covering the largest section of the budget, with Leicester, Norfolk & Suffolk, Gwent, North Wales and Greater Manchester all reporting this. In addition, training costs were mentioned by West Yorkshire as costing a total of £119,720 in the last financial year. As well as this, Merseyside also mentioned that it had significant costs due to training and IT infrastructure implementation. Metropolitan police stated a total of 198 staff members have undergone a type of cyber training since 2013. Finally, a common trend of either a new part of the cyber unit opening, or a merger with another unit, causing a rise in budget amount is also apparent for Bedfordshire, Gwent and North Yorkshire police forces.

4.2 Cybercrime: A Survey of Public Knowledge and Perceptions

4.2.1 Question 1

What is your age?		
Answer Options	**Response Percent**	**Response Count**
16 to 24	71.1%	101
25 to 34	13.4%	19
35 to 44	4.9%	7
45 to 64	10.6%	15
65 or older	0.0%	0

Table 3: Breakdown of results for Question 1 of Cybercrime: A Survey of Public Knowledge and Perceptions

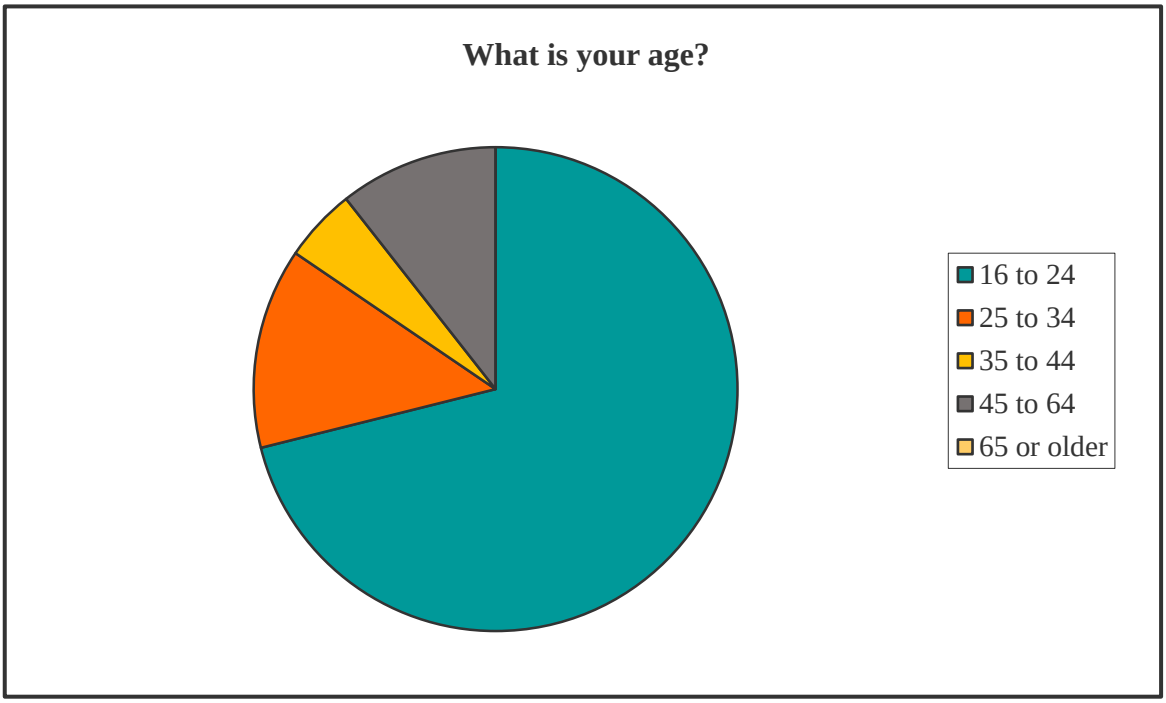


Figure 2: Pie chart illustrating the breakdown of results for Question 1 of Cybercrime: A Survey of Public Knowledge and Perceptions

16 to 24 year olds was the largest age demographic to partake in the survey at 71.1%, with 65 and overs being the lowest at 0%.

4.2.2 Question 2

What is your gender?		
Answer Options	**Response Percent**	**Response Count**
Female	75.9%	107
Male	22.7%	32
Prefer not to say	0.7%	1
Other (please specify)	0.7%	1

Table 4: Breakdown of results for Question 2 of Cybercrime: A Survey of Public Knowledge and Perceptions

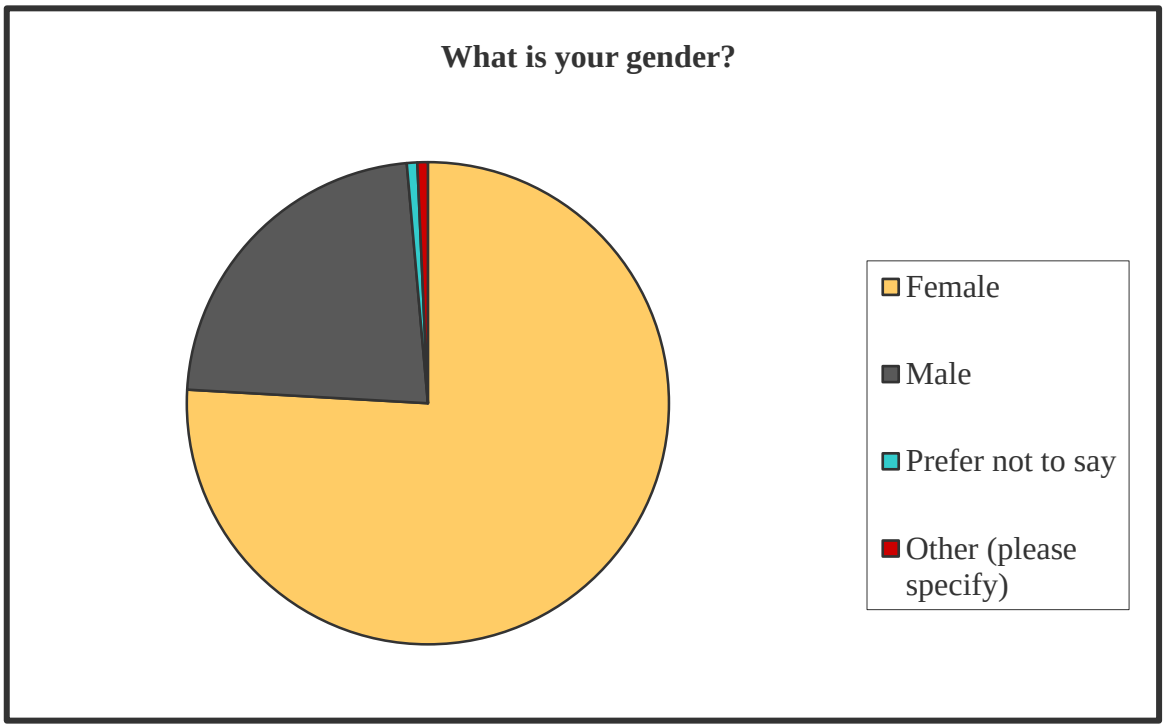


Figure: Pie chart illustrating the breakdown of results for Question 2 of Cybercrime: A Survey of Public Knowledge and Perceptions

4.2.3 Question 3

How many internet-enabled devices do you own?		
Answer Options	**Response Percent**	**Response Count**
0	0.0%	0
1	3.5%	5
2	26.8%	38
3	32.4%	46
4	22.5%	32
5 or more	14.8%	21

Table 5: Breakdown of results for Question 3 of Cybercrime: A Survey of Public Knowledge and Perceptions

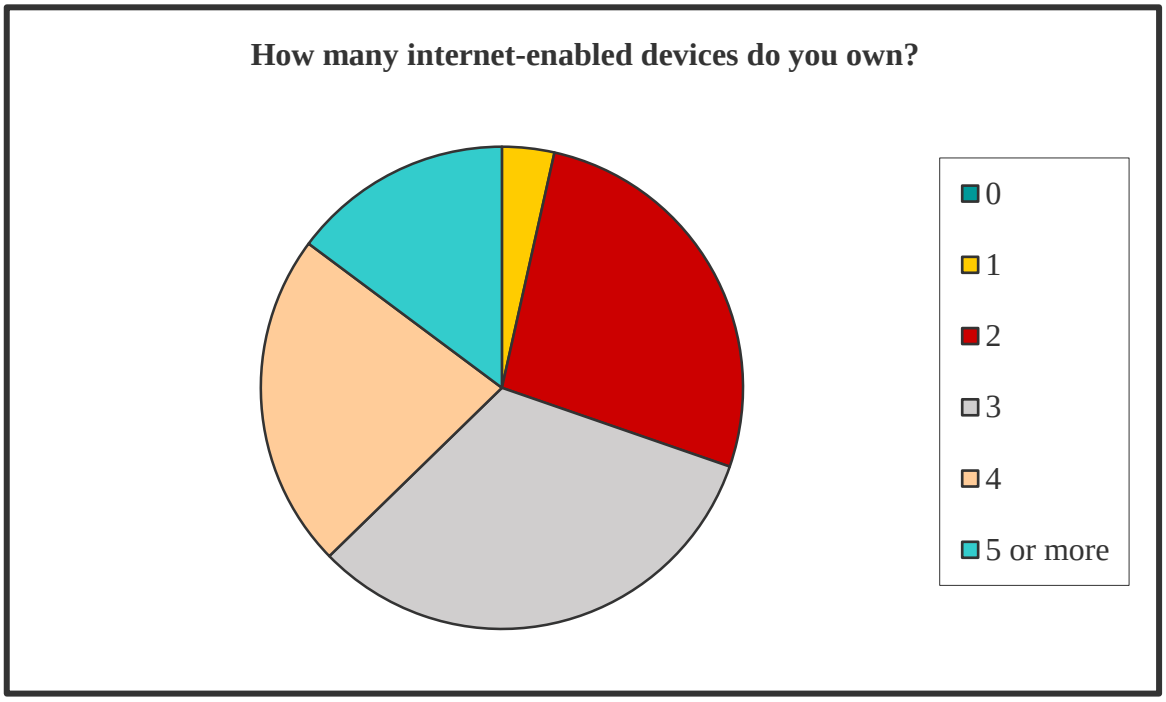


Figure 3: Pie chart illustrating the breakdown of results for Question 3 of Cybercrime: A Survey of Public Knowledge and Perceptions

The majority of the participants of this survey own 3 internet-enabled devices, with all participants owning at least 1.

4.2.4 Question 4

Have you, or has anyone that you know personally, ever experienced a cybercrime?		
Answer Options	**Response Percent**	**Response Count**
Yes, definitely	75.4%	107
Yes, possibly	11.3%	16
No, I do not think so	11.3%	16
No, definitely not	2.1%	3

Table 6: Breakdown of results for Question 4 of Cybercrime: A Survey of Public Knowledge and Perceptions

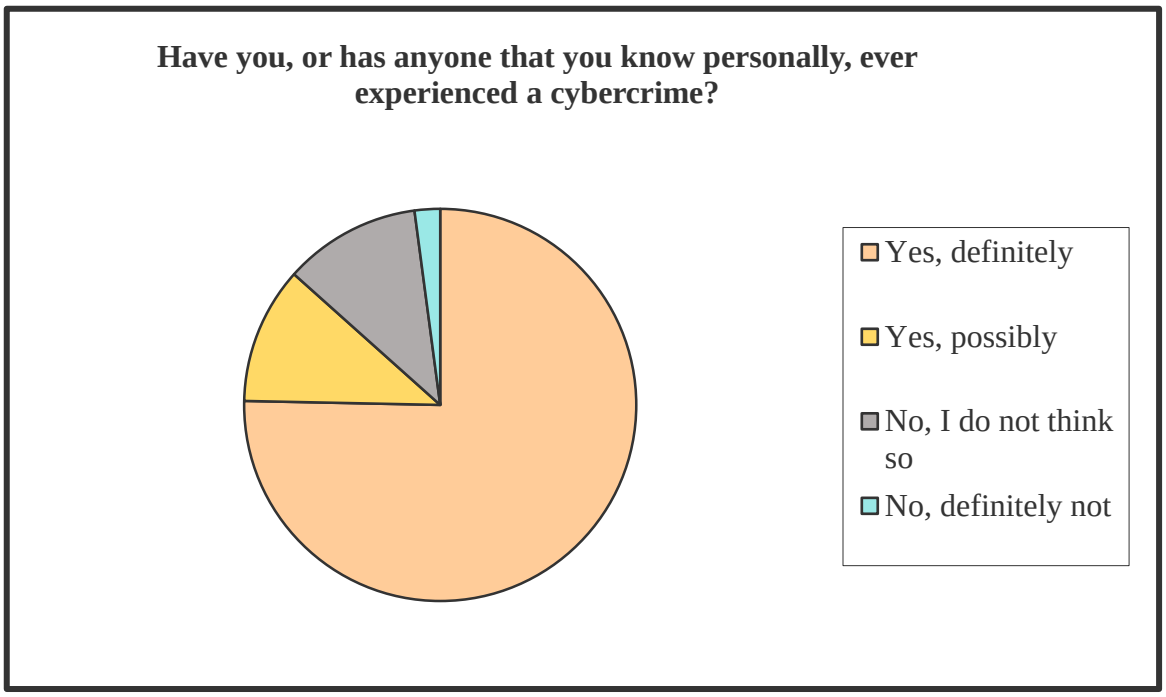


Figure 4: Pie chart illustrating the breakdown of results for Question 4 of Cybercrime: A Survey of Public Knowledge and Perceptions

75.4% of participants believe that they, or someone they know, have been subject to a cybercrime. The respondents that answered that they had 'definitely not' been subject to a cybercrime, all answered 'I have little/no knowledge' to question 6 of this survey.

