POLICE AND CRIME COMMISSIONER FOR LEICESTERSHIRE

POLICE AND CRIME PANEL

Report of	**CHIEF CONSTABLE**
Subject	**CYBER CRIME**
Date	**WEDNESDAY 28TH MARCH 2018 – 1:00 p.m.**
Author	**DS CHARLES EDWARDS**

Introduction

1. For the purpose of this report cybercrime has been defined as any offence which involved the use of a computer or network in order to commit a criminal act. Broadly speaking cybercrime is divided into two types:

    - "Cyber Enabled Offences" (CEO) are any offences which utilise a computer or network in order to facilitate the commission of an offence, such as the sharing of indecent images and fraud.

    - "Cyber Dependent Offences" (CPO) which can only be committed using a computer or network, including: website defacements; denial of service attacks; malware; and hackings.

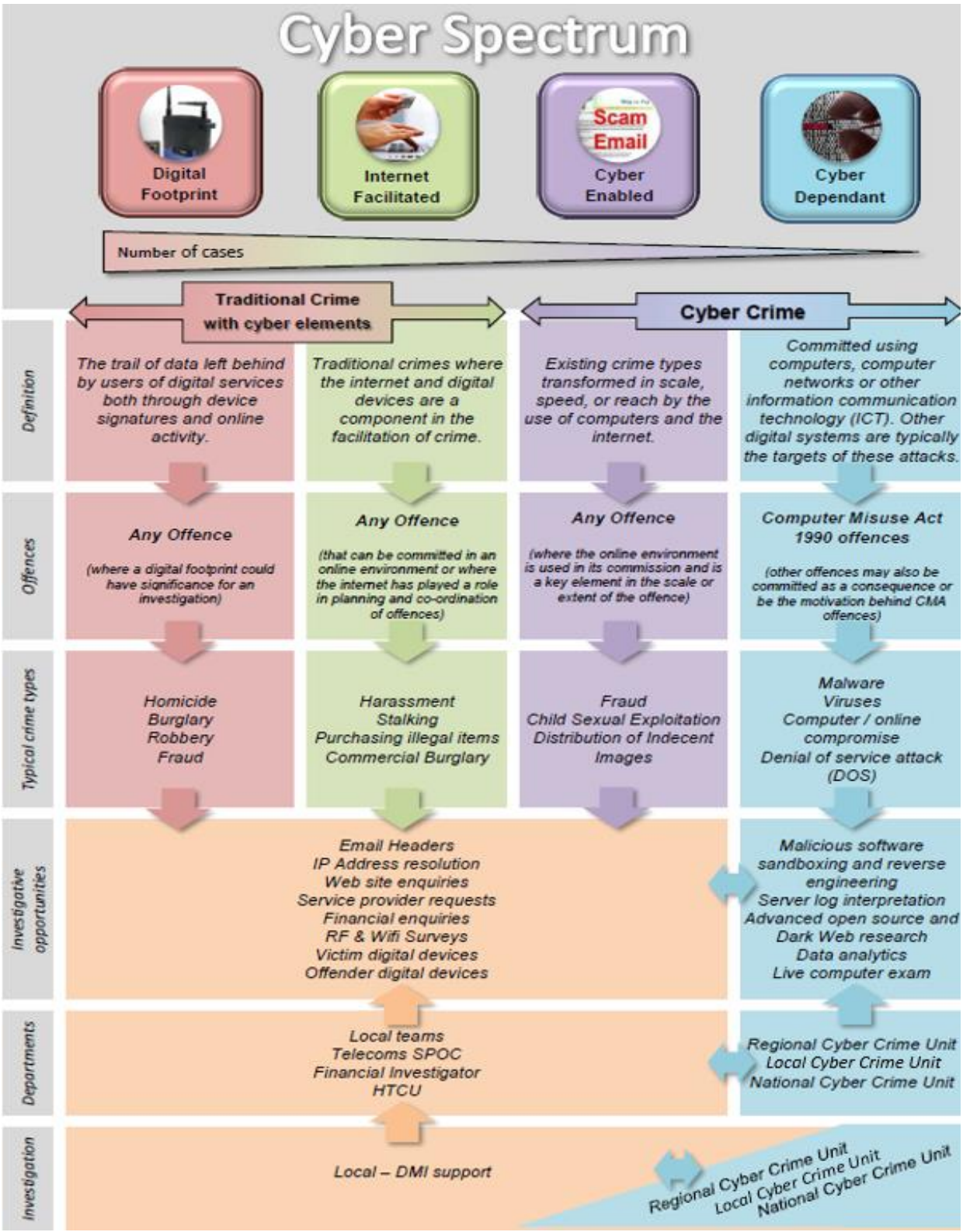
2. This report outlines the police approach to managing cybercrime, including some of the new and emerging developments in the field, as well as some of the key challenges.

