To: Business Coordination Board

From: Chief Constable

Date: 24 March 2015

COMPUTER ENABLED CRIME/CYBER CRIME

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") cybercrime capability and to outline how this will develop further over the forthcoming year.

2. Recommendation

2.1 The Board is invited to note the contents of the report.

3. Background

3.1 In July this year the Constabulary's Force Executive Board (FEB) supported 'a Strategy for Change' with regard to the development of the Constabulary's cybercrime capability based on the 4P Model.

- **PREVENT** … our communities from becoming victims of Cyber Crime
- **PROTECT** … vulnerable groups, working in partnership to reduce risk
- **PREPARE** … our staff and our response to meet the demand
- **PURSUE** … those engaged in Cyber Crime

In addition there was support for:

- The Establishment of the Cyber Crime Steering Group
- Roll out of the National Centre for Applied Learning Technologies (NCALT) Cyber Crime Training
- Recruitment strategy to enhance our 'technical skills' capability

- The roll out of Mainstream Cyber Crime Training (MCCT)
- Establishment of Cyber Crime Unit (CCU)

4. PREPARE

4.1 The Cyber Crime Steering Group chaired by DCS Hebb has met and agreed an in depth delivery plan based on the 4P model.

4.2 NCALT training has benefitted from a reasonable take up. As of October 2014 the 3 packages: Introduction, First Responder and Investigation show 543, 400 and 754 officers respectively having completed the training.

4.3 The MCCT courses are underway, and by the end of December 2015 the Constabulary will have trained 144 officers - more officers than any other Police Force in the country. At the same time the Constabulary remains on track to deliver the training to a total of 225 PIP2 Investigators across the Constabulary.

5. PURSUE - Cyber Crime Unit (CCU)

5.1 The Cyber Crime Unit (CCU) was established in February 2015 and will work alongside the Fraud Team. In effect we will build a Cyber/Fraud Investigative capability in recognition of the intrinsic link between the two. An organogram is at Appendix A.

- As a specialist capability the CCU will carry out investigations in its own right such as those described below and also work with the Eastern Region Special Operations Unit (ERSOU).
- Cyber dependant crime[i] that falls outside of the responsibility of ERSOU CCU for example a Denial of Service rather than a Distributed Denial of Service Attack.
- Cyber Enabled crime[ii] beyond the capacity and capability of local investigators for example complex cyber enabled fraud.

5.2 In addition to core investigation the CCU will provide tactical advice, support and training to frontline staff, investigators and Senior Investigating Officers, together with an operational response to cybercrime in action where resources are available. The CCU Detectives will also provide the Constabulary with a Digital Media Investigator[iii] capability. This is a newly developed role that has emerged from the College of Policing as a result of the Communications Capabilities Development Programme. The function will predominantly support serious crime investigations undertaken by the Territorial Policing Command or Investigations collating and coordinating all matters relating to communications data and technology media.

5.3 The CCU will grow to become a centre of excellence within the Constabulary and work with colleagues across the region and at ERSOU to develop a much needed force capability, reflective of the threat, harm and risk posed by cybercrime.

6. PREVENT and PROTECT

6.1 The recent Her Majesty's Inspectorate of Constabulary (HMIC) Strategic Policing Requirement review highlighted that the Constabulary, like the majority of forces, is developing its understanding of the threat posed by a large scale cyber-attack but has access to specialist resources from ERSOU or the National Crime Agency. We also

have a developing Information Security governance regime that will further examine and support development of our own cyber security capability. Where we do need to prioritise is in relation to the Prevent agenda: stopping people becoming victims in the first place; and the Protect agenda: working in partnership to reduce risk and supporting victims of cybercrime.

6.2 It is reported[iv] that 80% of all known cyber attacks could be defeated by embedding basic information security practice and the Government has published extensive guidance for individuals and businesses to support this. In October 2014 our own "Get Closer" campaign was dedicated to cybercrime, targeting Cambridgeshire businesses and residents who are most likely to become victims of cybercrime and providing online safety advice.

6.3 To support this it is proposed that the Constabulary establishes within the CCU a Prevent/Protect Co-Ordinator post. It is recommended that this post should initially be offered as a 12 month contract.

6.4 The main aim of the role would be to lead on the delivery of protective security and preparedness advice to residents, businesses, sites and organisations relating to the cybercrime threat, be responsible for implementing a cybercrime prevention plan, and provide a Single Point of Contact role for Cybercrime threat reports. The role will facilitate a number of key events / conferences attracting business from across the county with an emphasis on the promotion on the governments "cyber essentials" scheme. The role will also exploit partnership opportunities in the arena of cyber security and look to harness the skills of industry experts to support increased cyber prevention techniques and awareness.

