Minutes

Minutes of the Thames Valley Police and Crime Panel held on Friday 27 November 2015, in Council Chamber Cherwell District Council Bodicote House, Bodicote, Banbury OX15 4AA, commencing at 11.00 am and concluding at 1.00 pm.

Members Present

Councillor Patricia Birchley (Buckinghamshire County Council), Councillor Angela Macpherson (Aylesbury Vale District Council), Councillor Kieron Mallon (Oxfordshire County Council), Curtis-James Marshall (Independent Member), Councillor Chris McCarthy (Vale of White Horse District Council), Councillor Bob Pitts (Wokingham Borough Council), Councillor George Reynolds (Cherwell District Council), Councillor Dee Sinclair (Oxford City Council) and Councillor Quentin Webb (West Berkshire Council)

Officers Present

Clare Gray

Others Present

David Carroll (Deputy PCC), Paul Hammond (Office of the PCC), Ray Howard (Thames Valley Police), Richard List (Thames Valley Police), Jacob Rickett (Office of the PCC), Anthony Stansfeld (PCC) and Ian Thompson (Office of the PCC)

Apologies

Councillor Julia Adey (Wycombe District Council), Councillor Margaret Burke (Milton Keynes Council), Councillor Robert Courts (West Oxfordshire District Council), Councillor Emily Culverhouse (Chiltern District Council), Councillor Trevor Egleton (South Bucks District Council), Julia Girling (Independent Member), Councillor Jesse Grey (Royal Borough of Windsor and Maidenhead), Councillor Iain McCracken (Bracknell Forest Council) and Councillor Ian White (South Oxfordshire District Council)

1. Declarations of Interest

There were no declarations of interest.

2. Minutes

The Minutes of the Meeting held on 25 September 2015 were agreed as a correct record subject to an amendment to item 2 – Minutes:-

“Dee Sinclair had expressed concern about taxis applying for licences in other local authority areas to the area they were trading in and also the need for local authorities to have a co-ordinated system. “

(01895) 837529
contact@thamesvalleypcp.org.uk
www.thamesvalleypcp.org.uk
@ThamesValleyPCP

3. Public Question Time

There were no public questions.

4. Themed Item - Cyber Crime

Detective Chief Superintendent Ray Howard and Acting Asst Chief Constable Richard List were in attendance. A/ACC Richard List introduced the item. Crime is changing moving away from burglary into an era of "new" crimes such as modern slavery, CSE and also cyber crime, which is largely driven by powerful changes in technology. In 2025 computers will be 25% more powerful.

Cyber crime sits in the middle of all risk. Reference was made to an iceberg; under water lay crime which not been reported to the police. The police have to look for this crime and this is a huge change in the criminal landscape. It is not a crime type; cyber crime is a crime theme and cuts across all types of crime in terms of investigation and the need to seize cyber equipment. A picture was shown of how life had changed in eight years with the prevalence of smart phones and tablets. Technology is part of main stream society in a short space of time. It creates opportunities for crime and this can be compared to the advent of the motor car. There is a mass of digital information and evidence out there. Figures include:-

- 182.9 billion emails sent and received each day worldwide
- 1 website in 1991 to 1 billion in 2014
- Internet users 2,925,249,355
- In the UK 21 billion texts and 50 billion instant messages sent per year – instant messages are free and texts cost money therefore instant messaging is increasing
- 24 million broadband lines in the UK
- 15 million twitter users in the UK
- UK mobile phone subscriptions 89.9 million
- Facebook holds 219 billion photographs worldwide
- Percentage of teenage girls who claim to have been bullied on Instagram – 9% - there are other websites used for bullying purposes
- 50 billion devices will be connected to the Internet by 2020 – the internet of things which could be cars, washing machines, household goods etc.

Cyber crime is defined as:-

Cyber Dependent Crimes, 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 commit further crime).

Cyber Enabled Crimes. '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. e.g. girl sending pictures of herself over the internet to a person in Turkey. The computer was then seized and following investigation it was found out that the perpetrator had been in contact with hundreds of people and the police need to understand of those contacted who are victims or defendants.

