Policing the Cyber Threat

Exploring the threat from Cyber Crime and the ability of local Law Enforcement to respond

Matthew Hull
Computer Science Department
University of Chester
United Kingdom
1327982@chester.ac.uk

Thaddeus Eze
Computer Science Department
University of Chester
United Kingdom
t.eze@chester.ac.uk

Lee Speakman
Computer Science Department
University of Chester
United Kingdom
l.speakman@chester.ac.uk

Abstract - The landscape in which UK policing operates today is a dynamic one, and growing threats such as the proliferation of cyber crime are increasing the demand on police resources. The response to cyber crime by national and regional law enforcement agencies has been robust, with significant investment in mitigating against, and tackling cyber threats. However, at a local level, police forces have to deal with an unknown demand, whilst trying to come to terms with new crime types, terminology and criminal techniques which are far from traditional. This paper looks to identify the demand from cyber crime in one police force in the United Kingdom, and whether there is consistency in the recording of crime. As well as this, it looks to understand whether the force can deal with cyber crime from the point of view of the Police Officers and Police Staff in the organisation.

Keywords – Cyber; Police; Crime; cyber crime; cyber policing

I. INTRODUCTION

The true scale and impact of cyber crime is an unknown due to issues in how it is reported and the lack of awareness about cyber threats and cyber security.

In 2015, Her Majesty's Inspectorate of Constabulary (HMIC) said that:

"Those who commit digital crime create victims. Those victims demand and deserve the support and help of the police, as much as any other victim of crime"

Traditional crime and criminal behaviour is moving away from the physical world where the associated risks are greater as UK Policing has become adept at tackling such criminality. Crime is moving online where it is easier to commit offences on much greater scale, with greater ease and a reduced risk of being caught. Furthermore, the cost of launching a large online criminal campaign, such as the distribution of ransomware, is considerably lower than the potential return [1]. Thus, cyber crime can be committed on an unprecedented scale.

It is easy for people to become engaged in cyber criminality from an early age, drawn in by the challenge and thrill of low level criminality and the apparent lack of an authoritative presence online [2]. They are also able to take advantage of cheap, and sometimes free, easy to use tools and techniques to aid their activities which are seen as 'cool'. Cyber crime 'as-a-service', the ability to hire or purchase tools or services which allow individuals with little to no technical experience to conduct sophisticated cyber-attacks, has also had a significant impact on the scale of cyber crime [3].

The research for this paper was initially produced to support the ongoing work being conducted within UK Policing in order to inform best practice, identify risks and identify opportunities to build upon the current strategic response to the cyber threat. Furthermore, it sought to improve cybersecurity practices. Cybersecurity is not simply about the technical ability of individuals or organisations, but is more often focused on simple advice and preventative measures. It is a key role of the police to provide such advice, and investigate instances where cyber security has failed. Cyber-attacks are crimes, and ultimately require investigating. Policing has to move from a traditional 'analogue' approach to crime investigation to tackle the digital threats that are growing in severity and frequency.

The data for this research is drawn from previous literature, a review of crime statistics and a survey of police officers and police staff in one of the 43 police forces in England, Wales and Northern Ireland. The aim of this study is to improve the way in which local police forces can build their capabilities around cyber crime prevention and investigation by identifying issues which may be acting as a blocker.

A. Defining Cyber crime

A question which sparks considerable debate, and has done for some time, is 'What is cyber crime?' One reason for the underreporting of cyber crime is because people simply do not understand what it is [4]. It is not difficult to see why this is the case when one considers the lack of clarity and consistency when it comes to defining cyber crime.

Some commentators suggest that cyber crime is nothing more than traditional crime committed in a different way. In 2001 Grabosky said that it is *'...less a question of something completely different than a recognisable crime committed in a completely different way' [5]*. For example, driving away from a robbery in a car would not necessarily be referred to as vehicle crime.

This is a view which is also shared by several other leading academics in the field of cyber criminology. They say that although there is an increase in 'cyber crime', this is

not necessarily representative of 'new' crime types or offences that haven't previously existed [6]. Moreover, so called cyber crime when dealt with in the criminal justice system is treated no different to, and even 'feels' like any other traditional crime type [7].

Ford and Gordon [8] argued that there are two categories of cyber crime. They said that the primary factor in the commission of the offence is key to the category under which the offence sits. If technology, such as computers or the internet is the primary factor then the offence sits under category 1. This includes offences such as the development and spread of malware. Category 2 on the other hand includes offences where the primary factor is a 'human' element, such as online grooming or harassment. This could also include the facilitation of existing crime types with the assistance of technology.

