For Information	
Public	**Public**
Report to:	**Strategic Resources & Performance Meeting**
Date of Meeting:	**6th November 2019**
Report of:	**Chief Constable**
Report Author:	**DCI Lee Young**
E-mail:	**Lee.young@nottinghamshire.pnn.police.uk**
Other Contacts:	
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 ON LINE

1. Purpose of the Report

1.1 The purpose of this report is to provide an update on Nottinghamshire Police's:

- Current investigative capacity and capability for cyber-related demand.
- Collaborative and preventative approaches to reducing cybercrime.

2. Recommendations

2.1 That the meeting notes the content of this report.

3. Reasons for Recommendations

3.1 To ensure that members are aware and updated on the force's strategy in relation to tackling cyber-enabled crime and keeping people safe on line.

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

4.1 **Contextual Summary**

4.1.1 Information technology is an integral part of most day to day activities; criminal activity is no exception to this and virtually any crime can be made easier or more effective through the use of computer resources. Whilst there are various interpretations of cybercrime, the Home Office adopts the following definitions of which are employed for the purpose of this report:

- **Cyber-dependent crimes**: offences that can only be committed by using a computer, computer networks, or other form of Information and Communications Technology (ICT). These acts include the spread of viruses and other malicious software, hacking, and distributed denial-of-service (DDoS) attacks, i.e. the flooding of internet servers to take down network infrastructure or websites. Cyber-dependent crimes are primarily acts directed against

computers or network resources, although there may be secondary outcomes from the attacks, such as fraud.

- **Cyber-enabled crimes**: traditional crimes where the scale or efficacy of the offence through the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud, child sexual exploitation and distribution of Indecent images).

- **Online crime**: As per the definition of cyber-related in the Crime Survey for England and Wales, this relates to any offence where the internet or any type of online activity was related to any aspect of the offence.

4.2 **Resources and Investigative Structure**

4.2.1 Nottinghamshire Police has resources dedicated to the investigation of cyber-dependent crime and the activities associated with prevention and protection work streams. This Cybercrime team works alongside Fraud and Financial Investigations teams, collectively forming the Economic and Cyber Crime Unit (ECCU). The Cybercrime team is an early adoption of the national cybercrime model and is described as being regionally tasked but locally delivered. It comprises:

1 Detective Sergeant

2 x Pursue Investigators

2 x Cyber Protect and Prevent Officers

4.2.2 The East Midlands project (part of the National Cybercrime model) has been in existence since February 2018 operates to a number of targets that are focussed exclusively around cyber-dependent crimes. the allocation of 2x Pursue Investigators is sufficient to absorb the current workload. The number of reported cyber dependent crimes to the Police/Action Fraud remains relatively low. However, crime surveys indicate that the businesses and the public have a significantly different attitude to reporting when comparing against conventional or even cyber-enabled crimes. Reporting trends are likely to increase as the capability in forces becomes more apparent and publicised and therefore the expectation is that resourcing in this area of business will need to increase.

4.2.3 The most commonly reported cyber-enabled crimes are associated to fraud (acquisitive crimes) and are referred to the ECCU (Fraud), whereas cyber-enabled sexual offences are managed by the appropriate strand of the Public Protection Department. The Digital Forensic Unit (DFU) provide technical support through evidential examinations of devices (phones, tablet, computers

etc.) and additionally host a team of Digital Media Investigators who are able to support investigations through technical expertise or tactical advice.

4.2.4 A proposal for the development of Nottinghamshire's digital service is under consideration by the Chief Officer Team. If accepted, this would centralise digital capabilities, modernise IT infrastructure and expand resources through a program-of omni-competence to build resilience for future demand.

4.3 **Fraud demand and investigative capacity and capability**

4.3.1 Nationally, a third of all crimes are fraud offences with 3.6 million (reported) incidents experienced in the year ending December 2018. **86% of these are cyber-enabled**. The situation in Nottinghamshire reflects the national trends.