Crime prevention and detection usually works on three points; the offender, location and the victim. This falls apart with cyber-crime as there is no location or multiple locations and often no boundaries. A new system is now used with people, processes and technology but this is more complicated to address.

The **key threats** were outlined as follows:-

Key Threat 1 - The large scale harvesting of personal and business data to commit fraud offences against UK individuals and organisations. E.g Structured Query Language (SQL) attack involving Talk Talk where the company did not have the necessary guards.
Key Threat 2 - The targeted compromise of UK networked systems to modify, delete or steal data to gain competitive advantage, undermine user confidence, inflict reputational damage or gain control of infrastructure. e.g similar to industrial espionage and can damage a business. Criminals can buy DDoS attacks for $150 dollars. A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information. Big companies can usually resist these attacks but some small and medium companies do not have the capability.
Key Threat 3 - The targeted disruption of access to UK networked systems and services. There is a big risk from terrorist groups and there have been cyber footprint attacks in Canada, Estonia and the US. The Internal Revenue Service has had data stolen through cyber crime.
Key Threat 4 - The increasing volume of cyber dependent criminality is due to 'traditional' organised crime groups becoming technologically aware. For example gangs in London usually associated with guns and drugs now buy software off the shelf and make money through cyber crime with little chance of being caught.
Key Threat 5 - The gap between law enforcement and criminal capacity and capability is increasing. The police need to have access to modern day technology.

80% of cyber crime is preventable which is high. It was important to get this message out to people in order to keep their security systems updated and to take sensible precautions around personal data and changing passwords.

Local responsibilities:-

- Awareness of emerging national and regional structures
- Awareness of local responsibilities
- Understanding of Remit

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 / National Fraud Intelligence Bureau, including crimes in action. As an example, this may include incidents of: -

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

4 P's
There is an **Action Plan** and Neighbourhood Teams lead on this.

- Prevent

- Protect
- Prepare
- Pursue

It is important that the Force are ready for a major cyber attack. The full investigation of this is unlikely to come to TVP but the Force may need to deal with some consequences of this. There are many ways the Force can pursue low level cyber crimes.

Action Plan highlights

- National, Regional and Local strands
- Identification of necessary technology - upgraded intelligence offices with up to date laptops and better access to technology
- Communications Plan
- Increased training – The College of Policing is linked into the National Centre for Applied Learning Technologies. There is training for the Mobile Command Communications Team. For more specialist training there is the Digital Media Investigation course.
- Dedicated Open Source capability – this is where the Force can find out what is on the internet and what is not protected. For example they can look at social media to pick up any issues and evidence on crimes.
- Partnership work www.getsafeonline.org. Members were informed that this was a key website to look at and promote. Cyber Essentials which is an industry supported certification scheme developed by the UK Government to measure their cyber security systems.
- Organisational Learning – The Serious Organised Crime Unit share information so the Force can learn from it.
- Budget allocated for new and emerging technologies

Child Exploitation and Online Protection Centre – the sharing of indecent images is increasing

- Internet packages from across the world with UK IP addresses identified
- Regulation of Investigatory Powers Act – to identify IP addresses, intelligence and see if there is any threat, prioritise and action
- Intelligence
- Risk Assessment
- Action – Police Online Investigation Teams (POLIT) or Area

National Fraud Intelligence Bureau/Action Fraud – The Force that has the suspect living in that area picks up the crime but sometimes it can be where the victim or business is located. With a combination of resources from the Local Force, Regional cyber capacity and National Cyber Crime Unit the aim is to work together to prevent the UK from a high level systems attack and economic disruption. Examples of this include Sony and South Korea.

- National Response
- Worldwide Reporting
- Central Triage
- Suspect based allocation to Forces
- Intel Checks and local Triage
- Economic Crime Unit (complex cases) or local CID response

Five key points:-

- Cyber Crime is increasing and technology offers opportunities for crime.

