Item 6b

Cyber Assurance Report

May 2021

D/Supt Deryck Rees

Dr Kirstie Cogram

Contents

Introduction

This assurance reports reflects the subject and scope agreed between the OPCC and Constabulary in March 2022.

It is recognised across policing and government that cybercrime is a significant threat to the UK and policing is struggling to keep pace with the resulting increasing demand and complexity of cybercrime.

At a strategic level, cybercrime is recognised by the NPCC and Association of Police & Crime Commissioners as a specialist capability. In October 2017 Chief Constables' Council agreed that every force should have their own dedicated cybercrime unit tackling cyber dependent crime. National funding was identified to help achieve this.

Avon and Somerset is in a good place. We have used the funding to build and invest in our Cyber-dependent crime capability through high quality training and application of those skills in an area of policing which is not well known, but it is vital for public and business confidence. We have our own team delivering against the National Cyber Security Strategy and Serious Organised Crime Strategy. They also assist the force to meet the responsibilities under the Strategic Policing Requirement to be able to respond to major cyber incidents and undertake complex digital investigations.

Cyber Crime is wider than one team and this assurance report looks at the wider landscape.

It sets out some ideas how as a force we are / will contribute to the "Tackle Cyber Crime" national outcome and local priority setting.

Within this report we have added some extra commentary on some capabilities and we have in an appendix, summarised the training offer in this area and some case studies which will provide added insight and are designed to contextualise some of the demand and issues in this report.

It is hoped this document can be used as a reference document beyond the governance meeting hence it is split into parts and lengthier than a normal assurance report.

Definition of Cyber Crime

How Cyber Crime is defined is vital. It is the starting point of how we start to discuss and assure. Cybercrime is an umbrella term used to describe two closely linked but distinct ranges of criminal activity:

Cyber-dependent crimes (CDC) - crimes that can be committed only through the use of Information and Communications Technology ('ICT') devices, where the devices are both the tool for committing the crime and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity).
Cyber-dependent crimes fall broadly into two main categories:

- Illicit intrusions into computer networks, such as hacking; and
- The disruption or downgrading of computer functionality and network space, such as malware and Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks. This includes Viruses, worms, Trojans, Spyware and ransomware.

Cyber-enabled crimes (CEC) – are traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft). Cyber enabled crimes cover the following categories:

- Economic related cybercrime, including fraud and intellectual property crime (piracy, counterfeiting and forgery)
- Online marketplaces for illegal items
- Malicious and offensive communications, including communications sent via social media, Cyber bullying/trolling, Virtual mobbing
- Offences that specifically target individuals, such as: Disclosing private sexual images without consent, Cyber stalking and harassment, Coercion and control, Sextortion
- Child sexual offences and indecent images of children, including Child sexual abuse, Online grooming, Prohibited and indecent images of children
- Extreme pornography obscene publications and prohibited images

Whilst cyber enabled crime is the greater volume of crime, cyber dependent crime often requires greater technical skill and tools, as well as have more damaging impact such as that experienced during the WannaCry attack that affected the NHS phone system (see case study). Consequently, it requires more specialist skills and capabilities to investigate it.

Digital Footprint: There is also a third category of investigation to consider and that is digital footprint where a crime that is not a cybercrime has a digital element. For example, Murder, drug supply, RASSO, OCGs. Most, if not all investigations have a digital element that will often require specialist knowledge to progress the evidential capture and investigation.