Cyber crime has no current definition in UK law. However, it is widely accepted amongst government and law enforcement that cyber crime involves various types of criminal activities which make use of IT systems such as computers, mobile devices and the internet. With some similarities to the work conducted by Ford and Gordon, in the UK cyber crime is generally broken down into two areas; Cyber Dependent Crime, and Cyber Enabled Crime.

According to the 2010 UK Cyber Crime Strategy, Cyber Dependant Crimes are 'new' offences, which make use of new technologies and techniques [9]. Cyber Dependant Crimes rely on IT, networks and/or digital devices to be able commit the Actus Reus of an offence. These are 'true' cyber crimes or 'pure', and include things such as hacking, the spreading of malicious software (malware), and denial of service attacks etc. These types of cyber-attacks are those offences which were created by the Computer Misuse Act 1990.

On the other hand, Cyber Enabled Crimes were defined in the same strategy as being traditional crimes, which can be increased in scale and reach through the use of computers, computer networks, or other forms of information communications technology such as mobile devices. One of the most common and impactive forms of cyber enabled crime in the UK is that of cyber enabled fraud [10], which amounts to over 35% of all crime in England and Wales.

Despite these two cyber crime 'types' appearing in the 2010 Cyber Crime Strategy, various law enforcement agencies and government bodies in the UK make use of different definitions of cyber crime.

For example, The Home Office, for crime recording and counting purposes do not use the term 'cyber crime' and refer to 'Online Crime'. 'Online Crime' is defined in 'The Nature of Online Offending' report which was published in 2015. It says that an online crime has occurred if…

"…On the balance of probability, the offence was committed, in full or in part, through a computer, computer network or other computer-enabled device. This included sending or receiving emails; use of social networking sites such as Facebook, Twitter or chat rooms; use of forums, blogs or websites; messaging services such as Blackberry Messenger (BBM) and communication via online video game networks or Skype. The terms 'computer, computer network and other computer-enabled devices' include those offences committed using: desktop computers or laptops, in the home or in the workplace; mobile phones, smartphones, tablets and other telecommunications devices linked to computer networks; and any other identifiable computer system or network that produces, processes and transmits data."

The body which is responsible for the development of police learning and skills, the College of Policing has produced the 'Cyber Spectrum'. The cyber spectrum's definitions of cyber enabled and cyber dependent crime are consistent with other definitions of these crime types. As such, the College of Policing appear to be trying to keep a common approach and giving consistent advice to officers. However, the cyber spectrum introduces two further terms; Internet Facilitated Crime, and Crime with a Digital Footprint.

B. The Underreporting of Cyber crime

With the development of computer technology, one of the greatest and most significant breakthroughs in terms of human evolution [11] we have entered a new cyber age. This digital world in which we now live and the various elements on which it is built is commonly referred to as the cyber landscape.

Technology and the speed at which it is evolving is presenting opportunities for people to access data and information from anywhere in the world, whenever they want, in the palm of their hand without being constrained to physical cables or connections[12]. It took 75 years for 50 million people to start using the telephone after it was invented [13]. It took only 4 years for the same number of people to start using the World Wide Web after its inception in 1989, then only 3 months to reach 50 million users of Facebook.

Technology has, unsurprisingly, been embraced by criminals who seek new opportunities to commit crime. This 'cyber crime' poses a significant threat internationally and here in the UK. In 2010, Gottschalk said that the opportunities available to cyber criminals are almost endless, and the interconnected world in which we live has generated a multitude of new crime types and modus operandi, as well as new threat actors [14].

Although it is difficult to provide a true picture of the volume of cyber crime in the UK, experimental figures estimate that more than 5.5 million cyber crimes occur in the UK each year. Of these, just over two thirds (3.6 million) are computer related fraud offences [15]. Despite this being experimental data, as it is the first time cyber crime has been included in the UK Crime Statistics by the Office for National Statistics, it provides a good indication of the prevalence of cyber crime in the UK [16].

The main reason for the incomplete picture is the apparent lack of reporting of cyber crime by victims. According to McGuire & Dowling this is due in part to people not being aware of what cyber crime is, and the difficulty in categorising the multitude of crime types and associated offences.

The National Crime Agency also sees the underreporting of cyber crime as a 'serious problem' and that this is ultimately hampering the disruption and prosecution of cyber criminals [17]. One of the main issues with regards to under-reporting is when corporations are the victim of a cyber attack. Some businesses might simply be unaware that they have been breached, while others might have concerns about the reputational damage and lack of customer trust if they report being a victim of a cyber attack [18].

