| For Information | |
|---|---|
| **Public** | **Public** |
| **Report to:** | **Strategic Resources & Performance Meeting** |
| **Date of Meeting:** | **4th November 2020** |
| **Report of:** | **Chief Constable** |
| **Report Author:** | **DCI Yvonne Dales** |
| **E-mail:** | **Yvonne.dales@nottinghamshire.pnn.police.uk** |
| **Other Contacts:** | **T/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 Commissioner notes the content of this report.

## 3. Reasons for Recommendations

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

## 4. Summary of Key Points

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

4.1.1 **Cyber Dependent Crime -** Within the financial year period 2019/20, which runs between April and March there were 497 Action Fraud crime reports which equates to 0.45 Action Fraud crime reports per 1000 of the population in Nottinghamshire. This compares with 412 Action Fraud crime reports on the previous year, a rise of 26% and far exceeds the 15.6% increase nationally. Despite this increase, Nottinghamshire achieved the second highest cyber dependent judicial outcomes in the country for 2019/20.

4.1.2 **Fraud Crime –** 2019/20 saw 11,720 frauds reported in Nottinghamshire, which is an increase of 6% compared to the last year and only marginally down on the increase nationally. In the same period 2019/20, Nottinghamshire recorded the fourth highest volume of judicial outcomes for Fraud (263).

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 86% of all police reported fraud has some cyber element.

4.1.4 The above figures only include those crimes reported to Action Fraud. The gaps between the Crime Survey for England and Wales and Action Fraud suggest that the gaps between experienced and reported fraud and cybercrime remain. Therefore the true scale and threat remains largely unknown.

## 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 The dedicated Cybercrime team continues to work closely alongside the Fraud and Financial Investigation teams, collectively forming the Economic and Cyber Crime Unit (ECCU).

4.2.3 In light of the increase in reported cybercrime for Nottinghamshire and particularly when compared to the rest of the East Midlands region, a business case was submitted earlier this year to secure additional national funding to support an uplift in resourcing for Cyber Crime. The bid was successful and provides funding towards the salaries of two additional detectives, an enhanced contribution towards the Detective Sergeant salary, an Intern and the part -funding of a Digital Evidence Examiner.

4.2.4 In addition to this, the team have also been successful in securing additional national funding for a Nottinghamshire Police Cyber Investigator to support the Cybercrime team and improve the provision of victim support, pro-active advice and local investigations and intelligence. The proposed pilot project is an innovative collaborative arrangement between Nottinghamshire Police and Vision West Nottinghamshire College to recruit an individual from within their Cyber Security Technologist NVQ, for a period of 2 years.

## 4.3 Investigative capacity and capability

4.3.1 The Economic & Cyber Crime Unit has benefited from a growth in staffing numbers. Integrating these officers with the experienced Detectives on Fraud creates an effective learning environment and future proofs the department, in being able to provide enough investigative resilience for what is a rapidly growing crime type. The department is virtually at full establishment. Until the end of 2019 Fraud resourcing was circa 50% establishment.

4.3.2 The Economic & Cyber Crime Unit has also recently recruited additional staff to form a dedicated Triage Team. The purpose of this new team being to 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.

4.3.3 The Triage team 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 Initially, the agreement is that the new team will run as a pilot and then for its effectiveness to be mapped against the forecasted business benefits, which may or may not influence any future staffing requirements.

4.3.5 As highlighted in earlier reports, Nottinghamshire Police's ECCU also has two dedicated Fraud and Cyber Protect Officers. Supervision of these officers falls to the Detective Sergeant who has 'day to day' line management for both the Cyber Protect and Prevent Officers and the Triage team. This arrangement ensures that the team's activities are coordinated and minimises duplication.

4.3.6 In the past year, more detectives within ECCU-Fraud have enrolled and completed the Associate Programme for Cyber Digital Investigation, part of the sustained commitment to the development of an Omni-competent workforce.

## 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 a number of 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. In the event that the national funding should cease Nottinghamshire Police will consider refocussing the team's efforts according to the wider cyber-related investigative demand.

## 4.5 **Key Achievements**

### 4.5.1 **Prevent**

Cyber Choices is a national initiative co-ordinated by the National Crime Agency and delivered by Cyber Choices teams within Regional Organised Crime Units and Local Police Force Cyber Teams. The Cyber Choices network was created to help young people make informed choices and to use their cyber skills in a legal way.

The main referrers to the cyber choices network are schools and therefore it has been a priority within the East Midlands region to increase awareness within schools. The strategy adopted to achieve this was to provide training, in partnership with the local safeguarding boards, to all designated safeguarding leads (DSLs) of schools within the different force areas. The trainings primary objectives were to increase awareness and understanding of cyber dependant crime and ensuring school policies include cybercrime, which would facilitate more referrals to cyber choices.

Nottinghamshire's Cyber Protect and Prevent Officers delivered training in Cyber Choices to both the city and county DSLs. This resulted in a significant increase in referrals made by Nottingham's schools, with 43% of all referrals made across the East Midlands coming from Nottingham.

Since October 2019, Nottinghamshire's Cyber Team have engaged with 12 'Prevent' candidates. This has included one from an NCA operation and the rest have been through Cyber Choices. The team 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 are able to prove they are willing to work within the scope of the law, they can provide them with tools to increase their knowledge.