4.2.5 Question 5

How would you rank the seriousness of the following experiences?				
Scenario Options	Not serious at all	Moderately serious	Serious	Very serious
Opening a malicious email/website	4	29	52	54
Online grooming, harassment or bullying	1	6	21	111
Online purchases being made in your name	2	4	24	109
Your online banking username and passwords being compromised	3	1	13	122

Table 7: Breakdown of results for Question 5 of Cybercrime: A Survey of Public Knowledge and Perceptions

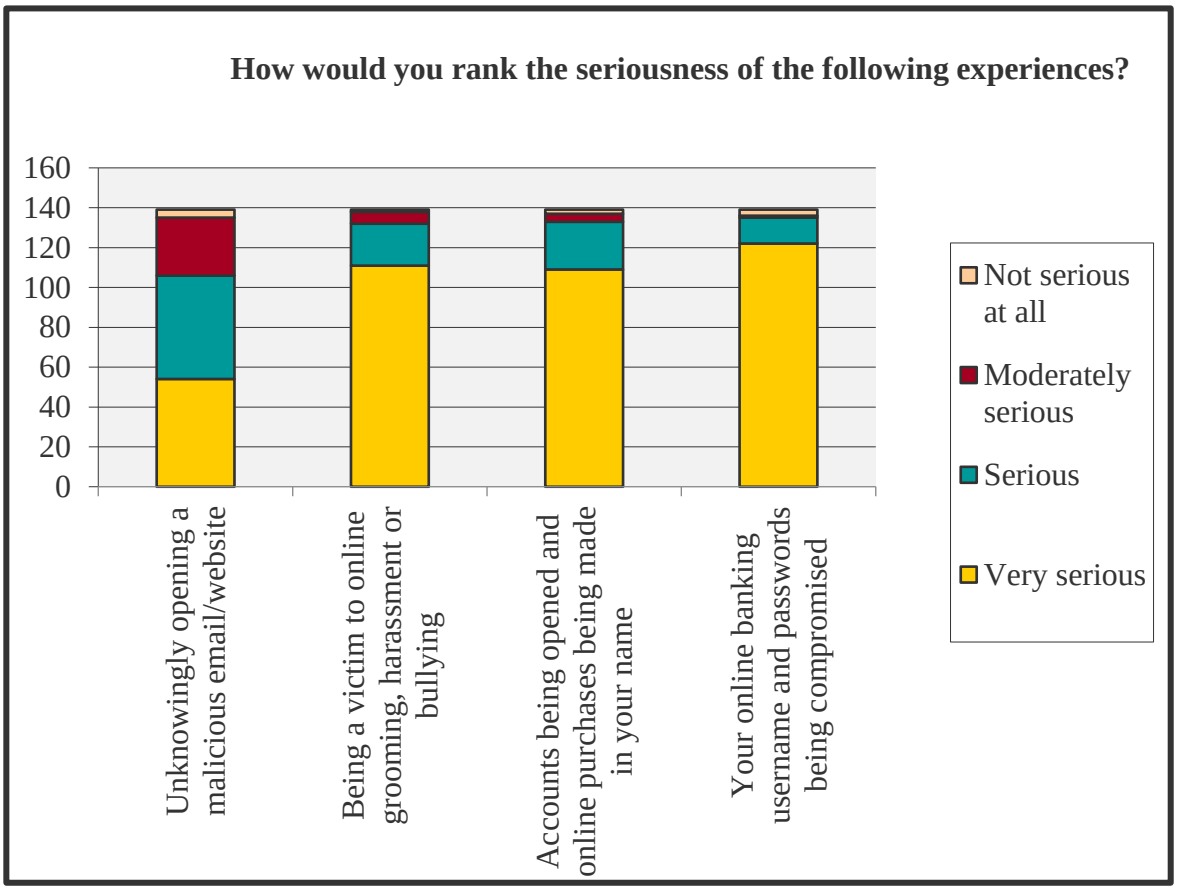


Figure 5: Bar chart illustrating the breakdown of results for Question 5 of Cybercrime: A Survey of Public Knowledge and Perceptions

Option 4, the option relating to cyber fraud, was deemed the most serious type of cybercrime by participants, with option 1 concerning malicious content being deemed the least serious.

4.2.6 Question 6

If you have any knowledge on cybercrime, where did you access this knowledge?		
Answer Options	**Response Percent**	**Response Count**
Through mandatory education	19.7%	27
Through voluntary education	26.3%	36
Place of work	34.3%	47
Voluntary research	31.4%	43
Local police force's website	2.2%	3
Government's website	5.1%	7
I have little/no knowledge	33.6%	46

Table 8: Breakdown of results for Question 6 of Cybercrime: A Survey of Public Knowledge and Perceptions

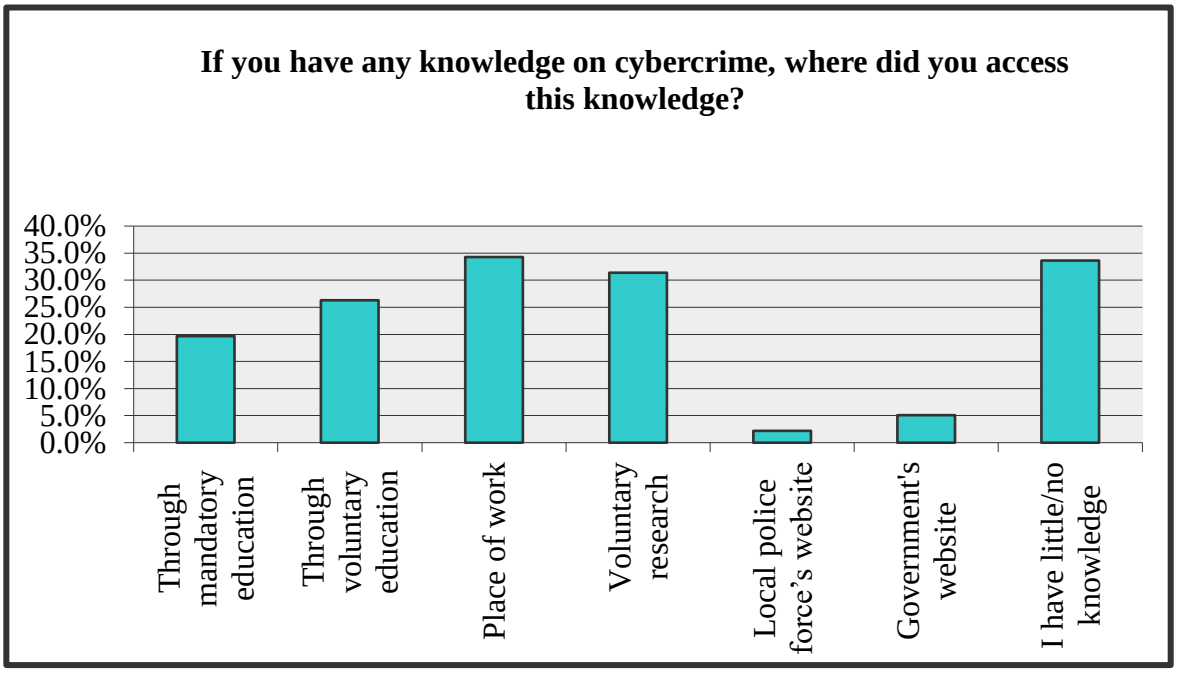


Figure 6: Bar chart illustrating the breakdown of results for Question 6 of Cybercrime: A Survey of Public Knowledge and Perceptions

The largest option chosen for this question was the participant possessing ‘little or no knowledge’. For the participants with knowledge, the majority have accessed this through their place of work, with the least having accessed it from their local police forces website.

4.2.7 Question 7

To what extent would you rank your knowledge on the following areas?				
Answer Options	**No knowledge**	**Moderate knowledge**	**Good knowledge**	**Strong knowledge**
I could correctly define the differences between the surface web, the deep web and the dark web	58	56	17	6
I am aware of the Tor encryption tool	101	20	5	11
I know what Bitcoin is and how it differs from normal currency	72	36	18	11

Table 9: Breakdown of results for Question 7 of Cybercrime: A Survey of Public Knowledge and Perceptions

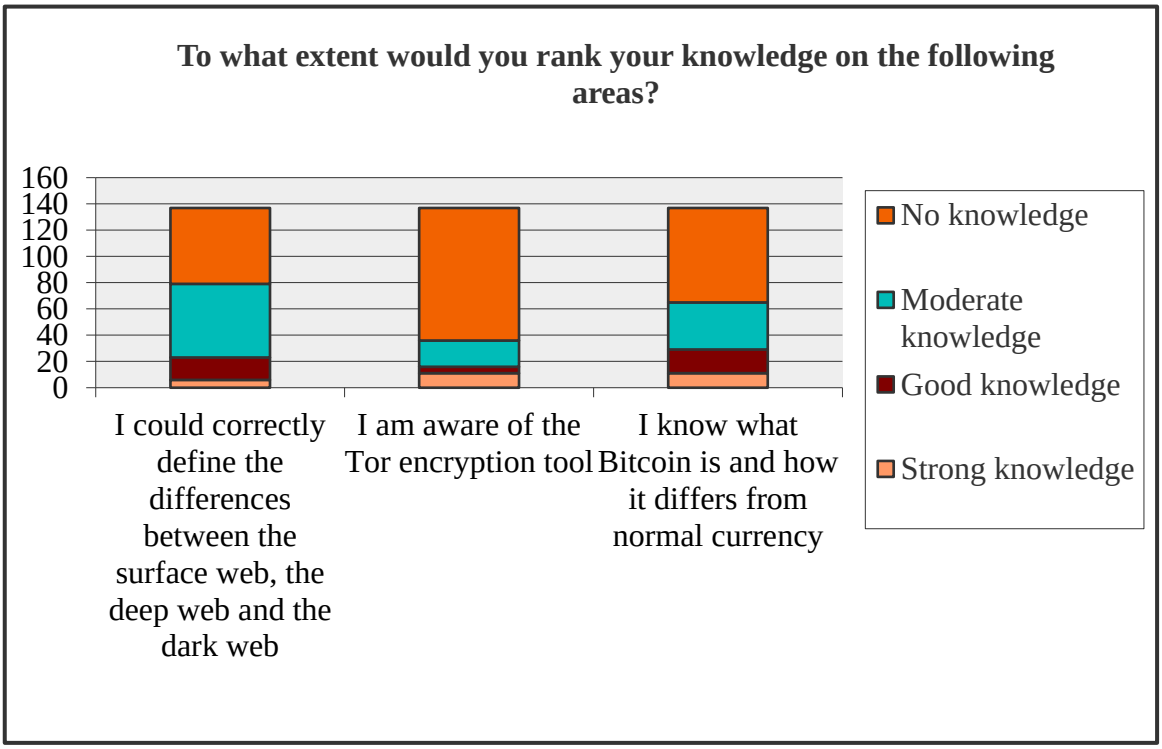


Figure 7: Bar chart illustrating the breakdown of results for Question 7 of Cybercrime: A Survey of Public Knowledge and Perceptions

'No knowledge' was the most popular option choice for all 3 statements. For those who answered 'strong knowledge' for all three statements, 72% of these participants accessed this knowledge through voluntary education (sixth-form and above).

4.2.8 Question 8

How much do you agree with the following statements?					
Answer Options	**Strongly disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly agree**
Cybercrime is a growing problem in the UK	2	0	13	58	63
I can tell a phishing/spam email apart from a legit one	2	10	19	76	29
I know where to look for cybercrime information	8	47	37	35	9
I have sufficient knowledge of cybercrime	18	55	31	24	8
The more cybercrime knowledge I possess, the less vulnerable I am to being a potential victim	2	26	17	60	31
It is the government's responsibility to provide this knowledge to UK citizens	1	6	33	67	28

Table 10: Breakdown of results for Question 8 of Cybercrime: A Survey of Public Knowledge and Perceptions

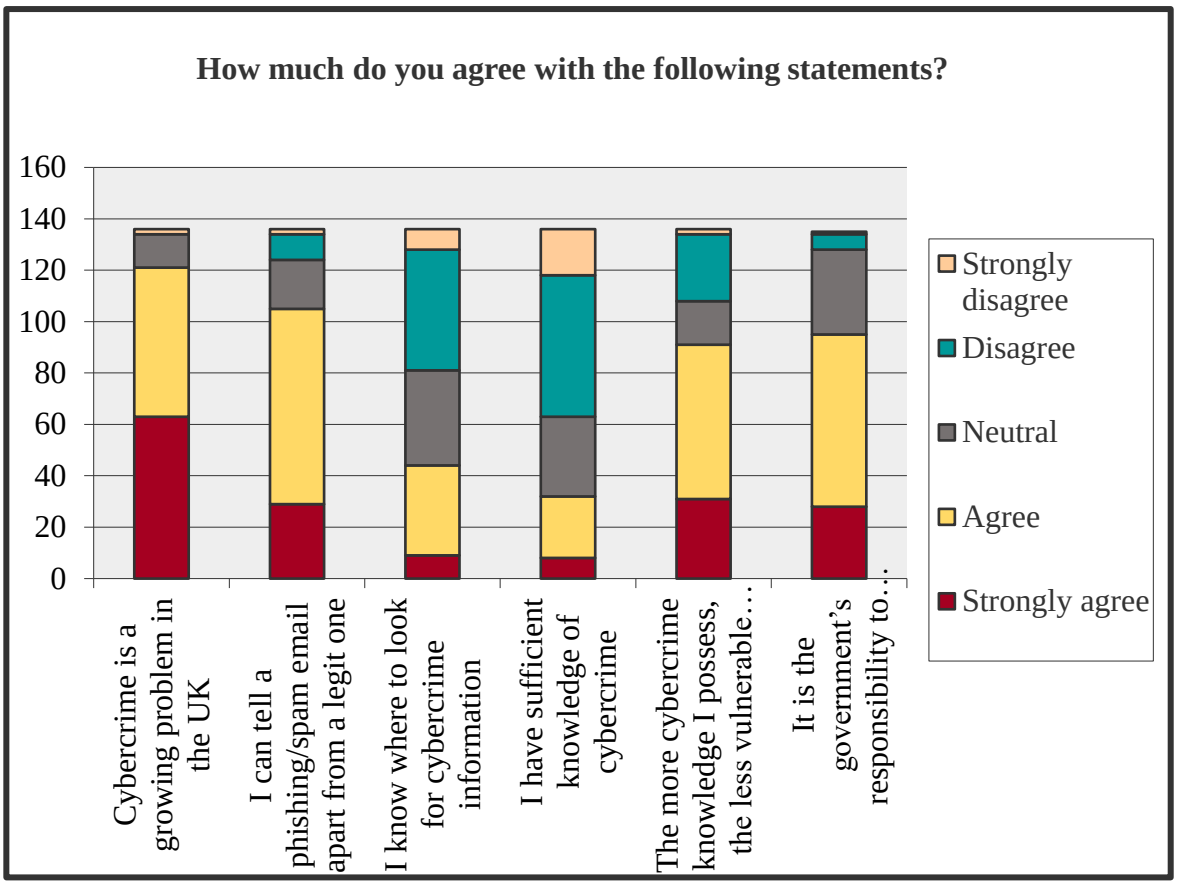


Figure 8: Bar chart illustrating the breakdown of results for Question 8 of Cybercrime: A Survey of Public Knowledge and Perceptions

The most common choice for statement one was 'strongly agree', with only two participants disagreeing with the statement. The two participants who disagreed with the first statement both selected 'little or no knowledge' for question 6. More participants disagree with knowing where to access cybercrime information (statement 3) then agree. Each of the 8 participants who stated they have sufficient cybercrime knowledge (statement 4), selected either 'voluntary research', 'voluntary education', or 'place of work' for question 6. The most popular answer choice for statement 5 was 'agree' followed by 'strongly agree'. Finally, only 7 participants in total disagree that it is the UK government's responsibility to educate citizens on cybercrime risks.