Demand

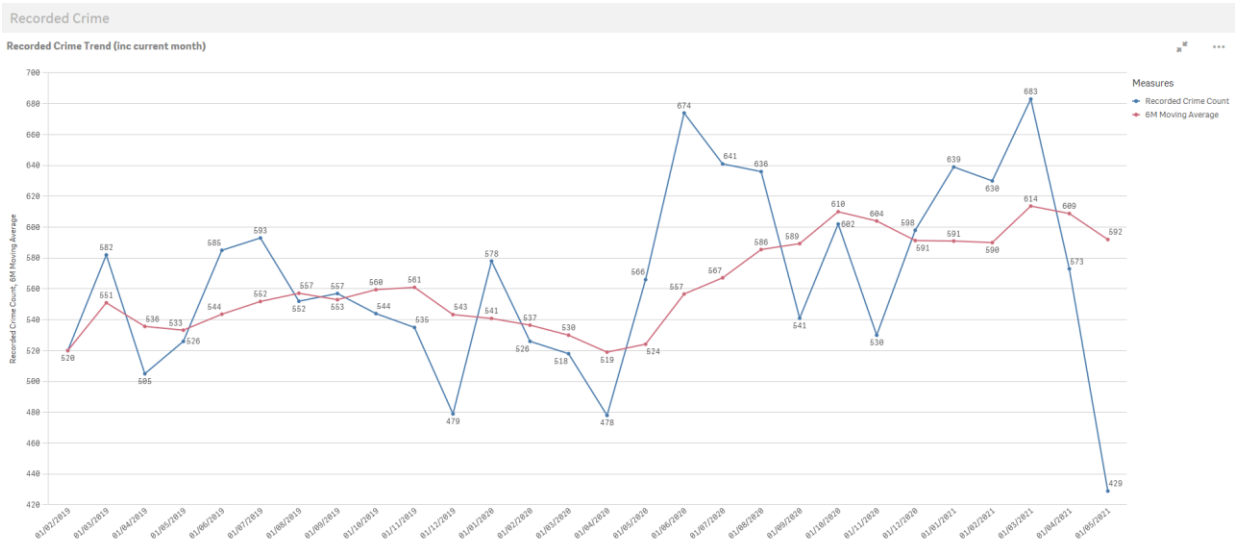
Measuring "Cybercrime" in totality is challenging for all forces. There is no one single measure which provides clear insight across this thematic. Some time ago, as a force, we moved to measuring "Cyber Crime" by way of tagging a Storm Call Card (Call for Service) at first point of contact and this automatically populates within the Niche Crime Report. This measure is showing over a 120% increase on previous expected seasonal levels and this rise has been sustained over the last few years.

On average 34 crimes are tagged in this way every day. Looking at the previous 7 days crimes which are being actively investigated (from the 20th May 2021), over 70% of these crimes are Malicious Communications and Harassment. Specific call scripting in the communication centre for those call types and blackmail offences mean that this is driving the recording. All of these crimes are investigated in the main, by teams in the Response Directorate, either through attendance or at desktop in the Incident Assessment Unit.

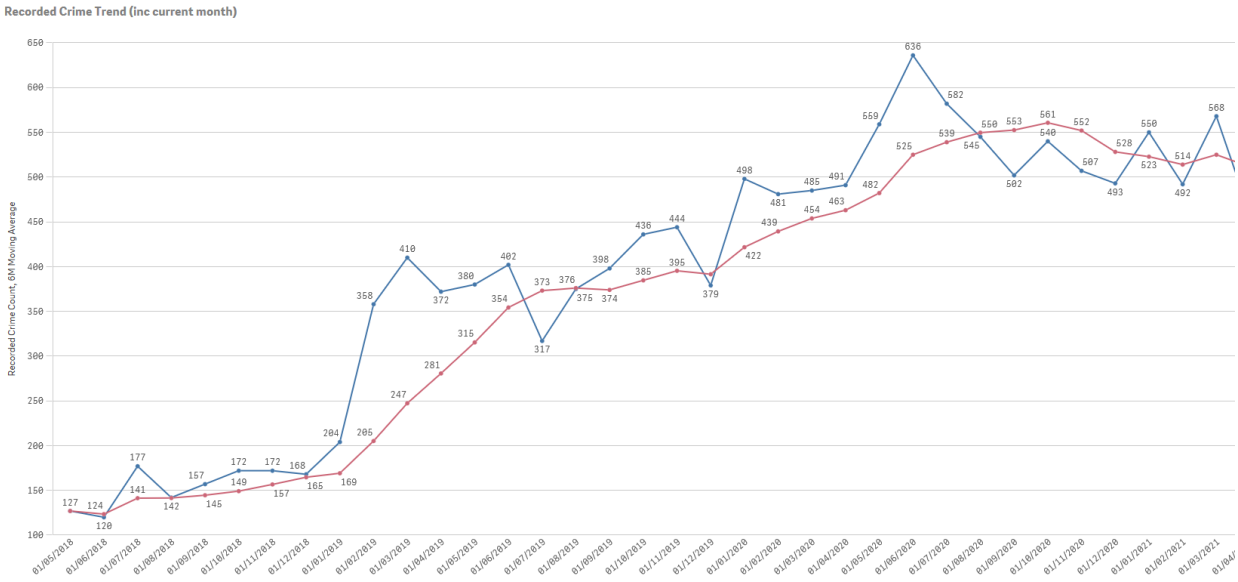
This illustrates the day to day, business as normal but growing demand on front line staff of Cyber-enabled crimes. In most cases, this involves social media platforms and threats e.g. Instagram and Facebook. These range in severity and some are domestic abuse. This measure is useful for showing the demand on front line staff but is only part of the picture. It does not show complexity or the demand from crimes that have a digital footprint.

