AVON AND SOMERSET POLICE AND CRIME PANEL

REPORT OF THE POLICE AND CRIME COMMISSIONER

CYBER CRIME BRIEFING

15 MARCH 2017

PURPOSE

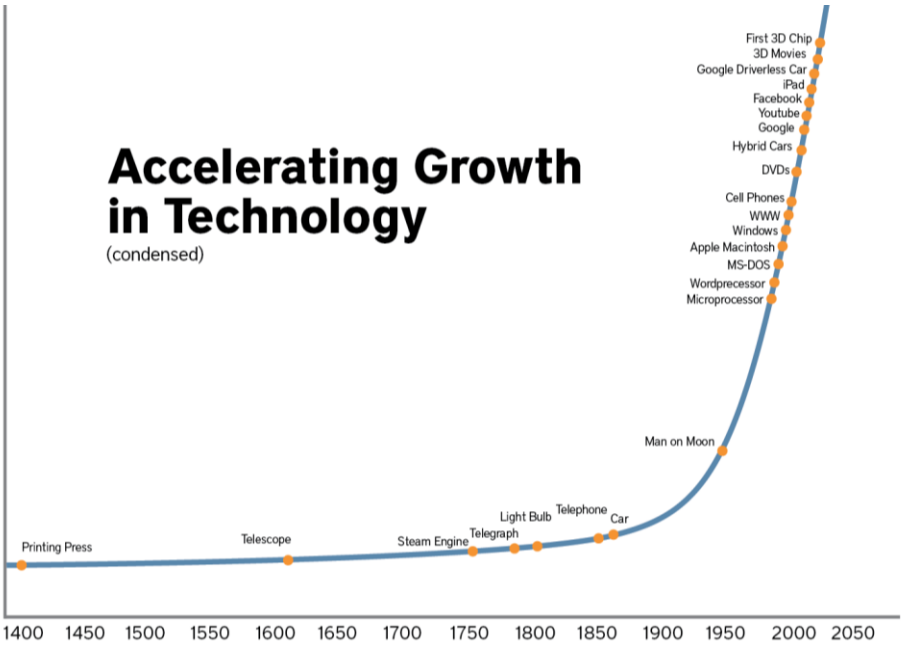
The purpose of this report is to provide a briefing on the Commissioner's activity and oversight of work in relation to Cyber Crime, a high-level description of the Constabulary approach, and to prompt discussion on how Panel Members can support prevention and awareness activity.

OVERVIEW

Cyber Crime is defined as 'the use of networked computers or internet technology to commit or facilitate the commission of crime' (ACPO Cyber Crime Strategy 2009), and covers two broad categories:

- **Cyber-dependent crimes** are new crime types, reliant on the use of technology (such as cyber-attack, denial of services, malware attacks);
- **Cyber-enabled crimes** are pre-existing crime types operated via internet enabled technology (such as malicious communications, blackmail, fraud and child sexual exploitation)

The following chart illustrates the scale and pace of accelerating growth in technology, and demonstrates the challenge to policing in a digital age. Cyber-crime is identified as a national threat, with 5.8m incidents in the last year, representing 50% of all recorded crime (Source: ONS). Cyber-crime is recognised as being significantly under-reported.



AVON AND SOMERSET APPROACH

The **Avon and Somerset Digital Investigation and Prevention Strategy (2017)** sets out the approach to tackling cyber-crime, based on four strands:

- **PREVENT** communities from becoming involved in cyber-crime activity;
- **PROTECT** communities, particularly vulnerable groups, from becoming victims of cyber-crime;
- **PREPARE** staff and the local response to meet demand; and
- **PURSUE** those engaged in cyber-crime.

Delivery of the action plan aligned to the strategy is coordinated by the Constabulary Digital Investigation Working Group, with oversight by the Assistant Chief Constable.