4.3.2 Within Nottinghamshire Police, fraud offences are the responsibility of a dedicated unit managed within the Organised Crime Department and are specialist investigators in their field. Significant investment has taken place in the past 12 months in terms of facilitating officers' attendance on the Specialist Fraud Investigation Programme. This course is focused on embedding the nationally recognised Fraud Investigation Model, requiring officers to consider as part of learning alternative investigative approaches e.g. disruption and preventative opportunities. As previously highlighted, Nottinghamshire Police has recognised the value in drawing together fraud, cyber and financial investigation expertise to form the Economic and Cyber Crime Unit (ECCU) which is in keeping with national fraud strategy guidance being developed by the NPCC and City of London Police. Developing a degree of omni-competence between these functions is a current aspiration of the ECCU, which will allow resources to be used more flexibly in managing demand and increase professional development opportunities for officers and staff.

4.3.3 Nottinghamshire Police's ECCU also has two dedicated Fraud and Cyber Protect Officer posts. The post-holders key role is to research, develop, coordinate and implement measures (working with colleagues and partners both internally and externally) to improve the identification and response to vulnerable fraud victims in Nottinghamshire. The Protect Strategy is hugely important and there is a national understanding that we cannot investigate our way out of fraud. Consequently protecting future victims and preventing repeat victimisation is a priority aim and performing this work is challenging. In recognition of this and in response to a mature understanding of this theme of it has been necessary to re-evaluate roles accountabilities, responsibilities and decision-making requirements. There is now confidence that the role is correctly defined, graded and attracts candidates of the right calibre with appropriate skills to deliver on its objectives.

4.3.4 Fraud demand reaches Nottinghamshire Police from a variety of sources, this includes 'calls for service' and referrals disseminated by the National Fraud Intelligence Bureau (NFIB). It should be borne in mind that where a cyber-enabled fraud is committed, the likelihood is a computer misuse offence (cyber-dependent crime in effect) has also been committed. A good example of this would be in the case of Payment Diversion Fraud (previously known as Mandate Fraud). Mandate fraud is when victims are manipulated into altering automated payments (direct debit/standing orders) or bank transfers, by purporting to be an organisation they make regular payments to, for example a subscription service or component of the business supply chain. These frauds are often traced back to a 'mail server breach' where the originating company have been the victim of a cyber-dependent offence. Investigation of that offence is generally overlooked in favour of the more conventional fraud element. This is generally considered to be a gap in capability, knowledge or training.

4.3.5 Cyber-crime, specifically cyber-dependent crime, is growing, is dynamic and in general alignment with the faced pace technological changes that are seen societally. Cyber-enabled criminality adds complexity to existing crimes but does not mean that it should be treated differently to other offences. Traditional separation between investigators and highly skilled technical specialists is a gap that needs to be narrowed as these crime types have become the norm, rather than the exception. Upskilling a larger proportion of the operational workforce is challenging and requires investment. This is acknowledged at Government and NPCC level and also features at local delivery level in Nottinghamshire. Progressive increase and wider distribution of skills within the ECCU is a clear management objective, underpinned by the departmental ADA submissions. Examples of this have been to train a Financial Investigator and Fraud Investigator to provide tactical advice on the investigation of crypto-currencies (Bitcoin etc.) and to extend DMI training to a proportion of fraud investigators. Additionally, energy has been expended to achieve formal cyber qualifications/accreditation for cyber investigators which demonstrates a commitment to professional and continued development. (Associate Programme for Cyber Digital Investigation)

4.3.6 A further outcome agreed at the Extraordinary Force Executive Board is to develop a fraud triage capability. The purpose of this innovation is designed to develop a new structure, designed to improve our effectiveness and efficiency in dealing with all reported fraud, identify vulnerability at the earliest opportunity, determine the level of investigation and apply agreed disposal options. (Acceptance criteria, cease & desist, specialist investigation etc.)

4.4 **Performance targets**

4.4.1 Established national targets, adopted regionally and locally already exist for the delivery of the cyber-dependant program.