To centralise and gain a better picture of the volume of cyber crime, the Government launched Action Fraud. Part of the City of London Police since 2013, Action Fraud is the UK's national reporting and recording unit for all fraud and cyber crime [19]. For crime recording purposes, offences under the Fraud Act and the Computer Misuse Act are recorded centrally by Action Fraud, and as such do not appear on the crime statistics for police forces across the country.

Another unit involved in this process is the National Fraud Intelligence Bureau (NFIB), which reviews all crime reports made to Action Fraud with a view to identifying trends, emerging threats, and investigative opportunities. If there are such opportunities, details of the report are forwarded to the local police for where the suspect or the victim (if no suspect is identified) lives for further investigation. This in turn ensures that where crime patterns are identified, there can be an evaluation and a coordinated response on a national level, thereby providing a better response to cyber crimes [20].

However, since its inception and roll-out in 2008, Action Fraud has been subject of much controversy and criticism. Apart from the name suggesting the body only deals with fraud offences, in 2013, Action Fraud cited 'IT problems' when over 2500 crime reports were lost [21]. The same year, the function of Action Fraud was called into question and the government was accused of politicising the recording of fraud and cyber crime in a process which was regarded as defragmented and not conducive to an appropriate call to service for victims of cyber crime.

More recently, at the Police Superintendents Association of England & Wales conference in September 2017, the Deputy Head of the National Cyber Crime Unit, Oliver Gower, criticised Action Fraud for the way in which it currently operates and that the service to victims is poor [22]. He added that there is little to no communication or support offered to victims and an even smaller chance that victim's reports will be investigated. Of the estimated 2 million cyber dependent crimes in the last 12 months, only 28,000 of those were reported to Action Fraud. Of those, a mere 3500 were referred to police forces for further investigation. Gower explained that it was this lack of response and the poor reputation of the process that causes the lack of reporting. Gower did however remind the conference that Action Fraud is not the only issue, and that of the 3500 referrals, local forces only went on to investigate 12% of them.

II. Methodology

The research for this paper employed two separate data collection methods.

Firstly, a review of crime figures and referrals from Action Fraud/National Fraud Intelligence Bureau was used to identify the current threats to the citizens, businesses and organisations in the area subject of the study, and to see whether there was any correlation between the demand on the force and the general perceptions of the cyber threat in the locality.

Crime statistics were obtained from a combination of the Forces' crime recording system (Niche) and Business Objects Systems (BOS). These statistics included the details of all recorded crime, and crime which was given an 'online crime flag'. It is these statistics which are used to inform the national crime recording figures for the Home Office.

As well as looking at the forces crime statistics that are provided to the Home Office, the research also considered referrals which were received from the National Fraud Intelligence Bureau (NFIB). This includes all fraud offences, as well as cyber dependent crimes such as hacking or denial of service attacks, where NFIB have identified possible lines of enquiry and therefore require investigating.

A review of all recorded crimes in the force during the review period was also conducted using key word searches which looked at the Modus Operandi (MO) of the crime that had been recorded. The modus operandi is normally provided by the investigating officer when the crime is recorded, and details 'how' an offence has taken place.

Secondly, a questionnaire was issued to all Police Officers and Police Staff in the force to gauge the general perceptions of key cyber crime and cyber security topics. To provide qualitative data to support the quantitative element of this research, a general view of the current impact of cyber crime on policing was obtained via open questions asking for the participants to give their thoughts.

III. Crime Data Results

A. Recorded Crime

What is apparent from the data obtained is that the issues discussed earlier such as the inconsistent approach to defining cyber crime, appears to have made the recording and reporting of cyber crime inconsistent too.

The data for this part of the research has come from three separate sources, yet all appear to give a different picture about the demand from cyber related crime.

Having conducted a search of all crimes using a keyword search against the modus operandi (MO) of recorded crimes between April 2016 and March 2017, 1703 crime incidents were identified. These range from malicious communications to sexual offences. These crimes are cyber enabled, as the Force in question is not required to record cyber dependent crime. The following tables give a breakdown of the various offences identified from MO keyword searching.

Table 1 shows the various offences based on Home Office Crime Groups which have been identified in the MO keyword search. These are the generic crime types which are recorded by the Home Office for statistical purposes.

