Creating a safer
Cambridgeshire

To: Business Coordination Board

From: Chief Constable

Date: 01 March 2018

Fraud and Cybercrime Investigation Unit Update

1. Purpose

1.1. The purpose of this paper is to provide an update to the Business Co-ordination Board ("the Board") on progress taken to develop Cambridgeshire Constabulary's ("the Constabulary's") fraud and cybercrime capability and to outline how this will develop further over the forthcoming year.

2. Background

2.1. The Fraud and Cybercrime Investigation Unit (FCIU) was formed in September 2015 and was tasked with developing the fraud and cybercrime capability for Cambridgeshire Constabulary based on the 4P Model.

- PREVENT … stopping people from engaging in Cybercrime and Fraud
- PROTECT … vulnerable groups and communities, working in partnership to reduce risk
- PREPARE … our staff and our response to meet the demand
- PURSUE … prosecute and disrupt those engaged in cybercrime.

3. Scale and Extent

3.1 In the last 12 months there has been a 32.5% rise in crimes which have been identified as being cyber enabled or cyber dependent. Cyber related reports to

Action Fraud have risen by 29%. It is recognised that in line with national research, there is likely to be under reporting.

3.2 41% of recorded cyber offences relate to crime categorised as violence against the person, which includes harassment and various forms of malicious communications. 25% related to fraud and 10% theft and handling offences.

3.3 The greatest volume of offences are recorded in the Peterborough local authority area (28%) and across the county, of known victims, 64% are female. Of known suspects, 75% are male.

3.4 The impact of non-acquisitive crimes cannot be measured, but data shows that the average financial loss is £4,246. There is a wide variation across the crimes from less than £1000 to over £100,000.

4. Prevent

4.1 Two prevent officers are now employed in ERSOU. They are tasked with identification of high risk subjects who might be drawn into cybercrime through experimentation. These roles seek to divert people by introducing them to legitimate pathways, such as STEMETTES, The National Cyber Security Challenge as well as local projects. These staff members are new in post but it is expected that there will be good liaison between them and the FCIU.

4.2 The FCIU conduct a response to “Prevent” individuals, servicing cease and desist notices.

4.3 The FCIU hold a list of legitimate coding opportunities for individuals to become involved in.

4.4 There is a referral pathway to the National Crime Agency (NCA) for individuals who are at risk of committing crime or who have already committed low level cyber offences. The programme is designed to route their interests into legitimate pathways including streaming into government services.

5. Protect

5.1 A Cyber Security Adviser has been in post since February 2016 and focuses on small to medium-sized businesses within Cambridgeshire.

5.2 The Cyber Security Advisor engages with businesses and communities within Cambridgeshire and Peterborough to provide cybercrime and fraud prevention advice (i.e., through presentations, signposting to relevant trusted websites for free and impartial advice, sharing relevant campaigns from partners).

5.3 They also:

i. Analyse datasets and profiles received from Action Fraud to inform decisions on force strategic action working with internal and external stakeholders and partner agencies to raise awareness of current trends in cybercrime and fraud.

ii. Create and maintain a network of relationships within government, law enforcement (local, regional, national and international), industry, academia and business to encourage joint working to tackle cybercrime and fraud related problems within the local communities.

iii. Coordinate local activities in conjunction with the Get Safe Online policing partnership programme, local banks and businesses, local council and academia and the Office of the Police and Crime Commissioner. Activities have included a Get Safe Online live event over two days in central Cambridge (attended by 12,000 people and over 80 local businesses), two cybercrime conferences (one public and one business) and supporting events arranged by local banks, local council and businesses.

iv. Created the Community Cyber Ambassador (CCA) to raise awareness at a grassroots level within communities. 120 individuals within the force, services partners (Fire and Rescue Service) and local communities in Cambridgeshire have been given awareness training and promote awareness within their local communities.

v. Horizon scanning of future technologies to identify new ways of working and partnerships and emerging threats and trends in fraud and cybercrime.

5.4 The FCIU has helped to implement the banking protocol within Cambridgeshire. This protocol means that bank staff can alert police to when they feel a customer maybe being scammed. Even though this has only been running since September 2017 it has already prevented £101,450 from being fraudulently obtained from Cambridgeshire residents.