3. Figure 1 below outlines the range of different types of cybercrime.

Recommendation

4. The Panel are asked to note the report.

Figure 1: The Cyber Spectrum



Types of Cybercrime

5. The main volume of cyber offences occur within the CEO category with approximately 85% of reported frauds and 70% of child sexual exploitation, through indecent images of children, occurring on line.

6. Online frauds and offences of harassment/abuse through online methods (primarily social media based) are very common. In addition the police cybercrime unit has dealt with crimes such as “Cyber Enabled” blackmail offences, diversion of business telephone systems to premium rate numbers (commonly called PBX dial through frauds), denial of service incidents (flooding the resources of a targeted system) and ransomware attacks where offenders withhold access to data, or threaten to publish it, unless a ransom is paid. In relation to ransomware attacks, the majority of demands for funds are now in online cryptocurrencies such as BitCoins where the value can fluctuate on a daily basis but have led to ransoms being as high as £30,000 for data.

7. Victims of cybercrime tend to be members of the public, but there has been a growing trend for services such as libraries, leisure centres and vets to be targeted, usually because they have poor IT security and “Cyber Hygiene” systems.

8. The police’s response has ranged from practical “Cyber Hygiene” advice through to the use of sensitive and complex investigative techniques involving regional and national partners. Officers dealing with the higher tier of technical offences rely upon highly specialist training and development which is both challenging and expensive to source.

9. The skills of police officers and staff dealing with cybercrime are highly specialised and increasingly in demand beyond the boundaries of the local police area. Because of this the National Police Co-ordination Centre (NPoCC) has developed a register of suitably skilled and qualified individuals across all police areas to enable the deployment of resources beyond local police boundaries in response to large scale regional or national incidents.

Police response to cybercrime

10. Leicestershire Police has developed a dedicated team to investigate all “Cyber Dependent” offences over the last 20 months. At the same time it has trained dedicated “Cyber Protect” officers to spread information security messages both internally and externally. This team is made up of a Detective Sergeant and 2 Detective Constables in line with the national unit setup model with the support of a dedicated Cyber Protect member of staff.

11. This team is supported by the force Digital Media Investigator Team made up of 10 officers/staff, enabling the local force to provide a service, which is on a par with the best nationally. This support allows 24/7 coverage for serious offences enabling a fast response to incidents in order to maximise evidential opportunities at the first opportunity.

12. The Digital Hub has successfully pursued external funding opportunities which has enabled access to the appropriate equipment and resources, such as a specialist router examination kit and the training up of the Force

Priority team to deal with elements of cybercrime within routine investigations.

13. Leicestershire Police has forged partnerships with key leaders within the Digital Forensic market and is now testing several pieces of equipment which will put it at the very forefront of digital policing.

14. Seven volunteers have also been recruited, particularly via links with universities, to support research and skill sharing with external organisations. These links have enabled the development of new techniques and the deployment of specialist skills at particular crime scenes. For instance we are in the process of recruiting a lecturer from De Montfort University who has a very specialist skill set around network forensics. He has already secured key evidence in a cybercrime incident where a business was attacked by an ex-employee.

15. To increase the resilience of the Cyber Crime investigation team we have conducted a scoping exercise internally and have identified those with skills in the cybercrime arena. Two officers with the necessary investigative mind-set and awareness of digital technology have been supported in undertaking the detective process before potentially joining the Cybercrime Investigation Team.