The predominant crime group which appears to make up the bulk of offences is violence against the person. This includes offences such as harassment, malicious communications as well as physical violence.

TABLE I. CRIMES RECORDED BY HOME OFFICE CRIME GROUP IDENTIFIED IN MO SEARCH

Home Office Crime Group	
Violence against the Person	1057
Sexual Offences	184
Other Offences	161
Theft / Handling Stolen Goods	153
Public Order	96
Criminal Damage	18
Burglary	16
Drug Offences	9
Vehicle Offences	7
Possession of Offensive Weapons	1
Robbery	1

Table 2 shows the top 30 crime types based on their Home Office Descriptor. What can be seen is that most of the crimes involve malicious communication and harassment offences. These almost without exception appear to involve social media networks such as Facebook, or messaging applications such as WhatsApp in the commission of the offence.

The count of sexual offences (n=184) appears from *Table 2* to be high because of various sexual offences against children. Upon reviewing, several of these crimes include incidents of online grooming via social media networks, as well as the possession and distribution of indecent images of children (IIOC) which involve first generation images of abuse which has taken place in the county.

Blackmail offences also appear high in frequency. Except for two offences (blackmail by email following business transactions), all the blackmail offences identified were sextortion incidents (n=59). Sextortion offences, sometimes referred to as webcam blackmail, occur when a perpetrator uses a fake identity online in order to persuade the victim to perform sexual acts for them using a webcam. The acts performed in front of the webcam are recorded by the perpetrator who then threatens to share the video with the victim's family and friends. A financial demand is made of the victim to stop the perpetrator from distributing the video. Sextortion offences present a significant risk as victims are extremely vulnerable, and have resulted in several victims committing suicide [23].

Matters which do not appear to be included in the list of blackmail offences identified via the MO keyword search include five incidents of 'hacking extortion' or 'DDoS extortion', which have been referred by the National Fraud Intelligence Bureau (NFIB), following reports to Action Fraud.

One such example of DDoS extortion comes following an email being received from the hacking group 'The Armada Collective', who threatened to launch a DDoS attack on the victim's company unless a demand for 1 Bitcoin is paid. This MO is not uncommon, and The Armada Collective have a history of using this tactic, but rarely follow through with the attack although victims will often pay the demand through fear [24].

The recording of Hacking Extortion and DDoS extortion by NFIB is unusual in that they are simply blackmail offences, and like sextortion, would ordinarily be recorded by the Constabulary. It is not clear why Action Fraud would record these types of crime, and can only add to the confusion around the role of Action Fraud in the recording and reporting of crime.

On this topic, one individual responding to the survey said:

"Frequently I find it hard to determine where cyber crime should be recorded, either locally or via action fraud or directly with providers such as banks, internet providers etc. This makes it hard to answer questions raised by members of the public who contact police for advice and reassurance."

TABLE II. COUNT OF CRIMES IDENTIFIED BY MO SEARCH

Home Office Crime Description	
Malicious Communications	600
Harassment	357
Obscene publications etc.	121
Sexual activity involving a child under 16	79
Sexual activity involving a child under 13	69
Blackmail	61
Public fear, alarm or distress	52
Other theft	50
Assault without injury	35
Other Offences against the state or public order	32
Assault with Injury	27
Stalking	20
Theft in a dwelling other than from automatic machine/meter	12
Racially or religiously aggravated public fear, alarm or distress	12
Other notifiable offences	11
Threat or possession with intent to commit criminal damage	11
Threats to kill	11
Theft from the person	10
Burglary in a building other than a dwelling	9
Shoplifting	9
Perverting the course of justice	9
Rape of a female aged 16 and over	8
Criminal damage to a dwelling	7
Exposure and voyeurism	6
Theft or unauthorised taking of motor vehicle	5
Possession of controlled drugs (cannabis)	5
Sexual grooming	5
Sexual assault on a female aged 13 or over	4

Assault without injury on a constable	4
Theft or unauthorised taking of a pedal cycle	4
Handling stolen goods	4

B. Crimes flagged as being 'online crime'

In comparison to the crimes identified via the MO keyword search, crimes that were given an online flag by the Force and therefore recorded as national crime statistics, appear to be significantly lower in frequency.

What can be seen is that during the review period the crimes identified from the MO search account for 3% of all crimes recorded, compared to crimes with an online flag which account for less than 1%.