- It will change – significantly. The Force need to keep up with how criminals are thinking and identify risks.
- Disruption and Prevention are key – volumes of people involved in cyber crime are vast but they can be stopped at source. The Force has a Communication Plan. Two dates highlighted were Black Friday and Cyber Monday.
- It is different – a fundamental historical shift
- The Unknowns – the Force need to keep their eye on the ball and see what is coming over the horizon before there is any criminal activity.

The PCC said that one of the most difficult areas was understanding the impact of cyber fraud on the Thames Valley. The Home Office have calculated between £35 and £65 billion nationally and with those figures in mind looking at the Thames Valley as the second biggest economic zone, this could account for £2-3 billion, which can be compared with burglary at £7 million or £30-35 million for rural crime.

The following questions were asked:-

Cllr Quentin Webb asked about **victims of cyber crime**? A/ACC Richard List reported that the main way of reporting cyber crime is Action Fraud. This is a national system which has had positive and negative feedback. Positive in terms of it being a good system for intelligence and triage; negative regarding victim support as the organisation does not update victims. The other way to report is a 'service call' through the local police. These calls generally refer to assignments that are typically distributed to public safety professionals that require their presence to resolve, correct or assist a particular situation. Action Fraud comes under the City of London which the police triage. They are then put into crime packages which can be investigated locally. Det Chief Supt Ray Howard commented that there was a big issue in terms of reporting which was very low, particularly from a business perspective there were concerns that one third of businesses had not reported a DDoS attack. This needs to be changed nationally so people are encouraged to report cyber crime and for it to be kept confidential. Some crimes are embarrassing to report such as personal internet dating sites. The public need to be reassured that the police will be very supportive as it can be easy to fall victim to cyber crime with the level of sophistication and psychology used.

Cllr Patricia Birchley asked the PCC whether the police should be responsible for policing the internet? The PCC reported that there were not enough trained people to deal with the scale of the problem. There needed to be a separate national agency similar to GCHQ that could deal with complex cyber crime, which cuts across force boundaries. The police should be enforcers' not detailed investigators. People using the internet for crime were experts and the police force were limited in number, particularly for this type of expertise. He was concerned that some victims report crimes through Action Fraud which then disappear into the system and the victim has no feedback. A recent company lost £52,000 and this was considered below the threshold to be investigated. Less than 2% of crimes are investigated by Action Fraud which showed the scale of the problem.

Cllr Angela Macpherson asked about a body of expertise being built amongst school children. Det Chief Supt Ray Howard reported that this was being undertaken by Estonia who had suffered a major cyber attack. Unless the UK experienced an attack of that scale, this would not be pushed forward by the Government. However, there was a natural improvement in people's knowledge as younger generations start employment. A/ACC Richard List reported that there were regional level partnerships in place with industry who pass on information to the police. Officers particularly work with schools on cyber crime and there is a huge amount of available information on the internet for young people and parents. Parents need to educate their children on basic precautionary measures. As mentioned before

80% of crime could be prevented which is key. Information filters down on an international basis through the hierarchy to the National Cyber Crime Unit downwards. There is the Cyber Security Information Sharing Partnership which was launched in March 2013 which allows the Government and Industry to share information on current threats and managing incidents on a secure platform. School children are educated on being safe e.g SMART poster but parents need to keep well informed as well. It is difficult to monitor phones particularly. Get safe on line was a very useful website.

Cllr Bob Pitts asked about how Members could inform residents about cyber crime and also how young children who have commited crimes could be used to help prevent cyber crime.
Det Chief Supt Ray Howard referred to the Thames Valley Fraud Alerts and also the Get Safe Online website which would be helpful to promote at public meetings. In terms of using hackers he gave an example of a crime committed in 1998 which was the first ever virus called the Morris worm. The person was convicted but is now a Professor at the Massachusetts Institute of Technology. The other area to raise awareness was the use of dating sites. The PCC reported that a major terrorist plot was cyber enabled and engineered by a 14 year old who found people on the other side of the world to carry out the attack for him.

