POLICE, FIRE AND CRIME PANEL REPORT

Meeting Date	9th March 2023
Report Title	Cybercrime

If you require this information in a different language or format, please contact the Office of the Police, Fire and Crime Commissioner at info@northyorkshire-pfcc.gov.uk.

Purpose of this report

To give an update to Panel members of the work the North Yorkshire Police (NYP) have being doing in relation to Cybercrime. The report will also provide the panel with an overview of the work of the North-East Business Resilience Centre.

Summary of key content

This report will provide panel members with;

- Information on the NYP Cybercrime unit.
- Examples of some of the cases the unit have been involved in.
- Update on the work of the unit with local Communities and Business.
- Information on work across regions.
- Information on the work of the North-East Business Resilience Centre

Background

The North Yorkshire Police Cybercrime Unit is made up of one sergeant and five police officers. They offer a 24-hour policing response and are charged with dealing with the four pillars of the Serious and Organised Crime Strategy - Pursue, Protect, Prevent and Prepare with cyber-dependant crimes.

- Pursue - prosecuting and disrupting people engaged in serious and organised crime
- Prevent - preventing people from engaging in this activity
- Protect - increasing protection against serious and organised crime
- Prepare - reducing the impact of this criminality where it takes place

This work aligns with the Strategic Policing Review[1] and the Home Office Outcome Delivery plan[2] to

- Reduce cybercrime.
- Increase support for victims and potential victims of cybercrime.

[1] Found at Strategic policing requirement (publishing.service.gov.uk)

[2] Found at Home Office Outcome Delivery Plan - GOV.UK (www.gov.uk)

- Reduce the wider fear of cybercrime and increase the public's satisfaction with cyber policing.

The work of the Cybercrime Unit

The unit primarily deals with complex cyber-dependent crimes, which broadly speaking fall into two main categories:

- Illicit intrusions into computer networks, such as hacking; and
- The disruption or downgrading of computer functionality and network space, For example, malware and Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks

Hacking is a form of intrusion targeted at computers, including mobile phones and personal tablet devices. It is the unauthorised use of, or access into, computers or networks by exploiting identified security vulnerabilities. Hacking can be used to:

- Gather personal data or information of use to criminals, deface or hijack websites
- Deploy ransomware, rootkits, trojans, viruses, worms etc.
- Launch DoS or DDoS attacks

Denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Distributed denial-of-service (DDoS) is where the attack source is more than one, and often thousands of, unique IP addresses. A common method is to flood an internet server with so many requests that they are unable to respond quickly enough. This can overload servers causing them to freeze or crash, making websites and web-based services unavailable to users.

- **Ransomware** is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption.
- A **rootkit** allows someone to maintain command and control over a computer without the computer user/owner knowing about it. Once a rootkit has been installed, the controller of the rootkit can remotely execute files and change system configurations on the host machine.
- A **Trojan** Horse Virus is a type of malware that downloads onto a computer disguised as a legitimate program.
- A computer **virus** is a piece of code that can copy itself and typically has a detrimental effect, such as corrupting the system or destroying data and is similar to a computer **worm**.

Cybercrime investigations

Notable cybercrime Investigations (PURSUE)

In 2022/23 the unit investigated over 140 cyber-dependant Action Fraud referrals. All of these were investigated, and all victims received robust cyber-PROTECT advice to prevent them becoming repeat victims. These offences ranged from social media account compromises to multimillion pound businesses who had fallen foul of ransomware attacks, exfiltration of customer data and later blackmail. Often, these complex investigations are linked to Russian speaking cyber-threat actors who are operating in regions outside of the UK. Many of these investigations are complex and protracted in nature, with these incidents not officially known to limit reputational damage.

In November 2022, Europol announced the arrest of a Russian national linked to 'LockBit' ransomware attacks targeting critical infrastructure organisations and high-profile companies worldwide, one victim of which was a North Yorkshire based company who had paid £73,000 (6 Bitcoin) in ransom demands back in November 2020. The suspect was arrested in Ontario, Canada, following an investigation led by the French National Gendarmerie with the help of Europol's European Cybercrime Centre (EC3), the FBI, and the Canadian Royal Canadian Mounted Police (RCMP). NYP are currently liaising with the RCMP via the Northeast Regional Cybercrime Unit for the North Yorkshire victim to receive recompense from the seized cryptocurrency assets.

In February 2022, acting on information from the National Cybercrime Security Centre, officers were deployed to an agricultural distribution business (with an annual turnover of over £35,000,000) and provided first line cyber incident support, which prevented ransomware from being deployed and the business network becoming encrypted. This investigation is still ongoing.