4.2.9 Question 9

Considering the ever growing rate of technology use in society, how much would you agree with how beneficial it would be to start mandatory basic computer science learning in schools?		
Answer Options	**Response Percent**	**Response Count**
Strongly disagree	0.7%	1
Disagree	0.0%	0
Neutral	6.6%	9
Agree	38.2%	52
Strongly agree	54.4%	74

Table 11: Breakdown of results for Question 8 of Cybercrime: A Survey of Public Knowledge and Perceptions

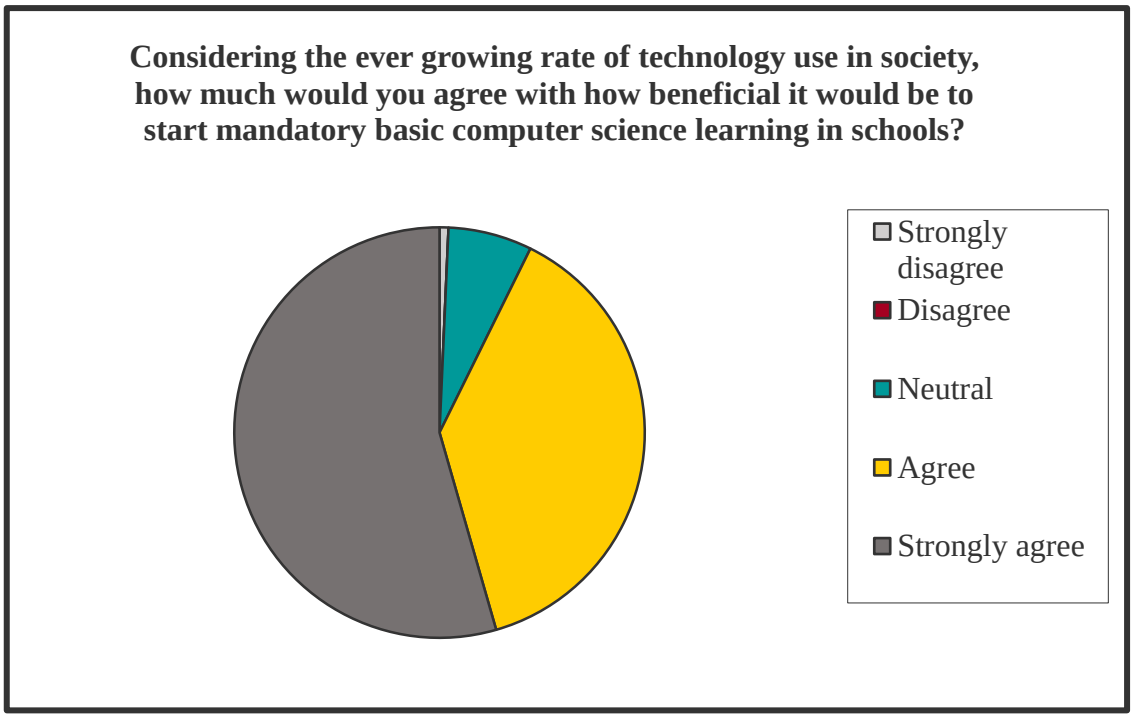


Figure 9: Pie chart illustrating the breakdown of results for Question 8 of Cybercrime: A Survey of Public Knowledge and Perceptions

A vast majority of the participants selected ‘strongly agree’ or ‘agree’ for question 9, with only one participant disagreeing. The participant who selected disagree for this question

also disagreed with statement 1 of question 6, that cybercrime is a growing problem in the UK.

4.3 Cybercrime: A Survey on Expert Opinion

4.3.1 Question 2

What is your age?		
Answer Options	**Response Percent**	**Response Count**
18-24	25.0%	2
25-34	12.5%	1
35-44	12.5%	1
45-60	37.5%	3
61 or above	12.5%	1

Table 12: Breakdown of results for Question 2 of Cybercrime: A Survey on Expert Opinion

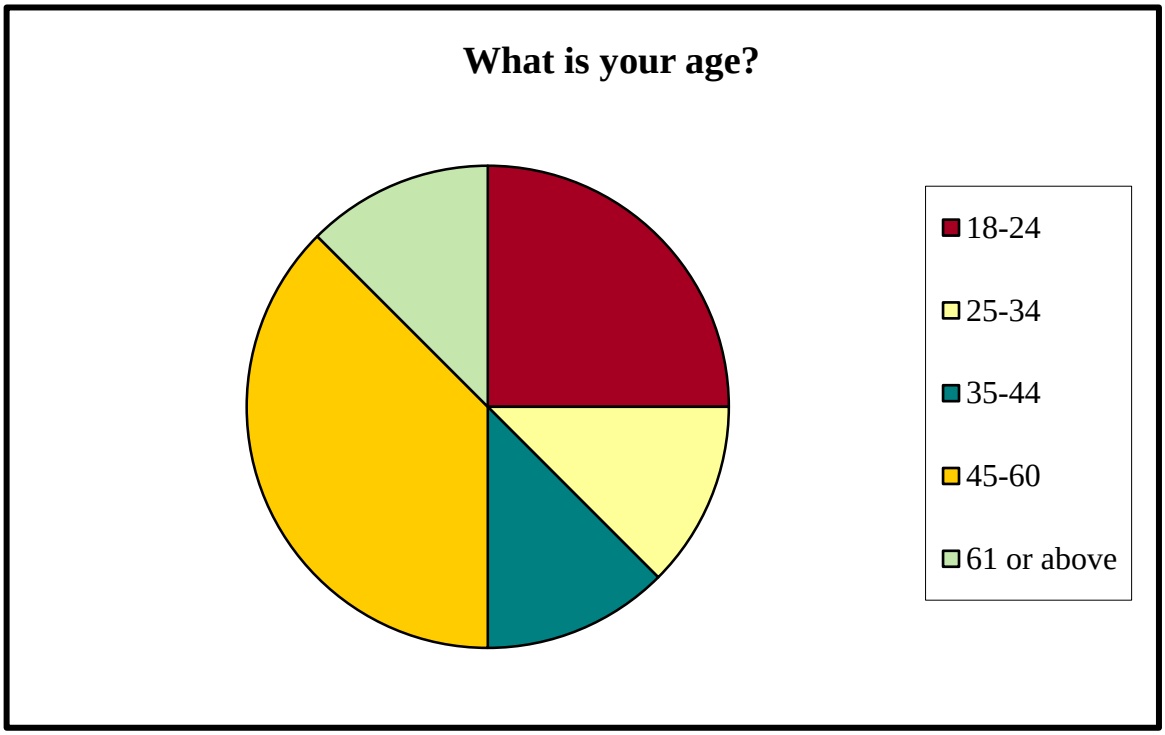


Figure 10: Pie chart illustrating the breakdown of results for Question 2 of Cybercrime: A Survey on Expert Opinion

At least one response was generated from participants for each age group listed.

4.3.2 Question 4

The government's National Cyber Security Strategy 2016 makes the following statements, to what extent do you agree?					
Answer Options	**Strongly disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly agree**
There is a lack of computer science expertise in current society	0	0	1	3	4
Cyber criminals are one step ahead and our strategies for combatting the crimes have so far not kept pace	0	0	0	2	6
Almost all successful cyber-attacks have a contributing human factor	0	0	0	3	5

Table 13: Breakdown of results for Question 4 of Cybercrime: A Survey on Expert Opinion

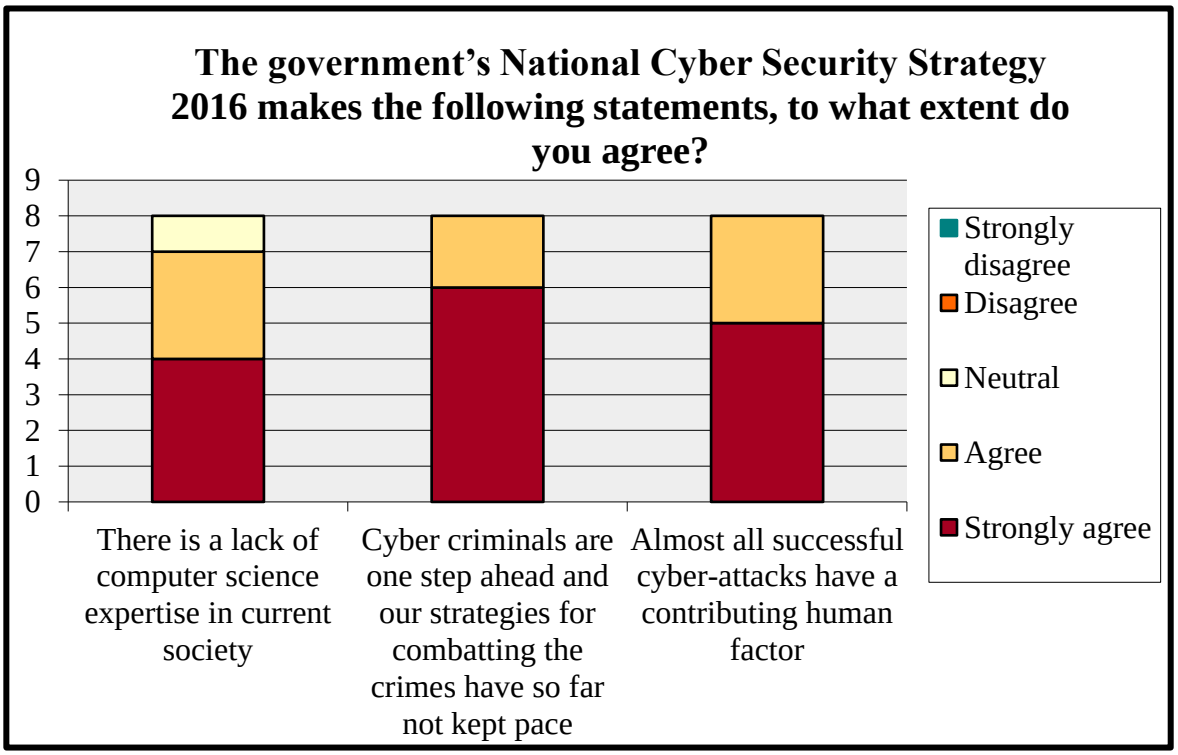


Figure 11: Bar chart illustrating the breakdown of results for Question 4 of Cybercrime: A Survey on Expert Opinion

Question 4 shows a clear correlation of the agreement of the statements, with only one respondent selecting neutral for statement one. All other responses were either agree or strongly agree from all 8 participants.

4.3.3 Question 5

Crime reports show that even though reports of cybercrime to police forces is increasing, the amount that result in a judicial outcome has stayed consistent at 17%. Considering this, how strongly would you agree with the following statements?					
Answer Options	**Strongly disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly agree**
There is a need for better international cooperation between policing bodies	0	0	1	2	5
Lack of training for the use of computer forensics within policing bodies is a problem	0	0	1	4	3
Lack of citizen knowledge on cybercrime is a problem	0	1	0	4	3

Table 14: Breakdown of results for Question 4 of Cybercrime: A Survey on Expert Opinion

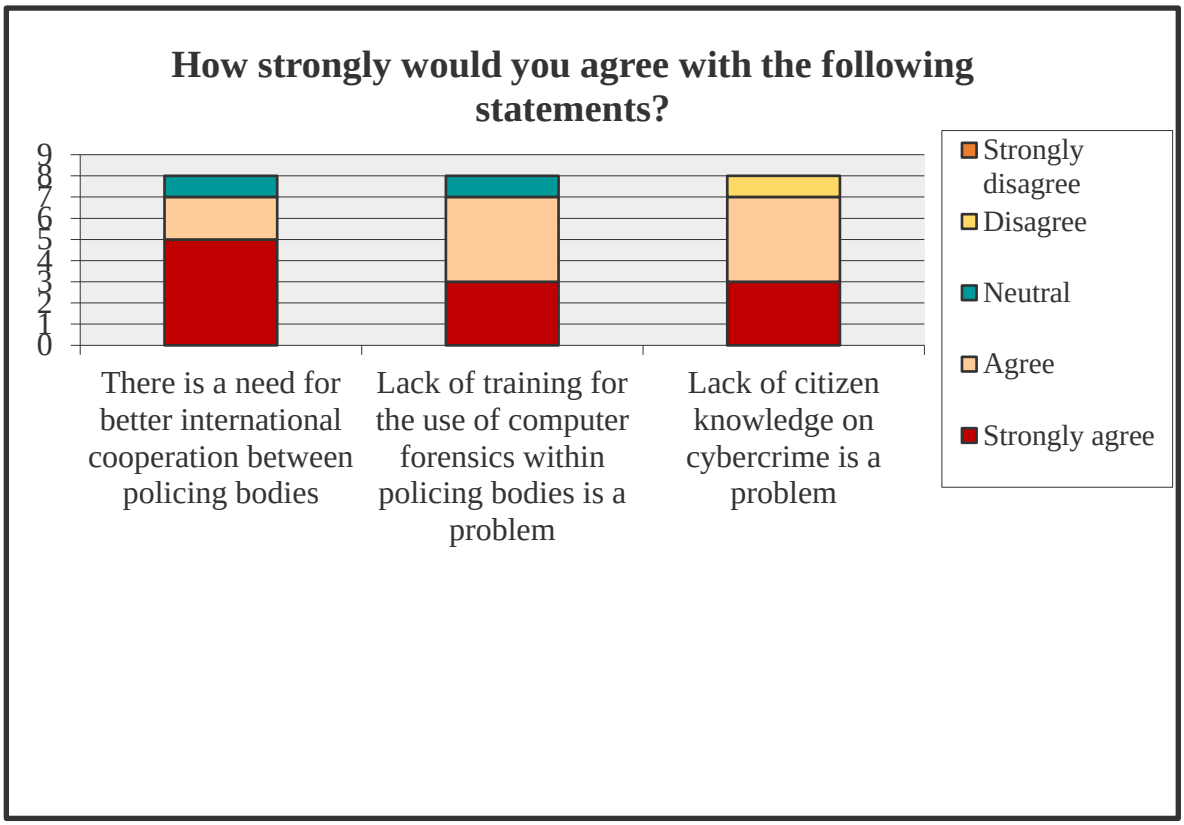


Figure 12: Bar chart illustrating the breakdown of results for Question 5 of Cybercrime: A Survey on Expert Opinion

Question 5 yields similar results to Question 4 that more statements are agreed with by the participants as opposed to disagreed to.