The monthly figures appear to show that the volume of online crime and those identified in the MO keyword search are consistent in their volume, however there is on average 63% fewer online crimes reported to the Home Office. There would be an expectation that the two lines of this graph would/should be closer together if all 'online crimes' had been accurately captured. The number of these offences is shown as a comparison in *Fig. 1.*

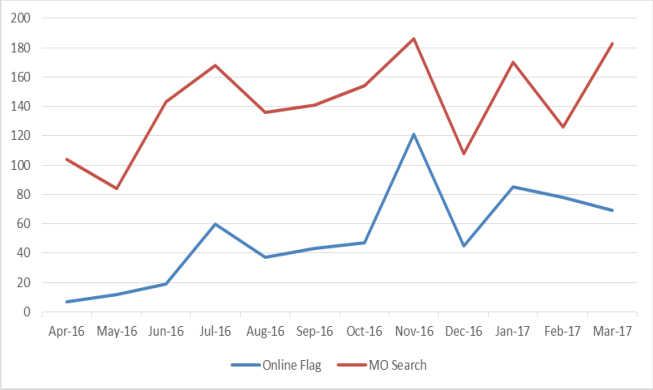

Fig. 1. Comparison of MO keywords and 'Online-Flagged' Crimes

There are several possibilities for this lower number of crimes with an online flag.

Firstly, the MO keyword search is not without its flaws in terms of its methodology. Although every care has been taken to remove crimes that do not truly reflect a 'cyber crime' or 'online' crime, the number of crimes identified could be fewer than the 1703 identified. However, it is unlikely that it would be more than 30% less based on the manual dip- sample of crimes used to test the methodology.

Secondly, crimes flagged as being 'online crime' are done so based on an individual assessing the crime and 'flagging' it where appropriate at the crime recording, investigation or closure stage. It may be the case that these individuals are not aware of the flagging process, or the correct definition of online crime. As the literature research suggests, there is much confusion over the definition of cyber crime, and if the person responsible for the flagging is unaware of the definition, they will not correctly assess the crime, and flagging opportunities will be missed. Or indeed, crimes will be flagged when there is no 'cyber' element.

C. NFIB Referrals

Of the 592 referrals received from NFIB during the review period, only twenty-two were cyber dependent crimes. These were broken down as follows in Table III:

TABLE III. CYBER DEPENDENT CRIME REFERRALS FROM NFIB

NFIB Code	Count
NFIB51A - Denial of Service Attack	2
NFIB52A - Hacking - Server	5
NFIB52B - Hacking - Personal	2
NFIB52C - Hacking - Social Media and Email	7
NFIB52D - Hacking - PBX / Dial Through	1
NFIB52E - Hacking Extortion	5

What is significant about this is that this is a very small number of criminal investigations over the course of twelve months. Despite this, 71% (n=207) of officers and police staff said that they deal with cyber dependent crime as part of their day job, with 59% (n=173) saying they deal with cyber dependent crime 'frequently' or 'occasionally'.

What must also be noted is that the number of cyber dependent crime referrals is by no means representative of the true number of cyber dependent crimes which take place in the area. Due to issues such as underreporting, or the fact that NFIB have not forwarded details of every reported crime, the true number is likely to be much greater.

IV. SURVEY RESULTS

The survey was completed by 292 individuals from across the Force. The initial questions in the survey looked to obtain details about the participants based on their rank, role, length of service, age, and gender.

Individuals were then asked about their understanding of the terms identified by the College of Policing in the Cyber Spectrum, i.e. Cyber Dependent Crime, Cyber Enabled Crime, Internet Facilitated Crime and Crime with a Digital Footprint. These terms were chosen for inclusion in the survey as the College of Policing provides the 'best practice' for policing in terms of knowledge and training. As such, these terms are used within any material issued by the College of Policing with regards cyber crime or digital investigation.

The results of this section seem to support the literature review in that the many iterations of the definition of cyber crime cause confusion (*Fig. 2*). Very few individuals can confidently say they know what any of the crime types (as defined in the College of Policing Cyber Spectrum) actually are. On average, 15% of individuals feel strongly that they understand the meaning of the 4 cyber crime types.

