Agenda Item No. 4

COMMUNITY OUTCOMES MEETING

TACKLE CRIME AND ANTI-SOCIAL BEHAVIOUR

12 SEPTEMBER 2017

SUBJECT: CYBER CRIME

Report of the Chief Constable attached

PURPOSE OF THE REPORT

1. This report outlines the Force's current position in relation to the policing of cybercrime.

RECOMMENDATION

2. That the Police and Crime Commissioner (PCC) uses this report to scrutinise Force activity in respect of cybercrime.

POLICE AND CRIME PLAN

3. As technology develops, so too does criminality and more and more crime is being carried out online. Crime carried out in "cyber space" is borderless and often comes with a level of anonymity for the offender which would not be seen with many conventional crime types, posing challenges for those who are trying to prevent, detect and prosecute such criminals. We need to do more to understand the threat of cybercrimes such as online fraud, grooming, and cyber bullying, educate the public about these risks, and work with others including private industry to develop the right tools and skill sets to properly investigate and prevent these crimes.

KEY INFORMATION

4. The PCC provided funding of £250,000 in 2015 to help set up a West Yorkshire Police Cyber Crime Team to develop the approach and facilitate learning amongst wider officers. More serious cybercrime is dealt with by the Regional Cyber Crime Unit, the PCC has met with both teams to hear about the work they do and their work will continue to be supported through collaboration and the funding attached to it.

5. The PCC is represented on West Yorkshire Police's Cyber Project Board which has oversight of the cybercrime response from a strategic level, tactical and district level.

6. The PCC is represented on and has met with West Yorkshire Police's Cyber Independent Advisory Board that comprises of partners from the public and private sectors and academia.

7. West Yorkshire Police and the PCC host information on their websites for members of the public and businesses on how to safeguard themselves online, and regularly promote this information through social media and the PCC's newsletter.

8. The PCCs Safer Communities Fund has funded 6 projects worth over £27,000 that have a cybercrime focus.

9. The PCC supported the national Safer Internet Day 2017 – the day is celebrated globally in February each year to promote the safe and positive use of digital technology for children and young people and inspire a national conversation.

10. The PCC is working with West Yorkshire Police to create and run a young person's cybercrime competition. The competition involves school children in years 7, 8 and 9 and involves them designing a cyber prevention resource.

PARTNERSHIP WORKING

11. The PCC supports a range of partner work and initiatives. Specifically the PCC has supported cyber prevention and awareness campaigns from the NSPCC, Get Safe Online and the NPCC.

WEST YORKSHIRE POLICE

Chief Officer Team
Briefing for PCC

Title: **Cyber Crime Update**

CoT Sponsor: **ACC Foster**

Report Author: **D/Insp Benn Kemp**

1. Background

The report contained in this paper outlines the general position and progress of the Force with regards Cyber Crime and follows on from a previous report dated the 07/03/2017

The report will outline the continued progress the Force have made in tackling Cyber enabled and dependant crime. In particular in understanding the threat, working with partners and the community to protect and prevent criminality whilst continuing to investigate those who offend. In the 6 month period since the last report the Force Cyber Crime Team has undergone a significant staffing change through the natural turnover of staff, because they are highly skilled and sought after.

Cyber dependant crime can only be committed through the existence of a computer EG; Hacking / Denial of service attacks

Cyber enabled offending is any criminal offence which when committed is aided by the use of a computer EG; Harassment over social media.

1.1 Force Position

- The policing strategy identifies that Cyber Crime is a priority risk area for the Force with regards to our purpose of reducing crime.

- The Force strategic assessment highlights that Cyber Crime represents a current and long term threat facing the force. The changing nature of Cyber Crime and criminality presents a challenge which requires a significantly different approach and skills to that of traditional policing.

- The forces "Attack Criminality strategic plan 2017/2018" features Cyber Crime detailing the resourcing and structure of the Cyber Crime Team and the placement of DMIs as key areas in achieving the strategic aims.

- West Yorkshire Police has a clear Cyber governance structure across strategic, tactical and operational levels with a Force Cyber Crime Team and a Cyber response at each District.

- West Yorkshire Police continues to be leading nationally around many areas of Cyber through innovative work such as the Independent Advisory Group and Cyber prevention activities. (details listed below)

- Cyber enabled and dependant offending continues to increase steadily in line with national levels.

2. Explanation

2.1 Offending -

2.1.1 Force Data 2016 key findings

During 2016 there were a total of 3087 Cyber offences recorded in West Yorkshire which is an 8.4% increase compared to the previous year (2015).

