Criminal Justice Committee
Wednesday 14 May 2025
15th Meeting, 2025 (Session 6)

Challenges facing Business and Vulnerable Individuals in Scotland from Cybercrime

Note by the Clerk

Introduction

1. On 14 May, the Criminal Justice Committee will undertake an evidence session with witnesses on the challenges facing businesses and vulnerable individuals in Scotland from the risks of cybercrime.

2. While this topic can cover a variety of areas, it should be noted that the focus of this session will **not** cover elements of child exploitation, which is an area that received substantial debate in the public realm.

3. The aim of the session is to inform parliamentary debate on the impact of cybercrime in areas which receive less debate in the public realm. For example, the impact on the lives of on individuals like the elderly, as those in employment and the wellbeing of the business community across Scotland.

4. The session will also consider how authorities in Scotland coordinate with key partners across the UK and internationally, with the aim of-

   - Gaining an oversight of how sophisticated cybercrimes have become today, and what are we likely to face in the coming years?

   - Discussing how policing/law enforcement bodies prioritise their response to cybercrimes?

   - Considering whether policing bodies have the tools and resources necessary to properly investigate cybercrimes reported to them?

   - Considering whether laws on cybercrime are keeping pace with developments?

   - Looking at how key justice sector/business/civil society partners are working to try to help protect people and businesses in Scotland from the latest cybercrime threats?

- Considering what actions, if any, the Committee could take to help support key policing/justice sector/business/civil society partners in combatting cybercrime.

Background

5. The following background information is taken from the SPICe Members briefing note on cybercrime.

6. The Scottish Government note that "defining cyber-crime is complex, with no agreed upon definition of the term".

7. This complexity arises from the fact that there is a debate around the extent to which cyber technology needs to be involved for the crime to be termed a 'cyber-crime'.

8. For the purposes of recorded crime (as defined in the Scottish Crime Recording Standard), a broad definition of cyber-crime is adopted that includes crimes in which cyber technology is in any way involved. This therefore includes the following types of crime:

    - Cyber-dependent crimes – where a digital system, infrastructure or Information and Communication Technology (ICT) device is the target or the principal or sole method of attack (e.g. spreading computer viruses, Distributed Denial of Service or hacking)

    - Cyber-enabled crimes – 'traditional' crimes where the internet has been used as means to commit the crime (e.g. online fraud, abuse or sexual crime).

9. This evidence session will consider both cyber-dependent and cyber-enabled crimes.

Data on cyber-crime in Scotland

10. The following data on cybercrime in Scotland has been provided by SPICe in its briefing note for Members and is reproduced here to aid the Committee's public evidence taking session.

11. The Scottish Government's Recorded Crime in Scotland, 2022-23 publication contains estimates of the levels of cyber-crimes committed in Scotland. Given that some cyber-crimes are 'traditional' crimes where the internet has been used as a means to commit the crime, they will not have specific crime codes.

12. Therefore, the estimates provided are based on a review of a random sample of crime records across Scotland for the types of crime that could, in theory, involve a cyber-element. The review considered which proportion, by crime type, actually were cyber-crimes in 2022-23.

13. Obviously, this analysis is based on a sample of police records therefore it does not provide information on the characteristics of all the cyber-crime committed in Scotland, as not all of these crimes will be reported to the police, for varying reasons.

14. The table below outlines the increase in the estimated number of cyber-crimes from prior to the Covid-19 pandemic.

Table: Estimated number of cyber-crimes in Scotland

Year	Estimated number of cyber-crimes
2022-23	14,890
2021-22	14,860
2020-21	14,280
2019-20	7,710

15. In 2022-23, it is estimated that at least 5% of the crimes recorded by Police Scotland were cyber-crimes. This includes an estimated 26% of sexual crimes, 8% of crimes of dishonesty, 3% of non-sexual crimes of violence and less than 1% of damage and reckless behaviour.

16. Cyber-crimes within the non-sexual crimes of violence category included crimes of threats and extortion, stalking and those recorded under the Domestic Abuse (Scotland) Act 2018.

