west midlands
police and crime
commissioner

AGENDA ITEM 10

STRATEGIC POLICING AND CRIME BOARD
3rd December 2013

Cyber Crime – ACC Crime

PURPOSE OF REPORT

1. The purpose of this report is to provide members of the Strategic Police and Crime Board with an overview of Cyber Crime.

BACKGROUND

DEFINITION

2. The current ACPO definition for cyber crime is:

> *“The use of networked computers or Internet technology to commit or facilitate the commission of a crime”*

3. This is further broken down into:

- Cyber enabled crime – traditional offences that have in some part been organised or committed over the internet. This includes ‘existing’ crimes that have been transformed in scale or form by their use of the internet. The growth of the internet has allowed these crimes to be carried out on an industrial scale. The internet is also used to facilitate drug dealing, people smuggling and many other types of crime.

- Pure cyber crime (or cyber dependent) – new offences committed using new technology where a digital system is the target as well as the means of attack. These include attacks on computer systems to disrupt IT infrastructure, and stealing data over a network using malware (the purpose of the data theft is usually to enable further crime).

OVERVIEW

4. Cyber Crime is a complex issue that has been identified by the Government as a Tier 1 National Threat. In response, the Home Office have set up the Cyber Crime Reduction Partnership and National Cyber Crime Unit (NCCU) within the National Crime Agency (NCA) to tackle it.

National

9. At a national level, the NCA is responsible for leading, supporting and coordinating the response to the most serious incidents of cyber-dependent crime. The NCA will work with partners to deliver this response, harnessing the skills and capabilities of wider law enforcement, industry and others to deliver the most appropriate response. The NCCU's remit includes:

- Leading the investigation of the most serious incidents of cyber-dependent crime
- Driving the up-skilling of cyber investigation in law enforcement
- Leading law enforcement's relationships with key partners to tackle cyber crime, including industry, the intelligence agencies and international partners.

Regional

10. At a regional level, capacity is being built into the Regional Organised Crime Unit (ROCU) where a dedicated Regional Cyber Crime Unit (RCCU) will be established. The RCCUs will work flexibly either to support NCA-led investigations, to lead their own investigations or coordinate or support local investigations that may have been escalated through the regional tasking process. Such escalation could include intelligence-led proactive operations, reported crime or National Fraud Intelligence Bureau (NFIB) packages where a number of reports are found to be a linked series or the activity crosses several Force boundaries. Within that remit, it is proposed that in the future the regional capability needs to be able to respond to time-critical incidents and crime reports of significant scale and complexity, including:

- Cyber crime and cyber-enabled crime facilitated by malware or phishing.
- Computer and Network Intrusions (with various motives and objectives).
- Denial of Service attacks and website defacement (with various motives and objectives)

Local

11. Local Police Forces must be able to action reports of cyber-dependent and cyber-enabled crime directly from the public and as packages from Action Fraud/NFIB, including crimes in action. As an example, this may include incidents of:

- malicious communication
- fraud
- harassment
- child exploitation
- money laundering.

12. Local Forces may also be asked by the NCA undertake activity, or to support national or regional level investigations.

FORCE RESPONSE

13. The West Midlands Police response has been to identify a Gold lead (T/ACC Burgess) who in turn has appointed a Silver commander responsible for producing a plan of action (Detective Chief Superintendent Graham). This has led to the creation of a Force Cyber Crime Board, which is made up of representatives from a number of departments across the Force and has also invited colleagues from other Forces to share their experiences.

14. The approach being taken by the Board is to reflect the National Serious and Organised Crime Strategy. Cyber crime is repeatedly referred to in that document, and as such the Board are developing tactical responses using the four main headings contained within the strategy with the following aims:

    - Pursue

      To establish strong, effective, collaborative organisations and develop our investigative capabilities and cooperation with others. This will better enable us to attack criminal finances and make maximum use of effective legal powers.