In respect of crimes with a digital footprint, it has been shown from research and assurance that RASSO cases in almost every case have a “cyber” element in relation to digital devices and digital media. Of 631 Rapes under investigation, 4 have been tagged as “cyber” which reinforces that the current force measure should be seen as only part of the demand and part of the narrative.
The below graph illustrates this point - the corresponding and interconnected growth in recording of Malicious Communications and the rise in this measure of Cyber-enabled crime.

Malicious Communication Crime Volumes



Total Recorded Crime with Cyber Tag added



An indication of demand growing in "Digital Footprint" investigation is that the Digital Forensic Unit has seen the highest number of submissions for mobile phones in March and April 2022 since before May 2019 - 117 and 97 mobile phones respectively. The pandemic is part of this picture, but it is a key piece of insight. The current average examination of a mobile phone by South West Forensics for Avon and Somerset takes 9 weeks to be completed.

Demand - Cyber-dependent crime (CDC)

Demand from Cyber-Dependent Crime is measured nationally. It is one of the recommendations of this report that we seek better ways to track and measure this internally.

The national picture has seen a 15.2% increase in cyber dependent crime with estimates of losses calculated nationally as having increased from £5.4m to £9.6m in the past year. Nationally, there is still significant under reporting – The Crime Survey of England and Wales found that only 4% of victims of computer misuse crime reported the offence to the Police or Action Fraud. The main reasons cited for this are: Too trivial, private matter or not worth reporting. Organisations are underrepresented with only 9.6% of reports coming from organisations. 45% Cybercrime reports nationally are reports of the hacking of social media and e-mail.

Double extortion ransomware attacks continued to rise (where data is stolen as well as files encrypted which results in a ransom to decrypt the files and a ransom not to release the data) and Cyber enabled fraud accounted for 80% of all fraud (slight decrease of 4 – 5 % on last year).

The local picture of demand is mostly informed by the **NFIB Cyber Crime National Dashboard**. The latest data shows ASC had 854 reports in the last 12 months. These were broken down -

- 415 – Hacking of Social Media and Email
- 228 – Computer Virus / Malware / Spyware
- 112 – Hacking personal
- 82 – Hacking Extortion
- 9 – Hacking Sever

Force data and national data do not currently align. The regional cyber coordinator in the ROCU (Regional Organised Crime unit) is working to clarify some of these issues with the City of London Police and NFIB. Our data shows that during the same period, the Cyber Team received **332** reports of CDC from Action Fraud. This was an increase of **48.2%** over the period April 2019 to March 2020 (**224**) but is clearly less than 854 reports recorded nationally. Not all reports are disseminated to forces and work is ongoing to understand this more. If all were disseminated the impact on the team would be significant.

The national process is that the NFIB "weekly list" is shared with Cyber Teams nationally for all CDC, this is reviewed and investigated as appropriate. The Cyber Team currently have 60 incidents under active investigation.

Future Demand – It is predicted and reported nationally that demand will continue to grow in this area of policing. In relation to CDC, complexity and sophistication will continue to increase.

There is no doubt that in meeting challenges and our aspirations in crime investigation e.g. RASSO, the focus and need for the highest quality digital strategies to inform crime investigations and obtain the very best outcomes is a demand which will grow across the investigative landscape.

Capacity and Capability

Force Cyber Crime Team

Avon and Somerset Cyber Team is responsible for investigating all Cyber-dependent crime. Local delivery is provided across PURSUE, PROTECT, PREPARE and PREVENT (4 P's).

The team responds to the national need to "focus is on an improved victim experience, an effective investigative response, targeted local cybercrime prevention messaging and work to identify and divert young people vulnerable to going down a path to cybercrime. Forces will also work with businesses and organisations to help them develop effective incident response plans and test them. The Force Cyber Crime Units will also be centres of excellence and guidance to the wider force helping mainstream cyber skills and knowledge into other areas of policing." - This is the mission of the Cyber Team.

In February 2021, the NPCC (National Police Chiefs Council) published a paper entitled "Force Cyber Crime Units NPCC Minimum Capability Standard."

This is a key document which outlines and defines the roles, training, and national performance reporting requirements for force cyber teams.

