POLICE AND CRIME COMMISSIONER FOR LEICESTERSHIRE

ETHICS, INTEGRITY AND COMPLAINTS COMMITTEE

PAPER MARKED

G

Report of	**CHIEF CONSTABLE**
Subject	**CYBER CRIME**
Date	**FRIDAY 20 MARCH 2020 – 2:00 p.m.**
Author	**CHARLES EDWARDS**

Purpose of Report

1. To provide information the Committee with information regarding how the Force address Cyber Crime.

Recommendation

2. The Board is asked to note the contents of this report.

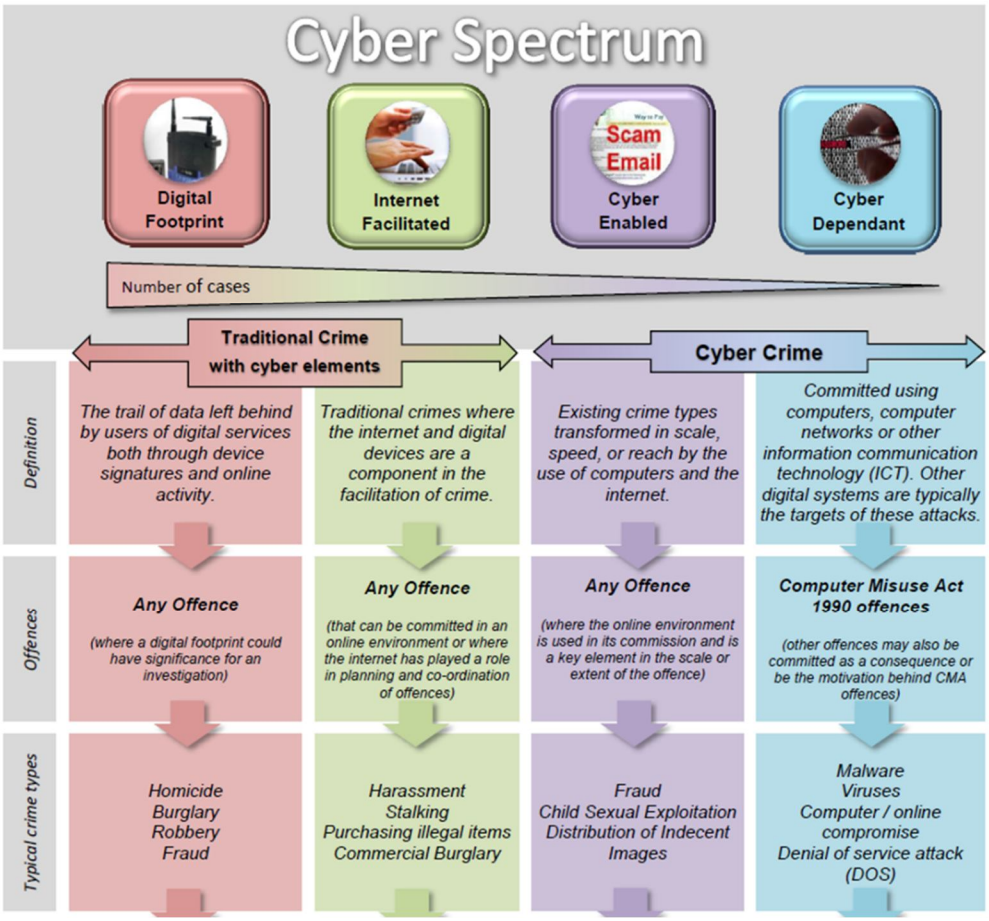
Background

3. The definition of Cybercrime is:

- "Criminal activity carried out by means of computers or the internet..."
- "...Computer crime, or cybercrime, is any crime that involves a computer and a network either to commit offences or intended as the target"
- *Wikipedia/Oxford Dictionary (2015) Cybercrimes: Fraud, Harassment, Child Grooming, Theft.*

4. With the very vague nature of the above definition you can imagine that there are few offences now that do not fall under the umbrella of a Cybercrime ranging from Online Frauds, Grooming, Social Media harassments all the way through to Attacks on Companies I.T infrastructure.

5. Due to this Cybercrime is split down into four different areas shown on the Cyber Spectrum:



6. With that in mind all investigators across the force have a raised awareness through inputs during development programmes, online support and a centralised team of digital media investigators who regularly provide inputs at briefings and training days. This allows them to deal with the offences within the Digital Footprint and Internet Facilitated areas and we have dedicated units such as the Economic Crime Unit and Paedophile Online spend the majority if not all their time dealing with Cyber Enabled offences.