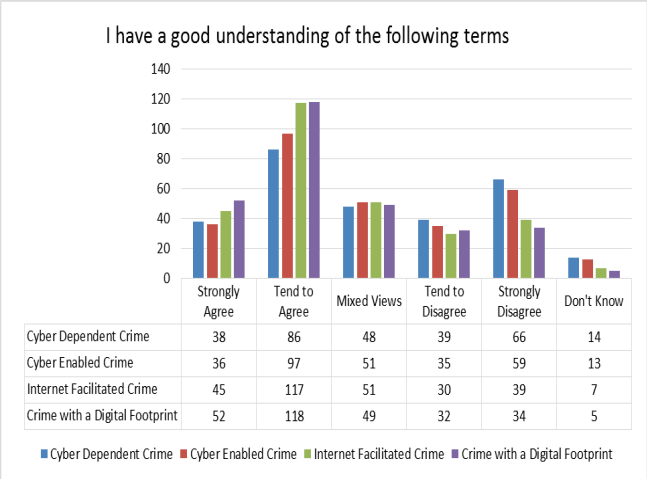

Fig. 2. Attitude of officers & staff with regards their understanding of cyber crime definitions

Most individuals feel that they have a limited understanding of the definitions, by saying they tend to agree they have a good understanding of the terms. Although this appears to indicate a good understanding of the terms, it may be more a case of an 'educated guess'.

Of the definitions where people are less certain about their levels of understanding, cyber dependent crime causes the most confusion with 36% (n=105) of participants stating they have a limited understanding of the definition. Cyber dependent crimes are 'new' crimes and covered by the computer misuse act, and it is these such offences which some officers feel require a specialist response.

Several questions in the survey specifically sought to determine the confidence of employees of the Constabulary; firstly, around dealing with reports of cyber crime or cyber crime investigations, secondly on providing cyber security advice to members of the public. These questions were posed to better understand the ability of officers and staff to deal with reports of cyber crime.

An overwhelming number of individuals (56% n=163) state they are simply not confident to deal with cyber crime, a significant result which is heavily weighted towards this response [*Fig.3*].

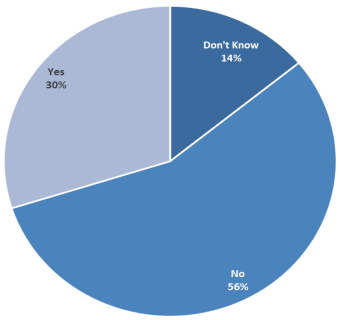

Fig. 3. Response to the question 'Are you confident to deal with cyber crime?'

This lack of confidence would likely have a negative impact on the employee's ability to provide a quality service to a victim given that they state they regularly deal with cyber crime. Despite the fact that officers are trained investigators, and other members of police staff such as PCSO's are specifically trained to protect and reassure the public and therefore have the ability to deal with cyber crime, their lack of confidence will mean they potentially offer a substandard service. In practice, the techniques used to investigate cyber crime are no different to any other crime provided an investigative mind-set is applied. Also, the evidence is found in the same places as most traditional crimes. What is concerning is that despite this lack of confidence, officer and staff workloads will often include cyber enabled or dependent crime.

The responses to the survey suggest that a significant cause for the lack of confidence appears to be because of the apparent overall lack of training received by officers and staff (42%, n=182) as seen in *Fig. 4*.

One individual said that:

"Frontline officers are unskilled in this and are expected to be able to investigate or suggest avenues of investigation when not only do we have insufficient skills but we do not know what the force can actually do"

The main form of training currently available is in the form of online e-learning packages which officers are expected to complete themselves. The current cyber crime e-learning modules provided by the College of Policing are not mandatory. Given the lack of confidence in individuals in this area of policing, consideration should perhaps be given as to whether e-learning is a suitable medium for training.

It is argued that e-Learning has its place and has its advantages. Arkorful & Abaidoo suggested that e-learning is useful due to the fact that individuals are able to choose the time and place they wish to complete their learning [25]. Furthermore, e-learning packages allow for users to complete the course material at their own pace, in a way which is cost effective to the training department or training institution due to there being no requirement for paid staff to teach the material.

Others argue however that depsite the apparent advantages, e-learning is not suitable, particulary when considering a complex subject. Criminal investigation skills require a degree of practical experience in order to be able to develop understanding. The most significant concern with reagrds e-learning is the lack of interaction between a learner a teacher or colleague [26]. Face to face interaction allows for the exchange and challenge of views and ideas, and ensures experiential learning can be used [27]; something which is essential in a practtical, skilled profession such as policing.

Fig. 4. Why officers and staff aren't confident to deal with cyber crime

The survey participants went on to say that they do not feel as though they have the appropriate skills, knowledge and training. 57% (n=164) of individuals do not feel equipped to deal with cyber enabled crime, with slightly more, 59% (n=171), ill-equipped to deal with cyber dependent crime.