The role of the Cyber Team is to:

- Investigate 100% of **all** cyber dependant crime (CDC) disseminated the forces
- Provide 100% of **all** CDC victims with specialist advice
- Provide support to cyber enabled crime (CEC) investigations held by others

Funding: In order to support forces to develop and maintain the required capability at the local level, The Cabinet Office's National Cyber Security Programme fund allocated resources to support the initial build during 2018 and 2019. Force cybercrime units were eligible to bid for grants to assist them in the development and maintenance of capabilities in terms of developing the infrastructure including accommodation, vehicles, hardware, software, licencing and training. Some staff costs were supported, but any staff paid for through the grants had to be match funded by the force.

This funding was due to cease on 31.03.2021 and to ensure that we continued to have this capability and to ensure it is on a sustainable financial footing, the force has funded the posts permanently through the Uplift programme.

The team investigates, educates and informs, mentors, works with Specials and Volunteers, and carries out specialised functions such as [redacted]. They conduct evidential scene visits for murder and high harm incidents and are tactical advisors for Crypto Currency investigations including seizure and storage.

Cyber Protect

The Cyber Team has two Cyber Protect (CP) Officers whose role it is to:

- Deliver cybercrime prevention advice to businesses and the public. The CP officers have the specialist knowledge and credibility to advise businesses and individuals how to protect themselves and respond to incidents to recover to business as usual as quickly as possible
- Help organisations build resilience to respond to cyber incidents.
- Force Single Point of Contact to develop staff understanding and capability.
- Undertake local campaigns in response to local threats

The opportunity here is to really support business's be resilient to attack in the context of a Covid bounce back as the country economically recovers.

We need to amplify further our messaging through both the constabulary, but also through the OPCC and showcase how this protect strand, by effectively targeting vulnerable victims, supports them from being victims again.

Digital Media Advisors (DMAs)

Capability has been enhanced by the recruitment of Police Staff funded by the Precept. In the financial year 2020/21, the Cyber Team has recruited and mentored nine DMAs. The role, provided as part of the PCC's precept funding was to:

- enhance the skills and abilities within the core Investigation teams in the context of complex crimes with a digital foot print and Cyber-Enabled Crime within the CID.
- bring about more timely investigations where digital evidence was key with high quality investigative strategies and adding practical value to other investigators with their enhanced knowledge.

These staff will be part of the main 4 CID teams with two based on each team, north and south of the force. Recruitment was completed by March 2021 and the staff are at different stages of development. 5 are embedded with their teams after mentoring and in force training, 3 are being mentored and 1 is in force training. All will be a minimum of PIP1 Investigators – 4 already are.

Initial feedback is very positive, but the capability needs to embed and mature.

On sergeant said in a feedback survey -

"They work in line with our shifts which is invaluable, they have a real passion for the job. They are available for regular chats for knowledge sharing in the office which benefits the team for cybercrime knowledge & in turn DMA gains knowledge from other non-cybercrime investigative opportunities."

This investment is subject to ongoing force benefits tracking and future assurance.

Cyber Specials Cyber Volunteers (CSCV)

In September 2019, the Cyber Team identified the need to enhance capabilities, and sought to do so by identifying and working with volunteers from within our communities with specialist skills gained from outside policing. This resulted in the creation of the **Cyber Specials Cyber Volunteers (CSCV) programme.** The recruitment of specials and volunteers with specialist cyber skills aligns cyber capacity

and capability with operational benefits and helps to build cyber skills by accessing specialist expertise not readily available to policing.

The CSCV program covers two specific areas:

- **Cyber Specials** – volunteers already giving up their time to policing as Special Constables, who take on additional work by supporting the Cyber Team with their technical expertise ('Specialist Specials'). This support can either be in a technical supporting role or assisting at scenes and warrants utilising their powers as a constable.

- **Cyber Volunteers** – Members of the public who apply directly following recruitment drives that are seeking specialists from within the digital and cyber world. These skilled people will help us keep up more with industry through their specialist skills

The background and skills possessed by the cadre of volunteer specialists is of direct benefit to the Cyber Team work, such as network analysts, systems developers, programmers and software engineers.

The NPCC Force Cyber Crime Units, Minimum Capability Standards state that to meet the minimum standard, each force is expected to recruit and utilise Cyber and Digital Specials and Volunteers to support the work across all 4P's and to promote the integration of CSCV into mainstream policing.

Avon & Somerset have an agreed volunteer role profile and have recruited 5 x Cyber specials from our existing Special Constabulary and have also recruited three Volunteers who commenced in post just this month. Processes are currently being implemented to ensure that cyber skills are captured when new Special Constables join the Constabulary.