Cyber dependant crime (offences committed under the computer misuse act such as hacking / DDOS) increased by 62% in 2016. There has been a further 30% increase in the first 6 months of 2017.

Over half of all recorded Cyber Crime in 2016 was classified as "Violence without injury" which captures offences such as harassment and unwanted contact with 2034 reported crimes a 40% increase on 2015 data. Of those malicious communication offences females aged 18-34 were identified as most likely to be victims been involved in over half of the offences. 70.6% of victims were female.

In 2016 591 Cyber flagged offences were involved sexual offending, the majority involving indecent images of children. This is a 32% reduction on the previous year.

Fraud was the third most common offence with 462 offences flagged. In 2016 a large proportion of offending involved social media, with Facebook the most popular medium with 42.2% of offences relating to this, this is consistent with 2015 data (42.1%).

Figure 1 – Comparison of Cyber categories by volume of total offending 2015 v 2016

It should be noted that these are the offences where a flag has been applied and the total reported offences are anticipated to be higher. The Force continues to drive performance around the application of Cyber flag on the crime system.

The Force has a more detailed understanding of Cyber related offending than other peers nationally.

Leeds had the largest number of offences recorded but per 1000 of population Calderdale had the highest rate of cybercrime in the force.

West Yorkshire Police have seen a continued rise in reported Cyber enabled and dependant crime in this 6 month period (January to June 2017) compared with the previous 6 months (July to December 2016).

In the last 6 months the Force has flagged 1754 Cyber offences, this represents a 32.4% increase on the previous 6 months. The majority of these are Cyber enabled offences with a small increase in flagged dependant offending. This overall increase is reflected through an increase in flagged sexual and indecent offences of 23% to a total of 266.

Harassment and unwanted contact offences represent the largest area of offending with a total of 1290 flagged offences in this period a 43.3% increase on the previous 6 months. This is attributed to a real terms increase in offending and an internal drive for the correct application of the Cyber flag.

2.1.2 Action Fraud data – (2016)

There were 6777 victim fraud reports in West Yorkshire averaging 565 per month a 4% increase from 2015. The reported loss / potential loss for these victims is £45,974,269 averaging £3,831,189 per month.

The top fraud in West Yorkshire was online shopping and auction fraud (1197 reports) and computer service software frauds (764 reports).

Of all reports 7.2% related to dependant Cyber Crime (6.7% reduction on 2015 data). The loss for dependant Cyber Crime averaged £87,425 per month.

Figure 1 – Cyber dependant offending dashboard October 16 – March 17

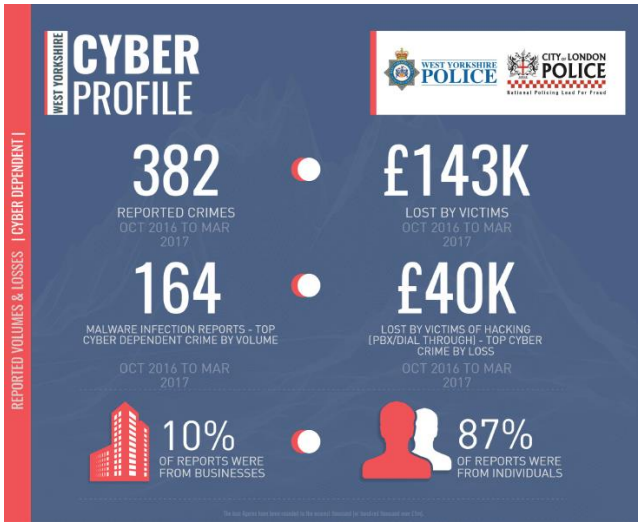

Figure 2 – Cyber enabled offending dashboard October 16 – March 17

Action Fraud data is generated nationally and is widely accepted to not be as accurate as Force data. The West Yorkshire Police Cyber Crime Team continues to work with the National Fraud Intelligence Bureau to improve the data. Such reasons for this include inaccurate IP data and inputting errors, also crimes recorded by Action Fraud are not necessarily sent onto to Forces to deal so no local crime would be generated.

2.2 Governance

Cyber governance is managed through the Cyber Strategic Board, chaired by the Head of Crime ACC Foster, meeting on a three monthly basis. (Work is ongoing to ensure this board and some boards under the digital policing gold group complement each other.) West Yorkshire Police remains 100% compliant with the College of Policing Cyber Crime Framework. We consider this document to becoming outdated in some parts and will be superseded by the requirements of the NPCC Digital Intelligence and Investigation programme.