7. Of specific interest I believe to this request is the more specialist Cybercrime investigation team which is locally named the Cybercrime Unit. This was setup in 2016 as part of an initial response to national and local demand and it is encouraging to see that two years later it was mandated that every force should have a unit similar to ours (we had a great head start!). The Cybercrime Unit deals with all reported Cyber Dependent offences within the Leicestershire area within a Regionally Co-Ordinated, Locally Delivered environment with support from centralised Home Office Funding.

8. The Cybercrime Unit of Leicestershire Police is made up of:

- 1 Detective Sergeant
- 3 Detective Constables
- 1 Police Staff Cyber Protect Officer
- 1 Police Community Support Officer

9. The unit sits within the Digital Hub at Force Headquarters where skills/resources and learning is shared with departments with similar leans.

10. The team has ownership for all aspects of dealing with Cyber Dependent crime with a more holistic view than most departments taking responsibility for all four P's as defined within the Counter Terrorism strategy (Pursue, Protect, Prepare, Prevent).

11. This means that the team is designed to:

- **Pursue:** Investigate Cyber Dependent offences,
- **Protect:** Provide contextualised advice to protect those vulnerable to being victimised,
- **Prevent:** Identify and refer those who are at risk of becoming offenders through diversion/prevention schemes
- **Prepare:** Working with local agencies/businesses to ensure they have suitable contingency plans in place to prepare for when it will happen (not "if").

12. Currently our work primarily comes through Action Fraud which is the national Fraud and Cybercrime referral centre though with an increasing amount coming from direct phone calls. The majority of cases we deal with fall under the following categories:

- **Malware** – Where malicious software has infected a computer (or entire business) and stops it working how it should. This is normally by encrypting files or removing functionality and often comes with a ransom demand. An example of this would be Wannacry, where a vulnerability was found in the operating system of computers that had not been updated meaning they ceased working unless a "ransom" was paid.

- **Unauthorised Access/Hacking** – The unauthorised access to accounts either individuals based or company based. This is often known as Hacking but can have occurred through a number of reasons and can have numerous outcomes as well. An example of this would be the recent Leicester City Football Club issue we investigated. This was where a foreign group found a weakness in the sales website and were then able to collect all financial details placed onto the site over a fortnight period.

- **Denial of Service Attacks** – Use of technical capabilities around software and hardware often world-wide to overload a website or businesses server rendering them unable to work. This has rarely happened locally (and is often linked to gamers) but nationally several large scale companies have been hit and is often associated with a Blackmail.

- **Website Defacement** – The change of a websites source code often to promote a political issue. Regular examples have been "Free Palestine" or ISIS propaganda.

13. We deal with on average 5 offences a week though the quantity fails to provide any relative usefulness around the time spent on each case. Regularly we have cases that take 4-8 hours to deal with and finalise with advice provided to minimise repeats. Within these there are often with lines of enquiry going out of our jurisdiction or to unresolvable entities which we ensure are reported back into the National Cybercrime Unit either for a larger

piece of work to be done or to support/empower them to have accurate figures of scale/damage to put pressure on responsible companies/countries.

14. At the other end of the scale we deal with infrequent incidents that hit businesses and individuals which can result in weeks or even months' worth of digital forensic and investigative work. We have had incidents that have cost businesses several hundreds of thousands of pounds or render them unable to operate at all for considerable lengths of time.

15. Common targeted business streams are those which rely heavily on I.T and use it regularly but do not consider themselves an obvious target and rarely have contingency elements in place. Groups such as Solicitors, Vets, Libraries and Dentists have been a recurring theme over the years with peaks and troughs around recent and current vulnerabilities in software used. In tandem to the criminal investigations into the Computer Misuse Elements we have also worked in corroboration with partner agencies from around the world including the FBI, Europol and the Information Commissioners Office developing links and contacts which have proven repeatedly beneficial.

16. Further to the investigative elements we have referred 3 individuals in to the EMSOU referral scheme ensuring that we do not criminalise unnecessarily those who are in need of support and may benefit from it to understand the social/moral issues of their actions and highlight the many strong career options they may have if they do so legitimately. We have ensured that over 1,000 of our own officers and staff have a heightened awareness of how to keep themselves and others safe online. We have provided contextualised Cyber Protect advice to over 10,000 individuals (approximately 5,000 in 2019 alone) from a range of backgrounds and this year are working to continue to expand the work we do to those at their most vulnerable in the Charity Sector with a police led conference at Police Headquarters in February.

