POLICE SCOTLAND

Author/Contact	**Assistant Chief Constable Stuart Houston**	Department / Unit	**Organised Crime, Counter Terrorism and Intelligence**
Date Created	**7th May 2025**	Telephone	
Attachments			

Criminal Justice Committee – 14th May 2025
Cybercrime in Scotland

Purpose

1. The purpose of this briefing paper is to provide the Criminal Justice Committee with an overview of how Police Scotland and key justice sector partners are working to protect people and businesses in Scotland from the latest cybercrime threats.

Background

2.1 The evolution and proliferation of Cybercrime has brought challenges to Police Scotland and Law enforcement globally. Policing is historically geographical, criminality in the digital age has broken the geographical ties and boundaries and we are faced with rapidly evolving technologies reducing the barriers and borders to cybercrime. Cyber dependent and cyber enabled crime have allowed cyber criminals to target the people of Scotland through sophisticated enterprises while increasing the complexity of identifying suspects and progressing criminal justice outcomes.

2.2 Police Scotland have consulted far and wide with law enforcement partners and are responsive to the changing threat landscape. Police Scotland understand that an agile and comprehensive approach to cybercrime is required through proactive investigations, preventing crime and protecting victims is key to mitigating this emerging threat. Police Scotland have decided to create a resolute Cyber and Fraud unit to address this and to evolve and develop new capabilities to support victims and tackle crime in the digital age.

2.3 In April 2025 Police Scotland brought together the departments of Cybercrime, Serious and Organised Crime Financial Intelligence Unit (SOC FIU), Cyber Harm Prevention (CHP) and the Policing in a Digital World Programme (PDWP) under a new Detective Chief Superintendent. This is the first step in an evolution process to improve our response to cyber and financial crime.

2.4 The Cybercrime threat spans different contexts, and covers a wide range of online criminal activity, from scamming and phishing through to sophisticated attacks against financial institutions and other large organisations. The cyber security threat that most of the British public are likely to experience is low sophistication cybercrime; cyber criminals often deploy commodity attacks, such as malware, with the aim of defrauding the public and businesses for financial gain.

2.5 Cyber-attacks, online child sexual exploitation, and online fraud, are complex crimes and manifest in diverse methodologies. Cybercrimes have a broad reach and inflict severe harm on individuals, public and private organisations, and a countries economy and security. Cyber criminals are agile and opportunistic with offenders showing elevated levels of adaptability to modern technologies and societal developments, whilst constantly enhancing cooperation and specialisation.

2.6 Most of the serious cyber-attacks have traditionally been carried out by Organised Crime Groups (OCGs), which comprise highly organised criminals operating much like a legitimate business, however, there is also a number of smaller, less-organised criminal groups and criminal micro-services trading on illicit forums and marketplaces, all supporting each other.

2.7 In 2020 Police Scotland recorded 7710 cybercrimes, this has risen rapidly year on year and figures recorded in 2024 recorded 18280 cybercrimes reported in Scotland.

Cybercrime Impact

3.1 Person – We continue to see the rise in crimes against the person utilising technology from Sextortion and CSAM (Child sex abuse material). Recently we have seen trends evolve from sexualised content being extorted to physical harm with online groups exploiting vulnerable individuals online to self-harm and share the content.

3.2 Business – Police Scotland receive approximately 300 reports per year of Cyber dependent crimes, mostly against business in the way of Ransomware, Distributed Denial of Service (DDOS) and network intrusions. These are exclusively dealt with by our Cyber Investigations department.

3.3 The impact to business can be significant approx. 40-50 Ransomwares are reported annually, while criminal justice outcomes are rare, they do happen through international collaboration.

3.4 However, Police Scotland prioritise victim support to advise victims how to recover and minimise the impact to their business whilst encouraging shared learning and coordination with partners.

Response

4.1 To improve and deliver new capabilities Police Scotland are developing the new Cyber and Fraud Unit in line with the UK national 4 P approach. Cybercrime Investigations already form part of Team Cyber UK (UK approach to mitigating the threat) which follows this approach.