6.5 With the establishment of the Victim's Hub the Constabulary has a responsibility to provide support to victims of crime. The most recent National Fraud Intelligence Bureau (NFIB) Cybercrime profile of highlighted that 28% of victims had suffered either significant or severe impact as a consequence of the crime[v]. Whilst the details behind this statistic are not known it does identify a need for the Hub to develop its understanding and build capability to provide the necessary support to such victims. This may be an area where additional commissioning support from the OPCC may be required.

7. Interdependencies and Future Developments

7.1 The establishment of the CCU is the first and necessary change. In addition there is a requirement for the adoption of a new title for what is currently known as the High Tech Crime Unit (HTCU.) To coincide with the establishment of the CCU the HTCU will be renamed the Digital Forensics Examination Unit (DFEU) so as to more accurately reflect their function. The responsibilities of the unit will remain the same – the examination and retrieval of digital evidence from devices.

7.2 The second step will be a slightly revised governance structure within Investigations, reflecting emerging best practice, which calls for a capability that joins the Intelligence, Investigation, Technical, Enforcement, Financial and Prevention activities relating to cybercrime under a single command. A model for the future would bring all of these elements together under a single department: the Central Intelligence Bureau (CIB). A model for such an approach is at Appendix B.

7.3 Across the region, forces and ERSOU are developing their capability albeit at differing speeds. There is communication through the ERSOU-led Cyber Regional User Group which adds value in the sharing of best practice. Within the Strategic Alliance (the Constabulary, Bedfordshire Police and Hertfordshire Constabulary), the Constabulary have been leading the agenda to build in economies of scale and other efficiencies in the development of the three forces individual capabilities by establishing 'Lead Responsible Officers' (LROs) for the common requirements of the three units. Each LRO will design the common requirements (e.g. training and IT equipment). This will build a framework for and maximise the potential to collaborate in the future either across the Strategic Alliance or regionally.

7.4 As regards collaborative options, there is immediately scope to pursue collaboration with Bedfordshire for a joint CCU hosted by Cambridgeshire. Hertfordshire had already set in place a model for a joint Cyber and Fraud Team, and this has been established.

8. Summary

8.1 The Constabulary has acknowledged the need to develop is capability to tackle cybercrime. Significant steps are being taken to ensure that the Constabulary is capable of responding to and investigate both cyber dependant and cyber enabled crime affecting victims, both individuals and businesses in the county. The delivery plan and associated work streams will enable this to continue, and will ensure that the Constabulary is able to meet the growing public expectation that we can tackle that which is the new volume crime.

8.2 The activity to mainstream this have been the most significant to date, and the Constabulary is leading the region in terms of its training programme, communications strategy and approach to building in efficiency from the outset. Work now needs to continue to develop for the future, focussing immediately on the establishment of the specialist unit within our current or future policing model, and to explore potential collaboration opportunities.

