Matthew Barber
Police & Crime Commissioner
for Thames Valley

Report to the Police and Crime Panel

Report title: Cyber and Digital Investigation & Intelligence

Date: 24th March 2023

Author and contact: D.Supt Andy Richardson (SEROCU) and Detective Inspector Sally Russell (TVP)

Purpose of the report: At the request of the PCP

Recommendations: For noting only

Executive Summary

A service plan has been created to define and focus the priorities and strategies for Thames Valley Police and the Regional Cyber Crime Units (CCU). This plan seeks to align service delivery based on the key strands of the Government's National Cyber Strategy 2022 and the force priorities for Thames Valley Police as detailed within the Thames Valley Police Strategic Plan 2019/2020.

The Police and Crime Commissioner (PCC), Matthew Barber in his Thames Valley Police & Criminal Justice Plan 2021-2025 underpin this force plan.

The Government's National Cyber Strategy has 5 Pillars;

- Pillar 1: Strengthening the UK cyber ecosystem, investing in our people and skills and deepening the partnership between government, academia and industry
- Pillar 2: Building a resilient and prosperous digital UK, reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are more secure online and confident that their data is protected
- Pillar 3: Taking the lead in the technologies vital to cyber power, building our industrial capability and developing frameworks to secure future technologies
- Pillar 4: Advancing UK global leadership and influence for a more secure, prosperous and open international order, working with government and industry partners and sharing the expertise that underpins UK cyber power
- Pillar 5: Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace, making more integrated, creative and routine use of the UK's full spectrum of levers Bringing this to a more local level this strategy reinforces the 4P framework of Pursue, Prevent, Protect and Prepare

Thames Valley Police and Hampshire Constabulary also have a joint digital strategy covering the wider forces digital portfolio. Alongside this strategy is a Joint Digital Investigation and Intelligence (DII) Governance Structure where the Joint Governance Board makes strategic decisions about developing DII capabilities and acts as a senior reference group to champion DII capability and capacity building, linking to the Digital Board, Joint DCC's Governance Board and JCOG where necessary.

The Board identifies any issues in delivering DII capabilities across the forces and takes responsibility for developing tactical plans and delivering operational outcomes and improvements for the benefit of frontline policing which are delivered through the respective in force DII coordination boards.

Matthew Barber
Police & Crime Commissioner
for Thames Valley

Report to the Police and Crime Panel

Detailed overview

The Thames Valley Police CCU is aligned and line managed by the South East Regional Organised Crime Unit (SEROCU) with a local focus but is also positioned within the National Cyber network. The UK Cyber network aims to deliver the cyber strategy within the four key objectives:

- Pursue: Prosecuting and disrupting people engaged in serious and organised criminality,
- Prevent: Preventing people from engaging in serious and organised crime,
- Protect: Increasing protection against serious and organised crime, and
- Prepare: Reducing the impact of this criminality where it takes place.

The Regional & Thames Valley Police Cyber Pursue team is made up of a team of Detectives working from SEROCUs Western Hub operating as part of a collaborated capability under the Regional Organised Crime Unit.

There is also a collaborated TVP and SEROCU Cyber Protect and Prevent team that works remotely across the South East as well as a Regional Dark Web Unit and works closely with the Regional Digital Forensic Unit.

The DCI, DI and DSs are required to participate in the National Cyber on-call function for Team Cyber UK. This requirement is a week covering the hours of 1600- 0700 covering the entire UK working closely with the NCA Duty Officer network and this requirement is performed four times year.

A Cyber Regional Coordinator at DS level ensures a close working relationship with Hampshire and Surrey/Sussex CCU's. This brings consistency and mutual support running from the National, Regional to Force.

As part of the Service Level Agreement (SLA) between SEROCU and Thames Valley Police, the TVP CCU provide the TVP Major Crime Unit with Detectives to assist with homicide investigations.

The majority of the Thames Valley Police CCU time and resource is committed to supporting the investigation and disruption of serious crime. They take ownership and investigate offences under the Computer Misuse Act and other cyber dependant crimes (crimes where devices / computers are both the tools to commit the crime and the target of the crime).

