STRONG AND SUPPORTIVE COMMUNITIES SCRUTINY COMMITTEE	Agenda Item No. 6
22 JULY 2015	Public Report

Report of the Head of Community and Safety Services

Report Author – Robin Sissons
Contact Details – 07921938092

SAFER PETERBOROUGH PARTNERSHIP – CYBER CRIME

1. PURPOSE

1.1 To provide Members with a definition of cybercrime and what different types of cybercrime there are; the impact it is having on the community; and what activity the Safer Peterborough Partnership is doing to impact on it.

2. RECOMMENDATIONS

2.1 Members are asked to scrutinise this report, to challenge where necessary and to suggest ideas and initiatives which will impact on this crime type.

3. BACKGROUND

3.1 Computers, the internet and electronic communications play an ever-increasing part in all our lives, with the use of the internet in the home, at work or in educational establishments now standard and we expect the rapid development to continue to accelerate. This has implications for safety and security as cyber criminals are quick to spot the potential vulnerabilities of new technologies and exploit them to commit offences or to try to frustrate detection of their activities.

3.2 The internet has transformed the way millions of people behave ranging from how they interact with others socially right through to the way they buy goods and services. For example, the UK is the leader in Europe in terms of the size of the internet shopping market. The annual average weekly spending online in 2014 was £718.7 million. This was an increase of 11.8% compared with 2013. The annual average weekly spending online in 2009 was £341.7 million, which means that this amount has more than doubled in the last 5 years.

3.3 As more and more of the nation's public and private assets are stored electronically rather than physically, often outside our jurisdiction, there will be more opportunities for crime. The public, businesses and government are all at risk from organised crime groups, and from those who would seek to harm individuals, particularly children. Whether the crime is fraud, data theft from individuals, businesses, or Government, or child sexual abuse committed through the online environment, the impact of crime initiated on the internet can be devastating for its victims. This is why it is so important that the Safer Peterborough Partnership recognises the impact cybercrime is having on the community and attempts to limit the harmful aspects.

4. CYBER CRIME DEFINITION

4.1 There is a wide range of offences that can be committed through communication technology. Cybercrimes are commonly considered as falling into one of two categories: new offences committed using new technologies, such as offences against computer systems and data, dealt with in the Computer Misuse Act 1990; and old offences committed using new technology, where networked computers and other devices are used to facilitate the commission of an offence. In the former are crimes such as hacking or breaking into computer systems to steal or alter data; in

the latter, crimes such as the transfer of illegal images or fraud. The former are often a precursor to the latter, based on motives of financial gain. However, while the focus is often on online fraud or child protection, there is a significant number of other offences committed through the internet, such as harassment, threatening behaviour and other anti-social activity.

4.2 The challenge posed by crimes initiated or committed through the online environment is not so much their identification as the nature of the environment in which they are committed. Cyber criminals can operate from anywhere in the world, targeting large numbers of people or businesses across international boundaries, and there are challenges posed by the scale and volume of the crimes, the technical complexity of identifying the perpetrators as well as the need to work internationally to bring them to justice.

5. TYPES OF CYBERCRIME

5.1 Hacking

This is a type of crime wherein a person's or business computer is broken into so that their personal or sensitive information can be accessed. Centrally-held data typically consists of bulk payment card and identity data stored in a database. This data is targeted by criminal hackers who try to overcome security measures protecting the data so they can steal it in bulk. Highly skilled criminals are constantly scanning operating systems and application software for new security vulnerabilities.

The impact upon business from internet crime can be significant, and can lead to loss of money, reputation and disruption to businesses. Potential breaches are a constant threat especially for large companies, perhaps reflecting the much larger electronic networks that such firms have, the greater number and expertise of the IT staff in identifying incidents, and the potential gain for an offender breaching security on a large network. The cost of a breach can range from tens of thousands in small companies to millions in large ones.

5.2 Intellectual Property Theft

This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy. This has had a massive impact on certain business areas.

5.3 Cyber Stalking

This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they may begin offline stalking along with cyber stalking to make the victims' lives more miserable.

5.4 Identity Theft

This has become a major problem with people using the Internet for cash transactions and banking services. In this cybercrime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name, forcing the credit card firms to suffer large losses, or they might sell the information to others who can use it in a similar fashion. Second, they might use individual credit card names and numbers to create new identities for other criminals. For example, a criminal might contact the issuing bank of a stolen credit card and change the mailing address on the account. Next, the criminal may get a passport or driver's license with their own picture but with the victim's name. With a driver's license, the criminal can easily acquire a new

Social Security card; it is then possible to open bank accounts and receive loans – all with the victim's credit record and background.

5.5 Malicious Software

These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

5.6 Internet Fraud

Schemes to defraud consumers are abound on the Internet and continue to accelerate due to the increased use of e-mails. There are many types of fraud targeted at the public, ranging from credit and debit card fraud, lottery scams, non-delivery fraud and fraud perpetrated through online auction websites. Additionally, the public is at risk from fraud involving fake goods, such as watches or clothing, or more seriously from fake and unsafe pharmaceuticals bought online. None of these are unknown offline, but cyber criminals are able to use the internet to perpetrate these offences on a mass scale and are able to use the internet to hide their real identities and locations.