17. Most of the estimated 1,830 crimes of threats and extortion were cyber-crimes and most of these cases relate to ‘sextortion’, where the perpetrator threatens to reveal evidence of the victim’s online sexual activity unless they receive some form of monetary payment.

18. In terms of the types of cyber-crime being considered in today’s evidence session, these will generally come under crimes of dishonestly, and they predominantly cover fraud.

19. Around half (51%) of the 8,520 recorded frauds were estimated to have been cyber-crimes. This has doubled from 3,450 in 2019-20. Just over a third (37%) of the records examined showed that the location of the perpetrator of a fraud cyber-crime was unknown, with a further third (32%) suspected or confirmed to be located outside of Scotland.

Today’s evidence on the Bill

20. At the meeting on 14 May, the Committee will hold an oral evidence session with-

- **Adam Stachura**, Associate Director of Policy, Communications and External Affairs, Age Scotland
- **David Keenan**, Chief Information Officer, Arnold Clark

- **Jude McCorry**, Chief Executive, Cyber and Fraud Centre – Scotland
- **Nicola Taylor**, Partnership Member, CyberScotland Partnership
- **Miles Bonfield**, Deputy Director, National Crime Agency
- **Chris Ulliott**, Head of Cyber Security, NatWest Bank
- **Assistant Chief Constable Stuart Houston**, Organised Crime and Counter Terrorism Intelligence, Police Scotland.

Written material

21. The annex to this paper contains written submissions which some of the witnesses have provided in advance of the evidence session today.

Clerks to the Committee
May 2025

ANNEX – WRITTEN SUBMISSIONS FROM WITNESSES

CYBER AND FRAUD CENTRE SCOTLAND (for businesses) and the Cyber and Fraud Hub (for Individuals)

www.cyberfraudcentre.com – supports organisations

www.cyberfraudhub.org – supports individuals.

Written Submission to Parliamentary session on Cyber Crime in Scotland

The Cyber and Fraud Centre – Scotland rebranded from the Scottish Business Resilience Centre in response to the growing threat of cyber and fraud. As Scotland's only cyber security social enterprise, our mission is to deliver accessible, affordable, and relevant services, focusing on the human side of security and victim support.

With a small team of 12, we support organisations across Scotland through incident response, training, services and community engagement. We are entirely self-funded and receive no direct funding from Scottish Government or any other agency. Generating £1m annually and reinvesting surplus to support the Cyber and Fraud Hub, which aids individuals and families affected by fraud.

We have supported organisations like SEPA, Western Isles, SAMH, Arnold Clark and Scullion law during their Cyber-attacks.

To support the Victims of the cyber attacks with a number of trusted Scottish technical and legal incident response organisation's, who go above and beyond for the victims.

Key Achievements (Past 5 years)

- Delivered NCSC 'Exercise in a Box' sessions to 2,500+ organisations, including those on Scottish remote islands.
- Trained 1,000+ business leaders via our Cyber Executive Education Program days.
- Provided free cyber training and services to small business and charities and guides for parents and older adults.
- Over 800 calls on our Incident Response line - In the last 12 months alone, we have received over 400 calls on our IR line across diverse cybercrimes including ransomware and business email compromise and other scams.

We had a huge increase in calls from individuals in relation to individual victims of fraud, so had to look at how we handled these, including a multimillion gold investment scam on an elderly lady in Scotland.

We spoke to Eddie Hawthorne from Arnold Clark, who also wanted to do something to support victims of cyber and fraud, about the idea of setting up a charity to support individuals working in partnership with the banks and policing, and he agreed to fund a charity for two years during startup phase. We set up the charity – The Cyber and Fraud Hub

Cyber and Fraud Hub Impact in year 1.

- Supported 280+ individuals
- Actively working on cases worth over £9.5m, including scams targeting vulnerable elderly victims, we have recovered or prevented nearly 800k of fraud too.

Key Challenges and Trends

Fraud is growing at a phenomenal rate; and we are only seeing the reported figures. People are reluctant to report fraud crimes because of the shame they feel and because they have been so badly affected, they then don't know who to trust.

