Cyber Crime – Link Member report 24th October 2017

1. Capability and Capacity

The Digital Investigation Unit (DIU) now consists of

1 DS
2 DC – Cyber Investigators
3 Digital Media Investigators (DMI)
1 Cyber Protect Officer
21 embedded secondary role Digital Media Investigators (investigators in other roles that also undertake the role of a DMI – a further 4 are being trained to cover some identified gaps in investigations and Intelligence department.)

2. Prevention

This remit is mainly covered by the ROCU (Zephyr) who have received significant investment in this area to deliver on a regional basis. Any opportunities for prevent intervention are referred to the ROCU by the DIU. A good example of this is Operation HOOKAROON which is an investigation into 2 x 16 year olds that have engaged in defrauding a major phone to phone banking system. Currently a joint investigation is being conducted with the National Cyber Crime Unit (NCCU) and referrals for prevent opportunities will be made.

3. Protect

A Cyber protect Officer is now in post since 31.05.2017 (2 year funded position)

The role of the cyber protect officer is to:

Complete presentations to SMEs, Community groups (vulnerable), Schools, Parents and Teachers in regards to online safety and Cyber Crime.

To date – the following audience numbers have received presentations:

Young people	Parents	Public Sector/ Charity	Business	Community Groups	Internal
81	60	29	36	42	94

The Cyber Protect officer is also participating in the Cop Shop within the Galleries twice a week over December to engage with the community in relation to cybercrime and online safety as well as providing support on installing apps safely with adequate controls in the run up to Christmas.

Review Niche cases and offer over-the-phone support in relation to online safety

The officer also provides advice and crime prevention advice over the telephone and the most frequent calls are victims of fraud in relation to software service fraud, romance fraud and telephone scams.

Domestic	Fraud	Computer misuse/ hacking	Sextortion	Harassment	Sexual offences
6	11	6	3	1	6

Review Action Fraud Statistics and Technology news to inform latest support and community messages. Trends are identified and used to feed into the regional cyber protect bulleting or to inform media communications.

Maintain an online internal blog on the latest cyber trends and social media applications and how these may affect the landscape within policing. These inform the force on techniques, best practices and new developments enabling officers to stay current in respect of digital trends.

4. Pursue

The central DIU team log all cases where assistance is given to investigations or the investigation is undertaken in total by the DIU. This assistance is recorded by department, area and crime type so that gaps in knowledge / use of the DIU can be identified as well as capturing good practice when dealing with crime types.

In the last 6 months, **662** new cases have been worked on by the DIU

Regional / National Issues / opportunities

Presence on:

- Cyber Regional Users Group (Tactical) – DS DIU
- Cyber Regional Users Group (Operational) – Manager – Complex Crime
- Cyber Regional Users Group (Strategic)– DSupt Complex Crime, Investigations
- Two weekly regional meeting / call with ROCU and regional forces to share intelligence and emerging threats / trends
- National Digital Media Coordination meeting
- National DIAG (Digital Investigation advisory group)

Issues being progressed are:
Regional interactivity / virtual team
Standardised DIU profiles and remits allowing interoperability
Progression of new techniques / sharing of best practice
Open source capability
Forensic interaction

Gloucester – Operation Crystalise which will form part of the national Digital Investigation and intelligence work stream. Ensuring embedding of DMI capabilities and Digital evidence opportunities throughout the force activity.

Embedding the Cyber Pathways framework

Currently reviewing all training delivery in force with CLAD to ascertain and ensure that DMI opportunities are woven throughout as part of business as usual

The DIU feed into the two weekly ROCU cyber protect briefing to share issues and emerging trends. This document is widely circulated amongst individuals and businesses outside of policing.

Strategic threat assessment;

Key risks highlighted that are directly relevant to the Digital Investigation Team include;

Risk 3- shortage of specialist capabilities due to an increase in the use of technology by criminals resulting in cyber enables offending rapidly becoming normalised. Challenge = keeping pace and providing appropriate specialist capabilities to maximise opportunities.

- To mitigate this we have provided tailored training inputs to the following departments;
  Call Centre, IAU (two separate training inputs 6 months apart), Live Cell, All Investigations staff, Telecoms SPOC office, CAB (Covert Authorities Unit), PSD, IRIS, TSU.
  Partner agency; Threshold Team, Social Services.
  Still to be delivered; Response, RPU/Tri Force, Cold Case team

- The DIU have commenced a force wide training mapping project, with the intention of reviewing all training products that ASC provide (delivered at all levels; new recruits to SIO's), to ensure that every course has a digital perspective. This is with the long-term aim of bringing all ASC staff up to a new baseline standard in respect of digital investigation.

- Early next year we are aiming to deliver a force digital awareness week- to make digital everyone's daily business

- The Force Cyber Profile is in the process of being created (DIU and Intel).

- Op Crystallise (National DII project)- we are currently reviewing our internal processes against this framework, so we are able to identify any additional opportunities we can explore/deliver

- Obtaining access to BERLA, NUIX from DFU

- Exploring 'ethical hacking' to see if we are able to consider this for ongoing proactive investigation

- Consideration of using Cyber volunteers e.g. Cyber Bobby van?

- Long term vision- expand the team so more of these specialist skills can be shared

- Force Open Day- stand