4.2 Aligning with this approach across the new unit will ensure it remains focused and is better aligned and coordinated with the other UK and international law enforcement agencies.

4.3 Due to the borderless nature of Cybercrime networks this approach is key to ensure Scottish, UK and international law enforcement agencies are aligned and collaborating to tackle the increasing and emerging threats from cyber dependent and cyber enabled crimes.

4.4 Technology plays ever increasing roles in all our lives and criminals are keen to exploit this to pursue criminality for financial gain or cause harm in crimes committed against the person (CSAM, Sextortion Etc). Police Scotland has and will continue to implement new capabilities to improve our response to Cybercrime and Fraud and protect the citizens of Scotland.

Partnerships

5.1 Police Scotland has identified and developed strong working relationships with several organisations across the cyber landscape in terms of law enforcement, public, private and third sector partners. Police Scotland regularly engage in national collaborations with the National Cyber Security Centre (NCSC), CoLP, and Regional Organised Crime Units (ROCU).

5.2 The following partners are also key to developing the Police Scotland response:

5.3 **National Crime Agency**

As Scotland currently falls outside of the Action Fraud reporting structure, cyber and fraud offences that occur within Scotland are reported directly to Police Scotland. NCCU Triage Incident Coordination and Taskings team (TICAT) support the devolved structures through regular tasking of cyber incidents to Police Scotland as part of Team Cyber UK (TCUK).

NCCU Prevent are supporting the Police Scotland Cybercrime Harm Prevention Team with their work to deliver the Cyber Choices programme in Scotland with a potential delivery date of 2026. Police Scotland are currently an active part of the UK Cybercrime Prevention Network along with the other ROCUs.

5.4 **Cyber Scotland Partnership (CSP)**

CSP is a collaborative leadership approach to focus efforts on improving cyber resilience across Scotland. Police Scotland continue to work with the Big Partnership, who led on communication deliverables, and other members of the CSP to ensure current initiatives and relevant prevention advice is made available for dissemination across the partnership’s networks. CHP are leading on this nationwide partnership of strategic bodies, brought together to promote cyber resilience to global organisations based in Scotland.

5.5 **Scottish Cyber Coordination Centre (SC3)**

Following on from several significant cyber-attacks on Scottish Public Sector organisations, Ministers announced that as a matter of urgency they were bringing forward proposals for the establishment of a recognised, authoritative, and collaborative function to combat the accelerating cyber threat. The Scottish Cyber Coordination Centre (SC3) was established to meet this requirement and address key cyber resilience challenges facing Scotland.

Significant ransomware attacks have occurred with companies in possession of policing data suffering large scale data breaches, resulting in private information pertaining to victims of crime, suspects and other members of the public being published on the dark web.

For this reason, Police Scotland have been working collaboratively with the CoLP and NPCC to explore how to further forge closer links and collaboration and are now integrated into the UK 24/7 CSI Gold Chief Officer Cadre as part of Operation DA1 (Defend as One).

The benefits of such an approach include efficient working arrangements between law enforcement agencies, early identification, and response to emerging threats. In addition, as an organisation it will enable us to be confident, capable, and resilient in the fast-moving digital world.

5.6 **Cyber and Fraud Centre**

Police Scotland continue to work closely with the cyber and fraud centre. Relationships made and maintained as we develop our Cyber and fraud unit will be key to developing capabilities and increasing awareness to prevent fraud and cybercrime going forward. As the cyber and fraud unit within police Scotland evolves, we envisage stronger partnership relations being key to our coordination of fraud and cybercrime.

Conclusion

6.1 Police Scotland is improving its capability to deal with ever evolving crime types and technology. Police Scotland recognise the need to continue to improve and enhance our service to the people of Scotland. The establishment of the Cyber and Fraud unit is the first large step which will allow us to improve our service and protect the people of Scotland. As the second largest force in the United Kingdom, Police Scotland understands the challenges and will invest with the help of stakeholders to identify and introduce the correct provisions to deliver against our goals and the 2030 vision of safer communities, less crime and supporting victims.