A Cyber Tactical Board meets monthly with District Cyber leads for each District attending, each district then has a Cyber board meeting with frontline officers and staff working to District action plans. This structure has proved effective in delivering the changes needed for Districts to meet the threat of Cyber Crime and deliver the Policing Plan. This group is working to a Cyber District action plan which will ensure that the entire force has a good standard of Cyber prevent, prepare, protect and Pursue across every District.

The Force also has a Cyber Crime Prevention Group made up of practitioners co-ordinating prevention work across the Force.

These structures are nationally innovative and have been nationally highlighted as leading practice. A number of other Forces are seeking to replicate this model and in the last three months we have hosted three Forces wishing to view our Cyber structures and response. West Yorkshire Police continue to work with partners in communities on the subject of Cyber.

3. Ongoing Work

3.1 Investigations

3.1.1 Cyber Crime Team – The Cyber Crime Team have gone through a significant staffing change and currently carry 5 vacancies for Cyber officers. This has resulted in a small workforce remaining and resulted in the need for further recruitment. I am pleased to report we have a candidate proceeding through vetting and a further 30 applicants going through a recruitment process to fill the other spaces.

In the last 6 months the Cyber Crime Team have continued to support around 30-40 investigations with specialist tactics and advice.

3.1.2 Digital Media Investigators – The Force has invested in specialist training to create 38 Digital Media Investigators within the Force. These assets are shared across the 5 Districts to reflect threat. The Force has been allocated only a handful of DMI courses for the current national training plan which we do not feel will meet the needs of the force. We have started to explore other options and have worked with the Force training school to develop a bespoke accredited training course which can ensure that officers working within the communities of West Yorkshire continue to have access to specialist knowledge for both serious and complex crime, and volume crime.

The Cyber Crime Team have planned a regional Digital Media Investigator day at Carr Gate Training Centre to be held in August. The day will feature guest speakers from across UK law enforcement and academia, this ensures that staff within West Yorkshire remain at the forefront of technological changes and developments.

3.1.3 Force wide training - The Force has continued to invest in the training of all staff around Cyber Crime. All new recruit Police Constables have three days intensive Cyber training allowing them to effectively use internet evidence and respond to Cyber threats. New Investigation Officers (IO) and Customer Contact Centre staff receive a Cyber input as part of their basic training. All Detective ranks receive Cyber inputs as part of their basic training. The Cyber Crime Team have continued to roll out training to all staff across the organisation with partners, though a reduction in available staff has impacted the current capacity to deliver. Safer Schools Officers and Crime Prevention Officers from across the Force have also received specialist Cyber Crime training inputs.

Of note in June a training event was held at Carr Gate which targeted all staff across the Force and was attended by nearly 100 people. The event provided inputs on banking risks around Cyber from City of London Police, investigations from the Cyber Crime Team, and Cyber engagement with young people from the PSCOs in Bradford. This day upskilled frontline staff in the latest prevention advice to share with the community.

In January the Chief Constable's Proceeds of Crime monies funded 30 senior detectives from across the Force (Detective Inspectors and above) to attended a two day GCHQ accredited course in, the training focused on effective responses to Cyber incidents. In this period we were able to repeat the training, which had 30 senior officers and staff attend from across the four regional Forces. This will assist in ensuring the Force is ready at all levels to respond to Cyber offending.

The Force remains committed to the development of staff to meet the challenge of Cyber Crime.

3.2 Prevention

3.2.1 Overview - West Yorkshire Police continues to focus heavily on the prevention of Cyber Crime. The Cyber Crime Prevention Group has met monthly and with the support of the Cyber Crime Team continues to work with Districts to drive prevention work.

The Force has pioneered a Scouting badge for crime prevention of which 50% focuses on Cyber, this requires the thousands of young people across the scouting network to engage with their parents and complete activities to gain knowledge and understanding of risks associated with Cyber and beyond. This has been trialled in KD and CD and the Force has worked with partners to develop the material around this and will be rolling this out over the next 6 months.

The Force has also reviewed and refreshed the prevention material available throughout the Force. This has resulted in a redesign and refresh of content on the Public facing website, the creation and production of new guidance documents for the public and some nudge cards. These tools ensure that officers and staff have material that is relevant to effectively safeguard the public and also gives the public tools to protect themselves.

The Force has aligned all of the safer schools presentations focused on Cyber so age relevant corporate inputs are delivered across the force to our younger residents.

The Force is about to launch a Cyber competition for all 11-14 years olds via the education network. Each secondary school in West Yorkshire has received an invite to participate in the event (around

1400 schools), pupils will be required to research and identify a Cyber problem, then identify how this can be prevented. They will then have to develop some prevention advice to be delivered in a medium of their choice such as an app, website, leaflet etc. Each school can submit one entry per year group. All finalists will be invited to Carr Gate around safer internet week where the winners will be announced.