- 100% of cyber-dependant crimes referred from NFIB will be investigated
- **100% of victims who report cyber-dependant crime to Action Fraud will get advice in person or over the telephone to prevent them becoming repeat victims**
- 75% of organisations and the public who receive crime prevention advice will change their behaviours as a result
- 75% of organisations who receive cyber-security advice will develop or review incident response plans and test them
- 100% of young people identified as vulnerable to cybercrime will contacted, and intervention from a cyber-prevent officer where appropriate

4.4.2 Nottinghamshire Cybercrime makes contact with all victims of Cybercrime and delivers approved advice in response to the circumstances. Processes are in place to follow up on the initial contact to measure the effectiveness of any advice given and indeed to establish if it has been acted upon by individuals or businesses. This provides further opportunity to deliver additional advice where required and has proved very successful. For example, in one particular case the victim of a social media and e-mail hacking by ex-partner scored very highly on our protect scoring process (showing very limited security knowledge) and upon reassessment had significantly lowered the score, reducing her level of vulnerability by adapting on-line behaviours. 4.5

Prevention and Collaboration

4.5.1 The focus for Force based Cyber Protect and Prevent Officer is delivering the approved main cyber security messaging from the National Cyber Security Centre to;

- Small to Medium sized companies (Sub 250 employees)
- Trade Bodies/Associations.
- Local Charities.
- Voluntary sector.
- Local educational trust/bodies.

Further activities include;

- Referral of suitable candidates to the Cyber Prevent Program, facilitated through the Regional Prevent Officer.
- Deployment to all victims of crime from the above categories and other victims based upon THRIVE.
- Promote Cyber Essentials within supply chain across the Force
- General cyber security advice to members of the public

4.5.2 **General Public Engagement & Awareness Raising Initiatives**

- Nottinghamshire Police has refreshed and continues to maintain its external Cyber Website by providing all necessary signposting for victims, this includes the following: **'Safeguarding children and vulnerable people'** (advice for young people and parents), The **Protect yourself - online checklist** is also available on the website and is designed for anyone to utilise. In addition there is also our **'Cybercrime advice for organisations'** offering advice to organisations on protecting themselves from Cybercrime including staff training support.

- Nottinghamshire Police's collaboration with the Get Safe On-line programme has provided materials for social media, campaigns and leafleting whilst also supporting bespoke events. This year, Get Safe On-line supported the police at three significant public events the Nottinghamshire County Show, the Retford Charter day and the Riverside Festival. It is estimated that the Riverside Festival alone reached over 10,000 people.

- BBC Radio Nottingham – Nottinghamshire Police's Cybercrime and Fraud Protect Officers now have a regular monthly slot discussing key trends and providing general cyber and fraud protect advice.

- Regular drop-in sessions at local Banks.

- Nottinghamshire Police issue alerts via social media utilising Facebook, Twitter and Neighbourhood Alerts.

- Working with MENCAP (the voice of learning disability) by supporting the roll out of their online safety workshops designed for people working with learning disability.

- Working with MENCAP, presentations to groups such as U3A, Fire Service and Nottingham Community and Voluntary Service with the aim of educating

professionals from other organisations to spread messaging to their service users.

- Working with educational establishments throughout Nottinghamshire to deliver Cyber Protect messages to students. The Cyber Officers attended the University of Nottingham and met with the International students as part of 'Fresher' events to deliver key protect messages alongside other potential scam trends where they are specifically targeted.

- Successful engagement at other public events, such as Mansfield Senior Citizen Fair, Wollaton Food Festival.

- Promoting Get Safe On line week (w/c 30th September 2019)

4.5.3 **Domestic Abuse**

Nottinghamshire Police identified a growing trend, linked to the break-up in relationships where one party would use the identities and personal details of their former partner to fraudulently obtain goods and/or credit facilities.

In some cases this crime had been enabled by the former partner accessing the victims' email account or accessing their on-line banking to facilitate these offences.

A more sinister trend was identified in relation to domestic abuse cases where the actions could be construed as coercive/controlling.

In addition to this, Nottinghamshire Police's Cyber Crime Unit also identified a significant number of domestic abuse investigations where valuable evidence of the offenders' behaviour could be adduced in relation to computer misuse act offences.

The Cyber Crime Unit worked with the Public Protection's Lead for Domestic Abuse and it was clear that limited guidance was being offered to victims concerning the risks of cyber security. It was also evident that there were gaps in knowledge across the wider Domestic Abuse community.