DEMAND AND PROBLEM PROFILE

The Avon and Somerset Cyber-crime Problem Profile was produced in 2016 to support development of the strategy, understand demand and inform targeted prevention activity. Key findings include:

- Recorded cyber-crime in Avon and Somerset has seen a 56% increase in the last year.
- Less than 10% of recorded cyber-crime offences have a successful outcome.
- 30% of cybercrime is against females aged 12-17, most of which are also 'Sexual Offence' or 'Malicious Communication'. The known offender data suggests that the vast majority of the offenders are of a similar age to the victim.
- Most common crimes reported to Avon & Somerset via Action Fraud are fraudulent online sales and the victim is very unlikely to know the offender, who may well not be in the area.
- 7% of crimes in the ASC area reported via Action Fraud were 'cyber dependent' and have a higher level of expertise for the offender (e.g. Ransomware/Malware).
- Crimes in Avon & Somerset reported via Action Fraud have increased by 10% in the last six months, equating to 5273 reports.
- Most fraud victims from Action Fraud are older people with the most affected cohort being female aged between 50-69.
- Avon & Somerset are ranked 12th highest force for reported frauds.
- Action Fraud referrals for investigation in Avon & Somerset number circa 5 per week.
- The National Fraud Intelligence Bureau report that victims of cyber-crimes enabled by hacking in Avon and Somerset are most likely to be in their 60s. 26% of these victims report they have been significantly or severely affected by the crime type.

REPORTING, INVESTIGATION AND VICTIM CARE

There is a three-tier response to cyber-crime and digital intelligence investigation within the Constabulary:

- Cyber-crime team (centrally located): comprising 1 Detective Sergeant, 3 Detective Constables and 1 Police Staff
- Three Cyber-crime teams (embedded in each Local Policing Area): comprising 3 Digital Media Investigators
- Local Policing Area / Specialist Department SPOCs (Single Points of Contact): ensure local investigations are effective and efficient.

The Regional Cyber Crime Unit is responsible for handling larger investigations.

Investment in dedicated digital investigation resources has increased by 51% in the past 3 months in recognition of the need to respond to demand and vulnerability, with an annual investment of £291,261. The creation of the new Digital Investigation Unit and Digital Media Investigators has significantly enhanced specialist instigative capability, guidance and advice and enables continual development of capabilities in a rapidly changing area of business. Additional capital investment has been made in the Getsafeonline annual contract (further detail below).

Members will be aware that incidents of online fraud are reported to Action Fraud, with cases referred back to Avon and Somerset for investigation as appropriate. PCC representation at a national level has strengthened oversight of the role of Action Fraud. At a local level, new investment has been made to enhance victim care through the creation of two new roles: a 'Fraud Protect Officer' and a 'Cyber Protect Officer'. These posts will have access to Action Fraud data on a daily basis and will assess victims reporting fraud crimes within the Avon and Somerset area to identify vulnerability and ensure appropriate enhanced support is put in place. In addition, the Operation Signature model of vulnerable victim safeguarding, developed by Sussex Police, will be implemented in Avon and Somerset from 1 April 2017. The approach has been evaluated by the HMIC and identified as best practice in protecting vulnerable victims of fraud.

PREVENTION AND AWARENESS

<u>Prevention Activity</u>

A range of activity is underway under the **'Protect'** strand of the Constabulary strategy, with a focus on those identified at the greatest risk of becoming a victim of cyber-crime. This includes:

- Regional Organised Crime Unit ('ROCU') cyber team providing briefings to business and Public Sector in the region and supported by Business South West, local Business Crime Reduction partners and via the PCC's Business Crime Forum;
- 35 PCSOs are trained to visit schools and a Force education package is in use;
- South West young people digital safeguarding group established with the Constabulary and the 4 neighbouring Forces;
- Internet Watch Foundation helpline takes calls from young people in relation to cyber bullying and internet enabled child abuse;
- Investment in new Cyber Protect Officer and new Fraud Protect Officer posts (described above) to coordinate campaigns, target education work and provide enhanced victim support to the most vulnerable victims and prevent repeat victimisation;

- Community Awareness Event on understanding how to stay safe online: an invitation to attend the event taking place on 3 April 2017 has been extended to Panel Members;
- Development of specialist police volunteers – including seeking help from academia, cadets and specials.

Advice and Information

The Constabulary has invested in a contract to enable access to information and guidance on how to safe online available at: www.getsafeonline.org/police/resources A wide range of materials can be found at the link, including:

- Short videos and leaflets offering practical advice on issues ranging from identity theft to how to use the internet safely in public places;
- Presentations tailored to businesses, young people, and older people;
- Campaigns

Panel Members are encouraged to view the resources available in advance of the Panel Meeting.

RECOMMENDATION

That Panel Members consider the contents of the report and discuss action that can be taken to support prevention and awareness activity.