Community work

Cyber Safeguarding & Community Event Engagement (PROTECT/PREPARE)

From December 2022 through to February 2023, cybercrime officers have been active across the county providing the latest advice from the National Cyber Security Centre to members of the public on how to PROTECT themselves online to ensure they do not become a victim of cybercrime.

Events have taken place in Scarborough, Malton, Whitby, York, Harrogate, Ripon, Skipton and Northallerton, with specialist cybercrime officers, giving the equivalent of 300 policing hours interacting with over 1500 members of the public.

Cybercrime officers also took this opportunity to visit many local independent small-medium sized high street businesses offering advice on how these organisations could plan for and how to recovery from a cyber-incident.

Other activities carried out in 2022/23 include bespoke presentations about cybercrime to Dementia Forward, Children's Family Services, Age UK Scarborough, Carers Plus, Harrogate Over 50's Forum, Barclays Bank & Northallerton Library Drop-In Sessions, Biz Group 66, Heworth Parish Council, Fifties and Thereabouts (York), Swainby & Potto Women's Institute, and supporting Humberside Tech Week.

Additionally, Cybercrime officers have delivered several sessions to NYP Police Constable Degree Apprenticeship student officers as part of their initial training to upskill them in digital investigation methods and scene considerations.

Working with businesses

Cyber Business Engagement (PROTECT/PREPARE)

In 2022, NYP invested in three Cyber Escape Room kits and have since delivered training to multiple businesses across North Yorkshire. This escape room offers a fun, interactive cyber-security exercise to teach staff good online security behaviours though a variety of problem-solving tasks. The escape room covers important topics, such as:

- phishing
- data leakage
- creating strong passwords

Teams compete to escape in the quickest time. Once everyone has escaped and the winner is declared, we explain each topic covered and how it affects the business's cyber security. This has been very well received and all businesses are now being offered this training post incident, as well ongoing work to reach out to businesses to increase staff awareness and build cyber-resilience.

Phishing is when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website.

Regional work

Work with Yorkshire & Humber Regional Cybercrime Unit (PREVENT)

North Yorkshire Police are currently working with the Regional Cybercrime Unit to deliver the Cyber SwitchUp 2023 event. This is a digital & cyber skills competition aimed at young people aged 11-16 years in Key Stages 3 & 4 who are attending schools in the Yorkshire & Humber region.

This event aims to showcase the digital, cyber skills and talent of young people across the region, educate and promote digital and cyber pathways for higher education, raise awareness of the diverse digital & cyber career pathways available to young people and promote 'Cyber Choices' messaging – encouraging positive and lawful cyber behaviours in young people.

Online registration began on the 27th of January 2023, with qualifiers running from 24th to 30th April 2023. This is followed by an in-person finals event which will be hosted in Harrogate on the 8th of August supported by cybercrime officers from across the whole Yorkshire & Humber region.

North-East Business Resilience Centre (NEBRC)

Established In November 2019 the North-East Business Resilience Centre (nebrcentre.co.uk) was the first of a network of resilience centres across the UK which are innovative Police led initiatives creating a unique Nexus between law enforcement, corporate business, and academia. Through the matching of private sector contributions, providing affordable membership options and the delivery of affordable cyber resilience services using the student talent pipeline the NEBRC will work towards a position of self-sustainability by 2026. As the NEBRC is a not-for-profit organisation led by the police it is trusted implicitly.

The NEBRC will raise cyber resilience across the Northeast of England and support the environment for economic development post pandemic, with a particular focus on micro businesses and Small to Medium size enterprises (SMEs) and third sector organisations, leaving .gov to the Protect network. The NEBRC is all about local neighbourhood policing in that it offers crime prevention to a section of the community previously not catered for nor encouraged to report crime, with only 10% traditionally captured as recorded crime.

Most businesses in the NE are micro (less than 9) and there are 468,000. There are 1460 members and NEBRC seeks to expand to 2% of market within 3 years (11,360). Many businesses suffered and closed over the pandemic- Yorkshire and Humber saw the smallest decrease in England and Wales over the pandemic compared to the UK and the (North) Northeast saw the largest decrease.

There is still more that organisations can do to protect themselves from cyber risks. For example, board-level involvement in cyber security, monitoring suppliers and planning incident response. The cyber security breaches survey reports that just over a third of businesses (35%) and three in ten charities (30%) have a board member or trustee with specific responsibility for cyber security. For businesses, this is higher than in 2018 (when it was 30%), but the proportion remains low overall. Moreover, the qualitative findings suggest that embedding knowledge and understanding of cyber security within management boards is a strong driver of behaviour change. The NEBRC is actively embedding this within the region.

