Agenda Item No. 4

COMMUNITY OUTCOMES MEETING

TACKLE CRIME AND ANTI-SOCIAL BEHAVIOUR

17 APRIL 2018

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 cyber crime.

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 cyber crime 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 cyber crime focus.

9. The PCC supported the national Safer Internet Day 2018 – 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 worked with West Yorkshire Police to create and run a young person's cyber crime competition. The competition was for school children in years 7, 8 and 9 and involved them designing a cyber prevention resource. The competition was a success and planning has started for the competition to run again.

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 1st August 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.

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 Police and Crime Plan details cybercrime as one of its key priorities, confirming that we need to more to understand the threat of cybercrimes such as online fraud, grooming and cyber bullying, educate the public about the risks and work with others to properly investigate and prevent these crimes.

- 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 threat assessment has reassessed the risk of Cyber-crime and this is no longer a top ten threat area.

- 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. Ongoing Work (August 17 to March 18)

2.1 Flagging

All crimes which are Cyber enabled or Cyber dependant should be subject to the application of a Cyber-crime flag. Each crime with a flag is reviewed by the cyber-crime team who, where required, write a bespoke digital strategy on the crime. This ensures that the investigating officer is conscious of the lines of enquiry that exist and how best to safeguard the victim. The flag also allows effective analysis of the crime types, trends and patterns of both enabled and dependant offending. These flags are applied by officers and only around 40% of relevant crimes were flagged.

2.2 Investigations

ACC Foster has mandated some additional work which has resulted in a 100% accurate 3 months period of flagging data (Oct 2017 to Dec 2017) and developed a process which will be 100% accurate in the future. This is been rolled out across each district and the results of this are being analysed. A detailed report should be available in the next period.

Early indications suggest in the three month period October 17 to December 17 a total of 2490 offences both enabled and dependant were identified. This is a significant increase on previously flagged data. Leeds district alone identified a further 1000 offences.

2.2.1 Cyber Crime Team

The force Cyber-crime team has completed the restructure process with Detectives now in post. The ongoing work through the tactical board has ensured that the cyber investigative capability of staff at districts has been improved significantly with tools, training and access to material. This has allowed the Cyber-crime team to focus on the most serious and complex cyber offending, reviewing all flagged crime and supporting these investigations.

The team is currently delivering a bespoke response to each referral which is passed from Action fraud in to the force. This is improving victim experience and delivering greater safeguarding and investigative opportunities.

2.2.2 Digital Media Investigators

The Force has invested in specialist training to create 38 Digital Media Investigators across the Force. These assets are shared across the 5 Districts and specialist teams to reflect threat. Whilst the force acknowledges that there is a need to increase the number of digital media investigators, this ambition has been hampered by the lack of training provided nationally by the college of policing. In response to this problem the force has invested in training resources to develop a bespoke advanced digital course, which will allow the force to train sufficient staff to the required levels to meet the needs of the force. This is anticipated to be completed by July 2018.

The Cyber Crime Team continue to deliver Continuous Personal Development events for both Digital Media Investigators and Senior Investigating Officers. All digital media officers have received specialist training around Wi-Fi networks and internet investigation within the relevant period.

2.2.3 Force wide training

The Force has continued to invest in the training of all staff around Cyber Crime to meet the current and anticipated threats.

All new recruit Police Constables have three days intensive Cyber training allowing them to effectively use internet evidence and respond to Cyber threats. These inputs are in the process of being refreshed by the force training school and cyber-crime team. 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.

Following a review and consultation period the force training school has developed a suite of training courses focused on cyber-crime which will be relevant for all staff. Starting with E-Learning packages for all staff right through to advanced courses for practitioners. These courses are the first of their kind within the UK and make best use of digital technology including virtual reality.

2.3 Prevention

2.3.1 Overview

West Yorkshire Police continue to focus heavily on the prevention of Cyber Crime, developing and delivering nationally innovative work.

The Force held the Cyber schools competition final at Carr Gate on the 7th February 2018 to coincide with safer internet day, this event was attended and supported by the PCC and the deputy head of

crime, Mr Ridley, along with partners at Barclays and the NSPCC. The final involved the 7 schools (50 children in total) presenting their work, ranging from apps which they had developed to theatrical performances all focused on cyber security. The winners were Corpus Christi academy who delivered a dance and drama production. The judges commented on the legacy of the work they had done and the amount of hours that were put into this. The final was livestreamed on social media with 4,000 views, following the event press articles appeared in local media. Each of the children received a medal and certificate whilst the winners won a guided tour of Carr Gate. Each of the groups work will be built into their schools curriculum for future year 7 students to benefit from the learning. Planning has started for this next year.