In order to obtain national funding, the CCU must review and form an investigation strategy for all cyber dependant crimes referred to the force by the National Fraud Intelligence Bureau (NFIB) which are crimes reported to Action Fraud.

These referrals include offences such as Hacking/Network intrusion, Denial of Service attacks, Data breach, Malware attack and typically the following factors are present;

- Small to medium business enterprise, public authority, government agency/department,
- Sophisticated methodology requiring detailed knowledge of malware, IT infrastructure, IT networks, IT Security, Hacking or Denial of Service methods,
- High value loss of data or impact due to loss of service,

- High risk of significant reputational impact to the victim or to Thames Valley Police.

Other cyber enabled crime (traditional crimes that have a high degree of digital involvement) such as mandate fraud, fraud, blackmail, and sextortion are generally investigated by area teams or by the Economic Crime Units with support provided by the CCU or the TVP DII Team.

The TVP CCU will however lead serious cases of cyber enabled crime which involve cryptocurrencies owing to the complexity of these investigations and a strategy has been developed to increase the necessary skills within the TVP Economic Crime Units to assist in some of this work.

The Regional CCU pursue team has a similar commitment to supporting the investigation and disruption of serious crime. They take ownership and investigate offences under the Computer Misuse Act and other cyber dependant crimes.

The Regional CCU pursue team is tasked by the National Cybercrime unit (NCCU) and form part of the wider NCCU and Regional Cybercrime network. The tasking process involves the NFIB and the National Cyber Security Centre and is directed by a monthly National Cyber Prioritisation and Tasking Meeting (NCPT) which is jointly chaired by the Deputy Director of the NCCU and the D/C/Supt Cyber NPCC lead. This process uses data collated from APMIS and the SOC Master List to assess the threat/harm and risk and allocate resources and investigations accordingly.

The Regional Dark Web team is tasked in a similar format and form part of a regional network under the title of Dark Web, Intelligence Collection & Exploitation (DICE).

A very recent success, which also shows how long some cyber investigations can take, is the conviction of a Dutch national of stealing more than £2 million of cryptocurrency which resulted in people losing their businesses and their inheritances.

Following a five-year investigation by the SEROCU CCU the man pleaded guilty to theft at Oxford Crown Court. The case centered around the IOTA cryptocurrency, which required users to have an 81 character ‘seed’ made up of capital letters and the number 9, to control their ‘tokens’.

In January 2018 there were numerous reports of the transfer of Iota tokens which had been taken out of the control of Iota owners around the world, without their knowledge and consent.

What the victims of these thefts had in common was that they all used the same website – iotaseed.io – to generate what they believed to be a random string of 81 characters. However these were predetermined, allowing the thefts to take place. The tokens were then transferred to a number of different cryptocurrency trading accounts and the amount stolen was valued at £2,156,000 from more than 100 victims.

SEROCU officers arrested the suspect in Oxford in January 2019 and then charged him after extraditing him from the Netherlands in April 2021 where he returned there when released on bail.

Report to the Police and Crime Panel

The Judge recognised the complexity of the investigation and gave commendations to a number of officers and staff who work on it and the next stage is returning the stolen money back to the victims as it was traced and seized.

The Regional Prevent team work in collaboration with the South East Regional Forces to support and enhance the capabilities for an effective regional response to the National Prevent strategy led by the National Cybercrime unit (NCCU).

All public messaging around Cyber Prevent is now branded as 'Cyber Choices' to highlight the positive intentions and separate the programme from other cyber prevent programmes. They aim to deter individuals from getting involved in cybercrime in the first place, moving deeper into cybercrime and/or from reoffending by targeting UK-based individuals with interventions proportionate to the risk they pose. The risk relates to both the risk of reoffending and the risk of causing serious harm.