16. In the future we are looking to lead the way nationally in the provision of digital policing training with the Digital Media Investigators developing our own custom built Open Source course which we currently deliver whilst also considering licencing the College of Policing's Digital Media Investigation Training course to allow the flexible and frequent training of our staff to a nationally accredited level maintaining its up to date or forward facing nature.

Links with National Crime Agency (NCA)

17. Leicestershire Police works closely with partners within the region offering mutual support and sharing lessons learned from incidents. Every Monday, issues and incidents are discussed and co-ordinated at a regional level to ensure they are adequately resourced. The feedback from this forms part of the Tuesday triage, incident coordination and tasking (TICAT) discussions where the regional teams liaise directly with the NCA.

18. Leicestershire Police provides quarterly updates to the National Police Co-Ordination Centre (NPoCC) of its capacity for supporting cross boundary threats or initiatives.

Awareness Raising

19. The Cyber Protect Officer (mentioned above) has engaged internally and externally to raise awareness about cyber protect initiatives. Over 600 internal staff have been presented to as well as over 400 external partners and businesses via conferences and networking events. This has included purchasing and rolling out a novel information security comedy sketch

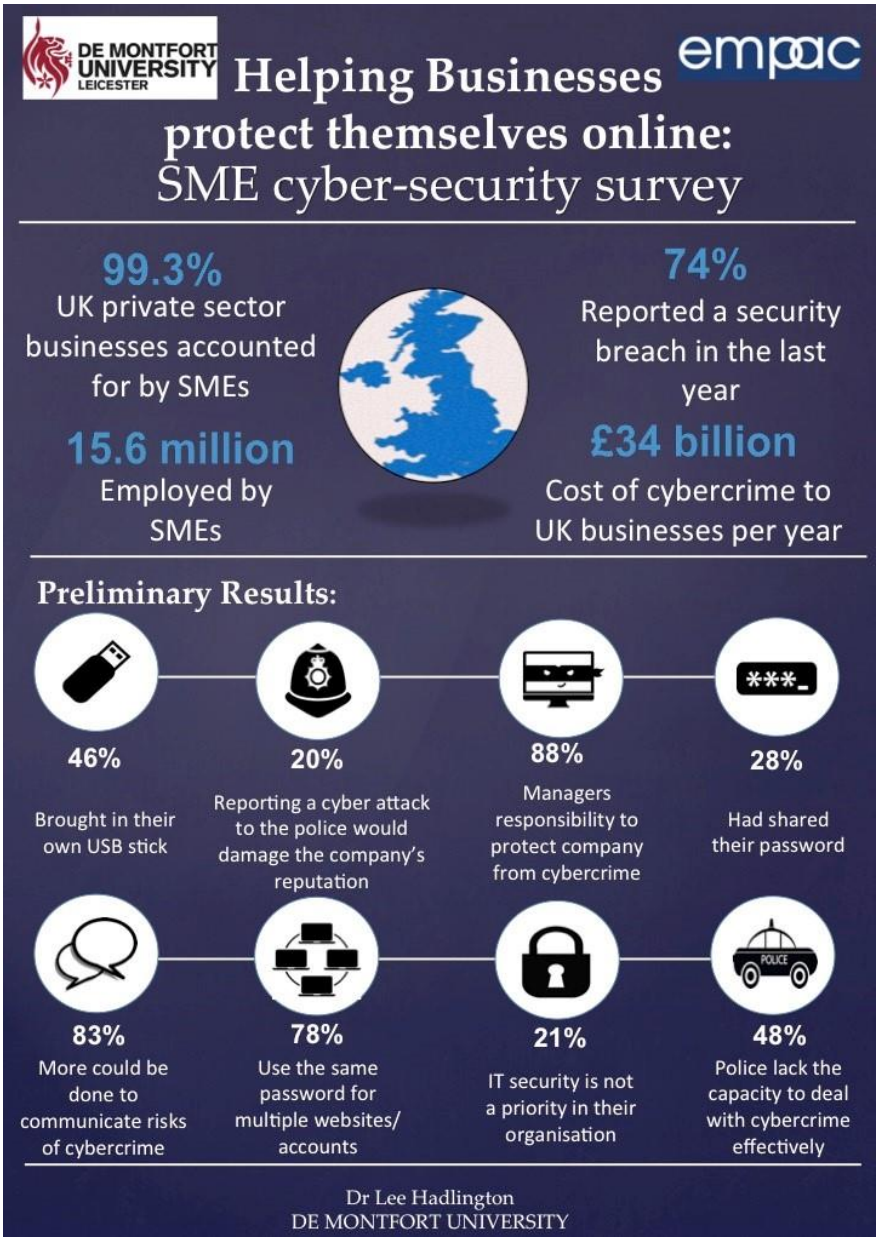
campaign to raise knowledge of threats, as well as running an internal testing exercise to provide examples and context/content for future presentations.

