Suffolk Police and Crime Commissioner

*Making Suffolk a safer place to live, work, travel and invest*

***In response to the set of questions arising from the Panel's workshop, most of which were operational, the Constabulary has produced the following report which supports the Panel to understand the work of the Cybercrime Unit and Cyber Investigators.***

## 1. Introduction

1.1 The following report provides an overview of the Norfolk and Suffolk Cybercrime Unit and also provides details of the new Cyber Investigators that sit within Neighbourhood Support Teams (NSTs) in Suffolk.

## 2. Background

2.1 The National Security Strategy 2010 identified organised crime and in particular large scale Cybercrime as a 'tier one' threat to national security alongside international terrorism. Furthermore, the Home Secretary's Strategic Policing Requirement lists organised and cybercrime as national threats that Chief Constables and Police and Crime Commissioners (PCCs) are required to address. The National Strategic Assessment Mid-Year review 2016 highlights the most competent financially motivated Organised Crime Groups (OCGs) as a principal threat to the UK.

2.2 Dedicated Cybercrime Teams/Units are one of the core requirements for Forces to effectively respond to Cybercrime under the Strategic Policing Requirement (SPR) and to build effective Digital Intelligence and Investigation (DII) capabilities. DII encompasses the policing capabilities needed in response to challenges posed by the digital revolution.

2.3 The Police and Crime Commissioner and Suffolk Constabulary are committed to the investigation and prevention of cyber offences and as such, have made significant progress and investment.

## 3. Norfolk and Suffolk Cybercrime Unit

3.1 The Norfolk and Suffolk Cybercrime Unit was set up in July 2015 and sits within the collaborated Protective Services Command. The Unit's mission statement is to contribute alongside regional, national and international partners, towards the provision of a safer and more secure cyber environment.

3.2 In designing and delivering the response, consideration is given to the four main objectives (4Ps) Serious and Organised Crime Strategy:

> <u>Pursue</u> those individuals who engage in cyber and serious crime and seek criminal justice outcomes;

Prevent those individuals from becoming and remaining in cyber and serious crime;

Protect the public from becoming victims of cyber and serious crime;

Prepare for the consequences of cyber and serious crime.

3.3 More recently, the publication of the National Strategic Assessment, National Control Strategy and National Intelligence Requirements of Serious and Organised Crime 2016 has highlighted the threat from Serious and Organised Criminals particularly in relation to Organised Immigration Crime, Child Sexual Exploitation and Abuse, Firearms, Cybercrime and Money Laundering.

3.4 The Norfolk and Suffolk Cybercrime Unit consists of a Detective Sergeant, four Detective Constables, four Digital Media Investigators, two Fraud Investigators, an Intelligence Analyst and a Cyber Security Advisor. There are police staff members working alongside officers and this has proven to be successful. The Unit has recently also recruited a 'cyber volunteer' to assist with the Protect agenda.

3.5 The work the staff are engaged in can be separated into five main areas:

Cybercrime Investigations

3.6 Proactively and reactively investigate serious incidents of cyber dependant crime including Malware (including BOTNET creation/exploitation), Distributed Denial of Service (DDOS) attacks, Web Defacements, Data Exfiltration, Computer and Network Intrusions/compromise (Hacking), Phishing, Vishing and other forms of Social Engineering.

3.7 The Cybercrime Unit has had a number of protracted investigations since its formation in June 2015. The complexity and level of skill required to investigate these offences should not be underestimated. The type of offences include the following:

- *Distributed Denial of Service/Malware* - In excess 30 investigations related to DDOS and Malware offences where businesses and individuals have been targeted.

- *Operation Metro* - Investigation into a £1 million pound in cash cyber-enabled fraud resulting in a local business in Suffolk becoming a victim. Prompt and thorough enquiries resulted in an identification of an organised crime network and eight suspects have been convicted. Taken together they received over 30 years in prison.

- *Operation Duston* - Investigation into cyber enabled credit card fraud, all 10 defendants have now pleaded or been found guilty. These defendants are part of an Organised Crime Group with two of the main defendants now subject to a Serious Crime Prevention Order.

- *Op Fringe* - Investigation into Network Intrusion into two significant local infrastructure agencies. This has been a significant investigation which led the team to the West Midlands and has resulted in an individual being currently on remand and will be charged with two offences under Section 1 of the Computer Misuse Act 1990.

- *Op Woodcock* - Initially reported as a million pound theft from lorry in Felixstowe. The enquiries have identified cyber enabled opportunities at an international level, with internet activity enabling the distribution of stolen devices. To date 12 suspects have been arrested with a further 5 planned. This enquiry has seen Suffolk Constabulary working with a significant Company with commercially sensitive business interests within the UK. This enquiry is recognised as Organised Crime and has been mapped as such.