In the future, the national cyber project team aims to deliver a National CSCV database which will allow the coordination and tasking of skilled cyber experts to provide support to local operational demands and enhance the national cyber response.

The ROCU

The relationship between the ROCU and ASC is a strong and positive one in relation to Cyber dependent Crime. The ROCU at a regional level has a small but higher level of technical capability than forces. [redacted]. Forces meet regularly with all stakeholders across the region in this field and there is a Strategic Steering group for the region chaired by a chief officer.

Performance

This section focuses on the performance of the Cyber Team. In order to qualify for national funding since 2018 the team has to meet the two 100% targets of –

- Investigate 100% of **all** cyber dependant crime (CDC) disseminated the forces
- Provide 100% of **all** CDC victims with specialist advice

Quarterly reporting is undertaken at the regional level (5 Forces) which feeds the national picture. Avon and Somerset have consistently met these requirements.

Bringing offenders to justice in the traditional sense is challenging regarding CDC. To put this into sharp focus, not one suspect across all 5 regional forces was charged with a Cyber-Dependent crime in Quarter

3 of 2021. The main reason for this is that most often the offenders are based and operate from an overseas jurisdiction. ASC was the only force to have one suspect convicted of a CDC in this quarter. There is very little difference in reporting of outcomes across all SW forces. This data is shared with forces.

In Quarter 3 ASC received 76 cases, all victims are contacted and offered advice and support as well as the investigation reviewed for investigative opportunities. One of the national KPI's is to stop victims becoming repeat victims – the Protect Strand. The Cyber Protect role is essential to this. In respect of this the following KPIs are reported on to the Home Office.

KPI 2: 100% of victims who report to Action Fraud will receive advice to prevent them becoming repeat victims (PROTECT). This target is achieved each quarter.

KPI 7: Victims who receive PROTECT advice intend to change their behaviour as a result

KPI 8: Increased number of activities / engagements / campaigns to be run in partnership

KPI 9: Increased number of volunteers supporting the Cyber PROTECT network

KPI 10: Increased number partnerships aimed at increasing our cyber capabilities

KPI 11: All materials delivered by law enforcement to follow national government-approved advice

Within this strand, the team in Quarter 3 reported reaching 361 individuals including targeted audiences through e.g. schools or working with the CSE prevention officer within Topaz – the force's disruption team for CCE (Children Criminal Exploitation) and CSE (Children Sexual Exploitation.)

The team provide support and guidance to the wider organisation in relation to Cyber-enabled crime and this is hard to fully quantify but is wide ranging and vast – see case studies.

To aid further improvement, a greater understanding of outcomes for all investigations is planned through Qlik visualisation which is in the production pipeline (along with Fraud outcomes). A further piece of assurance in relation to CDC crime disseminated to the force is underway supported by a Business Analyst and is looking at demand flow and timeliness which will inform a planned dip sample of investigative standards.

An addition to NICHE which reflects the College of Policing DMI Strategy template is due by end of June 2021. This has been designed to add value and quality to investigations by formalising the Cyber Teams' contribution to live investigations and it will also be a performance and qualitative measure to assure against in the future. An additional benefit of using a template such as this is that the template can be incorporated in the Investigation Management Document (IMD) that is now a required part of any case file submission.

The lead has been asked to look at further improvements in the relationship between the Cyber Protect role, Neighbourhood Teams and wider crime reduction and problem solving assets for the highest risk and most vulnerable victims to improve our service further.

A regional and local gap is analytical work to show trends and repeat victims which can be responded to more effectively in an evidence based way.

It has been recognised that even stronger links / understanding with corporate communications is needed and these meetings are planned to ensure national and local Cyber campaigns are maximised.

Recommendations / Risks / Opportunities

Recommendations

Until now, ASC have reported extensive outcomes outwardly and nationally and a new local performance framework / dashboard is to be designed over the next 6 months which will focus on Investigations, prevention, education, disruptions and reducing repeat victimisation. Visualized through Qlik, this will inform national reporting, local priorities and impact. The support of Performance and Insight is required and will incorporate the existing benefits tracking (The same request is relevant to Fraud.)

A task and finish group will be established to review the way the force measures "Cyber Crime" to ensure that we continue to maximise our insight in this area in context of demand. With a focus on Cyber dependent crime volume and trends, we can ensure we are matching demand to capability going forward.

The national direction is clearly in the future to quality assure CDC Investigations in the context of minimum standards. ASC plan to be ahead of this and suggest that this is added to assurance cycle in the next 18 months.

