For Information	
Public	**Public**
Report to:	**Strategic Resources & Performance Meeting**
Date of Meeting:	**2nd November 2021**
Report of:	**Chief Constable Guildford**
Report Author:	**DCI Yvonne Rainford**
E-mail:	**Yvonne.rainford@nottinghamshire.pnn.police.uk**
Other Contacts:	**Detective Superintendent Mike Allen**
Agenda Item:	**5**

*If Non-Public, please state under which category number from the guidance in the space provided.

CYBER ENABLED CRIME AND KEEPING PEOPLE SAFE ONLINE

1. Purpose of the Report

1.1 The purpose of this report is to provide an update on developments over the past 12 months in terms of the capacity and capability of Nottinghamshire Police to tackle cyber-crime and cyber-enabled fraud offences.

2. Recommendations

2.1 It is recommended that the Nottinghamshire Police & Crime Commissioner notes the content of this report.

3. Reasons for Recommendations

3.1 To ensure that the Nottinghamshire Police & Crime Commissioner is updated on the force's strategy in relation to tackling cyber-enabled crime and keeping people safe online.

4. Summary of Key Points (this should include background information and options appraisal if applicable)

4.1 **2019/20 Statistical Overview of Demand**

4.1.1 **Cyber Dependent Crime -** Within the financial year period 2020/21, which runs between April and March there were 545 cyber-dependent crime reports compared with 497 the previous year, representing a rise of 9.7%. Despite this increase, Nottinghamshire achieved joint third position nationally in terms of cyber-dependent judicial outcomes.

4.1.2 **Fraud Crime –** The number of actual reported offences in Nottinghamshire for the financial year 2020/21 totalled 12,201, a 4.1% increase from 2019/20 with all the reporting bodies - Action Fraud (AF), CIFAS and UK Finance recording increases. In term of our demand, this resulted in circa 3,000 NICHE occurrences being created in 2020/21 which including Calls for Service and investigations, National Fraud Intelligence Bureau disseminations and requirements for victim assistance Only. However, we recognise that these

demand totals will not represent all committed crimes as the Crime Survey for England & Wales estimates that only 15% is ever reported to the police. Nottinghamshire is currently ranked 6th highest in England and Wales for percentage of fraud judicial outcomes.

4.1.3 **Cyber-enabled frauds** are defined as those where the crime has an element of cyber, but technology was used to facilitate the crime, rather than the crime itself. Whilst it is not possible to give precise figures on those frauds that are cyber-enabled in Nottinghamshire, national estimates are that around 80% of all police reported fraud has some cyber element.

4.2 Resources and Investigative Structure

4.2.1 Nottinghamshire Police recognise that as more crime is committed online the distinctions between cyber-enabled fraud and cyber-dependent crime become less helpful. Consequently, whilst there are resources dedicated to the investigation of cyber-dependent crime, activities associated with prevention and protection work streams are encouraged to be less specific and designed to protect more people from harm.

4.2.2 Nottinghamshire Police's Cybercrime team provides a specialist and dedicated capability to investigate all cyber-dependent crimes whilst also supporting and guiding other departments in their progression of cyber-enabled investigations. We also ensure that the knowledge around current threats, trends and mitigation is provided and seek to upskill the organisation on cyber related matters such as the dark web and crypto currency. We are supported by the regional Cybercrime team who have responsibility for providing an element of coordination to our local response. Our demand and performance are measured against nationally agreed Key Performance Indicators (KPIs) which are examined through quarterly tactical delivery groups.

4.2.3 In light of the projected increases in online and cyber-enabled demand and responding to the recommendations in the above reports, we have bolstered our capacity by investing in an additional 9 Digital Media Investigator posts, bringing the force total to 13. This new capability will be designed to increase awareness of the cyber digital forensic opportunities, improve usage of digital forensic examination tools at scenes, and promote digital strategies designed to manage the demand more effectively. This will occur over the next 12 months and will be resourced by the recruitment of graduate investigators via the fast track to detective programmes and from officers from Local Policing released via Operation Uplift. The level of skill and specialist qualifications in this team will vary as the uplift to the team is still relatively new, however by pooling all these individuals together and forming a Digital Hub they will effectively support and mentor one another through shared learning.

4.2.4 In addition to this, the team have now introduced a Level 4 Cybercrime Apprentice and an individual on a one-year Internship Programme to collectively improve the provision of Victim support, proactive advice and local investigations and intelligence as well as fostering future talent.