5.5 Operation Signature phase 1 is currently in operation. Victims within Cambridgeshire are sent a bespoke factsheet regarding the crime they had reported to try and prevent further frauds occurring. Phase 2 is being developed in partnership with the Fire and Rescue Service, Age UK, Trading Standards, Victim Support and The Bobby Scheme. This phase is looking at how to identify and create an individually tailored action plan for those at the highest risk of repeat frauds.

6 Prepare

6.1 The FCIU was set up with two PCs who were to be technicians and two DCs who were to be investigators. It has become evident that this division of roles did not work and therefore all cybercrime officers are now both technicians and investigators.

6.2 A drop in session is run every two weeks to allow officers on division is discuss any cyber related crime they are investigating.

6.3 There are five online training packages (Introduction, First Responder, Investigation, Digital Communications, Social Media, Cyber Crime and Policing and Introduction to Communication Data and Cybercrime) which are available to officers. These are due to be updated by the College of Policing.

6.4 There is an acknowledged gap within IPLDP (initial PC training) and ICIDP (Detective training) where there is limited or no cybercrime inputs. This is being raised through Learning and Development and is likely to be addressed soon. There are some new learning apps which are being trialled to see if these are a suitable way of training and maintaining officer's digital awareness.

6.5 Mainstream cybercrime training (MCCT and MCCT2) was undertaken in 2015 and 225 officers were trained. This trains officers in open source investigations. This needs reviewing however to ensure that all new DCs are being trained.

6.6 Basic fraud investigation is being taught at both stages of training with inputs regarding financial investigations also being taught at the DC level.

6.7 Researching, Identifying and Tracing the Electronic Suspect (RITES) course has been taught to 23 officers within the Central Intelligence Bureau with a further 15 being trained mid-January 2018. This is a higher level of open source investigation than the MCCT training provides.

6.8 There have been 16 officers trained as Digital Media Investigators. These are an additional role to officers' main responsibilities and it was envisaged that these trained individuals would be able to give advice and guidance around any investigation which had a digital element. This will require a review to ensure capability meets the current demand.

6.9 The four Cyber Investigators within the FCIU are all trained DMIs and support divisional units. A Digital Media Coordinator oversees the DMIs, triaging the requests for support and disseminating the tasks to the most relevant DMI. This role sits within the FCIU at DS level.

7 Pursue

7.1 The FCIU works closely with ERSOU as well as supporting other internal departments.

7.2 Investigations can be tasked to ERSOU through the tasking process. ERSOU take on investigations which are regional/international issues, or which require technical expertise that is not available within the force.

7.3 The FCIU's remit is to deal with serious and/or complex crimes which local officers would not have the technical expertise or experience to be able to investigate effectively. The FCIU is tasked via direct referrals from divisional officer, the IMU or through the tasking process.

7.4 All sextortion investigations are investigated by the FCIU, due to the digital nature of the investigation and the acknowledgement of the risk to individuals.

7.5 The FCIU has the technical equipment to perform a triage function at a crime scene. This assists in the identification of what should be seized from the scene and where on the device it is stored for clearly direction through to the DFU. However full implementation and force awareness is still being implemented.

7.6 Since May 2017 the FCIU has investigated 52 crimes/incidents as well as providing support to an additional 60 divisional investigations and conducting 86 technical examinations.

8 Future developments

8.1 The FCIU is looking at trialling different apps on Police Officers phones which will help them to identify digital equipment for seizing and/or further investigation.

8.2 The role of the DMI will be critical with the fast changing environment that cyber enabled crime encompasses.

8.3 Cambridgeshire Constabulary have conducted a Local Policing Review. From the 30th April 2018, the FCIU will merge with Serious and Organised Crime Team becoming the Specialised Crime Team. This will provide greater supervisory resilience in the specialist arena.

9 Recommendation

9.1 The Board is recommended to note the contents of the report.

BIBLIOGRAPHY

Source Documents	
Contact Officer(s)	Detective Superintendent Mat Newman, Director of Intelligence, Cambridgeshire Constabulary