4.3.4 Question 6

In a recent City of London Police report, they estimated that 1.5million cybercrimes were not reported during 2014-2015, costing industries approximately £12billion in total. These crimes not being reported means the accurate scope of the issue cannot be determined. With what importance would you rank the following factors in this?			
Answer Options	**Low importance**	**Moderate importance**	**High importance**
Lack of computing knowledge in the industry sector	2	4	2
Companies prioritising their reputation	0	4	4
Lack of confidence in a judicial outcome	2	3	3

Table 15: Breakdown of results for Question 6 of Cybercrime: A Survey on Expert Opinion

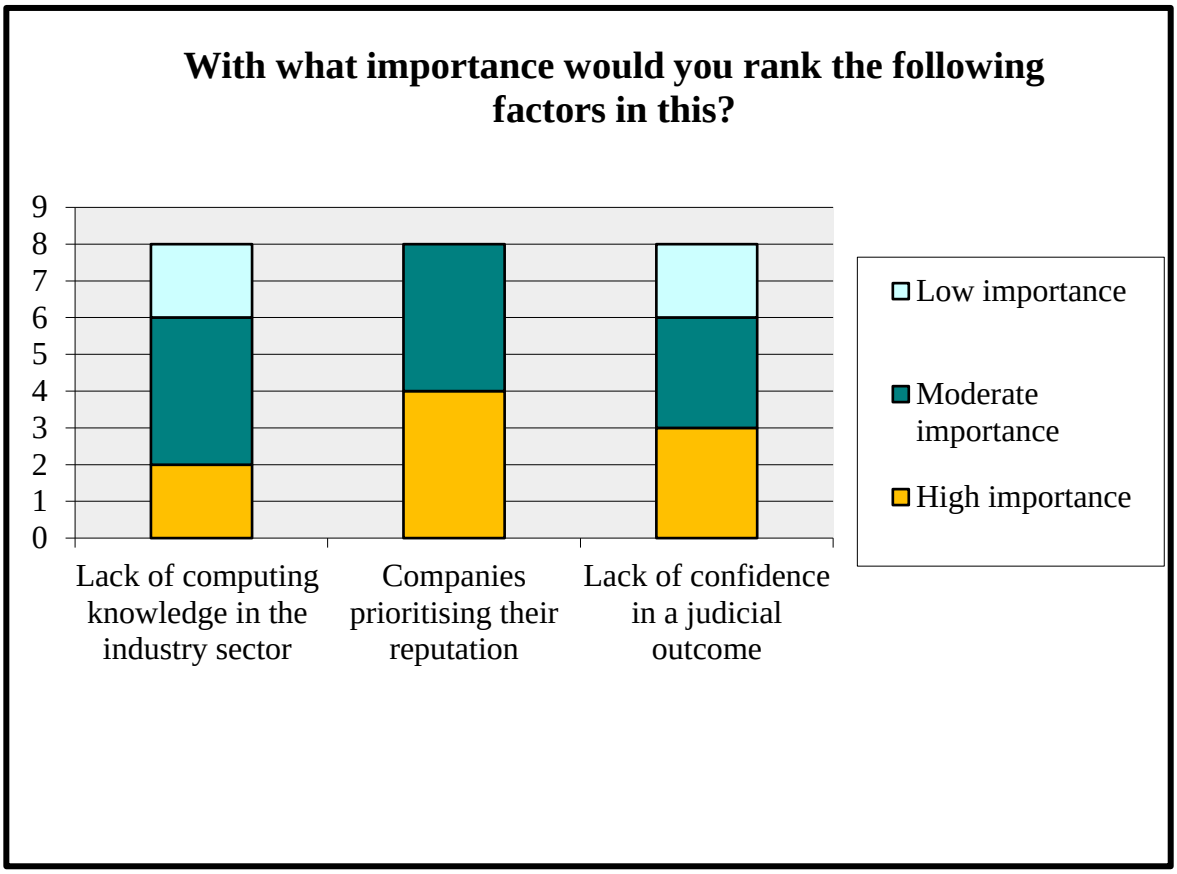


Figure 13: Bar chart illustrating the breakdown of results for Question 6 of Cybercrime: A Survey on Expert Opinion

Question 6 shows little correlation of results, with a variety of answers from the respondents for each statement.

4.3.5 Question 7

The College of Policing has a 'mainstream cyber-crime' training course. However, police forces are not bound by this and can opt out of the course. Considering this, how strongly do you agree with the following statements?					
Answer Options	**Strongly disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly agree**
The course should be mandatory	1	1	1	3	2
It would be less necessary for officers to complete this course if they had gained basic computer science knowledge during their school education	1	2	0	4	1
Only investigators who work specifically in a cybercrime unit should be required to complete the course	3	2	1	0	2

Table 16: Breakdown of results for Question 6 of Cybercrime: A Survey on Expert Opinion

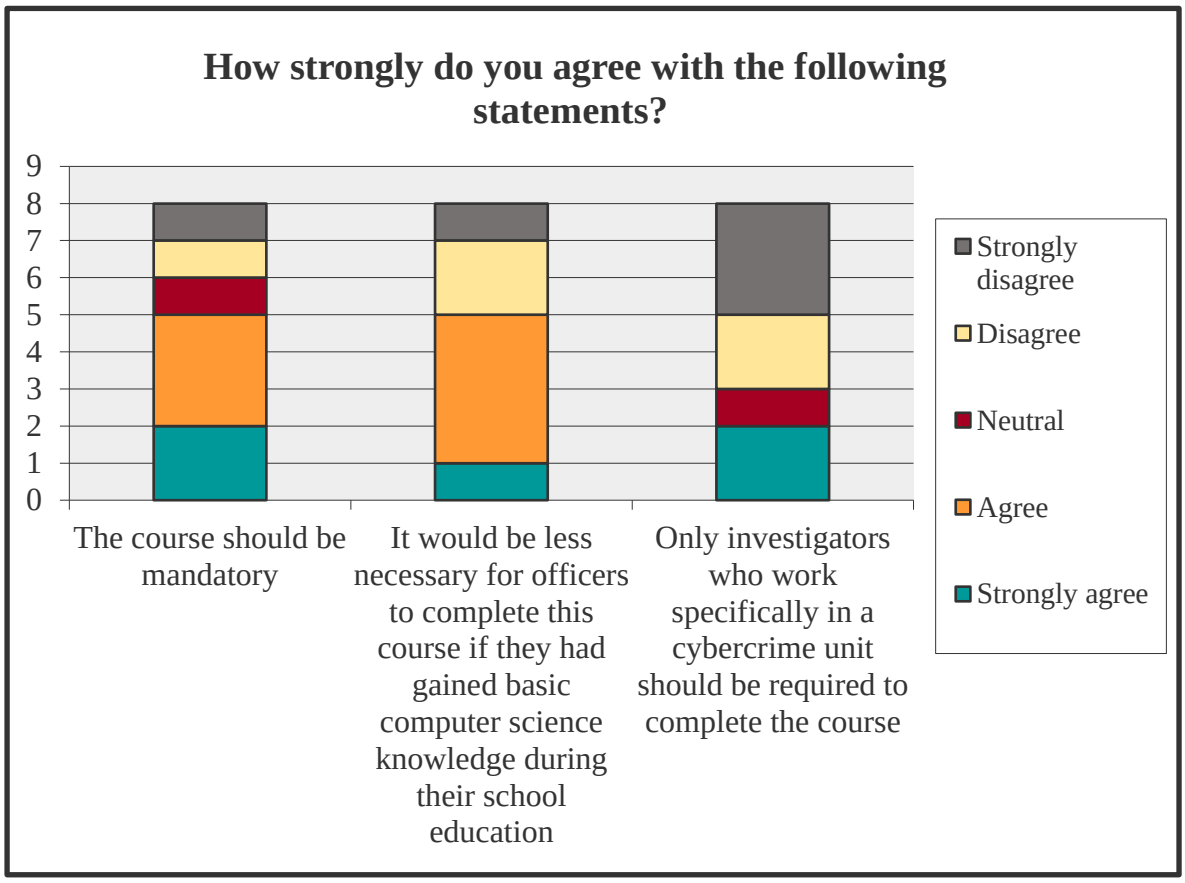


Figure 14: Bar chart illustrating the breakdown of results for Question 7 of Cybercrime: A Survey on Expert Opinion

The majority of the participants agree that the course set out by the College of Policing should be mandatory, which correlates to the outcome of statement 3, that the course should only be undertaken by those working in a cybercrime unit.

4.3.6 Question 8

When considering the statement that there is a cyber skills shortage in society, to what extent would you agree that these things would help?					
Answer Options	**Strongly disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly agree**
Basic computer science skills being integrated into mandatory school education	0	0	0	3	5
Current ICT teachers having computer science training available to them	0	1	1	1	5
Ability promote a more defined profession	0	0	3	2	3

Table 17: Breakdown of results for Question 8 of Cybercrime: A Survey on Expert Opinion

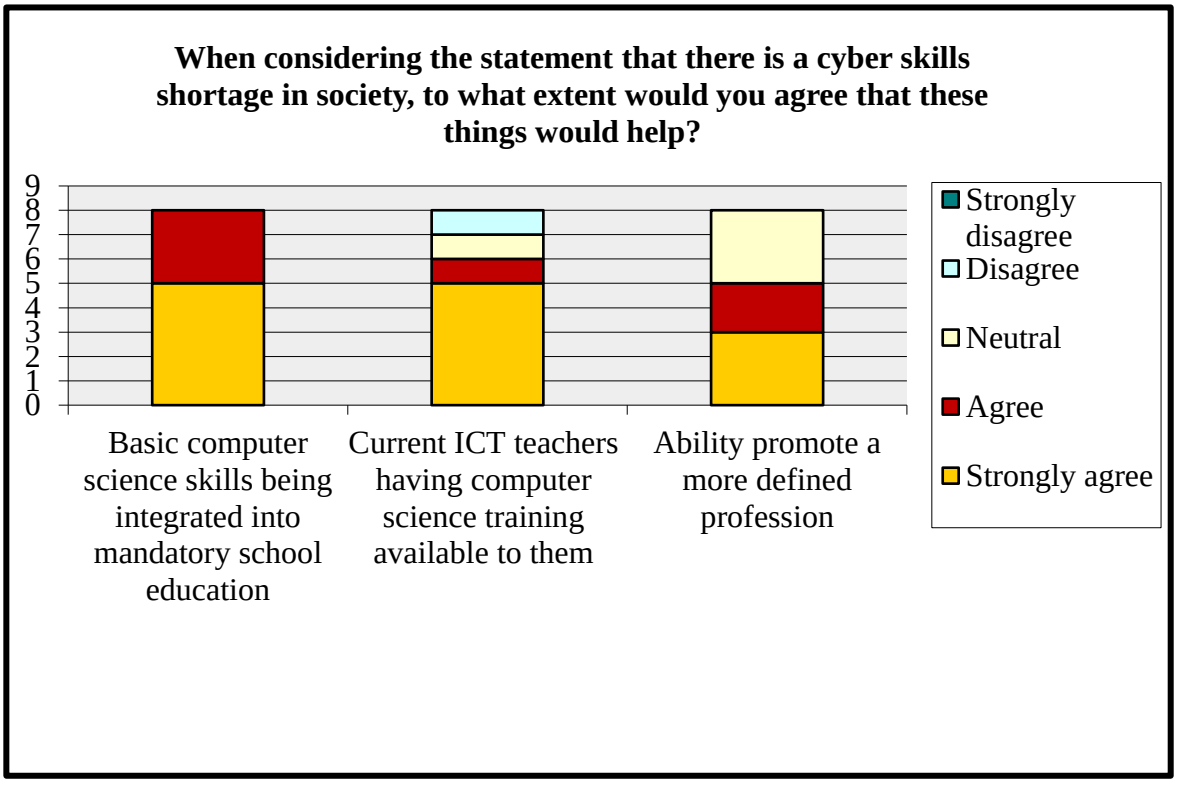


Figure 15: Bar chart illustrating the breakdown of results for Question 8 of Cybercrime: A Survey on Expert Opinion

Question 8 illustrates that all of the expert participants agree that cyber security and cybercrime knowledge should be provided to school learners whilst they are still in there mandatory school years.