4.3 **Investigative capacity and capability**

4.3.1 Proposals have now been submitted and agreed to realign the Cybercrime Unit and incorporate with Digital. The benefits of this approach are to bring our Cybercrime department and DMIs closer together to facilitate sharing of knowledge and ideas. We are keen to explore ways that we can effectively utilise the Cybercrime team to accelerate and advance the DMIs development to enable them to provide immediate support. This will reduce the reliance on our Cybercrime teams whilst simultaneously creating a pool of talented individuals and incentives for further career development either for existing roles or ones created in the future.

4.3.2 It has also been agreed that there will be a dedicated Cybercrime Detective Sergeant to oversee the Cybercrime team; this will be highly advantageous as there are also plans to increase the detective establishment and create four new posts that will focus more specifically on online activity.

4.3.3 Following the success of a pilot initiative last year the force has also now agreed to the permanent establishment of a dedicated Fraud Triage team. This team provide an improved service to victims by dealing more effectively and efficiently with their reports of fraud whilst also recognising and supporting any vulnerability issues to minimise the opportunities for repeat victimisation. now review all the reports at an early stage and assess against the acceptance criteria for fraud investigations. This ensures we demonstrate a consistent approach. Firstly, being able to identify fraud reports that require a proportionate investigation (public interest being a key consideration) and secondly, planned, and supervised investigations, which means that they are more likely to result in a positive outcome for the victim.

4.3.4 As highlighted in earlier reports, Nottinghamshire Police's ECCU also has two dedicated Fraud and Cyber Protect Officers, this is additional to the Cybercrime teams Protect and Prevent Officers.

4.4 **Performance targets**

4.4.1 Team Cyber UK (TCUK) is the term used to describe the excellent working relationships between force Cybercrime Units, Regional Cybercrime Units (ROCU), NCA National Cybercrime Unit, National Cyber Security Centre, and GCHQ.

4.4.2 Nottinghamshire Police's specialist Cybercrime Unit provides local delivery of the cybercrime response across PURSUE, PROTECT, PREPARE and PREVENT. The ROCU manage and coordinate the work of the team collating information on a quarterly basis against several strategic priorities and Key Performance Indicators, returning this information to the centre.

4.4.3 At present, the force has the capacity to meet the demand for Cybercrime dependent investigations tasked by the region notwithstanding that national

funding has been significantly reduced. The more challenging area is the forces' response to cyber-enabled crime and online and this is where the force has already invested heavily in the protect and prevent capabilities and introduced case acceptance criteria.

4.5 **Key Achievements**

4.5.1 In terms of being able to support the National Cyber Security Strategy and Serious & Organised Crime Strategy the force can confidently play its role in mitigating the impact of a major cyber incident with a dedicated cyber team and deliver a response across the 4 P's (Protect, Prevent, Pursue and Prepare).

4.5.2 Cyber is a force priority and a dedicated intelligence analyst and researcher provides information on the key risks and threats that could be reduced and prioritised through the force tasking process.

4.5.3 Consistently we have achieved 100% compliance against the national KPI relating to the investigation of all Action Fraud referrals notwithstanding our demand is the highest in the region.

4.5.4 The cyber protect and prevent officers are well supported by the regional engagement team's weekly calls to share knowledge and best practice, a regional protect strategy to ensure better coordination of the protect campaigns and regional websites developed for consistent messaging to individuals and businesses. Effectiveness of these campaigns is generally measured through the total reach in terms of the numbers accessing this information.

4.5.5 Nottinghamshire Police currently receive 500-600 new victim data reports each month. The Fraud/Cyber Protect teams identify the highest harm /vulnerability cases each moth to prioritise for victim care and crime prevention. Checking the most recent data our dedicated Fraud and Cyber Protect Officers make contact (either directly or through the Neighbourhood Policing Team) or send out information packs to approximately 100-120 victims each month. In addition, to this the force now has dedicated Fraud Triage Assistants based within the forces' control rooms who are scrutinising all fraud and acquisitive crime reports and ensuring that these are correctly dealt with either as a call for service, provided with immediate advice and/or signposted to the Protect team.

4.5.6 Combining the above figures with the protect/crime prevention service already afforded to victims by the investigators with the Specialist Fraud Team and the Protect work undertaken by the dedicated Cybercrime team, Nottinghamshire has the highest number of engagements for Protect in the East Midlands. To date, the Cyber Protect team have achieved 7,672,903 social media reach, over 4,773 direct engagements (presentations) and 864 victim contacts/engagements since the start of Q1 in 2020.