It is planned to assure the Digital Media Advisor role in relation to added value and contribution. It is suggested that this is fully reviewed when all of the DMA's are at full capability.

The Regional Cyber Group has sought clarification from South West Forensics in relation to the SLA regarding digital scene visits based on a number of occasions where scene visits were not able to be supported by the SW Forensics DFU. Clarity is needed on this capability for the region as this impacts on and stretches force Cyber Team capacity. ASC should have clarity on this capability and it be fully publicised across investigative teams.

Assurance should take place with front line officers in context of the growing demands of cyber enabled "volume" crime. This should be to confirm that they have the skills and knowledge to investigate and handle digital devices and evidence at pace but also to ensure training is continuously informed through such ongoing engagement.

Risks

[redacted]

Opportunities

This piece of assurance has highlighted the breadth of the Cyber Team footprint across training and CPD. The recruitment and delivery of the Digital Media Advisors and mentoring by the team has been excellent. The team have recruited volunteers and Special Constables and now need to work with them in relation to workload, contribution and development.

The funding of a post to coordinate Cyber Specials and Volunteers ends in September - and is vacant due to the post holder taking a new opportunity and in the context of temporary funding was not filled. Are their opportunities to mainstream this and enhance this role as below?

The Cyber Team training and CPD footprint is now arguably getting too extensive. The Uplift, in particular but not exclusively our ambitions around RASSO and the need for quality digital strategies and investigations is an opportunity to reflect on how we will deliver upskilling and training in this area. A realignment of the team is perhaps needed and wider discussion is recommended.

One proposal for example is to look at the requirements of coordination of not just specials and volunteers but a wider coordination role of mentoring and upskilling of DMA's as these skills are perhaps grown in context of Uplift. This reports seeks permission to continue engagement with stakeholders in this conversation and to come back with inclusive proposals working with other streams.

Ethnicity and gender data within nationally reported CDC crime is very limited, a review of local records show this is not recorded nationally in around 50% of cases. This will be discussed regionally in order to influence the national team. Further analytical work is required to understand victim and offender profiles in rich detail. A Problem Profile of Cyber Crime would be welcomed.

The Cyber Team – In Detail Staffing

The Cyber Team forms part of the Complex Crime Unit in the Investigations Directorate (CID).

Staffing

1 x Complex Crime Unit Manager (DCI equivalent) who also has responsibility for Fraud and Financial Investigation, including Asset Recovery.

1 x Detective Inspector – also has responsibility for Fraud and Financial Investigation including Asset Recovery

2 x Detective Sergeants

3 x Detective Constables

5 x Digital Media Investigators (Police Staff, 4.65 FTE)

2 x Cyber protect Officers (Police Staff)

0.5 Scale 4 Investigative Support (Police Staff)

3 x Cyber Crime Support volunteers

Digital/Cyber training for ASC (mainstream)

PIP 1 – 5 week course for Police Staff Investigators in MCIT, DIT, Remedy, ICAT and investigations.

- ¾ of a day Cyber landscape training covering [redacted]. They also receive information around how the internet works, IP + MAC addresses and the relevance to investigations. Approximately 9 x PIP 1 courses ran in the last year, 8/9 officers per course approx. - 73 officers in total.

Desk Top investigators

- ¾ of a day training covering the same topics as the above PIP 1 course. 8 officers per course, approx 7 courses in the last year - 56 officers

Intelligence /Open Source training – 2 days for intel staff [redacted].

- [redacted] COVID has meant that this has not been delivered over the last year until April 2021 when a course was held for 9 attendees.

PIP2 – formally the ICIDP (CID Course) - 4 week course with an additional 2 weeks interview course and 4 day Cyber course. As part of the PIP 2 portfolio, officers must attend the 4 day digital course – Evidencing Digital Investigations

[redacted]

4 courses have been held in the last year (32 students) and due to Covid restrictions there are now approximately 100 officers waiting for training. The college of Police publish stated objectives for the PIP1 and PIP 2 training and in force, ASD add practical elements to our courses to assist our officers going forward. Records are not held that demonstrate the number of staff that are trained to this level, however the course has been running for 8-9 years. There are 700 staff trained to use the OSB (Open Source Browser) and therefore a minimum of 700 staff are currently trained to the level of this training.