They work with all the South East Force CCU's in delivering regional Cyber Prevent activity (with ROCUs taking the lead and NCA coordinating and/or supporting) which includes:

- Outreach to strategic partners including education, probation and youth-offending services to ensure they have knowledge of the Cyber Prevent (aka 'Cyber Choices') and are able to identify subjects as early as possible,
- Tactical intervention activity with identified Cyber Prevent subjects based on assessed risk,
- Delivering the Cease and Desist tactic with authority from NCCU
- Post-conviction offender intervention and diversion in support of statutory risk owners (IOM, MARSOC, National Probation Service, Youth Offending Services),
- Subject debriefs, intelligence development and identification of potential covert human intelligence sources for cyber

The Regional team deliver this on behalf of the South East Forces in support of the national performance requirement of 100% of identified Cyber Prevent candidates (by the Force CCUs) will receive intervention activity proportionate to the presented risk.

The Regional and TVP Cyber Protect team work in collaboration with the South East Force CCU's to support and enhance the capabilities to ensure an effective response and to support the delivery of the National Cyber Protect strategy led by the City of London Police (CoLP).

Their role is to provide expert advice to external organisations to reduce the likelihood of becoming a victim of cyber-dependent crime, as well as supporting them in the mitigation of and recovery from those attacks, which do occur.

They deliver presentations to small/medium businesses and organisations to raise awareness of the current cyber threats that they face, as well as providing a direction to improve their cyber safety within their companies.

Smaller businesses are less likely to have the capability and resources that larger organisations may have, and therefore it is a key part of the role to include this type of support and this proactive approach aims to reduce the likelihood of a cyber-related crime happening, but also provides advice and support to reduce the impact on a business if a cyber-attack were to happen.

They Cyber Protect team also support all national and local cyber campaigns through a variety of different avenues. This includes social media campaigns, events in the community, Neighbourhood Watch channels and working with Local Authorities on community engagement events. Examples including live stream events to allow the public to ask questions about their cyber security or physical events where the public can speak to the team directly to take advice.

A Regional & TVP Cryptocurrency Unit has recently been formed who will lead on all cryptocurrency seizures for the Region and TVP. This includes the technical element of the seizure, the secure storage of the cryptocurrency and eventually realisation.

They will provide a specialist knowledge advice and guidance to all reactive cryptocurrency investigations and proactively seek to use intelligence to target those using cryptocurrency as a means to launder their criminal proceeds or conduct criminality as well as use current legislation and new legislation to deprive criminals of their assets.

As part of the Prepare strand the Thames Valley Police and Regional CCU's deliver training and presentations both internally and externally to individuals and businesses. Whilst they do not provide IT support to victims affected by Cyber Crime, they are able to offer comprehensive advice that, if followed, will reduce the chances of becoming a repeat victim and they are also able to escalate a situation through the Team Cyber UK network to identify an appropriate resource for more detailed advice on a case specific basis.

The Thames Valley Police and Regional CCU's promote and share any new and endorsed tools, which organisations can use to protect themselves further. An example of this is Police CyberAlarm and Police CyberAlarm 2.0, which is a free tool endorsed by the National Police Chief's Council, to allow organisations to monitor their internet traffic and firewalls for suspicious activity.

A growing cohort of Cyber volunteers in the South East also supports all elements of the 4P framework. This enables team members to access colleagues with additional skills, and often industry experience, when faced with problem solving or understand a cyber-related matter. This has specifically enhanced capability for Pursue investigations and Protect/Prepare interventions.

As part of the ecosystem to make businesses more resilience to the threat of being a victim of cybercrime, the Home Office and National Police Chiefs Council (NPCC) have funded a network of nine regional Cyber Resilience Centres across England and Wales overseen by the National CRC Group.

The South East Cyber Resilience Centre (SECRC) covers the policing areas of Thames Valley, Sussex, Surrey and Hampshire & the Isle of Wight. It is police led (by T/D/Supt Andy Richardson) and is a not for profit partnership with universities and business with its mission to help businesses of all sizes (although the focus in on SME's, micro businesses and sole traders) make themselves more cyber resilient.

The SECRC works will all of the Chamber of Commerce's, Local Resilience Forums and MPs as well as local policing. The latter being very important as Neighbourhood Officers are embedded in their communities and engage with businesses all the time.