Around one in five businesses (18%) and one in seven charities (14%) require their suppliers to adhere to any cyber security standards. Some had simply not considered suppliers as a potential source of cyber risk before, while some others simply did not consider their suppliers' cyber security to be their responsibility. Very few organisations (16% of businesses and 11% of charities) have formal cyber security incident management processes in place. For businesses, this is somewhat higher than in 2018 (when it was 13%), although again the proportion is still low overall.

Qualitative evidence suggests that organisations do not recognise a need to seek this information out for themselves. There are key influencer groups that organisations often expect to receive guidance from, such as their external cyber security providers, trade associations and regulators. As such, there is a role for the NEBRC in pushing out Government guidance, capitalising on the higher engagement in cyber security brought about by General Data Protection Regulations (GDPR). The Memorandum of Understanding (MOU) between the National Police Chiefs Council (NPCC) and the National Cyber Security Centre (NCSC) will facilitate the flow of guidance. The NEBRC provides affordable services, made affordable through our innovative talent pipeline made up of the best student ethical hackers from local universities.

The NEBRC has 2 Directors registered at Companies house one of which is the CEO running the company daily. Both are senior police officers with one being the regional Senior Responsible Officer (SRO) for Cyber.

The CEO delegates Student Services and Business Development to the 2 attached Detective Inspectors who will line manage staff in their portfolio namely: Client Relations Manager, Business Admin Assistant and Senior Student Supervisor. An external PR company, MK is employed for strategic marketing advice and press and media coverage. Internal Digital media is provided by NEBRC staff with occasional strategic input from MK. Accountancy services are outsourced to a local accountant, Q accountants. They handle payroll, tax returns and VAT issues leaving the transactional matters with the NEBRC. All HO (Home Office) support is drawn down from a local police force at the direction of the cyber-SRO for the Region. The NEBRC may also access paid consultancy services from the National Programme in respect of Student Services Senior role, legal advice, strategic review, as well as commercial growth. The board currently has 7 paying board members, the NEBRC will continue to seek further members in manufacturing, online retail, and agriculture.

The NEBRC has a robust approach to management with a regular meeting structure and reporting lines which ensure that the company interests are foremost and has won awards for Outstanding Cyber security Initiative and Outstanding Cyber Security Partnership at the Outstanding Security Performance Awards (OSPAs) in 2021 along with the National Cyber Award for Cyber Policing team of the Year in 2022. The CEO also won Highly Commended for Cyber Citizen of the year and Cyber Individual of the year also at the National Cyber Awards 2022.

The NEBRC offers clients core free membership which will include a newsletter, email alerts, general NCSC Guidance broken down into accessible and digestible easy bite size topics and invitations to events along with regular contact. In addition, clients may purchase support bundles which contain affordable cyber security services and help fuel the talent pipeline in the region by utilising current specially selected students.

Student cyber security consultant services are offered to small and medium enterprises with no more than 250 employees or third sector organisations who would ordinarily struggle with expenditure in this matter. The NEBRC appeals to a variety of audiences- neuro diverse, non-technical owners, CEO's, MD's, CISO, IT suppliers and enterprise companies and helps them understand the topic of security so that they do not disengage when they hit a 'brick wall' of understanding.

Educational content used to guide clients comes from the NCSC in forms of toolkits and resources and all client services are overseen by Detective Inspector Student services and the Student Services Supervisor in conjunction with paid consultancy available from the NPCC.

The NEBRC intends to help deliver the National Cyber security Strategy by setting out five strands:

- Growing the membership of the NEBRC by 2% a measured percentage of all SMEs in the NE.
- Developing revenue streams to achieve self-sustainability by 2026.
- Maximising current revenue schemes and grants.
- Improving connection with existing members through measured customer experience and engagement performance.
- Growing student services by links to Sheffield Hallam and Northumbria Universities and to the National cyber volunteers and specials programme in each Force to maintain a capability in each Force area.
- Accessing NCRCG (national support company established to support the network) and its income stream, also providing intelligence from the region to the National steering group.

Work of the Commissioner and OPFCC (Office of the Police, Fire and Crime Commissioner)

The Commissioner fully supports the work of the NEBRC has attended engagement events in relation to Cybercrime and Fraud. These include; Engage with Chamber of Trade to promote this work, attended a workshop with the National Crime Agency on Cybercrime and Fraud and networked with NEBRC and looks forward to collaborating with them to support delivery of their exceptional services to a wider range of business across North Yorkshire and York. The Commissioner is aware of some complaints raised to the OPFCC in relation to Action Fraud and is planning to take some of these concerns forward.

The Commissioner has had personal experience of cybercrime and fraud through a close family member and recognises the impact cybercrime and fraud has on the communities on North Yorkshire and York. and will hold a Public Accountability Meeting during 2023 with a specific focus on this topic.