Annex b) Cybercrime Update

To provide information in relation to national and local cybercrime issues, as well as an update on Dorset Police's approach to dealing with this area of criminality.

Background and National Context

It is widely recognised that cybercrime is a significant threat to the UK and the demand and complexity of cybercrime is increasing. The National Cyber Security Strategy 2016-21 stated that while we are 'critically dependent on the Internet', that it was 'inherently insecure and there will always be attempts to exploit weaknesses to launch cyber attacks'. Further it concluded that, despite considerable efforts taken by a wide range of agencies, that nationally, 'the majority of businesses and individuals are still not properly managing cyber risk'. The strategy set out objectives to defend the UK against the evolving cyber threats; deter those determined to attack UK cyber space; and develop expertise to meet and overcome future threats and challenges.

The National Crime Agency's National Cyber Crime Unit (NCCU), alongside a wide array of policing and security bodies, including Regional Organised Crime Units (ROCU), are working collaboratively to deliver the National Cyber Security Strategy. This has supported the development of a significant capability at national and regional level to tackle the large scale threats.

At the strategic level, cybercrime is recognised by the NPCC and Association of Police & Crime Commissioners as a specialist capability. In 2017, the NPCC Specialist Capabilities Programme identified just one-third of forces had a dedicated cybercrime unit and cybercrime capability with the remaining forces looking to implement units in the near future. In October 2017 it was agreed that every force should have their own dedicated specialist Cybercrime Unit tackling cyber dependent crime, which should be 'regionally managed and locally delivered'.

To assist forces in the implementation of their cyber capability, and to ensure national consistency, a 'Force Specialist Cyber Capability Minimum Standard' has been produced and agreed through the National Police Chiefs Council as the standard for equipment, training, funding opportunities etc.

National guidance states that each force should create a capability on the following four areas (otherwise known as the 'Four Ps'):

Pursue: Disruption and prosecution of those committing cybercrime
Prevent: Prevent people becoming involved in cybercrime
Protect: Reduce the vulnerability amongst our communities from the threat of cybercrime
Prepare: Ensure the necessary capabilities exist to tackle cybercrime

The Regional Cybercrime lead is ACC Julie Fielding. Dorset Police's Strategic Lead is Detective Chief Superintendent Mark Cooper. Detective Sergeant Tim Farrell is the contact for Dorset Police's Dedicated Cybercrime unit.

Local Context

There has been a 30% increase in reported cyber enabled and cyber dependant crimes between 2016/17 and 2017/18 in Dorset. Within this increase, there has been a 49% increase in cyber enabled sexual offences, some of which can be attributed to an increase in the use of dating websites and applications. It is believed that these rises are the consequence of not only an increase in crime, but also an improvement in the accuracy of cybercrime recording following extensive training.

Of further note:

- Victim losses as a result of fraud and cyber offences were estimated at £5.7million in 2017/18 which is a slight decrease on the previous year.
- In the Dorset force area, there were almost the same proportion of individuals and businesses as victims.
- Six out of 20 victims reported a severe of significant impact from the crime.

Force Cyber Priorities, Strategies, and Local Initiatives:

Dorset Police currently has a capability in each of the Four Ps and is working in collaboration with Devon and Cornwall Police, and the wider region, to enhance those capabilities.

The Force's dedicated cybercrime unit are involved in investigations on a daily basis, from providing investigative support to traditional offences to assisting in the search for missing persons. The cybercrime unit provides a number of services to officers and investigators across the force from providing advice to officers, to conducting Digital Media examinations at scenes to leading on Cyber Dependant crimes.

A new cybercrime Prevention Officer has also been appointed, to replace the previous post holder, Jake Moore, and will take up the role in the next few weeks. This role is in addition to the cybercrime Protect element and enhances the education that the Force already provides to members of the public and local businesses around cybercrime prevention. The post holder will continue to work closely with local Businesses and Organisations to reduce the number of victims of cybercrime.

The Protect officers are increasingly working closely with the ROCU Cybercrime Protect team to ensure that advice provided to businesses and local infrastructure organisations is of a high standard and current particularly in. In Dorset however, there is additional focus on providing cyber advice to community groups and individuals, as the county's demography means that there is a large percentage of elderly people, who can be particularly vulnerable.

The two Digital Capabilities Units (Dorset Police and Devon and Cornwall Police) which will be fully shaped under the Alliance project over the next few months, are already working together and are providing support to each other when required. The two units have submitted a joint funding bid under the National Cyber Development Plan. If successful, this will improve staff numbers, equipment and training and will lead to Force Cyber Units working even more closely with ROCU Cyber teams, improving the response to Action Fraud/NFIB reporting. This additional funding should ensure that the units are better able to respond to the 4P plan around cybercrime and provide expert support to the Dorset Police Fraud team.

Recent notable case:

A recent example of cyber dependant criminality was that of a former pupil from a school in Poole, who was hacking into the school's computer network. The school reported unlawful access to the network which appeared to only occur at the weekend.

Investigative work by the unit revealed that the access was being gained from an address linked to an ex-pupil. He was arrested, his premises searched.

It became apparent that he was using the computing power of the school network to 'mine' a crypto currency, similar to Bitcoin. He was only carrying out this activity at the weekend as he realised that accessing the network during the working week was more likely to be noticed.

He admitted the offence and received an adult caution. He forfeited the cryptocurrency that he had manufactured and it was converted into sterling to the value of £3,200.