PCDA officers complete the COP curriculum which includes digital policing and basic i3 awareness and additionally the Cyber Team provide a 4 hour input in year 2 for which the learning objectives are;

- Understand how criminals engage in cyber dependent crime (CDC)
- Impact of cyber dependent crime on individuals and businesses
- Digital investigative opportunities available for CDC and cyber enabled crime (CEC)
- Identify specialists within the police who can assist in the recovery of digital data
- How to obtain information from a service provider

NCALT The COP have recently produced an NCALT package called Op Modify (consists of 11 modules) to address gaps in knowledge / awareness and training. Consideration will be given to mandating this training for all operational staff.

CYBER TOOLS APP A Cyber Tools App (National Policing App) is in the process of being rolled out to all staff work devices so that staff have practical digital and cybercrime advice readily available. This will improve general knowledge across the force.

Training and CPD Commitments of Cyber Team

Recognising their enhanced capabilities, the Cyber Team regularly provide training and continual professional development (CPD) to internal stakeholders.

The training provided covers material specific to the group receiving the training but will include an overview of the Cyber Team and digital investigative opportunities for all such as Internet of Things (IoT), Wi-Fi surveys, Radio Frequency Propagation Survey (RFPS), telematics, router examinations and social media to name but a few.

The following have received inputs over the last twelve months:

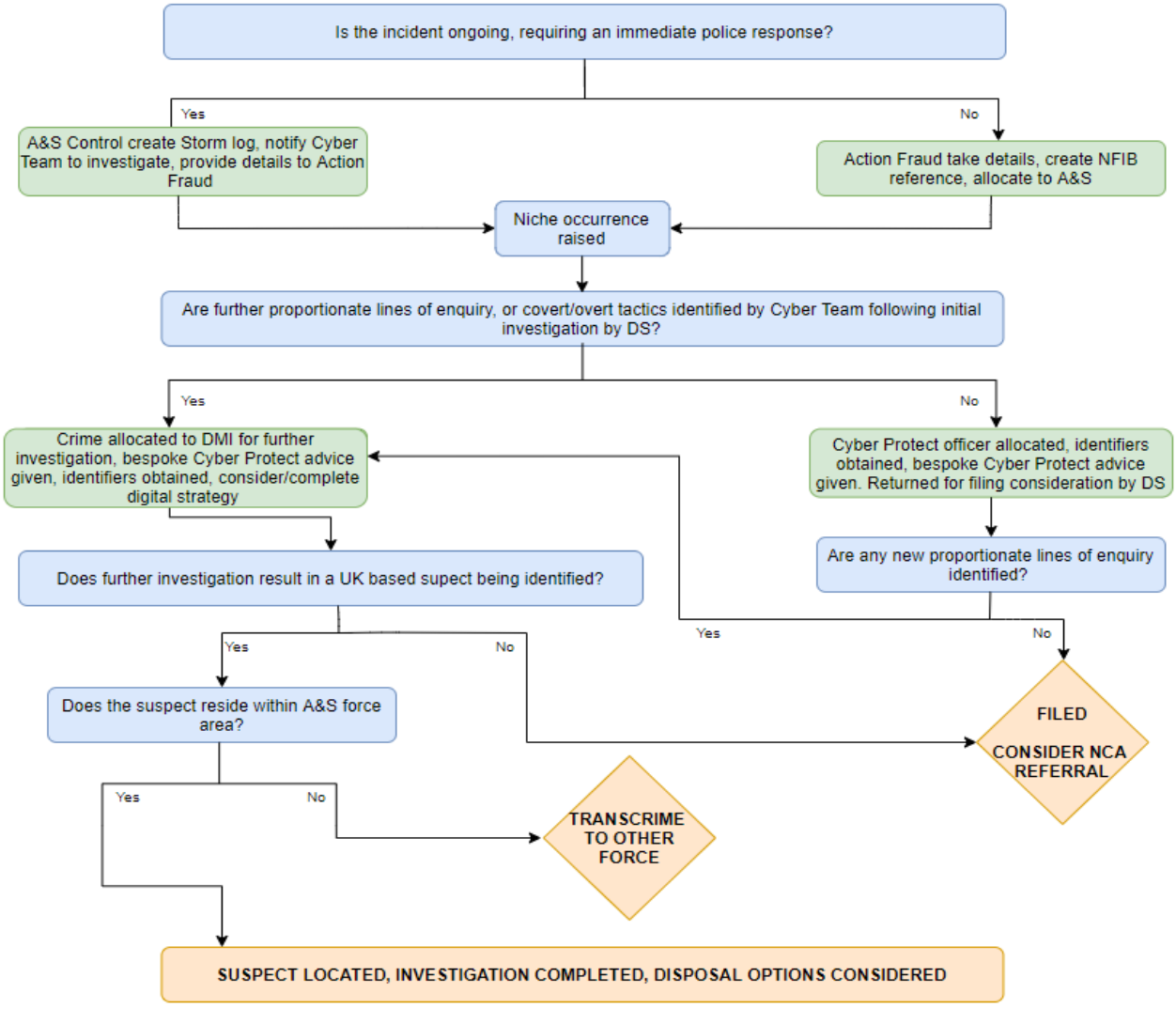
- PCDA (year two) – 360 students each year, for the next three years
- Evidencing Digital Investigations (previously MCCT)
- Child Death
- Designated Investigator (PIP1)
- PIP 2
- PC>DC
- ISM (previously DI and DS course)
- Intel Investigators
- SSAIDP
- Scene Liaison Officers
- Patrol/DIT CPD
- OST CPD
- Investigations CPD
- Offender Managers CPD
- Op Topaz CPD
- Op Ruby CPD