Cllr Dee Sinclair commented that she was relieved to hear the police say crime is changing rather than reducing which is misleading, particularly when looking at the prevalence of cyber crime. It was important to raise awareness and focus local meetings such as Neighbourhood Action Groups on key issues such as cyber crime rather than the old traditional concerns such as parking. Education of the public to the vulnerability of this crime was crucial for the young and older generation. Days such as Black Friday were an opportunity to do this. Are all Police Officers given training in cyber crime? What about visibility of police officers ?

- A/ACC Richard List reported that there was training at different levels. There was online training (NCALT in full above). There were seven modules which covered basic awareness of cyber offences. The next level up was for the MCCT (in full above) which was a course designed for detectives. It was a week long and funding had been pump primed from the Home Office looking at cyber crime, the internet and social media. There was a higher level Digital Media Investigators course where people were trained to advise senior investigating officers dealing with serious offences. The challenge going forward is to keep the training relevant. Private sector providers work with the Force to fill any training gaps which is across the region including Hampshire, Sussex and Surrey.
- Visibility was a difficult issue with cyber crime. The police were visible on internet law enforcement and there was visible information about policing on this area which they were looking to develop. There was a lot of information for vulnerable young people in terms of bullying. Visibility and awareness had to be undertaken in partnership and the Force were only one part of that. Other partners included schools and parents. In terms of adults they were working with Age Concern as some older people did not update their security and were still using Microsoft 98. The presentation will be circulated to Members so that it could be used to help increase awareness.

Curtis-James Marshall commented that training, education and building on expertise including partnerships with industry had to be the way forward. He expressed concern that it must be difficult to recruit and offer the right level of pay and benefits competing with the private sector. This was a national issue which should be addressed by the Government and PCC's should use their influence. GCHQ go to the Shoreditch area (known for companies with technical expertise) to recruit. He was concerned about the value of in house training using NCALT.

Cllr Angela Macpherson asked a question about perpetrator profiles? Are they involved in other forms of offending? Det Chief Supt Ray Howard reported that it was difficult to analyse across several areas with the way information was collected. However, they did do this for child abuse looking at who was involved, how often they offended and other information on co-offenders and criminal records. The difficulty was that cyber crime was so broad that this type of work was insurmountable. There was some work being carried out by Cambridge University on this area. http://www.cam.ac.uk/research/news/ . One of the issues was that cyber crime was global therefore looking at a crime in Slough Magistrates Court would have no meaning to a criminal in Russia. Software as a service is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. This model makes it very easy to commit crime by buying skills and training and gaining access to the 'dark web'. Another area was the 'gaming' industry which the police were looking at. Some young people did not see cyber-crime as an offence.

Cllr Patricia Birchley referred to technology facilitating terrorist attacks and examples where terrorists were using the blackberry system to contact each other which was difficult to track. Acting Det Chief Supt Ray Howard referred to the 2011 riots which were a watershed in the social media world where the police did not have the right intelligence on social media. The Force at the time just had stand alone google computers. The Home Office is now funding IT to investigate social media and look at trending and what people are saying. There are open source capabilities which offer new information to the Police and prevent crime and disorder in a more effective way.

Cllr Quentin Webb referred to performance recording and whether cyber crime was recorded under its own area or type of crime? Det Chief Supt Ray Howard reported that with cyber crime it is not referred to as one type of crime but is a theme of reporting. It was problematic for example rape often involved social media but was recorded as a rape. Pure cyber crime was recorded under the Computer Misuse Act as this was straightforward. Most cyber dependent crime was recorded under the crime itself. It was important to flag this more to get a picture emerging more effectively on cyber crime. This was a huge threat not currently borne out in police crime figures.

A/ACC Richard List reported that to monitor the efficiency of the Force it was important to see the performance level to control or fight cyber crime and the PCC can view that increasingly. However this was a national problem which was being addressed at the regional level but it was still not possible to show the true element of cyber crime.

Ray Howard and Richard List were thanked for their presentation and questions. The Vice Chairman emphasised the public cyber street wise campaign https://www.cyberstreetwise.com/ and suggested that it may be helpful to look at whether a Working Party should be set up to look at this item in more detail.