4.5.7 Notable successes for the team include an on-line competition launched across all Nottinghamshire schools to increase cyber awareness and the delivery of training in Cyber Choices to the Designated Safeguarding Leads resulting in 43% of all referrals made across the East Midlands coming from

Nottinghamshire. The Cyber Choices network was created to help young people make informed choices and to use their cyber skills in a legal way.

4.5.8 Work being conducted in Nottinghamshire to tackle and prevent cyber-crime has earned the force a national award. Kirsty Jackson, one of Nottinghamshire Police's Cyber Protect and Prevent Officers has also been successful in achieving one of the forces' awards for 'doing things differently' and will be presented with her award later in the year.

4.5.9 We have worked closely with the College of Policing promoting the digital foundation learning products and the upgraded CyberDigiTools app. This provides practical information and advice on dealing with digital intelligence and investigation opportunities, as well as all the existing information on cybercrime. The tool has now been installed on 724 devices in force.

4.5.10 To date, Nottinghamshire's Cyber Team have engaged with 17 'Prevent' candidates. The team will work with referrals on a one-to-one basis to assess their capability and divert their skills into positive career paths, so they are not engaging in criminality. The team offer a mentoring scheme, educate around the Computer Misuse Act and if they can prove they are willing to work within the scope of the law, they can provide them with tools to increase their knowledge. An inspirational success story that emerged from these referrals was an individual who is now studying Computer Science and has become a supervisor at a Gaming station/workshop that he helped to set up.

4.5.11 As stated earlier, our Cybercrime team provides a specialist and dedicated capability to investigate all cyber-dependent crime. Many of the investigations will take considerable time to conclude and it is not possible to comment on some of the individual cases whilst these are still impending. It is important however to highlight the following:

- Cyber detectives provide a prompt response to Ransomware attacks (1- 2 a fortnight currently) and conform with the regional standards for attendance and reporting of these incidents. For out of hours reports the Fraud Triage Assistants highlight reports directly to the Cybercrime team so that they can be dealt with. Although most of the cases are perpetrated by foreign threat actors, the response to identify the method of attack, strain of ransomware, evidential/intelligence opportunities are extremely valuable to the National and International response.

- Cyber pursue also provide advice and prompt attendance/assistance at scenes for crypto asset seizures. The force has seized over £100,000 worth of Bitcoin this year so far.

- The Cyber Apprentice has proven an extremely valuable resource to the Pursue side and has assisted in reviewing data on several cases. Most recently a website hosting company reported that they had been hacked by a former client. Prompt detailed analysis by our apprentice of the server logs confirmed that no computer misuse offences had been committed

- Op Raddichio. Although this is still an ongoing investigation into the "hack to order" of University Student's Snap Chat accounts, the information and evidence gained has helped to direct a targeted Cyber Protect campaign at the University.

4.6 **Conclusions**

Cyber threats are borderless and present as a global challenge.

Cybercrime continues to rise, and it is becoming increasingly difficult to separate these offences from more traditional crimes. The onset of the COVID-19 global pandemic has intensified the situation further with cyber criminals taking advantage of the growing numbers working from home and self-isolating.

Nottinghamshire Police's 5-year Cybercrime Strategy outlines what it will do to effectively manage cybercrime to minimise the impact of this rapidly evolving crime type on the residents and communities within the city and county. The strategy includes both the prevention and detection of offences, as well as the support provided to victims to prevent repeat victimisation.

5. Financial Implications and Budget Provision

5.1 There are no financial implications arising from this report however, the reduction in centralised funding requires review and consideration around future funding proposals to ensure business continuity.

6. Human Resources Implications

6.1 HR need to be engaged in the outstanding recruitment activity.

7. Equality Implications

7.1 There are no equality implications arising from this report

8. Risk Management

8.1 There are no associated risks regarding this report.

9. Policy Implications and links to the Police and Crime Plan Priorities

9.1 There are no policy implications arising from this report.

10. Changes in Legislation or other Legal Considerations

10.1 There are no changes in legislation arising from this report

11. Details of outcome of consultation

11.1 There has been no consultation on this report as it is for information only.

12. Appendices

12.1 None

13. Background Papers (relevant for Police and Crime Panel Only)

13. None

NB
See guidance on public access to meetings and information about meetings for guidance on non-public information and confidential information.