The Safer Peterborough Partnership has seen an increase in a particular ploy. Lonely vulnerable persons attempt to make friends through the use of social media. The offender strikes up a friendship by explaining that they live in a foreign country. After some weeks they explain that they intend to visit Europe. However they then state that they have short term financial issues. The message asks the recipient to cover some cost on the promise that these will be returned in the near future. Should the recipient respond with a check or money order, they are told that complications have developed and that more money is required. Over time, victims can lose thousands of pounds that are utterly unrecoverable.

5.7 Child soliciting and Abuse

From a child protection perspective a key issue facing law enforcement is not simply the volume of child sexual abuse material that is being circulated, but the ease by which this medium offers child sexual predators the opportunity to network with each other to create and distribute content, as well as the opportunity to access new victims, either offline or through online spaces, such as instant messaging or social networking sites. Online paedophile networks can easily run into tens of thousands of suspect's worldwide. Cambridgeshire Constabulary and national agencies spend a considerable amount of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

5.8 Dark Web

The Dark Web is a term that refers specifically to a collection of websites that are publicly visible, but hide the IP addresses of the servers that run them. Thus they can be visited by any web user, but it is very difficult to work out who is behind the sites. And you cannot find these sites using search engines.

Almost all sites on the so-called Dark Web hide their identity using the Tor encryption tool which will hide your identity, and spoof your location. When a website is run through Tor it has much the same effect. Indeed, it multiplies the effect. Just as the end user's IP is bounced through several layers of encryption to appear to be at another IP address on the Tor network, so is that of the website. So there are several layers of magnitude of more secrecy than the already secret act of using Tor to visit a website on the open internet - for both parties.

5.9 **Hate Crimes, Harassment, Political Extremism**

Other forms of harm-based crime, such as racial or religious hatred, harassment, or political extremism, may be carried out by individuals or by organised groups and focus on particular issues.

Harassment and bullying are significant issues, especially for children, who often cite these as their own areas of greatest concern. The nature of the technology, which children often carry with them all the time, allows bullying to take place not only in school but continue outside. This can make the victim feel threatened and unable to escape the bullying, leading to a feeling of powerlessness. This is set to increase as it becomes normal behaviour within society, especially as the greatest use is within the young and as technology advances even further e.g. iWatch and similar devices become more popular.

The instant nature, availability, volume and ease of social networking coupled with the explosion of multiple mobile devices means that messages can be distributed worldwide very fast and reach a larger audience than ever before. This can be exploited by those who wish to promote violent extremism or terrorism.

6. TACKLING CYBERCRIME

6.1 It has been seen that most cyber criminals have a loose network wherein they collaborate and cooperate with one another. Unlike the real world, these criminals do not fight one another for supremacy or control. Instead they work together to improve their skills and even help out each other with new opportunities. Hence, the usual methods of fighting crime cannot be used against cyber criminals.

6.2 While law enforcement agencies are trying to keep pace with cyber criminals, it is not only proving to be a massive task but one that is accelerating. This is primarily because the methods used by cyber criminals and technology keeps changing too quickly for law enforcement agencies to be effective. In addition, the internet offers the potential for a criminal to commit offences across geographical and jurisdictional boundaries. This poses challenges for traditional law enforcement, even at a national level, as the same offence may be committed against individuals in many countries, at the same time; equally, the same act may be judged differently in each jurisdiction.

6.3 Those who commit cybercrime offences commonly seek to exploit this, undertaking their activities in one country but delivering the effect in another jurisdiction. This can assist in masking their undertakings and create difficulties for investigators in tracing them. In deliberately targeting their activities in or through jurisdictions where regulation or legislation is not strong, or where investigative or other co-operation is known to be poor, cyber criminals can minimise the risk of their activities being discovered or punishment being effected. International investigations require a time-critical response to help negate attacks as well as secure evidence.

6.4 With many forms of crime, the public and business understand the need to have proper security in place to prevent it. The same approach is required online, but the complexity of the technical solutions to provide security online can be confusing and difficult to understand for some users. Additionally, many data breaches have little to do with technology, but are caused by poor practice or carelessness. It is this that the Safer Peterborough Partnership needs to concentrate on if we are to protect the community of Peterborough.

7. CURRENT PREVENTION STRATEGY

7.1 The Safer Peterborough Partnership recognises that many of these international and national issues are beyond its capacity to have a true impact. With regards to these, its focus is on raising awareness and providing practical advice on how businesses and members of the community can protect themselves. This is done on devices that are likely to be used by potential victims

such as social media sites, websites and Android Apps as well as using more traditional crime prevention outlets such as Neighbourhood Watch etc.

7.2 Much work is done with the younger community within Safer Schools and Safety Challenge which is in addition to normal educational packages. These are done in a simple, fun way that often involve multimedia environments.

7.3 Proactive targeted work to identify the location of potential vulnerable victims takes place by the analytical team that sits within the partnership. Initiatives are then undertaken to interact with this section of the community so that they are alerted to the current criminal activity. This is dovetailed with national and local campaigns that are promoted by the partnership in partnership with other agencies such as the Citizens Advice Bureau.

8. IMPLICATIONS

8.1 Not applicable

9. CONSULTATION

9.1 Not applicable

10. EXPECTED OUTCOMES

10.1 That the committee develops a greater understanding of the impacts of cybercrime and supports and suggests new ways of tackling it.

11. NEXT STEPS

11.1 That any comment or further recommendation of the committee is duly noted and acted upon.

12. BACKGROUND DOCUMENTS

12.1 None

13. APPENDICES

13.1 None

This page is intentionally left blank