Before the Cyber team engage with any Cyber Choices/Prevent referral, they now conduct an in-depth protect visit with the young person's parent or guardian. This is to enable them to manage their child's online activity. Nottinghamshire Cyber Protect and Prevent Officers have contributed to the parent engagement process, creating a checklist/scoring process for officers to complete with parents to highlight any areas of cyber vulnerability in their home. The team have also produced an advisory document that mirrors all of the questions on the checklist to ensure that families have everything they need to improve their online safety. Where households score highly the team will conduct a revisit and re-assess to ensure a reduction in online vulnerability. Following a presentation by Nottinghamshire of the process to all the regional counter-parts, the checklist is now part of the standardised regional process with the intention of a national rollout.

Within the cyber choices referral process, the engagement officers are also required to offer where requested and complete an assembly on the Computer Misuse Act. The Cyber team have completed this in schools and

voluntary organisations, such as scout groups across Nottingham. Feedback was extremely positive regarding the engagement officers. The presentations had clear messaging for young people to assist them in keeping them safe online and to deter them from getting involved with cybercrime.

4.5.2 **Protect**

A recent review of the regional protect strategy has been completed, providing further clarity of roles and responsibilities of both local and regional officers. The structure of protect is going to be driven more by intelligence and evidence based policing.

Communication platforms have changed to assist in the sharing of current trends and Modus Operandi's (MO) of victims within local forces. The aim being to ensure a coordinated and targeted approach to our messaging and advice. Historically, the public have been overwhelmed with messages and these have become diluted as a result. The merits of this new approach were evident within the first week, when a Nottinghamshire Cyber Protect Officer highlighted a trend of using specific companies' brands to commit computer software fraud. This MO was agreed as similar to what was happening in Northamptonshire. The regional cybercrime team created a Computer Software Campaign for materials to provide support for consistent messaging, which was used on social media in force regions. Nottingham have also shared innovative ideas around concise messaging which will be supported by the region and will participate in targeted messaging on Webinars hosted by the region.

The Cyber Protect & Prevent Officers have been heavily involved in making improvements around Cyber Stalking and actively involved in approximately 55 cases since November 2019. This has included the design and production of a Cyber Stalking leaflet, which mirrors the other Domestic Abuse leaflets across Nottinghamshire; being distributed across Nottinghamshire by Equation, Women's Aid and Public Protection teams within force. The team have also created a PROTECT Cyber stalking checklist to support victims of Cyber Stalking and added this to the Nottinghamshire Police website.

Over the past year, the Fraud and Cyber Protect Officers have continued to carry out a number of engagement and awareness raising initiatives and events. With the advent of COVID-19, the team have utilised more innovative methods via partner agencies to distribute the key messages. For example in food parcel deliveries. The Protect Officers have maintained a high profile on social media with live weekly Instagram stories and quizzes. The stories on Facebook and Instagram reached between 2500-3000 people every time and the team also placed their posts/campaigns on social media which has collectively reached around 300,000 on Facebook with post engagements at 12k. On Cyber and Fraud Twitter accounts, the team reached 1 million.

4.5.3 **Pursue**

The Cyber Pursue officers, in addition to work allocated via the Action Fraud network, also conduct daily checks of crimes, which have been directly reported to Nottinghamshire Police. In some cases, this leads to specialist

advice being provided to officers, who are dealing with these crimes, and in other cases, the department take on the investigations. Some of these subsequently lead into Prevent referrals. This approach has led to numerous serious offences being investigated and has contributed to Nottinghamshire Police's high ranking in the positive disposals for cybercrime offences.

Two such examples are as follows: - A series of blackmails against vulnerable female university students, studying at local universities was identified, urgent enquiries were conducted and key evidence recovered from the scenes, further technical enquiries identified a suspect and linked into a national level investigation, providing key evidence. Joint working was conducted with another UK force and the result was that the suspect was charged with 65 offences. Another example is of a report of bullying between schoolchildren. This was identified as a Distributed Denial of Service (DDOS) attack and following the interview of the 14-year-old, evidence of numerous other DDOS attacks and research into much more serious cybercrime was identified. The suspect was given a Community Resolution and successfully referred into the Prevent Program.

4.5.4 **Conclusions**

Cybercrime is not a local issue and this is reflected in how Pursue operates. Numerous warrants have been undertaken, with officers from the Regional Cybercrime team and with officers from other Cybercrime units from around the country. In some cases, officers from different force teams will work in conjunction, on different elements of the same job. This is often coordinated from the Regional Team.

The Pursue team also undertake Protect work and, in addition to investigations often cover Protect elements. Sometimes this will be in relation to vulnerable victims and sometimes interacting with companies. Pursue officers are Associate Members of the Institute of Information Security Professionals (IISP) and hold the EC-Council Certified Network Defender qualification, in addition to digital forensic qualifications, which adds credibility to this advice. They work closely with the Protect teams and will often visit victims together, covering the different elements.

Work is also taken on through direct referrals from the Protect Team and through the Fraud Triage Team, where although not identified by Action Fraud for direct dissemination, it is felt that the Cyber Pursue team are best placed to provide the best service to the victims. Pursue officers also work closely with the Fraud and Financial Investigation teams and frauds linked to the original Cybercrime investigations are investigated.

## 5. Financial Implications and Budget Provision

5.1 There are no financial implications arising from this report

## 6. Human Resources Implications

6.1 There are no HR implications arising from this report.

## 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.

9.2 This area of business is linked to all of the Police and Crime Plan priorities but is particularly key to protecting people from harm.

## 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.