4.3.7 Question 9

The government plans to invest in technologies which do not rely on passwords for user authenticationTo what extent do you think these technologies would be suitable in your place of work?	
Answer Options	**Response Percent**
Definitely not suitable	25.0%
Possibly suitable	50.0%
Definitely suitable	25.0%

Table 18: Breakdown of results for Question 9 of Cybercrime: A Survey on Expert Opinion

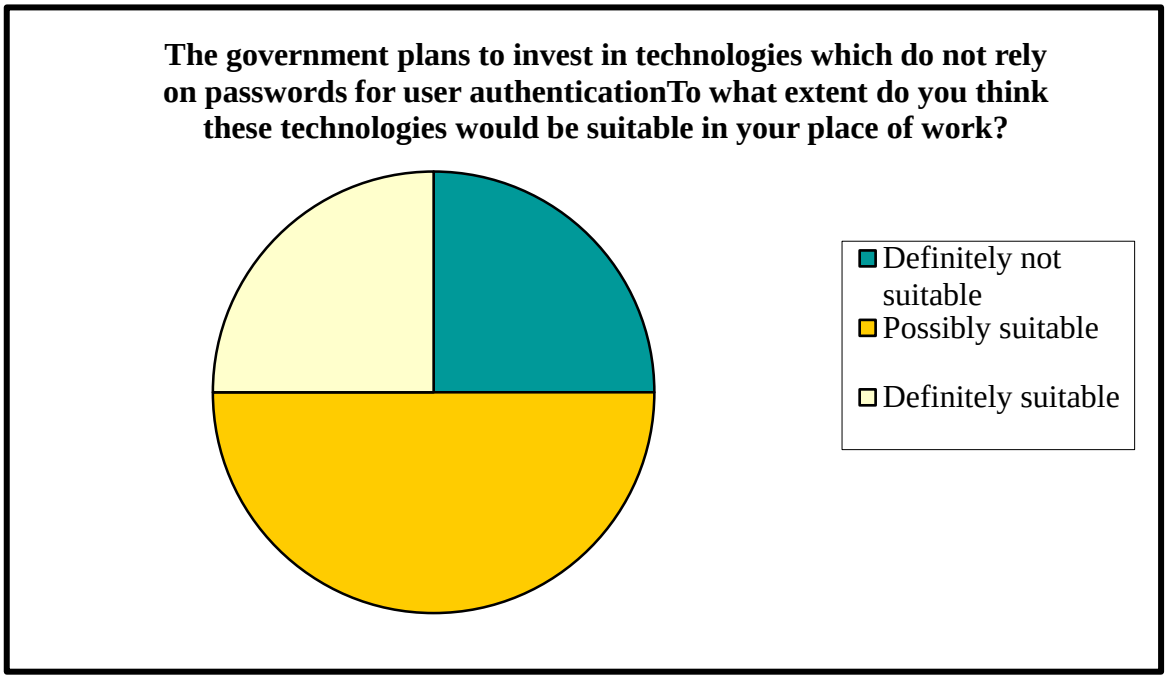


Figure 16: Pie chart illustrating the breakdown of results for Question 9 of Cybercrime: A Survey on Expert Opinion

The results from Question 9 show a very varied opinion on TPM and FIDO type technologies, which no correlation between answers shown.

Chapter 5 Discussion

5.1 Objective 1

In order to meet the aim of the first objective of this study, an in-depth analysis on the literature included in Chapter 2.1 was necessary to highlight the changes that have occurred within cybercrime and cybersecurity matters, and assess the role that technological advances have played in this area. Therefore, this section discusses how technological advances, since the birth of the digital era, have affectively shaped cybercrime in ways such as the types of crimes committed, methods for carrying out the offences and the time scale that it takes to do so. The literature highlights that all changes within society, ranging from social, economic or politically based backgrounds, cause social practises within communities to change; this theory can be applied to technological changes causing citizens to approach the way that they use devices differently. For example, the fact that the internet has become more accessible in recent years has led to a continuous increase in usage rates, but as the literature denotes, increased connectivity allows for cyber criminals to have more opportunities for attack. Furthermore, as technology becomes more popular in earlier stages of life, predatory crime rates raise; the correlation between the two stated in the literature in Chapter 2.1. Though some argue that as technology develops so do technical security measures, others counteract this argument by stating cyber criminals are often one step ahead in their endeavours; an example being the Aircrack-ng program for WIFI encryption tool hacking, as mentioned in the literature. Moreover, the increase in ways for which media coverage can be accessed by the public is argued as both helping and hindering cyber criminals; covering cyber security breach stories in the media spreads awareness for the necessary cyber security measures that people should take to the public, but also provides cyber criminals with a new incentive of ‘fame’ for their attacks (Yang, et al., 2012).

It is an undeniable conclusion from the literature contained in this section that there is a distinct correlation between changes in technology promoting changes in various aspects

of cybercrimes, with an implication that cyber criminals have been leveraging advancing technology since the dawn of the digital era. Similarly, Question 4 of 'Cybercrime: A Survey on Expert Opinion' (see Chapter 4.3.2) denotes that each of the 8 expert participants agreed with the statement that cyber criminals are one step ahead of the law enforcement attempting to combat it, implying that cyber deviant individuals leverage advancing technology at a faster pace than those combatting it.

5.2 Objective 2

UK law enforcement, including the UK police forces, ROCU's, the National Crime Agency (NCA), Home Office and other government bodies, have undoubtedly changed their strategies in order to attempt to meets the needs of successfully combatting on cybercrime within the UK. First of all, as Chapter 2.2 denotes new specialist units, such as the NCCU ran by the NCA, and the NCSC ran by Government Communications Headquarters (GCHQ), have been implemented into the nation's security network in order to meet the demands set out in the NCSS (2016). In addition, evidence of this factor can also be seen in research method 1 of this study, whereby 17 of the 43 local police forces in the UK gave evidence of additions of cyber units into their establishments at some point from 2006 onwards. Furthermore, all cyber units that feature in the data display results of increasing budget amounts from their creation to the present day, thus indicating that both more time and money is being put towards the combatting of cybercrime at a local level.

Contrastingly, as O'Connor (2012) outlines in Chapter 2.2.1, local police forces are most often responsible for the investigation of smaller scale cyberattacks within their domains, which raises the question as to whether the 26 police forces in the UK that do not possess a dedicated unit to cybercrime are efficiently equipped to tackle the problem. Results that can be seen in Chapter 4.3.5 state that the majority of expert participants of the survey hold the opinion that the 'mainstream cyber-crime' training course set out by the College of Policing should be mandatory for all police force members, which correlates to the outcome of statement 3 of the same question, that the course should only be undertaken by those working in a cybercrime unit. Thus it can be questioned whether the staff of police forces without a cyber unit are receiving the training that it is believed by experts to be needed for effective cyber policing. Similarly, information from the Freedom of

Information research approach (see Chapter 4.1) shows that both staff pay and cyber related training prices are the major cost producing aspects of a cyber unit within a police force, implying that local forces that have suffered from budget cuts (Fisher, 2016) may not have the resources to provide the necessary training to relevant officers.

As well as police structural changes, UK legislations have changed to accommodate cybercrimes, as mentioned in Chapter 2.2.2. However, though the NCSS (2016) aims to strengthen international links, the loophole of, as Brenner (2008) phrased it, 'a safe haven' for cyber criminals still exists within nations who do not match legislations with the UK's Computer and Misuse Act 1990. Subsequently, there still exists a way in which cyber deviant members of society can commit crimes without risking sentence. This point is also shared in Chapter 4.3.3, whereby 7 out of the 8 expert participants stated that there is a need for better international cooperation between policing bodies in terms of the law and the exchange of information. Another essential on this point is made by Woolaston (2017), who depicts that the investigation into the very recent NHS cyber-attack concerning the WannaCry virus was halted in the UK when links to the North Korean hacking group Lazarus where identified as potentially being the cause.

5.3 Objective 3

Arguably the most important point that is highlighted often throughout the literature outlined in Chapter 2.3 is that there is a shortage of individuals in the UK who possess specialist cyber skills. Not only does the literature share this point, Question 4 of the 'Cybercrime: A Survey on Expert Opinion' survey also shows that all of the expert participants shared the view that there is a lack of computer science expertise in current society. Much of the literature, such as the NCSS (2016), argue that schemes are already in place for law enforcement officials, UK adult citizens and school learners to educate themselves on cyber security matters. However, as already outlined in Chapter 5.2, there are existing barriers that cause many members of UK police forces to be unable to take part in the said educational training, resulting in that cyber skill shortage gap still existing for that category.

Question 4 of the 'Cybercrime: A Survey of Public Knowledge and Perception' survey states that a total of 75.4% of participants believe they, or someone they know, have been

the victim of at least one cybercrime, which denotes that the public are aware of the scale of the problem in the UK. In addition, for question 6 in the same survey the largest option chosen for this question was the participant possessing 'little or no knowledge' when concerning cybercrime/security relations, which clearly indicates that the public are also aware of their need for education on these topics. Also, the same question depicts that only 7 participants have ever accessed cyber knowledge via a government owned website, which contradicts the statement made in the NCSS (2016) that the government will provide the public with necessary basic knowledge. Similarly, results from Question 7 of the same survey state under a third of the participants agreed that they were aware of where to obtain cyber information should they choose to do so, again contradicting the aim made by the NCSS. However, an agreement that can be seen between the NCSS and the survey results is that both indicate that the government is responsible for providing necessary knowledge to the public, with only 7 respondents disputing this.

Furthermore, much of the literature puts forward the argument that if more members of the public had basic cyber security training, less industry cyber security breaches would occur; thus emphasising the need for companies to enforce basic cyber security training resources on their employees, such as the government's Cyber Essentials scheme. Also, the study by Ben-Asher & Gonzalez (2015) conveyed at least basic information and network security knowledge is necessary for each end user in a business environment for intrusion detection to occur more prominently. Additionally, the NCSS (2016) claims that almost all cyber security breaches have a contributing human factor, again highlighting the difference that all society members possessing basic cyber knowledge could make in terms of combatting cybercrimes.

Equally important is the considerations made to the education received by children who are still in mandatory school education. The literature argues that members of society in this age demographic are the most suitably equipped to lessen the skill gap, due to growing up in the 'digital era'. However, the research conducted by Kaspersky Labs (2016) states that there is a clear indication that this age group are more inclined to use their cyber skills for factors other than career related motives, such as for hobbies or financial gain. Therefore, here exists a need for this general attitude of the age group to be somehow be altered, in order for them to want to harness their cyber skills to aid law enforcement in the country.

On the same topic, the literature explores the variety of extra-curricular or 'talent specific' education schemes that are in place for the younger generation to take part in in relation to cyber security learning, as well at the Computer Science GCSE subject that was added to the UK curriculum in 2013. However, it can be seen from the relevant literature that a common trend can be seen in all of these education options, that they are indeed optional. There is no mandatory learning currently in place for children in mandatory education. It can be questioned whether this sufficiently ensures that the younger generation will possess the necessary cyber security and cybercrime knowledge to fill the skill gap, as the NCSS (2016) states that it aims for. An agreement that can be seen between the literature and the 'Cybercrime: A Survey of Public Knowledge and Perception' survey here is 92.6% of participants agreed that it would be beneficial to start some form of mandatory basic computer science learning in schools. Moreover, as it can be seen in chapter 4.3.6, the result from a similar question in the expert survey also illustrated all 8 of the participants thought basic computer science skills becoming mandatory in school education instead of optional would help. Therefore, it can be seen here that there is a trend of opinion within the literature, the public survey conducted for this study and the expert survey conducted for this study, that the government is missing a requirement for ensuring that the younger generation is sufficiently knowledgeable in order to protect themselves from cybercrimes, as well as equipping them to fill in the cyber skill shortage gap.

5.4 Aim of the study

The aim of this study was to access whether the complete combined provisions that set out to combat cybercrime in the UK make a genuine attempt in regards to all aspects. First of all, the introduction of digital forensics, a method of evidence collection analysis now used widely today, is an example of a successful application of the leveraging of advancing technology in the policing of cybercrime today. Examples such as this show that law enforcement, as well as cybercriminals, are capable of using technology to their advantage in these regards, but the combined opinions of both the literature and the expert survey respondents state that it is the cybercriminals who are staying 'one step ahead'.

Secondly, if organisations such as the National Cyber Crime Unit and the National Cyber Security Centre only associate their investigative work with cybercrimes that are deemed

of a larger scale, then it can be questioned as to whether the 26 police forces in the UK who do not possess a dedicated cybercrime unit, with specifically trained cyber-specialist officers, are left sufficiently equipped to handle the investigation and damage control of small local cybercrimes. In addition, the literature denotes that cyber training for law enforcement staff is a large expenditure that many forces will not incorporate into their budgets, and therefore this implies that many officers will still be left with a lack of cyber knowledge despite the National Cyber Security Strategy (2016) stating that all those involved in cybercrime policing should have access to at least basic cyber security and computer science knowledge.

Finally, and arguably the most considered aspect of the cybercrime combatting method to be addressed, is the shortcomings of the techniques being applied to the education of the younger generation. The current method in place consists of sourcing and nurturing individuals who have an interest or talent in computer science learning, and giving them sufficient resources to expand on their knowledge and skills; this has the aim of addressing the computer science skill gap in society. However, the method, although potentially effective for its aim, is not inclusive for protecting the younger generation from being victims of cybercrimes themselves. Without any mandatory education being featured in either primary or secondary school in the UK, the only students who will learn basic cyber security skills are those who chose to do so, thus helping to protect them against cybercrimes by the ability of recognising potential threats and combatting them appropriately. These threats could consist of cyber-dependant crimes, such as hacking or sending malware, or they could consist of cyber-enabled crimes that may result in the unknowledgeable child being subject to a crime such as cyber-bullying or cyber-grooming. In the first survey conducted for this study, the ‘Cybercrime: A Survey on Public Perception and Knowledge’ Question 5 (see Chapter 4.2.5) highlighted the opinion that the majority of the public respondents hold that being protected from crimes such as cyber-bullying and cyber-grooming is of ‘high importance’. Therefore, the UK’s strategy should cater more to this factor.

6 Conclusion

The first objective for this study was to gather relevant literature on the evolution of cybercrime, and interpret this literature to be able to understand how aspects of cybercrime have changed as a direct result advancing technology. The literature obtained was sufficient in providing the knowledge that cybercrime has changed in correlation with technological advances, with information on how this has impacted rates of cybercrimes as well as methods for the illicit activities.

In regards to the analysis of how law enforcement agencies in the UK have changed their strategies in accordance with cybercrime rates, the literature obtained successfully informed of the details of changes that have been undertaken since cybercrime was recognised as a national problem. Furthermore, the research in the form of the Freedom of Information requests allowed for interpretation of which police forces in the UK possess cybercrime units, and the budgets that these have been allocated on a yearly basis. This information was useful to establish the structural policing changes that have occurred, but a limitation of the research method was that for the police forces that did not have a dedicated cybercrime unit, no information was acquired. Thus this study does not include the knowledge of how these police forces approach local cybercrime attacks.