Also, when we do support victims, they are reluctant to tell their stories for fear of retribution or people thinking they were 'stupid' – so the stories go untold, and it is difficult for people to understand the real threats.
Other areas of note:

- Ransomware remains a growing threat, cyber-attack incidents like SEPA and Arnold Clark highlighted gaps in coordinated support during holiday periods, and over the last few weeks we have seen large retail organisaiton's impacted which in turn has now impacted residents in our remote island communities.
  Additionally:

  - There is still a feeling that 'it will never happen to me'. The hardest part of our job is to get individuals and organisation's to spend the time making themselves more resilient and preparing for an incident.

  - In Scotland, there is a real community effort around the 'good people' in cyber to pull together to help the victim in times of crisis, we have seen this on all the high profile attacks, but we do have a concern around capacity across the organisations and agencies if we had 2-3 high profile attacks at the same time, which is a huge possibility. (we have seen this with the 3 large retailers attack down south over the last few weeks)

  - We have a dependence around threat intelligence from private organisations and also law enforcement outside of Scotland – who are now under budgetary pressure or geo-political changes and challenges to keep supporting their own entities. We may not receive the same level of support going forward as we did historically.

- AI and data tools will likely enhance attacker capabilities. Cyber should be underpinning all our efforts around growing the economy and should be part of AI and start up investments, we are generating more and more data and complex modelling and IP, but we are not doing enough if sometimes anything to protect it.

- We are not investing enough in proactive areas to prevent cybercrime, or around innovation and Cyber and Fraud seems to be a forgotten entity.

- Smaller organisations see cyber security as too expensive, but there are lots of things organisations can do to make themselves more resilient in a cost-effective way, and we want to continue our work as a social enterprise to ensure that they do this – and by doing this we are making Scotland more secure.

- We need to learn from the past few years of Cyber attacks and build a more secure future

Policy Considerations

- Greater investment is needed in proactive cyber prevention and innovation.

- Laws around stolen data sharing should be modernised. Data taken or shared from the dark web after a cyber-attack **is** stolen data. The sharing or distribution of it should be a criminal offence. We also need to look at how we can arrange injunctions against the sharing of data across countries and jurisdictions.

- I know this is outside the remit of the Scottish Justice System, but we really need to raise this conversation and ensure our laws are in line with the way technology and crime exists

- Proceeds of crime should help fund prevention and victim support. Scotland have made some significant seizures around proceeds of crime, but this money is not going back into policing in Scotland or into organisation's like ours to help prevent the crime. Proceeds of Crime can be used by Police Forces down south.

- Cryptocurrency scams are a growing concern for us all, and we need to invest in very expensive technology, training and licensing to be able to look at this, disrupt the criminals, provide evidence and get arrests. We don't have a budget for this in Scotland and this is heavily invested in other law enforcement agencies down south.

- Elderly victims are particularly vulnerable. Systems must be more accessible and supportive. We created a dedicated resource to support information sharing, which is freely available - A Guide to Avoiding Fraud and Scams for Older People — CyberandFraudHub.

Call for Collaboration, ownership and funding.

At Cyber UK this week in Manchester – Richard Horne the CEO of NCSC has said that "Britain's intelligence services are seeing a "direct connection between Russian Cyber attacks and physical threats to our security" Malign actors in Moscow are "waging acts of sabotage, often using criminal proxies in their plots, he also said that domestic security service MI5 were seeing the hacking threat from Russia manifesting "on the streets of the UK against our industries and our business, putting lives, critical services and infrastructure and national security at risk"

He told the CYBERUK audience that the role of the information security community was not just about protecting systems, it's about protecting our people, our economy and our society from harm"

Scotland will not be immune to these threats, and we should see them as very real, we need to see cyber security as an inclusive movement with international collaboration to protect our nation.

Cyber and fraud prevention in Scotland benefits from strong collaboration across policing and other law enforcement government and industry. This co-operation is unique and worth celebrating but needs continued support, ownership and investment to thrive. We can all do much more to prevent and protect and stand out even more as a nation around the good things we are already doing. Cyber and Fraud Centre and the hub will continue to work alongside key partners and stakeholders to continue to support organisations and individuals.

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.