    - Prevent

      To raise awareness of the reality and consequences of cyber crime and intervene to stop others being drawn into other types of cyber crime. We will develop techniques to deter people from continuing in cyber crime and establish an effective Offender Management framework to support work on Pursue and Prevent.

    - Protect

      To protect national and local government and improve protective security in the private sector. On an individual basis, we will seek to protect people at risk of being victims.

    - Prepare

      To ensure major cyber crime incidents are brought to a rapid and effective resolution. We will also ensure communities, victims and witnesses affected by cyber crime have the support that they need.

15. This strategic response manifests itself in a number of ways, many of which are still in their embryonic stage. There are many tactics that are used in the world of Pursue, and WMP is constantly seeking ways in which it can improve its investigative capability. As the Serious and Organised Crime Strategy has the same themes as the Contest Strategy, experiences are being brought across as to how we can better engage in the Prevent and Protect spheres.

16. The nature of cyber crime means that it does not sit within any single portfolio. Crimes can range from reports of bullying on Twitter through to Denials of Service attacks on large businesses. As such, preventing and detecting cyber crime, just like crime, is the core business of every department within WMP.

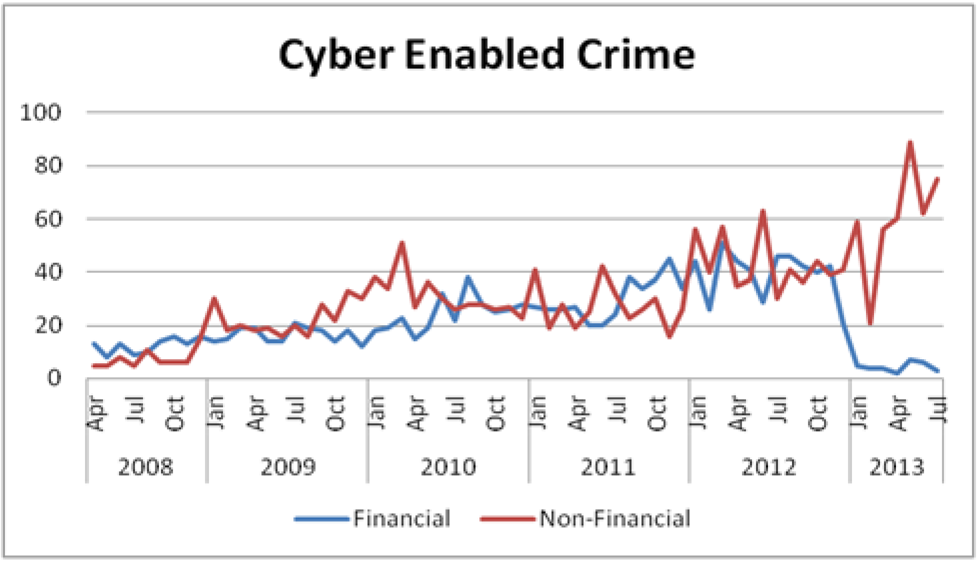
17. For many years officers have been giving advice to individuals and businesses around crime prevention. One of the challenges around cyber crime is to educate staff to offer

similar advice, but around cyber security. The aim is to bring this activity into the mainstream, so that advising around online security is as routine as offering advice on physical security. A training package is currently being developed with Learning and Development that will be delivered to all front line staff. This will better equip them to deal with the evolving challenge of cyber crime and allow them to provide an improved service to victims of crime.

18. While outside the scope of Prepare in this context, the Local Resilience Forum has a responsibility to ensure that business continuity plans exist that allow core business to continue to be delivered when faced with a number of threats, including cyber threats. This includes key aspects of the region's infrastructure including power, health services and emergency responders.

ANALYSIS

19. Nine of the top ten cyber crimes are financial crimes. However this is not reflected within WMP statistics since the creation of Action Fraud, as evidenced by the graph below.