V. Conclusion

Cyber crime is here to stay, and the opportunities for criminals will continue to grow as technology advances. With this comes the continuing challenge for law enforcement agencies to protect members of the public from becoming victims and to protect the critical infrastructure of the UK and the business that operate within.

The UK remains a target for cyber criminals, and if it remains a key financial and digital hub it will continue to be so. However, the UK is responding, putting in place safeguards to ensure it remains a safe place for its citizens and businesses, and proves to be an ever more hostile place for the cybercriminal. However, despite the successful national and regional response, issues are highlighted at a local level within the 43 police forces.

This research has highlighted that there is much confusion with regards the definitions of cyber crime and this has resulted in various issues, such as how cyber crime is recorded at a Force level, and ultimately how it affects national statistics. This confusion over the definitions of cyber crime also affects officers and police staff who are expected to identify and investigate cyber crime. Without knowing what they are dealing with, they are less confident to investigate these offences, and often investigative opportunities are missed.

Haven examined the crime datasets, there is an indication that there is potential under-reporting of 'online crimes', based on the difference between those reported to the Home Office and those identified through the MO keyword search.

There is also lack of consistency with regards the data collated and evaluated by Action Fraud and the National Fraud Intelligence Bureau. As discussed in the literature review, there has been some criticism of the way Action Fraud and NFIB operate and whether they are fit for purpose. The data reviewed seems to support some of these views, as do the views of the officers and staff who took part in the survey.

Unfortunately, until the issues with Action Fraud and the way in which the Home Office choose to collate data on cyber crime are resolved, we are likely still to have an unclear view of the impact of cyber crime and therefore the demand on local law enforcement.

As well as the lack of understanding about cyber crime definitions, there are also limited levels of understanding of the cyber threats and crime types which local police forces are expected to investigate. These offences are seen as being complex crimes, requiring a specialist response, despite becoming more mainstream.

Officers and police staff are frustrated at the lack of guidance and training issued by the College of Policing, and locally. They are aware that cyber crime is on the increase and there is an expectation that they will deal with more of these crimes in the coming years. Police Officers and Staff want to provide the best possible service to members of the public during criminal investigations or through providing crime prevention advice. Without suitable training, they feel that they will not be able to meet the growing demand from cyber related crimes.

VI. Recommendations

This research has highlighted key topics and issues, some of which could and should be explored further. Based on the findings of the research, several recommendations are made which could be considered by each local police force, as well as nationally. These recommendations are made with the view of improving the overall levels of service members of the public receive with regards cyber crime, or investigations involving digital evidence.

Firstly, there must be a consistent and multi-faceted approach to the training of police officers and police staff, with practical examples of how cyber crimes can be investigated. This must make use of face-to-face learning and could be aided by, but not reliant on, e-learning packages. There is also an argument that this training could be tailored to suit the needs of different roles within the organisation. For example, call takers indicate that they need to be able to provide advice on capturing evidence early, and providing preventative advice whereas detectives conducting investigations need to know how to use digital evidence to support their investigations and how to present this at court.

There is a need to clearly define the difference between 'Cyber Crime' and 'Digital Investigations'. It was found that officers and staff sometimes wrongly presume that a crime with some form of digital evidence is in fact a cyber crime. This isn't always the case and almost all crimes will have some form of digital evidence, whether this is CCTV or telecommunications data.

If Action Fraud is to continue being responsible for recording cyber crime statistics, there must be a suitable and consistent way of flagging cyber/online crimes locally to assist in determining the demand on individual organisations.

There is a need to improve the process by which Action Fraud operates. Reported crime figures must be more readily available to local police forces so that their demand can be measured. Furthermore, Action Fraud needs to provide a more timely response to victims, and by working more closely with UK Police Forces, the number of crimes being investigated needs to increase. Action Fraud also has a key role to play in informing members of the public what cyber crime is and how it can be reported.

References

[1] Mitnick, K., & Simon, W. (2002). The Art of Deception: Controlling the Human Element of Security. Indianapolis: Wiley.

[2] Aiken, M., Davidson, J., & Amann, P. (2016). Youth Pathways in to Cyber crime. UCD Geary Institute for Public Policy. Aiken and Davidson.

[3] Europol. (2017). The Internet Organised Crime Threat Assessment. European Cyber crime Centre (EC3). Europol.

[4] McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. Home Office.

[5] Grabosky, P. N. (2001). Virtual Criminality: Old Wine in New Bottles? *Social and Legal Studies, 10*(2), 243-249.