- *Op Parlingo* - Investigation Cyber Harassment of a community group chat app company based in Ipswich. User blocked from website started a targeted campaign against the company by posting extreme pornography on their website and threats made against company directors. The suspect has been arrested and has been cautioned for the offence.

- *Op Wheel* - Fraud investigation where an individual has gained a significant IT contract by false representation. Charged with Fraud.

- Investigation into a local business which sustained harassment on line via Facebook. The defendant has been charged with harassment.

- Investigation for an offence under the Computer Misuse Act 1990. The defendant took unauthorised control of a website belonging to a Waveney taxi business. He hacked into and sabotaged the dispatch system used to deploy taxis. On being sacked from the company, he continued to access the computer systems remotely, removing tariffs from the taxi company system so that drivers could not log onto the system and manage the jobs. The defendant changed the business telephone number and website so it diverted to a rival taxi company and also uploaded offensive material.

  The defendant has pleaded guilty to an offence under Section 3 of the Computer Misuse Act 1990 and was sentenced to16 months' imprisonment suspended for two years, a five-year restraining order not to contact two individuals at the company, 250 hours of unpaid work and was ordered to pay £1,000 compensation to the victim. This was the first conviction of an offence under Section 3 in Suffolk and Norfolk.

- Live investigation into Private Branch Exchange (PBX) Hacking intrusion into Voice over Internal Protocol (VOIP) service provider where 17 calls were accessed.

3.8 The Digital Forensics Unit (DFU) supports investigations across both Constabularies and is a leader in its field of expertise for forensic analysis of mobile and computer devices and is working in partnership with a major software provider to develop an automated service for digital analysis of devices.

3.9 The DFU for Suffolk only, between 01/04/15 and 01/01/16, has analysed 189 cases consisting of 816 computers and 486 mobile devices - this resulted in 173 terra bytes of information being processed.

3.10 The DFU for Suffolk only, between 01/04/16 and 01/01/17, has analysed 184 cases consisting of 818 computers and 365 mobile devices and again this has resulted in 173 terra bytes of information being processed.

Digital Media Investigations

3.11 This specialist work includes writing Digital Strategies/Profiles for Senior Investigating Officers and Local Review Officers for OCGs. The staff are trained in router analysis and examination, capturing volatile data, advanced open source research and tracing emails and data communication over the internet. Advice can be provided on areas including the deep and dark web, cryptocurrency including Bitcoin.

3.12 The Digital Media Investigators (DMIs) have provided support to many major investigations including Op Perspex (Child Sexual Exploitation) and Op Shoelace (attempted murder).

3.13 All Lead Responsible Officers (LRO) have access to Digital Media Investigators (DMI) for the investigation into OCGs.

3.14 The role has developed and the skills of the investigators have proven to be a valuable resource.

3.15 Some of the work has included the following:

- Assisting the Public Protection Teams with visits to High Risk Registered Sex Offenders - conducting physical examinations of all computer devices, removable media and WIFI router examinations. Advice given to offenders regarding software applications that could be considered 'anti-forensic'.

- Surveying mobile phone and mast technology which is underway in Operation Vivaldi to validate and link crime scenes, through mobile devices, of up to 27 burglary dwellings.

- Attending crime scenes - Wi-Fi/router analysis. Providing full evidential event logs downloaded from routers, this is evidenced in operation Starlight (Stranger Sexual Assault in Aldeburgh) where this technology was utilised.

- Assisting with digital profiles and advanced open source for Major Investigation Team (MIT) and serious crime including high profile missing person.

Fraud Investigations

3.16 Proactively and reactively investigate fraud investigations which are considered complex and serious. The fraud trained staff are able to provide advice regarding financial intelligence and enquiries, assist with referrals to the Regional Economic Crime Unit and the Regional Asset Recovery Team. They provide ongoing support to the Incident Crime Management Unit regarding the investigation of volume fraud.

3.17 The unit is currently investigating seven complex fraud cases. The types of offences include mortgage, pension, mandate, accountancy and other types of fraud which have a cyber element.

3.18 Operation Porto - Money Laundering Investigation supported by Ipswich Borough Council and the Regional Economic Crime Unit. The fraud is centred on the activities of male running a property letting agency in Ipswich who is fraudulently offering a

complete rental package then signing clients up to various utility and council charges without their knowledge.

3.19 There are a number of vulnerable victims who have provided statements. The main suspect has been arrested.

3.20 The fraud investigators have provided specialist advice in relation over 100 investigations.

3.21 The unit retains oversight and responsibility for offences relating to electoral irregularities and provides returns to the Electoral Commission.