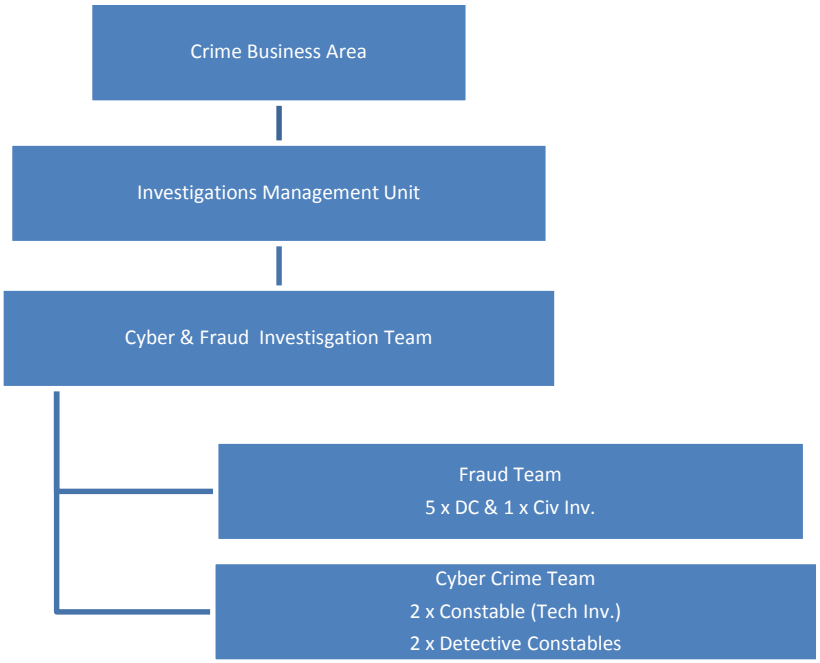
9. Recommendation

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

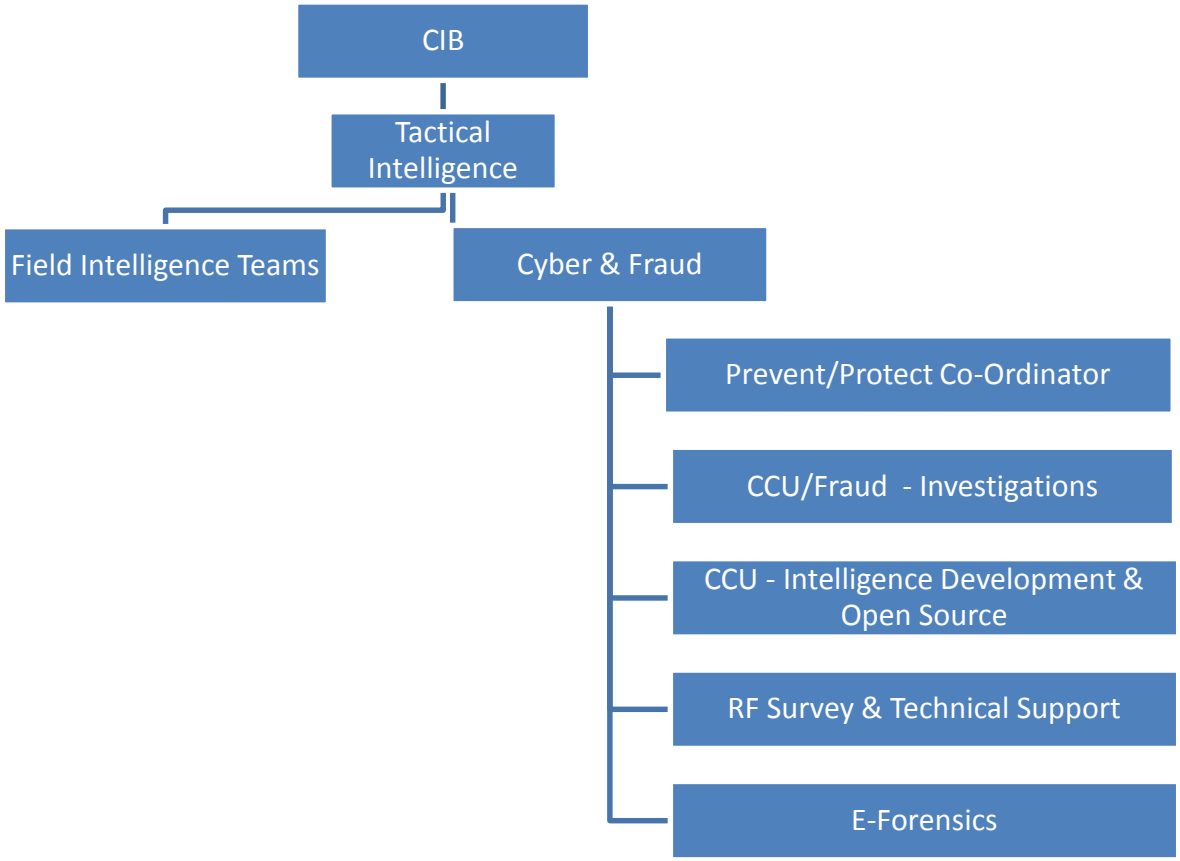
BIBLIOGRAPHY

Source Document	
Contact Officer	T/D/Supt Kevin Vanterpool, Force Cyber Crime Lead, Cambridgeshire Constabulary

Appendix 1 – Cyber Crime Unit - Organogram



Appendix 2 – A Future Model for Tackling Cyber Crime



[i] 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).

[ii] 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.

[iii] DMI – Experienced Investigators responsible for the development and maintenance of an investigations digital media strategy covering communications data, digital forensics and open source material.

[iv] Ian Lobban, Director GCHQ – 10 Steps to Cyber Security 2012.

[v] Severe - have received medical treatment as a result of this crime and/or at risk of bankruptcy. Significant - impacting on health or financial well being