20. There has been a clear push to upskill and raise awareness of the risks of cybercrime and the need to provide training opportunities to maximise exposure to the risk and opportunities of digital policing. Inputs are now delivered by the Digital Hub to new starters (of all roles/ranks), including new detective constables and new detective inspectors. At a national level we have taken responsibility for senior information officer training around digital tactics and opportunities.

21. Working with key partners including industry and academia has allowed Leicestershire Police to access vulnerable and hard to reach communities by training up staff and providing them with the necessary resources and presentations tailored to their audiences.

22. Research undertaken by Leicestershire Police's own police support volunteer – a Cyber Psychology Professor at De Montfort University – has helped highlight the concerns of SMEs and has allowed several business networking events and conferences to be set up with tailored presentations and targeted communications.

23. Further research is being funded by the strategic partnership fund and has helped provide infographics such as the below to give contextual information/evidence of people's opinions and feelings in relation to cybercrime.



24. In addition, Leicestershire Police has worked in tandem with GetSafeOnline, a national resource, to allow the customisation of a "Leicestershire-centric" page branded with our own and partners logos/banners enabling us to focus on localised issues.

25. One of the key drives for the foreseeable future is to ensure increased awareness across Leicestershire Police and the wider community of methods to reduce the risks posed by cybercrime. Annex A outlines some of the key messages that are presented to internal and external audiences.

Person to Contact

Charles Edwards DS
Tel: 0116 248 3950 Email: charles.edwards@leicestershire.pnn.police.uk

Rob Nixon, Deputy Chief Constable
Tel: 0116 248 2005 Email: rob.nixon@leicestershire.pnn.police.uk

Annex A

Key messages to the public

The key messages are all designed to be easy to share yet highlighting that the human factor is often the main weakness within any organisation.

Anyone can be a victim no matter how big or small a company is. Saying this over 75% of victims of Cybercrime could protect themselves by following simple instructions.

Keep up to date! Whatever devices, operating systems, software or apps you use, always ensure you are running the most up to date versions. Updates include security patches to fix vulnerabilities!

Antivirus Make sure you have up to date antivirus installed and running for all devices you use to access the internet and email

Passwords You need to have a different password for everything you log in to. Make sure you're using #ThreeRandomWords to create a strong, separate password for each account.

iTunes Scams NO legitimate debt can be paid in iTunes vouchers - #HangUp on that call

Courier Fraud Neither the Police nor Banks will ever contact you to:

1. transfer money to a safe account;
2. withdraw funds for safekeeping;
3. assist with a covert investigation
   OR

4. collect cash, bank cards or PIN numbers

#TakeFive and REMEMBER – emails, texts and phone calls can all easily be spoofed. Don't automatically assume any contact is genuine until you have verified that it is.

GetSafeOnline – www.getsafeonline.org/Leicestershire is the key site to signpost people to for advice both individuals and businesses.

Underreporting is still very high especially within the business community. Reporting must be encouraged through Action Fraud – www.actionfraud.police.uk and 0300 123 2040. This must be advertised through the forces and partners channels wherever possible as is the only means of having a holistic overview of what is happening outside reporting to ourselves.

This page is intentionally left blank