Summary

- **Panel Members to use their influence to ensure that preventing cyber crime is highlighted at local public meetings, with parents and with local partners, including the get safe online and cyber street wise websites**
- **PCC to continue to influence the Government on prioritising cyber crime and ensuring that adequate resources are invested into this area including developing young people and specialised training**

- **Following the PCC elections, Panel Members may wish to reassure themselves that cyber crime remains a high priority within the Police and Crime Plan and how the PCC will measure success in delivering his objective.**
- **To consider whether a Working Group should be set up to look at this area in more detail.**

5. Report of the Preventing Child Sexual Exploitation Sub-Committee

The Vice-Chairman of the Child Sexual Exploitation Sub-Committee reported on the first meeting which had been held on 3 November 2015. He reported that the NSPCC website shows that over 2,400 children were victims of sexual exploitation in gangs and groups from August 2010 to October 2011. 10% of children on Child Protection Plans had suffered some form of sexual exploitation. There were 476 occurrences linked to CSE in 2014/15. The Crown Prosecution Service prioritised CSE and there was a joint protocol which helped ensure that both organisations are prepared and empowered to deal with the changing nature of case work and to provide greater consistency in the handling of these cases.

The Police and Crime Commissioner reported that a study was being carried out by Oxford University on CSE and also there was a national Independent Inquiry into Child Sexual Abuse which will investigate whether public bodies and other non-state institutions have taken seriously their duty of care to protect children from sexual abuse in England and Wales which would be led by Hon Lowell Goddard. The PCC commented that he hoped this Inquiry would also look into the Operation Bullfinch recommendation (see two below).

In terms of the future Work Programme, Cllr Angela Macpherson reported that it would be useful to look at the co-ordination of partnership working across the Thames Valley as many local authorities are looking at this issue from different angles and it was important that recommendations are actioned and collected together.

The Panel AGREED the following recommendations:-

1. **That the Scrutiny Officer should speak to the LSCB in Oxford to gain a better understanding of any issues concerning language schools and if necessary invite them to a future Sub-Committee meeting.**

   This was raised as a concern by the PCC and a Panel Member because this area was not regulated.

2. **That the PCC and Panel Members lobby Government to implement the Bullfinch recommendation or to look at the opportunity to commission independent academic work subject to available resources due to limited budget.**

   The Bullfinch recommendation not implemented was as follows:-

   "With a significant proportion of those found guilty nationally of group CSE being from a Pakistani and/or Muslim heritage, relevant government departments should research why this is the case, in order to guide prevention strategies'

3. **That the most effective MASH model be scrutinised by Sub-Committee Members and as appropriate Panel Members should promote the adoption and implementation by all local authorities across the Thames Valley of best practice. That the Sub-Committee look at the co-ordination of work undertaken by the MASH's across the whole of the Thames Valley.**

   The PCC expressed concern about the ability to provide resources for six MASHs in Berkshire which could impact on their effectiveness. Members thought it would be helpful to identify best practice which can be shared and to ensure that there was good co-ordination across the Thames Valley.

4. **That the Panel Members be asked to identify which of their Authorities scrutinise their LSCB's and at what frequency**

   As the LSCB were not held to account by another body (a government report states that the Chief Executive and Lead Members, through Scrutiny Committees, should be more central to the governance process to ensure that the Chair and the Board are held to account) Members thought it would be helpful to obtain feedback from Panel Members on how their LSCB are held to account and at what frequency.

5. **That the PCC be asked whether it would be possible for the Hotel Watch Scheme to be rolled out across the Thames Valley.**

   This was a recommendation from the Bucks County Council Inquiry Report (Minute 6) for Buckinghamshire and the suggestion was that this should be extended to the Thames Valley if possible.

6. **For the Panel to scrutinise whether to there was a co-ordinated response in relation to licensing and transportation of children in the Thames Valley.**

   This was a recommendation from the Oxfordshire stock take report that regulation of these two areas could be more robust. The role of Licensing Authorities and Taxi drivers was also considered as part of the Bucks County Council Inquiry Report.