Cyber Security Advisor

3.22 The advisor co-ordinates, presents and provides social, technical and protective security advice to businesses, potential victims, the public and organisations relating to the threat of cybercrime. The work includes furthering the Prevent, Protect and Prepare strands of the Serious and Organised Crime Strategy and more recently the recommendations from the launch of the National Cyber Security Strategy 2016. The detail of the protect work is documented at 7.1.

Child Protection System:

3.23 The Child Protection System, which is managed by the Cyber Unit, provides intelligence of those involved in the viewing of indecent images of children.

3.24 The trained staff are responsible for the development of the intelligence packages for Suffolk, Norfolk and other Forces. This work is conducted under the name of Operation Bane. To date, over 85 packages have been completed for enforcement in Suffolk resulting in 77 arrests. The work has safeguarded in excess of 60 children.

## 4. NST- Cyber Investigators

4.1 Following an investment from the PCC in August 2016, the Constabulary recruited nine Cyber Investigators and a Cybercrime Supervisor. They are located at Lowestoft, Ipswich and Bury St Edmunds and work within the Neighbourhood Support Teams. They have received specialist training and to date have completed in excess of 350 digital media investigative enquiries supporting officers and staff within the County Policing Command (CPC). This has included open source, digital capture, missing person enquiries and analysis of mobile devices.

4.2 The Cybercrime Investigators have three principal functions: to work as part of the neighbourhood support teams, providing specialist tactical support and advice to volume crime with a cyber-element across the Force; to act as officer in the case, investigating cyber enabled offences, conducting interviews, preparing and submitting case files and to promote and deliver effective cyber prevent and protect messages.

4.3 The most common type of cyber enabled offences that are currently being reported in Suffolk and investigated by the Cyber investigators are:

Buyer Disputes – Non-payment or non-delivery of goods or services often involving EBay or Gumtree sites. These offences usually involve an element of Fraud and are often referred to Action Fraud.

Fraud – Attempt successful or otherwise to fraudulently obtain money from individuals using the internet. These can be phishing scams or fraud using chat rooms or dating websites (Romance Fraud).

Harassment/Malicious Communications – using social media, email and apps to distribute offensive or abusive messages to or about the victim.

Child Sexual Exploitation (CSE) – Sexual activity over the web or grooming through social media of a person under 16 years of age usually encouraging the victim to exchange pictures and/or videos and/or engage in sexual activity online. They have received specialist training and to date have completed in excess of 350 digital media investigative enquiries supporting officers and staff. This has included open source, digital capture, missing person enquiries and analysis of mobile devices.

## 5. Online Investigation Team/Exploitation

5.1 Suffolk has continued to take a robust approach toward those who possess or distribute indecent images of children. In the last 12 months the On-Line Investigation Team (OLIT) have dealt with 78 cases.

5.2 These cases originate from a number of sources including referrals from the National Crime Agency. The Constabulary has worked closely with the Eastern Region Specialist Operations Unit (ERSOU) in targeting individuals seeking to groom children on-line.

5.3 The Constabulary has also undertaken self-assessment activity to gauge its own ability to effectively respond to on-line grooming concerns. Additional resourcing into the wider exploitation area has been agreed and this includes a dedicated Detective Sergeant for the OLIT.

## 6. Overview of Current Themes

6.1 The commitment of Suffolk Constabulary and the PCC to dealing with Digital Investigation and Intelligence is evident in the level of investment since 2015. In establishing the Norfolk and Suffolk Cybercrime Unit there was a need to understand how Cybercrime was impacting on the communities of Suffolk.

6.2 A baseline assessment was completed which scoped the types of offences reported and themes. The findings were replicated in other Forces. Under-reporting in Suffolk, regionally and nationally continues to be an issue. Public understanding of what constitutes a Cybercrime and how to report is assessed as low amongst the wider public and some sections of industry. Protect based measures and education is a key area of the work of the Cybercrime Unit and the new Cyber Investigators.

6.3 The data collected as part of the baseline assessment provided the following themes:

- Between October 2015 and August 2016, there were 1639 crimes recorded on Athena (both Suffolk and Norfolk) with the keyword ‘cyber-enabled’. This has now changed to ‘on line’ crime. The majority of these were recorded ‘Malicious Communications’ followed by ‘Child and Domestic Abuse investigations’.

- Romance Fraud and Blackmail offences are still a theme in Suffolk. A recent edition of the National Fraud Intelligence Bureau (NFIB) threat update indicated that the App ‘Kik’ is being used more and more frequently to facilitate dating

fraud. It is believed to have been used in overseas cases of kidnap, murder and rape involving children. There are also cases of rape where the offender has befriended and developed a relationship online with the victim using dating websites such as Plenty of Fish.