Cyber enabled crimes by category 01.04.08 to 31.07.13

20. The majority of financial offences are fraud related which are now being recorded by Action Fraud. Action Fraud is the national reporting centre for fraud offences ensuring standardisation and recording of all fraud offences as 'national' crimes. There has been a dramatic increase in reports of fraud offences in the Force area to Action Fraud since its roll-out in January 2013. This coincides with the significant decrease in reports in the chart above.

Non-financial Cyber Crime

21. There are seven offence categories of non financial crime for the Force over the past 5 years, Violence, Sexual Offence, Breach of Order, Other, Hate Incident Non Crime, Criminal Damage and Drugs. Violence and sexual offences contribute 91 per cent of offence totals.

22. Cyber bullying is when one or more people try to tease, harass, threaten or embarrass another person using technology accessible via computers or mobile devices. Due to

the ease of access to smart phones and computers bullies can now harass a victim at any time via email, chat-rooms, and social networks. Although cyber bullying cannot physically hurt someone – the effects can be devastating with a victim eventually hurting themselves. Due to its 24/7 nature, escaping from it can be hard and victims can be left feeling very isolated, lonely, scared and vulnerable.

23. Cyber bullying is a topical media item and there have been high profile cases recently showing the devastating effect it can have. There have been no high profile cyber bullying cases like this in the Force area.

24. Sexual offences committed by cyber means are increasing year on year which is different to the Force trend of traditional sexual offences where levels are showing a small decrease over the past 5 years. This indicates that there is a switch from traditional methods to using the internet to commit or facilitate these crimes.

25. Possession and distribution of indecent photos and sexual activity with a victim under 16 contributes 93 per cent of this type of sexual offence reported to the Force. In the majority of offences the victims are under 16 or the photos are of children.

Financial Cyber Crime

26. Financial cyber enabled crimes are traditional acquisitive crimes that can either be performed or facilitated by using the internet.

27. The most common financial cyber enabled crime is fraud. Theft, Robbery and Handling Stolen Goods are included in the table below due the use of the internet to identify a victim or to sell stolen property.

Year	Fraud	Blackmail	Theft	Robbery Personal Property	Handle Stolen Goods	Total
2008	111	1				**112**
2009	195	2				**197**
2010	291	2				**293**
2011	352	3	1	1		**357**
2012	442	17	10	1	1	**471**
2013	15	11	4			**30**
Total	**1406**	**36**	**15**	**2**	**1**	**1460**

Financial cyber enabled crimes 01.04.08 to 31.07.13

28. Recorded cyber enabled fraud offences were seeing year on year increases through to 2012 but have seen a dramatic decrease during 2013 since the introduction of Action Fraud. This is due to their recording as national crimes. This, however, does not reflect the amount of victims in the Force area with Action Fraud holding 253 cyber enabled fraud records showing losses of approximately £350,000 during August 2013.

ORGANISED CRIME GROUPS

29. We are currently working with the NCA targeting a number of OCGs operating within the West Midlands area.

30. The Fraud Regionalisation Project was established by the Home Office in 2013 and a team has been created to tackle fraud with links to Organised Crime Groups. Operationally within the West Midlands the newly created team will sit within the ROCU

and provide an opportunity to address the threat posed by OCGs which will contain high proportions of both cyber enabled and pure cyber crimes.

CONCLUSION

31. Although the national issues are being addressed by the National Cyber Crime Unit, WMP recognises the emerging threats posed to its communities by cyber crime. Training of police officers and staff along with education of the community to prevention techniques is the key to reducing harm within the Force area. Ultimately trust and confidence will be influenced by the way in which we deal with victims, as with all other crimes.

FINANCIAL IMPLICATIONS

32. These matters are detailed in the above sections where relevant.

LEGAL IMPLICATIONS

33. These matters are covered in the above sections where relevant.

RECOMMENDATIONS

34. The Board is asked to note the contents of this report.

Stephen Graham
Detective Chief Superintendent
Head of Force Intelligence