The supply chain is particularly vulnerable to criminal attacks so one initiative that is already helping Policing is that all 4 Heads of Procurement have agreed that if any company would

like to bid to supply services to any of the South East Forces, they have to be a member of their local CRC.

The TVP Digital Intelligence & Investigation (DII) team seeks to ensure the Force can respond better to ever-changing technological advances and their impact on public and criminal behaviours. The team are made up of a DI, DS, DC's who are Digital Media Investigators (DMI), Digital SME Trainers and Internet Investigation and Intelligence Researchers.

The team offer digital tactical advice and strategy around any investigation/incident with a digital element (which include cyber enabled crimes and fraud) and the trainers offer subject matter expertise across all areas of training from policing foundations to specialisms.

DII Strategic objectives:

PURSUE

- Recognise relevant digital opportunities to achieve positive outcomes
- Understand feasible digital lines of enquiry
- Identify early opportunities to pursue offenders
- Collaboratively work with partner agencies and other law enforcement agencies

PREVENT

- Identify and assess risks and escalation factors in offenders
- Identify digital intelligence opportunities
- Highlight relevant consequences and outcomes of successful prosecutions and investigations

PROTECT

- Identify and safeguard those most at risk of digital threats
- Maximise partnership and collaboration to ensure best service to victims in line with the Victim's Code
- Raise awareness of current threats and exploits employed by offenders
- Provide appropriate and relevant advice to victims of crime to prevent re-victimisation and further loss

PREPARE

- Ensure the efficient identification, investigation and resolution of digital incidents
- Provide the workforce with the knowledge, understanding and skills in line with current digital threat landscape
- Provide the correct resources and equipment to enable effective digital investigation

Next Steps

The Strategic Policing Requirement (SPR) Strategic policing requirement (publishing.service.gov.uk) was released on the 20th February 2023 and continues with the previous six national threats, one of which is a national cyber event.

Report to the Police and Crime Panel

A paper also went to Chief Constables Council (CCC) earlier in February 2023 in response to the 2019 HMICFRS inspection into the police response to cyber-dependant crime where is made one recommendation (and a number of Areas for Improvement).

This paper proposed a revamped, consistent Regionally Managed, Locally Delivered structure that provides effective oversight and management across all areas of Pursue, Protect, Prepare and Prevent. This option would deliver the regionally managed, locally delivered model agreed at Chiefs Council in October 2017 and would allow for force teams' operational activity to be tasked, managed and held accountable by their Regional Cyber Crime Unit (RCCU).

A more integrated approach would bridge the significant gap between the local and regional response to cybercrime, improving efficiency, effectiveness, communication and joint working. This option would require some change management and changes to working practices.

This was Option 2 and was agreed at CCC however Option 3 which fully meets the HMICFRS recommendation had already been agreed and implemented by Thames Valley Police Chief Officer Group with the collaboration with SEROCU under Project Startech in 2021.

Whilst the SPR does not explicitly include Fraud in its own right, it has however been included within SOC (together with drugs and OIC) and shortly a fraud supplement will be produced providing greater detail on what is expected from forces regarding the response to fraud.

Fraud also accounts for 41% of all criminal offences in England and Wales and this proportion is increasing.[1] The overwhelming majority of these crimes are digitally enabled with victims not knowing (or caring) about the difference between cyber-enabled and cyber-dependent.

The challenge (and key) is education and following a few simple steps can reduce the chances of someone being a victim drastically.

- Use a strong password (3 random words, upper and lower case including number and special characters),
- Turn on multi-factor authentication,
- Update devices immediately when prompted,
- Back up data and keep a copy offline.

Conclusion

Thames Valley Police is very well positioned within the cyber arena as it fully meets the HMICFRS recommendation of a Regionally Managed, Locally Delivered service with its collaborated Cyber Crime Unit with SEROCU which investigate the more serious cyber dependent crimes.

In addition Thames Valley Police also has a mature Digital Intelligence & Investigation (DII) team which ensures the Force can respond better to ever-changing technological advances and their impact on public and criminal behaviours.

[1] The Strategic Policing Requirement – February 2023