Nottinghamshire Police's cyber team are now fully engaged with local Domestic Abuse charities like Equation who are able to support Nottinghamshire Police by spreading our Cyber security awareness to survivors. Furthermore, Cyber Protect & Prevent Officers have provided 'Cyber Awareness Training' to Equation highlighting how cyber methods can be used to stalk and control victims, for example by enabling the perpetrator to identify geographic locations and online activity. This effective partnership working has the added advantage increasing officer knowledge and understanding of domestic violence, helping the team appreciate the signs and risks of abuse. The Cybercrime Team have additionally supported the Public Protection Department in updating their training aides to incorporate cyber advice.

Nottinghamshire Police have developed literature that Equation are set to utilise in the design of a leaflet to mirror their corporate branding and have agreed to distribute these across Nottinghamshire on our behalf.

The Cybercrime Team intend to promote this work even further by offering staff training to all local domestic abuse charities to help reach more survivors with our Cyber Protect Advice. Last year, approximately 50% of individuals who were victims of cyber-dependent offences in the East Midlands region were victims of domestic abuse.

4.5.4 **Business**

Small businesses are often targets of Ransomware and DDOS attacks. Many small businesses do not have robust security measures as they do not employ an IT professional. This makes them vulnerable to these kinds of attacks and consequently, these businesses often pay ransom demands out of desperation.

The Cybercrime Team feeds into business networks which allow us to communicate the NCSC messaging to small businesses across Nottinghamshire.

- We use networks such as CSSC (Cross-sector Safety and Security Communications), D2N2 (local enterprise network for Derbyshire and Nottinghamshire), North Notts BID and FSB (Federation of Small Businesses) to send out alerts when there is a new trend to watch out for.

- We have featured in their newsletters and have been asked to deliver presentations to businesses. We use this approach to maximise our reach.

- The Cybercrime Team have now received training and are able to advertise Cyber Alarms – this is a Cyber Protect tool that will be rolled out to local companies providing them with an early warning of suspicious activity targeting their IT Network and offering an ‘MOT’ style health check. In both instances, these businesses will be able to instigate measures to defend their network accordingly.

This Protect tool will be delivered in a 3 tier format.

- Existing known victims

- Education and Health care trust (organisations where reputation is vital)

- Businesses not previously known to be victims.

Consequent reports from Cyber Alarms will ONLY lead to Nottinghamshire Police investigations where the Offender and Victim are both residents within Nottinghamshire

4.5.5 **Further collaboration opportunities, currently under development**

- An e-learning package has been created with the intention of this being shared with all front line Police and Fire Officers and a different version being used to educate the general public. The training covers the core messaging, which is aligned with the NCSC.

- Having identified a gap in education around the risks of Cyber Stalking, particularly in domestic abuse relationships we are currently in the process of trying to secure monies through Innovation funds to develop and implement a 'train the trainer' campaign for local domestic abuse charities and other organisations such as Nottingham City Homes. They will then be able to share this knowledge with those vulnerable to this offence.

4.5.6 **Conclusion**

This report demonstrates that Nottinghamshire Police have taken significant steps forward, not only in developing specialist capability but also in understanding how cyber-related crime is present within conventional offending. It also acknowledges that there are limits to the effectiveness of investigation as a control measure, with prevention and avoidance of re-victimisation being a key and developing area of focus.

The national cyber program and regional support has been instrumental in providing the right training, guidance and momentum to develop Nottinghamshire' current resource, however the funding for this program is expected to conclude by March 2020. It is essential therefore, that commitment to this capability is fully adopted by Nottinghamshire Police and that continued professional development forms part of that commitment. Cyber is a fast paced and dynamic area of policing and can only be effectively combatted by tracking the developments in technology and criminal methods and adapting to these changes.

Investment in specialist training that keeps pace with technical developments in offending are crucial to providing an effective response to pursue serious offenders, whilst more generalised training is required to enhance the skillset of frontline officers who can more widely support protective messaging and identify vulnerability at first point of contact. It is important not to regard cyber in isolation, but to consider it more broadly. Positive examples of this have been to join connected functions, such as in the Economic & Cyber Crime Unit, with further plans underway to create a Digital Policing Hub that will draw expertise together under one management structure.

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.

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.