[6] McCusker, R. (2006, December). Transnational organised cyber crime: distinguishing threat from reality. Crime, Law and Social Change, 46(4), 257-273.

[7] Wall, D. S. (2015, October 21st). The Internet as a Conduit for Criminal Activity. Information Technology and the Criminal Justice System, 77-98.

[8] Gordon, S., & Ford, R. (2006, August). On the definition and classification of cyber crime. Journal in Computer Virology, 2(1), 13-22.

[9] UK Home Office. (2010, March). Cyber crime Strategy.

[10] Office For National Statistics. (2016, July 21st). Crime in England and Wales: year ending Mar 2016.

[11] Grabosky, P., & Smith, R. (1998). Crime in the Digital Age: Controlling Telecommunications and Cyberspace. New Brunswick and London: Transaction Publishers.

[12] Wall, D. S. (2015, October 21st). The Internet as a Conduit for Criminal Activity. Information Technology and the Criminal Justice System, 77-98.

[13] Annan, G. (2012, May 1st). Reaching 50 Million Users. Retrieved September 1st, 2017, from Visual.ly: https://visual.ly/community/infographic/technology/reaching-50-million-users

[14] Gottschalk, P. (2010). *Policing Cyber crime.* Petter Gottschalk & Ventus Publishing ApS.

[15] Office For National Statistics. (2017). Crime in England and Wales: year ending Sept 2016. ONS.

[16] Muncaster, P. (2017, January 19th). ONS: Nearly Two Million Annual Cyber crime Incidents. Retrieved from Info-Security Magazine: https://www.infosecurity-magazine.com/news/two-million-annual-cyber crime/

[17] National Crime Agency. (2016). Cyber crime Assessment 2016: Need for a stronger law enforcement and business partnership to fight cyber crime. NCA Strategic Cyber Industry Group. National Crime Agency.

[18] Pultarova, T. (2017, February 14th). UK Companies Unaware of Cyber Attacks or Unwilling to Admit Breaches, Study Reveals. Retrieved September 23rd, 2017, from Engineering and Technology: https://eandt.theiet.org/content/articles/2017/02/uk-companies-unaware-of-cyber-attacks-or-unwilling-to-admit-breaches-study-reveals/

[19] Murray, A. (2016, July 6th). Fraud victims outside London have 'little chance' of police help. Retrieved September 27th, 2017, from The Telegraph: http://www.telegraph.co.uk/money/consumer-affairs/fraud-victims-outside-london-have-little-chance-of-police-help/

[20] City of London Police. (2010, July). General guide to the NFIB Information for Data Providers and the Public. Retrieved August 10th, 2017, from Gov.uk: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118482/general-guide-nfib.pdf

[21] Thed, M. B. (2013, July 22nd). Action Fraud Hotline Loses 2500 Cases in Just 8 Months. Retrieved September 20th, 2017, from The Daily Mail Online: http://www.dailymail.co.uk/news/article-2371791/Action-Fraud-hotline-loses-2-500-cases-just-months.html

[22] Avem Evolution. (2017, September 12th). Oliver Gower: PSAEW 2017 Annual Conference - Cyber crime Discussion. Retrieved September 20th, 2017, from Youtube: https://www.youtube.com/watch?v=Hc2ugSCOTSc

[23] Marsh, S. (2017, September 3rd). *Alarm Over Steep Rise in Number of Sextortion Cases in UK*. Retrieved September 17th, 2017, from The Guardian: https://www.theguardian.com/uk-news/2017/sep/03/alarm-over-steep-rise-in-number-of-sextortion-cases-in-uk

[24] Masters, G. (2016, April 26th). *Empty Email Threats Reap Payoff for Armada Collective*. Retrieved September 17th, 2017, from SC Magazine: https://www.scmagazine.com/empty-email-threats-reap-payoff-for-armada-collective/article/528543/

[25] Arkorful, V., & Abaidoo, N. (2015, January). The role of e-learning, advantages and disadvantages of its adoption in higher education. *International Journal of Instructional Technology and Distance Learning, 12*(1).

[26] Young, J. (1997, October 3rd). Rethinking the Role of the Professor in an Age of High-Tech Tools (Archive). Retrieved September 30th, 2017, from The Chronicle of Higher Education: http://www.chronicle.com/article/Rethinking-the-Role-of-the/98112

[27] Felicia, P. (2011). Handbook of Research on Improving Learning and Motivation through Educational Games: Multidisciplinary Approaches. Retrieved September 30th, 2017, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.473.3094&rep=rep1&type=pdf