The Chief provided a featured article in the Yorkshire Post which was positively received and provided crime prevention advice. This was then followed with a Cyber week in the Yorkshire Post with features from officers and others focused on Cyber.

3.2.2 District Highlights – Within West Yorkshire each District continues to undertake bespoke work tailored to their communities needs and join together for significant events such as Safer Internet Day. All Districts continue to make effective use of social media to promote these messages.

Bradford District have created a small District Cyber Team made up of PCSOs focused on providing prevention advice. The team continue to provide advice and guidance to primary schools across Bradford with great success.

Kirklees officers worked with Huddersfield University drama undergraduates to develop a Cyber themed play focusing on the risks young people face. This was opened by the PCC and well received. This is now been made in a video to ensure future students at KD high schools benefit from the learning.

Wakefield continue to hold successful engagements events in key locations on a regular basis with partners such as the NSPCC, O2 and Barclays Digital Eagles.

Leeds District through their Crime Prevention Officers have delivered crime prevention advice to businesses through established networks. Recently supporting banks across Leeds in holding online safety events.

Calderdale continue to deliver inputs to young people across schools to great effect.

3.2.4 Regional Prevention Group - West Yorkshire have taken a lead role in forming a regional campaign group with representatives from each of the four regional Forces, South Yorkshire Police; North Yorkshire Police and Humberside supported by the West Yorkshire OPCC. The group have devised a calendar of campaigns that will be supported over the next twelve months to highlight the threat areas. DCI Smith (Regional Protect officer) will be doing a monthly Facebook Live event to highlight the regional activity each month. Key themes have been supported with social media coverage and prevention guidance.

4. Forthcoming significant work

4.1 Police Knowledge Fund

The police knowledge fund concluded on the 31/03/2017 where a conference was held attended by the Chief and other senior figures from UK law enforcement and academia. This collaborative project between West Yorkshire Police and Leeds Beckett University funded by the HEFCE and the College of Policing has been ground breaking and delivered some nationally significant results.

The findings of the project were presented to the strategic board last month. The Force is looking to develop an action plan to ensure that the development are embedded within the Force.

A number of activities are already ongoing around this work.

The final results are not officially published until September 2017**.**

4.2 Review

The Force Cyber Crime Team will be undergoing an internal review to ensure it remains fit for purpose. The team was established over two years ago with a view to upskill the capability of the Force and mainstream some of the key skills. This has been realised and a review is required to identify the next steps for the Cyber Crime Team in terms of training, resourcing and strategic direction.

PSC SLT are identifying resources to complete this work.

4.3 Prevention

The Force Cyber school survey is due to close shortly and this will provide a wealth of learning for us and partners around the activities of young people online. Last year's survey delivered key information which was used to benefit and inform safeguarding boards across the force and upskill staff and officers.

4.4 Training

The Force is developing a modular training plan to ensure staff remain skilled in dealing with Cyber offending. The will be tiered relevant to an individual's position and role within the organisation. This will result in all staff and officers exceeding the national standards around Cyber training and ensure the Force remains at the forefront of Cyber.

The Force is also perusing a collaboration opportunity with the other Forces in the North East region to develop a training hub focused on Cyber. This is still in its infancy and further information will be available at a future Community Outcomes Meeting.

5. Strategic Risk / Legal Opinion

Cyber Crime continues to be a priority. Demand in Cyber Crime is increasing significantly and all UK Police Forces are facing a challenge to meet this.

West Yorkshire Police remain well placed nationally in understanding the current threat, but like other Forces nationally the understanding of the longer term threat is still not known. West Yorkshire Police are supporting national intelligence development right from the front line through to specialist resources' and the NCA to understand this.

The new Investigatory Powers Act covering communications data providers is still not in force, but this will allow new opportunities to protect the public further and investigate crime.

6. Community Impact

A range of communities are effected by Cyber enabled and dependant offending. The Force continues to support and advise communities on this matter through traditional means as well as engaging with new and emerging communities online and via other forms of media.

7. Equality and Diversity Consideration

The Cyber Crime Team continue to work with a number of organisations within the Cyber Advisory Group including a diverse range of charities to ensure prevention messages are delivered in the most appropriate way for all communities.

8. Human Rights consideration

N/A

9. Financial Implications / Affordability

The continued training of the team to maintain pace with the speed of technology is a challenge for budgets to maintain. The Proceeds of Crime fund has been key in providing funding for equipment and training for the Cyber Team and senior detectives.

10. Appendices

N/A