7. **For the Panel to ask their relevant Cabinet Member (County and Unitaries) that through their commissioning process that all sexual health providers are asked to facilitate the sharing of information on repeat referrals within a confidential environment for high risk children.**

   There was a similar recommendation to this one proposed through the Buckinghamshire County Council Inquiry Report. The Terence Higgins Trust operates a 'red flagging' system which makes practitioners aware of when they are dealing with repeat referrals. There is no sharing of information on children presenting frequently at different providers. Sexual Health Services are commissioned by the Public Health Team with the decision being taken by the relevant Cabinet Member who may be able to influence the sharing of information through the commissioning process.

6. Verbal report on the Police Funding Formula

The Home Office recently announced that it will be revising the policing funding formula, which determines the level of grant funding police forces receive from central Government. The formula was

being changed as it was out of date. There are five proposed principles behind the new proposal - being robust, stable, transparent, future proof and incentivising Government objectives.

The PCC reported that the Thames Valley Police were relying less on the Government Grant and were an efficient police force at roughly £100 grant per head of the population. The Thames Valley suffered considerably with funding compared to other Forces and larger police forces particularly suffer from the new formula. Some Forces could receive £165 per head with the new formula. The proposed new formula could lead to further cuts in the grant of at least £6-7 million per annum. The new formula took account of population, deprivation and the number of licensed establishments in the area and how close they were to police cells rather than how far away they were. A Force covering an area with 1000 public bars could receive the same funding as one with 100 bars. The last criteria would have an impact on Thames Valley because of the size of this region. It also impacted adversely on other large or rural geographic force areas such as Devon and Cornwall, Sussex, Cumbria, Surrey and North Yorkshire. In addition no account was taken of the number of roads in the formula and the cost of roads policing.

The Government had now delayed the funding formula by a year because of calculation errors.

The PCC's Chief Finance Officer reported that the 2016/17 grant settlement was expected on 17 December and there would be no budget projections until then. Cllr Dee Sinclair asked whether the criteria for the funding formula would be changed or whether it would be just re-calculated. The PCC reported that there should be far more consultation next year on the formula and the Home Office would write to PCC before the start of the next review.

The report was noted.

7. Tone from the Top - The PCC Response to the Report of the Committee for Standards in Public Life

In October 2014 the Committee on Standards in Public Life began an Inquiry into local policing accountability in England and Wales as to whether the accountability model was effective in supporting and promoting high ethical standards. In June 2015 it published its report 'Tone from the top – Leadership, ethics and accountability in policing'. The report made 20 recommendations to the Home Office, Police and Crime Commissioners, Police and Crime Panels and relevant Associations.

The Panel noted the attached response of the Police and Crime Commissioner and agreed the tabled response of the Panel.

8. The PCC's response to recent HMIC Reports

The PCC reported that he was required to publish comments on reports relating to the Force sent to him and the Chief Constable by Her Majesty's Inspectorate of Constabulary. The Chief Constable then presents comments to the PCC Policy, Planning and Performance meetings to facilitate transparency and accountability which are available on his website.

http://www.thamesvalley-pcc.gov.uk/Transparency/Agendas-and-Minutes.aspx

The last HMIC reports were discussed at the last Policy Planning and Performance meeting:-

- In Harms Way: the role of the police in keeping children safe
- Online and on the edge: real risks in a virtual world
- Building the picture: an inspection of police information management

- The welfare of vulnerable people in police custody.

The PCC reported that HMIC reports were a valuable source of information.

The Panel noted the report.

9. Report of the Complaints Sub-Committee

The report of the Complaints Sub-Committee held on 25 September 2015 was noted by the Panel.

10. General Issues

The report on general issues covered the following areas:-

- Police Funding Formula
- Bedfordshire PCC looking at ways to help budget cuts
- HMIC Police Efficiency Report
- Article on complaints
- Good practice for police and crime panels
- Terrorism.

The Panel noted the report.

11. Work Programme

The Panel noted the Work Programme and agreed that cyber crime should be looked at in more detail, including the Prevent agenda, taxi licensing and illegal traveller sites.

12. Date and Time of Next Meeting

29 January 2016 at Aylesbury Vale District Council

CHAIRMAN

This page is intentionally left blank