Finally, the use of two similar surveys, one catering for public responses and one designed for the responses of people who work within cybercrime in come capacity, allowed for an in-depth analysis of both public perceptions of cybercrimes, and knowledge limits of cybercrime in society. The use of the two different data sets was useful in comparing against literature in terms of deducing if all three data sets share the same views. This was particularly useful in determining whether the expert participants agreed with possible flaws in the UK strategy, such as the lack of mandatory computer science education. However, a limitation to this analysis can be seen in the amount of expert surveys received, as with any non-probability sampling method the reliability of an average view across a population increases with the amount of responses received. In regards to the objective of evaluating cyber security knowledge in the UK, the results from both surveys showed strict similarities with the literature obtained on the topic, with little discrepancies between the two. All three research methods came to the same key conclusion; the cyber skill shortage in the UK should be addressed in terms of promoting education and career options.

To conclude, the four research methods undertaken for this study allowed me to meet the objectives outlined in chapter 1.2, along with determining aspects of the UK cybercrime

combat strategy, that are considered amongst literature, experts and the public as lacking in being suitably thorough in their approach (see Chapter 5.4). Therefore, this dissertation met the objectives and overall aim of the study, but with a view that further work is necessary to more accurately define recommendations of changes to be implemented into the National Cyber Crime Strategy (2016).

6.1 Further work

This study marks the start of a collaborative approach in gathering all of the ways in which cybercrime is being tackled in the UK, but the limitations outlined in Chapter 6 should be addressed by further research in order to strengthen its conclusions. For example, further Freedom of Information requests should be made to the remaining 26 UK police forces, in order to request information on the processes for which they handle a cybercrime attack in their area. The conclusions drawn from the lack of dedicated cybercrime units were speculative in considering if they possess the necessary training, time and resources to effectively investigate small scale cybercrimes. Acquiring this information, therefore, would allow for a more accurate view to be drawn on this matter.

Secondly, by conducting further expert survey response requests, the reliability of the shared views of the experts that are denoted in the results section would increase, allowing for more weight to be placed on their conclusions.

Finally, much of the information in regards to the UK's cybercrime strategy was acquired from the NCSS (2016). This strategy is a governmental plan that is in place up until 2021, at which time analysis will be done to determine its successful and unsuccessful factors. Further research should be conducted to compare these factors with the conclusions drawn in this study, to interpret whether any findings of this study are accurately reflected in the improvements section of their conclusions.

References

Agency, N. C., 2017. *National Cyber Crime Unit.* [Online]
Available at: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit
[Accessed 10 June 2017].

Anon., 2008. [Online]
Available at: https://www.whatdotheyknow.com/
[Accessed October 2016].

Bell, R., 2002. The Prosection of Computer Crime. *Journal of Financial Crime,* 9(4), pp. 308-325.

Ben-Asher, N. & Gonzalez, C., 2015. Effects of cyber security knowledge on attack detection. *Computers in Human Behaviour,* Volume 48, pp. 51-61.

Bocij, P. & McFarlane, L., 2004. Cyberstalking: A Discussion of Legislation and the Perpetrators. *Justice of the Peace,* 168(21), pp. 393-396.

Bowling, B. & Foster, J., 2002. Policing and the Police. In: M. Maguire, R. Morgan & R. Reiner, eds. *The Oxford Handbook of Criminology.* Oxford: Oxford University Press, pp. 910-953.

Brenner, S., 2008. *Cyberthreats: The Emerging Fault Lines of the Nation State.* 1st ed. New York: Oxford University Press .

Britz, M., 2004. *Computer Forensics and Cybercrime: An introduction.* 1st ed. New Jersey: Prentice Hall Press.

Broadhurst, R., 2006. Developments in the globa law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies and Management,* 29(3), pp. 408-433.

Brown, C., 2015. Investigating and Prosecuting Cyber Crime: Forensic Depenencies and Barriers to Justice. *Internation Journal of Cyber Criminology,* 9(1), pp. 55-119.

Bryman, A., 2012. *Social research methods.* 5th ed. Oxford: Oxford University Press.

Byrant, R. & Byrant, S., 2014. *Policing Digital Crime.* 1st ed. Abingdon: Routledge.

Casey, E., 2011. *Digital Evidence and Computer Crime Forensic Science.* 2nd ed. Salt Lake City: Academic Press.

Castells, M., 2002. *The Internet Galaxy: Reflections on the Internet, Business, and Society.* illustrated ed. Oxford: Oxford University Press.

Center, B. P., 2014. *Today's rising terrorist threat and the danger to the United States: Reflections on the tenth anniversary of the 9/l I Commission report,* Washington: Homeland Security.

Chaabane, A., Manils, P. & Kafaar, M., 2010. *Digging into Anonymous Traffic: A Deep Analysis of the Tor Anonymizing Network.* Melbourne, 2010 4th International Conference on Network and System Security (NSS.

Clancy, T. K., 2011. *Cyber Crime and Digital Evidence: Materials and Cases.* 1st ed. New York: Matthew Bender & Company, Inc.

Clapper, J., 2013. *Worldwide threat assessment of the US intelligence community,* Washington: Senate Select Committee on Intelligence.

Clough, J., 2012. The Council of European Convention on Cyber Crime: Defining 'crime' in a digital world. *Criminal Law Forum,* 23(4), pp. 363-391.

Clough, J., 2015. *Principles of Cybercrime.* 2nd ed. Cambridge: Cambridge University Press.

Cohen, L. & Felson, M., 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review,* Volume 44, pp. 588-589.

Collis, J. & Hussey, H., 2009. *Business Research: A practical guide for undergraduate & postgraduate students.* 3rd ed. Basingstoke: Palgrave Macmillan.

Congress, U. S., 2005. United Nations Convention Against Transnational Organized Crime. *Executive Report,* 109(4), pp. 108-116.

Consulting, P., 2014. *Cyber Crime Tipping Point: Survey Results,* London: s.n.

Crede, A., 1995. Electronic Commerce and the Banking Industry: The Requirement and Opportunities for New Payment Systems Using the Internet. *Journal of Computer-mediated Communication,* 1(3).

Cresswell, J., 2014. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches.* London: SAGE Publications.

Crime, U. N. O. o. D. a., 2013. *Comphrensive Study on Cybercrime ,* Vienna: United Nations.

Critcher, 2003. *Moral Panics and the Media.* 1st ed. Buckingham: Open University Press.

Csonka, P., 2005. The Council of Europe Convention on cybercrime: a reponse to the challenge of the new age?. In: R. Broadhurst & P. Gabrosky, eds. *Cybercrime: The Challenge in Asia.* Hong Kong: University of Hong Kong Press, pp. 303-326.

Cyberinsurance as a market-based solution to the problem of cybersecurity - a case study (2017) Kesan, J; Majuca, R; Yurcik, W.

Dantzker, M., Hunter, R. D. & Quinn, S., 2016. *Research Methods for Criminology and Criminal Justice.* 4th ed. Burlington: Jones & Bartlett Learning.

Davies, M. & Patel, M., 2016. *Are we managing the risk of sharing Cyber Situational Awareness? A UK public sector case study.* [Online]
Available at:
http://ieeexplore.ieee.org.libezproxy.bournemouth.ac.uk/document/7503292/?reload=true&

part=1
[Accessed 1 June 2017].

Dowland, P., Furnell, S., Illingworth, H. & Reynolds, P., 1999. Computer Crime andAbuse: A Survey of Public Attitudes and Awareness. *Computers and Security,* 18(8), pp. 715-726.

Edwards, L., Rauhofer, J. & Yar, M., 2010. Recent developments in UK cybercrime law. In: Y. Jewkes & M. Yar, eds. *Handbook of Internet Crime* . Cullompton: Willan, pp. 413-436.

Essays, U., 2013. *Explanation Of The Concept Of Research Onion Psychology Essay.* [Online]
Available at: https://www.ukessays.com/essays/psychology/explanation-of-the-concept-of-research-onion-psychology-essay.php?cref=1
[Accessed 12 June 2017].

Feilzer, M. Y., 2010. Doing mixed methods research pragmatically: Implications for the rediscovery of pragmatism as a research paradigm. *Journal of Mixed Methods Research,* 4(1), pp. 6-16.

Field, A., 2013. *Discovering Statistics Using IBM SPSS Statistics.* 4 ed. London: Sage.

Fisher, P., 2016. *Cyber Skills Shortage - Market InSight - Worldwide,* London: PAC Online.

Flick, U., 2011. *Introducing research methodology: A beginner's guide to doing a research project.* London: Sage.

Franke, U. & Brynielsson, J., 2014. Cyber situational awareness - a systematic review of the literature. *Computer Security,* Volume 46, p. 41.

Furnell, S. & Moore, L., 2014. Security literacy: the missing link in today's online society?. *Computer Fraud and Security,* 2014(5), pp. 12-18.

Gable, K., 2010. Cyber-apocalypse now: Securing the Internet against cyhertcrrorism and using universal jurisdiction as a deterren. *Vanderbilt Journal of Transnational Law,* 43(57), pp. 76-88.

Gast, M., 2005. *802.11 Wireless Networks: The Definitive Guide.* illustrated ed. California: O'Reilly Media, Inc.

Gibson, W., 1984. *Neuromancer.* 1st ed. New York: Ace Books.

Gideon, L., 2012. *Handbook of Survey Methodology for the Social Sciences.* 1st ed. London: Springer Science & Business Media.

Goddard, W. & Melville, S., 2004. *Research Methodology: An Introduction.* 2nd ed. Oxford: Blackwell Publishing.

Goode, E. & Ben-Yehuda, N., 1994. *Moral Panics: The Social Construction of Deviance.* 2nd ed. Oxford: Blackwell.

Goodman, M. & Brenner, S., 2002. The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology,* 10(2), pp. 139-223.

Goodman, M. & Brenner, S., 2002. The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law Information Technology,* 10(2), p. 139.

Grabosky, 2001. Virtual Criminality: Old Wine in New Bottles?. *Social and Legal Studies,* Issue 10, pp. 243-249.

Graceful, H., 2016. *UK Cyber Crime Law.* [Online]
Available at: https://www.gracefulsecurity.com/uk-cyber-crime-law/
[Accessed 10 June 2017].

Gummer, B., 2016. *National Cyber Security Strategy 2016-2021,* London: HM Government.

Herdale, G., 2014. *New cyber crime training is already leading to arrests.* [Online]
Available at: http://www.college.police.uk/News/archive/2014jul/Pages/New-cyber-crime-training-is-already-leading-to-arrests.aspx
[Accessed 15 May 2017].

HMG, 2016. *National Cyber Security Strategy 2016 to 2021.* [Online]
Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
[Accessed 10 May 2017].

HMG-DBIS, 2016. *Post-16 Skills Plan,* London: HMG Department for Business, Innovation and Skills.

HMG-DE, 2013. *Department for EducatioNational Curriculum in England: computing programmes of study,* London: HMG Department for Education.

Holden, M. T. & Lynch, P., 2014. *Choose the Appropriate Methodology and Understanding Research Philosophy.* Waterford: Waterford Institute of Technology.

Holt, T., Bossler, A. & Seigfried-Spellar, K., 2015. *Cybercrime and Digital Forensics: An Introduction.* 3rd ed. London: Routledge.

Hopkins, S., 2003. Cybercrime Convention: A Positive Beginning to a Long Road Ahead. *Journal of High Technology Law,* Volume 2, pp. 101-121.

In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Trap & Trace Device on E-Mail Account (2006) Sagan, Dr Carl.

InternetLiveStats, 2016. *Internet users in the world.* [Online]
Available at: http://www.internetlivestats.com/internet-users/
[Accessed 10 June 2017].

Jackson, M., 2000. Keeping Secrets: International Developments to Protect Undisclosed Business Information and Trade Secrets. In: D. Thomas & B. Loader, eds. *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age.* London: Routledge, pp. 153-173.

Jewkes, Y., 2015. *Key Approaches to Criminology: Media and Crime.* 3rd ed. California: Sage.

Khanna, R., 2017. *Bridging the cyber skills gap.* [Online]
Available at: http://www.thecsuite.co.uk/cio/security-cio/bridging-the-cyber-skills-gap/
[Accessed 15 May 2017].

King, Adam & Thomas, j., 2009. You Can't Cheat an Honest Man: Making ($$$s and) Sense of the Nigerian E-Mail Scams.'' Pp. 206–224 in Crimes of the Internet. In: F. Schmalleger & M. Pittaro, eds. *Crimes of the Internet.* New Jersey: Prentice Hall, pp. 206-224.

Kinney, S., 2006. *Trusted Platform Module Basics: Using TPM in Embedded Systems.* 1st ed. Oxford: Newnes .

Klahr, R. et al., 2017. *Cyber Security Breaches Survey,* London: HM Department for Culture, Media and Sport.

Kothari, C. R., 2004. *Research methodology: methods and techniques.* New Delhi: New Age International.

Kritzinger, E., Bada, M. & Nurse, J., 2017. *A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK,* Oxford: Oxford University Press.

Labs, K., 2016. *Kaspersky Lab Raises Alarm Over Critical Cybersecurity Skills Shortage, Says Youth can Bridge Gap - if Industry Lets it.* [Online]
Available at: http://www.prnewswire.com/news-releases/kaspersky-lab-raises-alarm-over-critical-cybersecurity-skills-shortage-says-youth-can-bridge-gap---if-industry-lets-it-598864161.html
[Accessed 21 May 2017].

Lewis, A., 1971. *New York Times,* 15 March, p. 37.

Macdonald, N., 2015. *Cyber Security : The Law Enforcement Skills Shortage.* [Online]
Available at: https://bucsu.bournemouth.ac.uk/blog/2015/february/11/cyber-security-the-skills-gap/
[Accessed 05 June 2017].

Majid, Y., 2013. *Cybercrime and Society.* 2nd ed. California: Sage.

May, T., 2011. *Social research: Issues, methods and research.* London: McGraw-Hill International.

Mcknight, G., 1973. *Computer Crime.* 1st ed. London: Joseph.

Milhorn, T., 2007. *Cybercrime: How to Avoid Becoming a Victim.* 1st ed. Florida: Universal.

Mitnick, K. & Simon, W., 2011. *The Art of Deception: Controlling the Human Element of Security.* 1st ed. New Jersey: John Wiley & Sons.

Morgan, L., 2016. *List of data breaches and cyber attacks in 2016* , Cambridge: IT Governance.

Morris, S., 2004. *The Future of Netcrime Now: Part 1 - Threats and Challenges* , London: Home Office .

Newman, G. & Clark, R., 2003. *Superhighway Robbery: Preventing e-commerce Crime.* illustrated ed. Cullompton: Willan Press.

