ABERDEEN CITY COUNCIL

COMMITTEE	Communities, Housing and Infrastructure
DATE	26 August 2017 – deferred from the meeting on 24 May 2017
REPORT TITLE	Thematic Report - Cybercrime Police Scotland, North East Division
REPORT NUMBER	N/A
DIRECTOR	Chief Executive
REPORT AUTHOR	Superintendent Kate Stephen, North East Division, Police Scotland

1. PURPOSE OF REPORT:-

1.1 This report seeks to inform the Committee of the risks posed by Cybercrime and the work being undertaken by North East Division and Police Scotland to reduce the risk of harm it causes to our communities.

2. RECOMMENDATION(S)

2.1 Members are asked to note the paper.

3. BACKGROUND

3.1 The volume and complexity of cyber-attacks against the UK are rising sharply with digital technology revolutionising every aspect of modern life; opening up new vulnerabilities and opportunities for criminal activities. It is estimated that the worldwide cost to victims of Cybercrime, including UK businesses, greatly exceeds the profits available to organised crime through more traditional criminal enterprises.

3.2 Threats come from a range of sources, many designed to extort money from victims, utilising a range of techniques. Some of the more common techniques are:

- **'Phishing'** - scams which are aimed at obtaining personal and financial information from the recipient.
- **'Spear Phishing'** – the use of a personalised communication, notionally from someone known to the receiver, to deceptively obtain personal and financial information from the receiver.
- **'Malware'** – an umbrella term for many of the most damaging software applications.
- **'Distributed Denial of Service (DDoS)' Attacks** – this is the inundation of internet traffic from a number of sources which overwhelm systems making them unusable.

- **'Ransomware' –** malware that locks your computer and mobile devices or encrypts your electronic files until you pay a ransom.
- **'Theft of Personal Information (IP Data)'** – especially of personal data, money and intellectual property.
- **'Acquisitive Crime'** - attempts to obtain money or other business assets through deception i.e. fraud, such as card-not-present (CNP) fraud.

3.3 Sexual related cybercrime appears to be on the increase and is becoming more prevalent amongst the younger generation. Children and young people are gaining access to internet enabled devices at a much younger age, whether a mobile phone, hand held computer device or a games console at home, it is more common than not for children have unregulated access to the online world.

3.4 Child Sexual Exploitation (CSE) crimes occur where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person into sexual activity either in exchange for something the victim needs or wants - like drugs or alcohol - and/or for the financial advantage or increased status of the perpetrator or facilitator and within the definition it specifically mentions that it can occur through the use of technology. North East Division is currently working with Barnardos to better understand both the scale and impact of CSE in the North East. The two year pilot will see a CSE Advisor working with the Police and other agencies to deliver awareness training. Whilst this is currently local to Aberdeen City at present, it is anticipated the success of the pilot will see CSE Advisors embedded across all 32 authorities in the future.

3.5 It is increasingly common for young people to naively share inappropriate images of themselves with their peers within what they understand to be a closed group of friends or acquaintances, only for those images to find their way, often maliciously, into the wider social media community (commonly referred to as sexting). This often results in devastating consequences - both legally and emotionally - for the individuals involved and their families.

3.6 Sexual related cybercrime reaches beyond children and young people. The online activities of many adults result in them leaving themselves vulnerable to exploitation. Intimate photos, shared willingly at the outset, are later used by individuals to extort money or other advantage from the subject (commonly referred to as sextortion), or simply to be maliciously released to the wider social media community (commonly referred to as revenge porn).

3.7 Government and Public Sector organisations have long struggled to provide a comprehensive cyber security strategy to protect all aspects of their digital assets. This has been evident with the recent infiltration into the website of Aberdeen City Council in January 2017. Similar 'hacking' type attacks have been experienced by City of Edinburgh Council, and Lincolnshire County Council as well as many other public bodies/organisations across the country, demonstrating the absolute need to improve, enhance and increase both organisational awareness and security measures. This has been recognised as an area of Risk which is being progressed through an action at the Local Resilience Partnership.

3.8 The Society of Information Technology Management recommend that Local Government must play an active role in cyber security prevention, as necessary, to prevent "a national cyber-attack that could be initiated locally, or local services could be penetrated and crippled, requiring a national response".

Structures

3.9 Reported cybercrime in North East Division will be investigated by the most appropriate resource and will very much depend on the level, scale and complexity of the investigation.