17. Because of the very nature of the Cyber Dependent investigations we take part in we are routinely having to gain raw access to large amounts of data that is both vital to the undertaking of the victim company it has come from and regularly contains personal and private information upon it. The team are cognisant of disclosure and relevance guidance around the Criminal Procedures and Investigation Act 1996 ensuring that only those of real value are examined and exposed to evidential scrutiny. The General Data Protection Regulations provide a strong framework on how to access, store and utilise data gained and working alongside the Information Commissioners Office we have had a great opportunity to test their guidelines and values.

18. The less common but often most impactive ethical considerations within those investigations we take part in come from the financially motivated/blackmail elements of Ransomware incidents. These incidents generally cause the loss of vital chunks of data, if not all of it, from a company with the sole purpose of demanding a "ransom" for the safe return of the data. In responding to these incidents a rationalised approach must be had to balance the businesses need to get up and running again as soon as possible, the plausible loss of all data from the company against the fact that the money may be going to fund terrorism or organised crime groups and on top of this may still not actually lead to the return of those files and folder originally lost. As the police we have national guidance to suggest the money is not paid for these reasons but we have on at least one occasion had to offer to support the victim to generate more actionable intelligence for our investigation and act to support them getting the best price they could for their data.

19. Finally it is worth mentioning that the “positive outcome” traditional element of the majority of quantitative measurements of impact upon a crime struggles in even more ways than most within Cybercrime investigation. Often anonymity of the suspect is gained through the very acts committed or through highly sophisticated software and hardware. Offenders are often identified overseas with the majority coming from countries we have no mutual legal aid treaty.

20. Those offenders who are located within the UK are dealt with in a thorough manner but with the poor sentencing guide lines, the lack of understanding within the Crown Prosecution System and the Criminal Justice System it is often more valuable to all parties and more proportionate to seek a Conditional Caution. With a single court case we have taking over 3 years from charge to get to court the need to support the victim in a timely manner and ensure the suspect has an adequate and appropriate outcome it is likely the case that very few Cybercrime investigations reach court.

Ethical Considerations (Update):

21. Cyber Dependent crime currently encompasses offences of a highly technical nature though which potentially do not have a level of impact in line with THRIVE assessment of other offences.

22. Is it ethical that due to funding and key performance indicators linked to this that we investigate 100% of reports where other areas of policing we do not?

23. Is it ethical that when so few offences reach a traditional positive outcome that we put some much training, resourcing and time into investigating offences of a Cyber Dependent nature?

24. Cyber Dependent offences are still in their infancy of being investigated and intelligence locally and nationally is poor. Through effective investigation with the correct resources both staff and equipment wise we are now generating a positive intelligence picture worldwide ensuring that the bigger picture of offending and victimology is understood.

25. Investigations that have had little impact locally but have been expeditiously and effectively investigated have allowed positive acts in other countries to allow victims of serious offences to be safeguarded and important enforcement work to take place.

26. Whilst positive outcomes are not high the work of the Cyber Dependent unit is primarily victim focussed prioritising the effective safeguarding of Leicestershire victims through mitigation advice, support and referral where required.

27. Offences not within the Cyber Dependent remit but are as technical are often not as well-resourced or are dealt with by staff without the complete understanding of elements within. Is it ethical that there is such a divide between understanding of digital elements and what are the force doing about it?

28. Offences such as Cyber Enabled Fraud or Blackmail through to grooming and child sexual exploitation are dealt with by officers with the necessary skills to progress such an offence to court. Whilst it isn’t possible to upskill them to understand all elements of the technical areas the Cyber Dependent Crime Unit & the Digital Media Investigation team within force are available and set up in order to provide appropriate strategy to maximise opportunities.

29. When purchasing equipment or funding training from both internal and external funding streams the added value that can be brought to Leicestershire Police is considered. This has in the recent time highlighted software that can more quickly identify and analyse links between child abuse offenders as well as mapping software to more quickly provide investigative guidance for serious organise crime investigations.

30. Are we doing enough work to identify and divert potential offenders at a young age from becoming criminalised in an area that is still not socially understood as being unlawful?

31. A robust prevention referral process has been created within Leicestershire to support/empower educational institutes to help identify and refer potential offenders who are either showing signs of offending or have offended but not to a level that criminalising them is appropriate.

32. Schemes are in place at a regional or national level to divert and de-escalate offenders to provide them with alternative approaches with career opportunities and social/ethical issues explained.

33. Inputs are being developed and delivered to schools through the use of novel presentation materials with the view to empower staff and champions at educational and entertainment facilities to have the knowledge and confidence to effectively disseminate the messages broadcast nationally.

Background Papers
None.

Person to Contact
Detective Sergeant 2877 Charles Edwards
Tel: 0116 248 3950
Email: charles.edwards@leicestershire.pnn.police.uk