O'Connor, V., 2012. *Common Law and Civil Law Traditions.* [Online]
Available at:
https://www.fjc.gov/sites/default/files/2015/Common%20and%20Civil%20Law%20Traditions.pdf
[Accessed 15 May 2017].

Oppenheim, A., 2000. *Questionnaire Design, Interviewing and Attitude Measurement.* London: Bloomsbury Publishing.

Orman, H., 2003. The Morris worm: a fifteen-year perspective. *IEEE Security & Privacy* , 99(5), pp. 35-43.

Saunders, M., Lewis, P. & Thornhill, A., 2007. *Research Methods for Business Students.* 6th ed. London: Pearson.

Scott, L., 2015. *ARCOM Doctoral Workshop Research Methodology.* Dublin, Dublin Institute of Technology .

Shields, R., 1996. *Cultures of the Internet: Virtual Spaces, Real Histories, Living Bodies.* London : Sage.

Shinder, D. & Cross, M., 2008. *Scenes of the Cybercrime.* 2nd ed. Massachusett: Syngress.

Sieber, U., 1998. *Legal aspects of computer-related crime in the information society, COMCRIME Study,* s.l.: European Commission .

Silverman, D., 2013. *Doing Qualitative Research: A practical handbook.* London: Sage.

Smith, F., 2010. The Development of Cybercrime. In: R. Lincoln & S. Robinson, eds. *Crime over time: Temporal perspectives on crime and punishment in Australia.* Newcastle upon Tyne: Cambridge Scholars Publishing, p. 214.

Smith, G., 2015. Management models for international cybercrime. *Journal of Financial Crime,* 22(1), pp. 104-125.

Smith, L., Smith, K. & Blazka, M., 2017. Follow Me, What's the Harm? Considerations of Catfishing and Utilizing Fake Online Personas on Social Media. *Journal of Legal Aspects of Sport,* 27(1), pp. 32-45.

Snyder, F., 2001. Sites of Criminality and Sites of Governance. *Social and Legal Studies,* Issue 10, pp. 251-256.

Spiller, N., 2002. *Cyber reader : critical writings for the digital era.* London: Phaidon.

Statistics, O. f. N., 2016. *Internet access – households and individuals: 2016,* London: Office for National Statistics .

Teddlie, C. & Tashakkori, A., 2009. *Foundations of Mixed Methods Research.* 1st ed. London: Sage Publications.

Thomas, D. & Loader, B., 2000. *Cybercrime: Law Enforcement, Security andSurveillance in the Information Age.* 1st ed. London: Routledge.

Trochim, W., 2002. *Research Methods Knowledge Base.* [Online]
Available at: http://www.anatomyfacts.com/research/researchmethodsknowledgebase.pdf
[Accessed 6 June 2017].

Turkle, S., 1995. *Life on the Screen: Identity in the Age of the Internet.* New York: Simon and Schuster.

Union, I. T., 2005. *Internet Reports: Internet of Things,* Geneva: International Telecommunication Union.

Urbas, G. & Choo, K., 2008. Resource materials on technology-enabled crime. *Technical and Background Paper,* Volume 28, p. 5.

Wall, D., 2007. *Cybercrime: The transformation of crime in the information oge.* 1st ed. Cambridge: Polity.

Webber, C. & Vass, J., 2010. Inside the Matrix: Representations of the Internet in Cinema. In: *Handbook on Internet Crime.* Devon: Willan, pp. 139-140.

Webster, F., 2003. *Theories of the Information Society.* 2nd ed. London : Routledge.

Wiles, J. & Reyes, A., 2007. *The Best Damn Cybercrime and Digital Forensics Book Period.* 1st ed. Massachusetts: Syngress.

Wiles, R. C. G. &. P. H., 2011. Innovation in qualitative research methods: a narrative review. In: 5, ed. *Qualitative Research.* s.l.:11, pp. 587-604.

Williams, C., 2007. Research Methods. *Journal of Business & Economic Research,* 5(3), pp. 63-71.

Wilson, C., 2005. *Computer attack and cyberterrorism: Vulnerabilities and policy issues for Congress,* Washington: Congressional Research Service.

Wilson, I., 2014. Cyber Threats to Critical Information Infrastructure. In: T. Chen, L. Jarvis & S. Macdonald, eds. *Cyberterrorism: Understanding, assessment and reponse.* New York: Springer, pp. 123-136.

Woollaston, V., 2017. *Security form 'confident' the WannaCry attack was caused by the Lazarus group.* [Online]
Available at: http://www.wired.co.uk/article/nhs-cyberattack-ransomware-security
[Accessed 25 May 2017].

Wykes, M. & Harcus, D., 2013. Cyber Terror: Construction, Criminilisation and Control. In: *Handbook of Internet Crime.* Abingdon: Routledge, pp. 214-227.

Yang, C. et al., 2012. *Analyzing spammers' social networks for fun and profit: a case study of cyber criminal ecosystem on twitter.* Lyon, ACM.

Yar, M., 2014. *Virtual Utopias and Dystopias: The Cultural Imaginary of the Internet.* Basingstoke: Palgrave Macmillan.

Zimmerman, P., 1995. *The official PGP user's guide.* 1st ed. Massachusetts: MIT Press .

Appendices

Appendix 1: Evaluative supplement

This section will look back over this Independent Research Project (IRP) upon completion, considering it being the largest and most complex piece of literature that I have produced to date. It will aim to not only specify the projects strengths and weaknesses, but also to highlight the knowledge and skills I have been able to obtain by completing it.

The main aim of this dissertation was to either identify flaws in the UK's cybercrime policing strategy, or to prove that no significant flaws are considered to exist amongst both literature and societal opinions. I am of the view that the research completed allowed for specific flaws to be identified by each of the four research methods (literature review, Freedom of Information requests, public survey and expert survey). However, although each of the research techniques produced some corresponding results, the literature review clarified the broadness of the topic, meaning that I was not able to consider each factor of policing in one project. In addition, in an attempt to consider the broad topic a more than usual amount of research had to be produced for one IRP, resulting in a difficulty of combining all of the results within the text allowance.

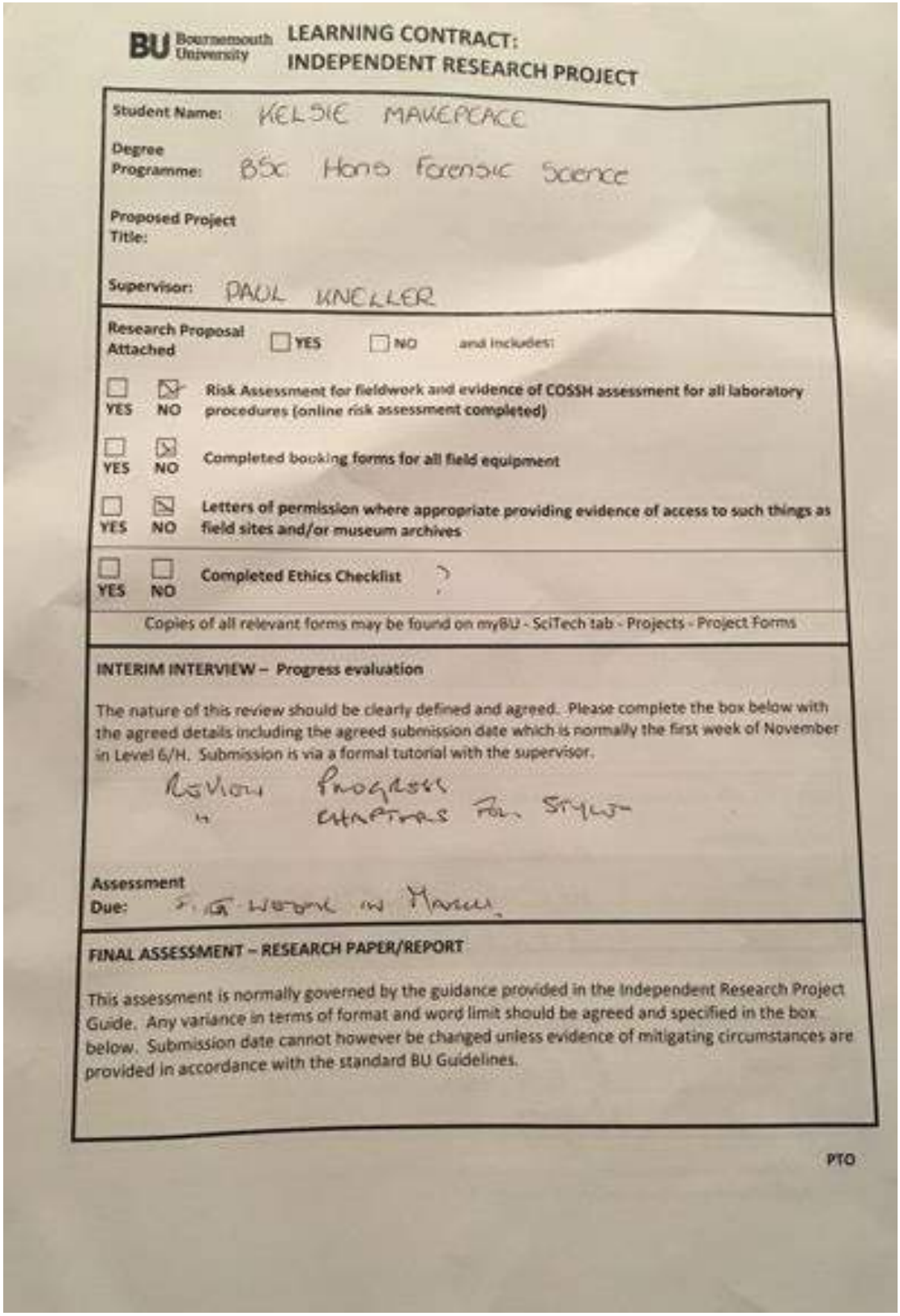
I have always had a keen interest in cybercrime, but with no prior computing education behind me, I chose to study the Forensic Law and Practice module in my second year of university, as oppose to Forensic Computing. Although I do not regret this decision, it became apparent to me quickly during the process of planning this dissertation that my lack of cybercrime knowledge could hinder my writing. Therefore, a weakness to this project was that a considerable amount of background research and learning had to be undertaken in order for me to effectively produce this piece of work. However, I believe positive aspects to this factor can be seen in that I was effectively challenge, and also able to take on the project with a completely fresh and unbiased viewpoint, something I may not have been able to do if prior education had been undertaken.

During my undergraduate 12 month placement with IBM in 2015, I was fortunate to obtain knowledge on analytical techniques such as SPSS, meaning that this project allowed for me to refine and expand on this skill. Similarly, having completed literature work on a

smaller scale, I was able to develop my online search tool techniques as well as my academic, critical and evaluative writing capabilities. Alternatively, having never created and distributed a survey before, this work meant I was able to learn how to consider suitable questions and actively market the surveys to the desirable participants. Therefore, this project has allowed me to advance my skills considerably; this will be very valuable when concerning my future career.

This project has developed my cybercrime and computer science knowledge immensely, as well as informing the readers of the factors of the UK's cyber policing methods that have flaws in the opinions of literature, experts and the public. Although it only attempts to address a broad topic, it could provide a basis for comparison when the report of the National Cyber Security Strategy 2016-2021 conclusions is released, to answer whether or not the perceived flaws are addressed in the results.

Appendix 2: Learning contract



BU Bournemouth University **LEARNING CONTRACT: INDEPENDENT RESEARCH PROJECT**

Student Name: KELSIE MAKEPEACE

Degree Programme: BSc Hons Forensic Science

Proposed Project Title:

Supervisor: PAUL UNELLER

Research Proposal Attached ☐ YES ☐ NO and includes:

☐ YES ☒ NO **Risk Assessment for fieldwork and evidence of COSSH assessment for all laboratory procedures (online risk assessment completed)**

☐ YES ☒ NO **Completed booking forms for all field equipment**

☐ YES ☒ NO **Letters of permission where appropriate providing evidence of access to such things as field sites and/or museum archives**

☐ YES ☐ NO **Completed Ethics Checklist** ?

Copies of all relevant forms may be found on myBU - SciTech tab - Projects - Project Forms

INTERIM INTERVIEW – Progress evaluation

The nature of this review should be clearly defined and agreed. Please complete the box below with the agreed details including the agreed submission date which is normally the first week of November in Level 6/H. Submission is via a formal tutorial with the supervisor.

Review Progress Chapters for Style

Assessment Due: F.G Work in March

FINAL ASSESSMENT – RESEARCH PAPER/REPORT

This assessment is normally governed by the guidance provided in the Independent Research Project Guide. Any variance in terms of format and word limit should be agreed and specified in the box below. Submission date cannot however be changed unless evidence of mitigating circumstances are provided in accordance with the standard BU Guidelines.

PTO

As the student undertaking the above project I agree to:

- E-mail my supervisor on a fortnightly basis with a progress report
- Meet with my supervisor at least once a month to discuss progress and I understand that it is my responsibility to organise these meetings
- Comply with the terms of this learning contract and the guidance set out in the Guide to Independent Research Projects
- I understand that this is an *independent* project and that I am solely responsible for its completion
- I agree to comply with all laboratory and fieldwork protocols established by the Faculty.