- Action Fraud report that PBX fraud has risen by 18% since November 2014 with significant and growing losses to businesses. It is predicted that 2016/2017 will see a rise in reporting of this kind of fraud, with small and medium enterprises (SMEs) particularly suffering. Hackers are now believed to be developing techniques enabling them to access mobile phones through the use of malicious apps. PBX Fraud is currently recognised as a Computer Misuse Act Offence by the home office, and therefore such cases are investigated by the Cybercrime Unit and Investigators.

- Ransomware is an emerging trend nationally and in Suffolk. According to open source, reporting is being used as a 'testing ground' for this type of malware before extending to other countries. Once the malware is downloaded instructions follow on how to remove it usually by paying a 'ransom' fee. Payment is required in the form of cryptocurrency such as Bitcoin.

## 7. Effectiveness of the Cybercrime Unit

7.1 The current investment for the Norfolk and Suffolk Cybercrime Unit for 2016/17 is £583,990 – this investment has provided the constabularies with an effective unit to deliver against the requirements of the SPR.

7.2 The DFU continues to deliver an exceptional service to front line policing and has been subject of Her Majesty's Inspectorate of Constabulary (HMIC) inspection in 2016. This was an extremely positive inspection and has resulted in other Law Enforcement Agencies (LEA) visiting the unit to look at triage through Forensic 21 and understand the processes the unit employs. The final HMIC report is awaited.

7.3 The joint Cybercrime Unit has also received visits from the Home Office, Office of Surveillance Commissioners (OSC) and the College of Policing all of which have commented on the effectiveness of the unit.

7.4 Since the implementation of the unit at Halesworth the team has developed expert knowledge of the local, regional and national cybercrime landscape - this is evidenced in the collaborative working with colleagues from the Eastern Region Specialist Operations Unit (ERSOU) and providing training opportunities for National Crime Agency (NCA) staff under Operation Hera.

7.5 The work undertaken by the Cyber Security Advisor is and has been invaluable within the Prevent and Protect strands for Cyber Crime and is set out in the Protect Strategy for 2017. This area of business is a cornerstone to effectively reducing demand and providing information and education for business and individuals to protect against cybercrime. The engagement plans achieved to date illustrate the effectiveness and importance of this role.

<u>Protect Strategy</u>

7.6 With the launch of the new National Cyber Security Strategy in November 2016, the intention of Suffolk Constabulary is to continue to build upon its existing framework and in conjunction with this new strategy, further strengthen our cyber security and digital related advice.

7.7 The recently drafted Protect Strategy 2017 outlines the activity and actions for the coming year. Work continues with the Community Safety Team and the new Cyber Investigators to ensure the prevent/protect messages are consistent and up to date.

7.8 Education and awareness around Cybercrime is of the upmost significance, both to the public and businesses within Suffolk but also within the Constabulary. Challenging and updating our perceptions of digital policing, utilising evidence based policing methodology and developing skills to counter these new challenges.

7.9 The Cyber Security Advisor has achieved many engagements with all members of the communities in Suffolk. To date there have been in excess of 100 business engagements, youth and community engagements and 69 cyber protect presentations.

7.10 Digital workshops have been designed and delivered to 15-17 years olds through the National Citizens Service.

7.11 Practitioner training has been delivered to youth offending teams and schools.

7.12 In term of business engagement, Operation Breach was a cyber security event in Suffolk that attracted 90 delegates from businesses, NHS, Fire service and other partners. This will be an ongoing yearly event available to both the business community and the wider public. Many small businesses have been contacted and work is ongoing with the Business Network International and the Federation of Small Businesses.

7.13 Cyber basic reviews have been conducted with small businesses in Suffolk; this assesses a company's controls to mitigate digital threats.

7.14 Work is ongoing through the Suffolk Chamber of Commerce to reinforce appropriate messages to the business sector. The PCC has been involved in this work and also worked with the Federation of Small Businesses to promote its roadshow in 2015.

7.15 The Cybercrime Unit intend to work in collaboration with the Trading Standards team to design impactful, joint campaigns and awareness messages to combat this threat. Following the Unit's attendance at Norfolk and Suffolk's Trading Standards 'Join the Fight' conference, it was evident that fraud can no longer be treated as just a financial threat but should also be seen as a public health and safeguarding risk.

7.16 Work continues with social media campaigns driven by the national lead for Fraud and Cyber Protect and the information resource, Cyber Aware.

<u>Legislation</u>

7.17 There are potential changes in current legislation in the offing (at various stages of consideration in Parliament) that assist with the investigation of crime with a digital element including the Online Safety Bill, Policing and Crime Bill and the Investigatory Powers Bill.