3.10 Clearly, the prevention of such offences in the first place is our starting point and we have a number of resources who provide preventative inputs and training on the subject to a wide ranging audience.

3.11 Locally, we have a cadre of School Liaison and School Based Officers who routinely deliver inputs on 'Internet Safety & Cyber Bullying' and 'Social Media & the Law' to school aged children as well as to parental/guardian groups and other adult audiences. Similarly, we have a small team of Crime Reduction Officers who regularly promote online safety in their written and face to face engagement with various community, community safety and business groups.

3.12 There are also a cadre of 'Web Constables' located throughout North East Division, embedded within our Community Policing teams, who, along with the School Liaison and Crime Reduction Officers receive ongoing training to maintain relevancy and further develop their knowledge base and awareness of trends. This ongoing training ensures the advice they impart is up to date and relevant to the audience to which they are engaging. Web Constables have most recently been actively involved in the recently launched 'Choices for Life Peer Mentoring Cyber Safety Programme'.

3.13 North East Division has strong links with and liaises regularly with the National Safer Communities Cyber Prevention Team; actively promoting the prevention materials developed by them and participating in national campaigns such as Safer Internet Day which took place on 7 February 2017.

3.14 The Division also continually promotes positive preventative messaging through the Division's Twitter page (@NorthEPolice), Facebook page (@NorthEastPoliceDivision) and via our partnership with AbSafe who provide crime reduction messaging on our behalf across the North East.

3.15 North East Division has recently begun piloting Neighbourhood Watch Scotland's 'Neighbourhood Alert' system, itself an online platform for providing members of the public who have signed up for it with targeted crime reduction and preventative messaging, which will provide a further platform for educating the public on the dangers of Cybercrime.

3.16 Counter Terrorism Security Advisors are also available upon request to deliver specific and bespoke inputs on the topic of cybercrime to local authorities and businesses. Such an input was delivered to Aberdeen City Centre Business Improvement District (BID) in December 2016 and Police Scotland would welcome the opportunity to carry out further inputs in Aberdeen City.

3.17 The above professionals regularly signpost partners and the public to the many excellent online resources available to assist in becoming better informed on such matters.

3.18 These include:

- The Centre for the Protection of National Infrastructure - *www.cpni.gov.u*
- The National Cyber Security Centre - *www.ncsc.gov.uk*
- Get Safe Online - *www.getsafeonline.org*

Conclusion

3.19 Cybercrime is prevalent across all aspects of modern life and Aberdeen City is no exception to this. It is likely that perpetrators will continue to refine and improve their abilities in this area of organised crime, driven by an expanding marketplace for the data they can obtain and the financial rewards available to them.

3.20 That said, there are currently no specific trends reported which are particular to the Aberdeen City area in terms of its infrastructure or main areas of industry, however a common issue nationally is a lack of knowledge on the importance of robust password management, ineffectual password discipline being an easy route for criminals to access individuals accounts and potentially their wider work infrastructure as a consequence.

3.21 Whilst technical mitigation will remain an important strand of prevention, it is imperative that the public, public bodies and businesses of all sizes are aware of the threats posed by the various types of threat and the steps they can take to reduce their vulnerability - both personally and organisationally - to attack.
In addition to a maturing framework of response across local, regional and national law enforcement, the needs to encourage better cyber security hygiene practices on private, public body and business levels is of the utmost importance.

3.22 Protecting people at risk of harm remains a key priority for Police Scotland. Across North East Division, we will continue to work in partnership to raise individual awareness and understanding of how people can protect themselves with the focus being primary prevention and early intervention.

4. FINANCIAL IMPLICATIONS

4.1 There are no direct financial implications arising from the recommendations of this report.

5. LEGAL IMPLICATIONS

5.2 There are no direct legal implications arising from the recommendations of this report.

6. MANAGEMENT OF RISK

6.1 Not Applicable

7. IMPACT SECTION

7.1 **Economy**

Not Applicable.

7.2 **People**

Not Applicable.

7.3 **Place**

Not Applicable.

7.4 **Technology**

Not Applicable.

8. BACKGROUND PAPERS

8.1 Not Applicable

9. APPENDICES (if applicable)

9.1 Not Applicable

10. REPORT AUTHOR DETAILS

Kate Stephen
Superintendent
North East Division
Police Scotland
01224 306054
NorthEastLocalPoliceCommander@scotland.pnn.police.uk