As the supervisor of this project I agree to:

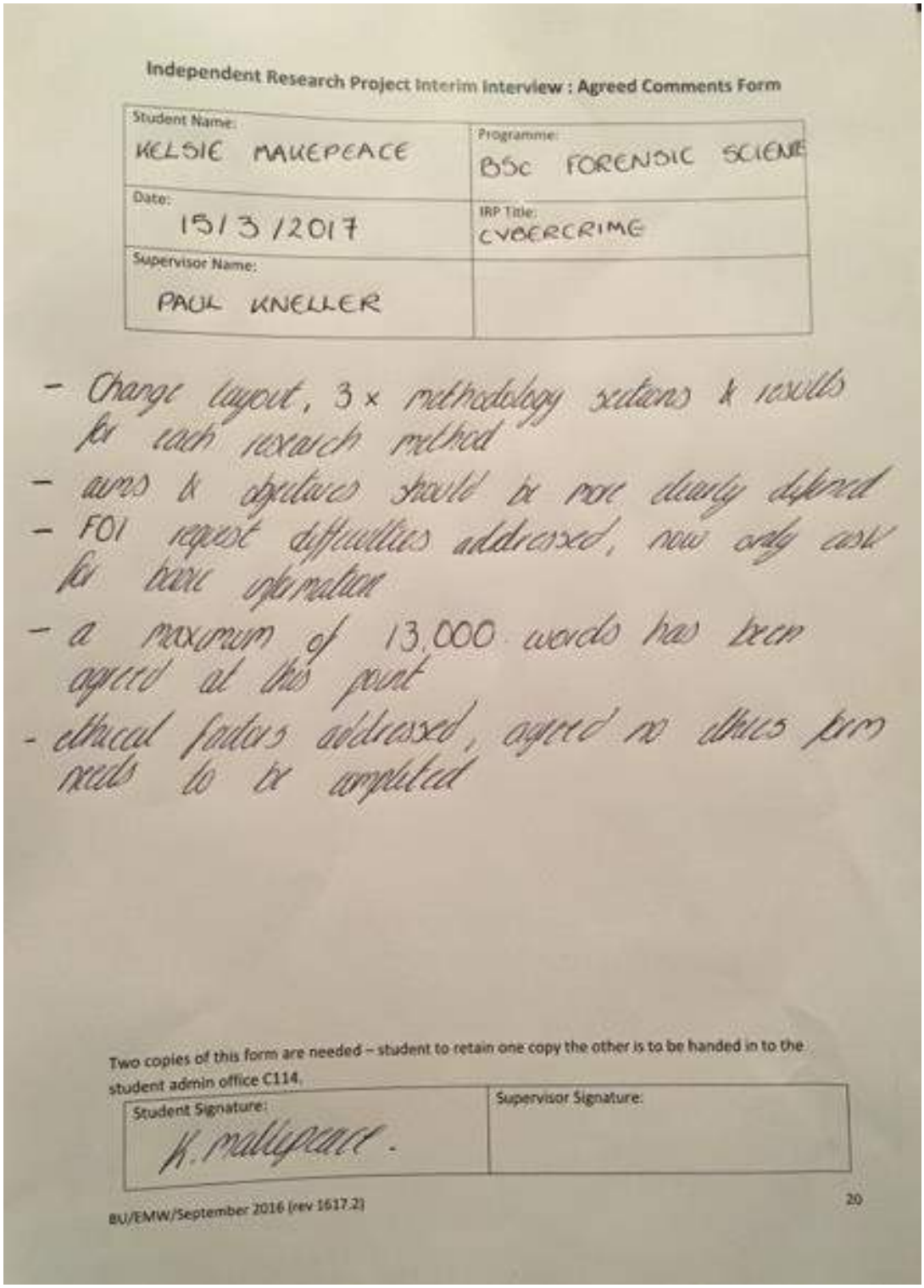
- Meet with the student undertaking this project on at least a monthly basis and to respond to the progress e-mails as appropriate
- To meet formally with the student during the first week in November to undertake the interim interview
- To provide guidance and support to the student undertaking this project bearing in mind that it is an *independent* research project. This is inclusive of commenting on drafts of the final report in a timely fashion.

Both of the undersigned parties agree to be bound by this learning contract:	
Student Signature:	K. Makepeace
PRINT NAME:	KELSIE MAKEPEACE
Date:	1/2/17

Supervisor Signature:	
PRINT NAME:	P. E KNOWLES
Date:	1/2/17.

When completed, this form should be handed in to SciTech Admin (C114) and a copy retained by the student to be included in an appendix to the final IRP document

Appendix 3: Interim review



Independent Research Project Interim Interview : Agreed Comments Form

Student Name: KELSIE MAKEPEACE	Programme: BSc FORENSIC SCIENCE
Date: 15/3/2017	IRP Title: CYBERCRIME
Supervisor Name: PAUL KNELLER	

- Change layout, 3 x methodology sections & results for each research method
- aims & objectives should be more clearly defined
- FOI request difficulties addressed, now only ask for basic information
- a maximum of 13,000 words has been agreed at this point
- ethical factors addressed, agreed no ethics form needs to be completed

Two copies of this form are needed – student to retain one copy the other is to be handed in to the student admin office C114.

Student Signature: K. Makepeace.	Supervisor Signature:

BU/EMW/September 2016 (rev 1617.2) 20

Appendix 4: Search terms

Key word/phrases searched	Number of sources used directly from search	Chapter
Digital era	2	2, 2.1
Cybercrime	8	2, 2.1, 2.1.1, 2.3, 2.3.3
Hacking	2	2.1, 2.1.1, 2.1.2, 2.2.2
Computer science	1	2.3.3
National Cyber Security Strategy	2	2, 2.3.3, 2.3.2, 2.2.4
Media influence on cybercrime	8	2.1.4
Cyberspace	3	2.1, 2.1.1
Internet Statistics	4	2.1.3, 2.1.1, 2.3.2, 2.3.3
Curador	3	2.1.1
Internet history	3	2.1.1, 2.1.3
Online environments	4	2.1.2, 2.2.3
Catfishing	1	2.1.2
Evolution of cybercrime	12	2.1.3, 2.1.4
Predatory crime	2	2.1.3, 2.3.3
Cybercrime policing	6	2.2, 2.2.1, 2.2.2, 2.2.3
International cooperation cyber	1	2.2.3
Cybercrime legislation	2	2.2.2
Cyberterrorism	1	2.2.2
Policing challenges cybercrime	3	2.2.3
Digital forensics	1	2.2.3
Cyber skills shortage	3	2.3, 2.3.1, 2.3.2, 2.3.3
College of Policing	1	2.3.1
Cyber security in industry	2	2.3.2
Cybercrime in education	2	2.3.3

Appendix 5: Surveys

1 What is your age?

- ◯ 16 to 24
- ◯ 25 to 34
- ◯ 35 to 44
- ◯ 45 to 64
- ◯ 65 or older

2 What is your gender?

- ◯ Female
- ◯ Male
- ◯ Prefer not to say
- ◯ Other (please specify)

3 How many internet-enabled devices do you own?

- ◯ 0
- ◯ 1
- ◯ 2
- ◯ 3
- ◯ 4
- ◯ 5 or more

4 Have you, or has anyone that you know personally, ever experienced a cybercrime? (e.g., receiving a phishing or spam email, hacking of an online account, internet trolling or harassment, online fraud, cyberbullying etc)

- ◯ Yes, definitely
- ◯ Yes, possibly
- ◯ No, I do not think so
- ◯ No, definitely not

5 How would you rank the seriousness of the following experiences?

	Not serious at all	Moderately serious	Serious	Very serious
Unknowingly opening a malicious email/website, resulting in a virus being installed onto your computer and damaging/destroying data files	○	○	○	○
Being a victim to online grooming, harassment or bullying	○	○	○	○
Accounts being opened and online purchases being made in your name	○	○	○	○
Your online banking username and passwords being compromised (hacked into)	○	○	○	○

6 If you have any knowledge on cybercrime, such as how any of them are conducted or ways in which to protect yourself from them, where did you access this knowledge? (please tick one or more)

- ☐ Through mandatory education (primary and secondary school)
- ☐ Through voluntary education (college/sixth form/university)
- ☐ Place of work
- ☐ Voluntary research
- ☐ Local police force's website
- ☐ Government's website
- ☐ I have little/no knowledge

7 To what extent would you rank your knowledge on the following areas?

	No knowledge	Moderate knowledge	Good knowledge	Strong knowledge
I could correctly define the differences between the surface web, the deep web and the dark web	○	○	○	○
I am aware of the Tor encryption tool, and understand how it enables both sources of	○	○	○	○

websites and visitors of websites to remain anonymous				
I know what Bitcoin is and how it differs from normal currency to make it more desirable for users of the dark web	○	○	○	○

8 How much do you agree with the following statements?

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Cybercrime is a growing problem in the UK	○	○	○	○	○
I can tell a phishing/spam email apart from a legit one	○	○	○	○	○
I know where to look for cybercrime information	○	○	○	○	○
I have sufficient knowledge of cybercrime so I am unlikely to be a victim	○	○	○	○	○
The more cybercrime knowledge I possess, the less vulnerable I am to being a potential victim	○	○	○	○	○
It is the government's responsibility to provide this knowledge to UK citizens	○	○	○	○	○

9 Considering the ever growing rate of technology use in society, how much would you agree with how beneficial it would be to start mandatory basic computer science learning in schools?

- ○ Strongly disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly agree

Cybercrime: A Survey on Expert Opinion

1. **Welcome**

To give you a bit of background as to the reason why I am conducting this survey - I am currently undertaking an independent research project that will go towards my BSc Hons Forensic Science degree at Bournemouth University. The study aims to compare the role that ever advancing technology has played in both the evolution of cybercrime and the policing strategies that are used to combat it. The results from this particular survey will be used to give an indication of the opinions of people who possess job roles that require computer science or cybercrime knowledge in some aspect.

The survey should only take around 5 minutes. I really appreciate you taking the time to complete this survey; it will provide me with very useful information for my dissertation research.

Thank you.

Kelsie Makepeace

Please note - the questions in this survey have been approved by my supervisor, Paul Kneller. If you have any problems with the questions, or would like further information on the use, please feel free to contact either myself on i7258355@bournemouth.ac.uk, or Paul on pkneller@bournemouth.ac.uk

1 What is your full name?

2 What is your age?

- ○ 18-24
- ○ 25-34
- ○ 35-44
- ○ 45-60
- ○ 61 or above

3 What is your current occupation and company?

4 The government's National Cyber Security Strategy 2016 makes the following statements, to what extent do you agree?

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
There is a lack of computer science expertise in current society	○	○	○	○	○
Cyber criminals are one step ahead and our strategies for combatting the crimes have so far not kept pace	○	○	○	○	○
Almost all successful cyber-attacks have a contributing human factor	○	○	○	○	○

5 Crime reports show that even though reports of cybercrime to police forces is increasing, the amount that result in a judicial outcome has stayed consistent at 17%. Considering this, how strongly would you agree with the following statements?

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
There is a need for better international cooperation between policing bodies in terms of law and the exchange of information	○	○	○	○	○
Lack of training for the use of computer forensics within policing bodies is a problem in terms of how to leverage the use of them in court compared to traditional forensic evidence	○	○	○	○	○
Lack of citizen knowledge on cybercrime is a problem due to an inability to accurately literate facts of a case when reporting it	○	○	○	○	○

6 In a recent City of London Police report, they estimated that 1.5million cybercrimes were not reported during 2014-2015, costing industries approximately £12billion in total. These crimes not being reported means the accurate scope of the issue cannot be determined. With what importance would you rank the following factors in this?

	Low importance	Moderate importance	High importance
Lack of computing knowledge in the industry sector (i.e., employees being unaware of security breaches)	○	○	○
Companies prioritising their reputation	○	○	○
Lack of confidence in a judicial outcome	○	○	○

7 The College of Policing has taken steps to ensure cybercrime is a core aspect of any investigators knowledge by introducing its 'mainstream cyber-crime' training course. However, police forces are not bound by this and can opt out of the course. Considering this, how strongly do you agree with the following statements?

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
The course should be mandatory; the college of policing has correctly identified the need for all investigators to possess basic computer science knowledge	○	○	○	○	○
It would be less necessary for officers to complete this course if they had gained basic computer science knowledge during their school education	○	○	○	○	○
Only investigators who work specifically in a cybercrime unit should be required to complete the course	○	○	○	○	○

8 When considering the statement that there is a cyber skills shortage in society, to what extent would you agree that these things would help?

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Basic computer science skills being integrated into mandatory school education, as well as having the current optional computer science GCSE for more advanced learning if desired	○	○	○	○	○
Current ICT teachers having computer science training available to them so that they feel better equipped to teach the students about cyber crime	○	○	○	○	○
A clearer route existing from school education, to university degree courses, and finally to related job opportunities, in order to be able to promote a	○	○	○	○	○

9 The government plans to invest in technologies like Trusted Platform Modules (TPM) and emerging industry standards such as Fast Identity Online (FIDO), which do not rely on passwords for user authentication, but use the machine and other devices in the users possession to authenticate. To what extent do you think these technologies would be suitable in your place of work?

- ○ Definitely not suitable
- ○ Possibly suitable
- ○ Definitely suitable

Appendix 6: Freedom of Information request example

Kelsie Makepeace 5 May 2017 Delivered

Dear Northamptonshire Police,

I was hoping you would please be able to help me with some information that I require for my university independent research project.
I am researching into how the increase of cyber crime rates has influenced budgets given to the cyber crime/security units within different public bodies. Therefore, please can you inform me, where possible, what the budget has been for this unit within your organisation annually from 2006 onwards? In addition, if this budget has been used for anything substantial that year (for example the addition of a high tech crime lab or a specific cyber crime project etc) please could this information be included?
Thank you for your help, it is very much appreciated.

Yours faithfully,

Kelsie Makepeace

Appendix 7: ‘Meningitis Now’ payment

← Reply ≪ Reply all → Forward Archive Delete Set flag ...

MN Meningitis Now
22:27

Recent Donation
To: kelsiemakepeace@outlook.com

Meningitis Now

Thank you for your recent donation of £14.20.

The reference number for this donation is 18131.

The bank reference is AuthCode: 467579.

GIFT AID
Please note that if you have requested this be treated as a gift aid donation then you must pay an amount of Income Tax and/or Capital Gains Tax for each tax year (6 April one year to 5 April the next) that is at least equal to the amount of tax that the charity will reclaim on your gifts for that tax year.

Tax claimed by the charity
The charity will reclaim 28p of tax on every £1 you gave up to 5 April 2008.
The charity will reclaim 25p of tax on every £1 you give on or after 6 April 2008.
The Government will pay to the charity an additional 3p on every £1 you give between 6 April 2008 and 5 April 2011.
This transitional relief for the charity or CASC does not affect your personal tax position.
If you pay income tax at the higher rate, you must include all your Gift Aid donations on your Self Assessment tax return if you want to receive the additional tax relief due to you.

Please notify the charity if you:
1. Want to cancel this declaration.
2. Change your name or home address.
3. No longer pay sufficient tax on your income and/or capital gains.
4. Would like to stop future pledged donations.

saving lives, rebuilding futures
www.MeningitisNow.org
twitter: @MeningitisNow
facebook: facebook.com/MeningitisNow
health unlocked: /meningitisnow
Fern House, Bath Road, Stroud, Gloucestershire GL5 3TJ