The Cyber Team will continue to provide inputs to other departments, with Remedy, IAU and Bluestone due to receive inputs in the coming months.

In addition to our internal stakeholder engagement, our DMI's and Cyber Protect officers also provide training and advice to external stakeholders. These have included the following:

- Bristol Social Services
- Schools
- BBC Radio Bristol
- UWEcyber School
- Financial Institutions
- Voluntary sector fostering and adoption agencies
- South Gloucestershire Social Services
- Colleges
- BBC Radio Somerset
- Chamber of Commerce
- Small and Medium sized Enterprises (SME's)

Cyber-dependent Crime – from Report to Disposal – Force Process



Spot Light - Cyber Team Case Studies

[redacted]

Campaigns

A local spike in reported crime linked to online child safety was identified (IIOC / Grooming / Sexting / Sextortion). The CP officers worked with other force departments to target parents to address a clear lack of awareness and understanding of technology and the risks this poses for their children daily. The CP officers hosted a series of webinars that were oversubscribed every time.

Following these webinars, the content was recorded into four videos which were uploaded to the ASC Cyber Protect YouTube Chanel to provide free easy access to parents that will keep them and their children safe online. These inputs were also recorded with sign language utilising one of our own PCSO's translation skills. This is an area that will continue to be expanded due to its scalability.

Prevent

Where appropriate individuals are referred to the ROCU Cyber PREVENT team for intervention if they are deemed to be at risk of committing cybercrime or have started to do so.

There are also develop developing regional Cyber Prevent Intervention panels that bring together the police alongside the private and voluntary sector delivering meaningful diversionary activities for vulnerable young people.

Disruption

'Niche 'Outcome 22' states; 'Diversionary, Educational, or interventional activity, not in the public interest to proceed'. 'Disruption' reporting is used nationally as the baseline method of calculating the impact of Forces in combatting serious and organised crime (SOC). *A disruption may be achieved by any activity covered by Pursue, Prevent, Protect or Prepare and will have involved some form of intervention which has resulted in a positive output or outcome against a threat*

The Cyber Team created a process to capture this data in Q4 2020/21 and will therefore use these to contribute to the overall HO returns from ASC. Disruption examples to date include: serving Cease & Desist notices for NCA Op Beguileful targets; providing specific tailored Cyber Protect advice (in conjunction with material from the NCSC) to SME's in relation to nationally recognised ransomware

strains and identifying and referring two young individuals subjects to the RCCU for Prevent intervention programmes .

Spot Light - Cryptocurrency Investigations

Cryptocurrencies are a form of digital or virtual currency that have become increasingly popular since Bitcoin, the first cryptocurrency launched in 2009. The system was set up to be a cross border payment that was peer to peer with no third party involvement or centralised legal oversight (such as a bank). In general, the identities of account holders are said to be 'pseudo-anonymous'. Whilst Bitcoin is the most widely known cryptocurrency, there are estimated to be in excess of 2500 actively traded different coins.

Fifteen members of the Cyber Team, Financial Investigation Unit and Fraud Team have undertaken cryptocurrency training from the NCA accredited provider CSI Tech. The trainees included SIOs and investigators who are now able to undertake the role of cryptocurrency tactical advisor to assist the force in dealing with the wide range of investigations that now encounter cryptocurrency. The split across the teams ensures that we are able to competently investigate cryptocurrency as well as be able to seize, store and confiscate those assets where appropriate. Seizure is particularly complex as the asset doesn't 'physically' exist.

[redacted]

The Cyber Team have investigated and assisted with numerous cryptocurrency investigations and seizures (this is an increasing area of work), including the following:

[redacted]