The force held events in each of the districts to coincide with safer internet day with emoji quizzes, live blogs along with a series of Facebook live events and media work across the forces social media accounts. This work engaged with over 1000 people in person and over 30,000 online. The activity received lots of praise online with many people commenting their appreciation of the work West Yorkshire are doing around this. Each of the events focused on keeping people safe online.

The force through POCA funding will be launching "The Matrix Cyber Challenge" this will be a technical competition focused on identifying those 11-18year olds who have advanced cyber skills, with a view to ensuring these are channelled in the right direction. This is been developed in partnership with the Regional Cyber-crime team, Gorilla Tech and the National Cyber Security Challenge. We are developing a website, where entrants will complete a series of technical cyber challenges to progress through stages to reach a final in September 2018. After each stage a prevention exercise is required to be completed. At the end of the contest a careers day will be held where all entrants will be invited to attend along with a number of public and private sectors partners to discuss career pathways and opportunities.

In year one this will only be open to those receiving schooling within West Yorkshire, but plans are in place to extend this to across the Yorkshire and Humber region. The National Cyber Security Challenge are very interested in the possibilities for delivering this nationally as this is the first and only contest of its kind within the UK.

2.3.2 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 continue to deliver inputs across all schools, this work has reached 35,000 young people and their parents. They held events in the Broadway shopping centre to support safer internet day.

Kirklees officers have recruited a small number of students from Shelley College as volunteers who are delivering peer to peer learning across other schools and their parent's evenings. Staff delivered a series of events at prominent locations across the district to support safer internet day.

Wakefield have now a permanent Cyber PCSO who has been delivering inputs across a series of schools within the district and partners. They held the first ever Cyber VLOG during safer internet day along with other partners which was well received.

Leeds District delivered inputs across schools through safer internet week along with drop in sessions at Leeds University.

Calderdale are delivering weekly crime prevention sessions at Calderdale and Halifax Library which have a cyber-crime focus. They also delivered a series of inputs through safer internet week across District prominent locations.

3. Forthcoming significant work

3.1 NPCC specialist capabilities programme – Cyber

The force has agreed to be part of a national NPCC pilot along with the other Yorkshire and the Humber forces which will develop and implement a "regionally managed, locally delivered" cyber provision.

This work is still in the early stages of scoping and delivery, but will ensure that all cyber reports across the region are received in one location and then disseminated. This will mean that 100% of victims receive an enhanced, bespoke service when reporting crime to the force or via action fraud, intelligence will be shared more effectively across the region, whilst it will place a requirement on the force to have dedicated staffing to complete prevent and protect work. It will enhance training, procurement and equipment provisions also. The force will gain access to national funding to deliver this.

I hope to provide a more detailed update in a future paper.

3.2 Staffing increase

The Police and Crime Commissioner and Chief Officer team have supported a significant uplift in staffing to support the cyber-crime team and districts in delivering an effective cyber provision across all crime types over the next 12 months. This will see the creation of a dedicated Detective Inspector for cyber-crime, a further Detective Sergeant and an increase of 28 dedicated Constables.

This will allow sufficient resources to provide a 24/7 specialist team of digital media investigators who will be able to provide support across all crime types. These staff will be based within the force crime management unit, ensuring that the advice is available at the earliest point of contact with the police. Further staff will be embedded within force training school to assist with the ambitious programme of training, whilst others will provide a dedicated prevent and protect function for the force.

This investment has ensured that the force continues to be at the forefront nationally around digital investigations across all crime types.

4. Strategic Risk / Legal Opinion

Cyber Crime has been reassessed as part of the annual threat assessments which has reduced the risk associated with Cyber-crime. Demand more than doubles each year but numerically these changes

are small in terms of volume. Cyber-Crime is increasing 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 fully known. West Yorkshire Police are supporting national intelligence development right from the front line through to specialist resources' and the NCA to understand this.

5. 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.

6. 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.

7. Human Rights consideration

N/A

8. 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.

The funding of new staff to focus on this area of policing is a welcomed addition.

9. Appendices

N/A