Published 12 December 2025
SP Paper 933
12th Report, 2025 (Session 6)

The Scottish Parliament
Pàrlamaid na h-Alba

Criminal Justice Committee

Cybercrime and cyber-security in Scotland

Published in Scotland by the Scottish Parliamentary Corporate Body.

All documents are available on the Scottish Parliament website at:
https://www.parliament.scot/documents

For information on the Scottish Parliament contact Public Information on:
Telephone: 0131 348 5000
Textphone: 0800 092 7100
Email: sp.info@parliament.scot

Contents

Criminal Justice Committee

To consider and report on matters relating to criminal justice falling within the responsibility of the Cabinet Secretary for Justice and Home Affairs, and functions of the Lord Advocate other than as head of the systems of criminal prosecution and investigation of deaths in Scotland.

justice.committee@parliament.scot

0131 348 5973

Committee Membership

Convener
Audrey Nicoll
Scottish National Party

Deputy Convener
Liam Kerr
Scottish Conservative and Unionist Party

Katy Clark
Scottish Labour

Sharon Dowey
Scottish Conservative and Unionist Party

Jamie Hepburn
Scottish National Party

Fulton MacGregor
Scottish National Party

Rona Mackay
Scottish National Party

Pauline McNeill
Scottish Labour

INTRODUCTION

1. During 2025, the Criminal Justice Committee undertook scrutiny of the challenges facing businesses and vulnerable individuals in Scotland from the risks of cybercrime.

2. The focus of this work was to help inform parliamentary debate and raise awareness of the impact of cybercrime and cyber-security.

3. For example, the impact on particular individuals such as the elderly, as well as the impact on those in employment and the wider business community across Scotland. The focus of our work did not cover elements of child exploitation, as that is an area that has already received substantial debate in the public and parliamentary realm.

4. The Committee scrutiny aimed at considering 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 we are 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, and
    - Looking at how key justice sector, business, and civil society partners are working to try to help protect people and businesses in Scotland from the latest cybercrime threats.

DATA ON CYBER-CRIME IN SCOTLAND

2024/25 Crime Statistics

5. The following data on cybercrime in Scotland has been provided by SPICe in its briefing note for Members of the Committee and is reproduced here to aid debate on the issue.

6. The Scottish Government's Recorded Crime in Scotland, 2024-25 publication contains estimates of the levels of cybercrimes committed in Scotland. Given that some cybercrimes are 'traditional' crimes where the internet has been used as a means to commit the crime, they will not have specific crime codes.

7. 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 cybercrimes in 2024/25.

8. Obviously, this analysis is based on a sample of police records and 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.

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

Police recorded cyber-crime in ScotlandRecorded Crime in Scotland, 2024-25, Accredited Official Statistics, Scottish Government (June 2025)

Table: Estimated number of cyber-crimes in Scotland

Year	Estimated number of cyber-crimes
2024-25	14,120
2023-24	16,890
2022-23	14,890
2021-22	14,860
2020-21	14,280
2019-20	7,710

Source: *Recorded Crime in Scotland, 2024-25 (Scottish Government - June 2025)*

10. According to Police Scotland, in 2024-25, an estimated 14,120 cyber-crimes were recorded in Scotland. This was a decrease of 2,770 crimes (or 16%) compared to the estimated volume for 2023-24 (16,890). However, Police Scotland state that levels also remain significantly above the pre-pandemic year of 2019-20 (7,710 cyber-crimes).

11. Police Scotland estimate that cybercrimes accounted for at least 5% of total recorded crime in 2024-25, including 27% of sexual crimes, 7% of crimes of dishonesty and 3% of non-sexual crimes of violence.[i] In 2024-25, 94% of crimes of

threats and extortion were estimated to be cybercrimes.

12. Police Scotland state that much of the increase in fraud since 2015-16 has related to cybercrimes, which are estimated to account for around half of all frauds (49%) in 2024-25. The estimated proportion of fraud identified as cyber-enabled increased significantly after the Covid-19 pandemic and has remained higher than pre-pandemic levels. [ii]

---

[i] Cybercrimes 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

[ii] Recorded Crime in Scotland, 2024-25, Accredited Official Statistics, Scottish Government (June 2025) (page 2 and page 13)

EVIDENCE TAKING

Written Evidence

13. Both the Cyber and Fraud Centre Scotland & Cyber and Fraud Hub and Police Scotland made written submissions to the Committee in support of their oral evidence on 14 May. Police Scotland also provided supplementary written evidence on gender data on cyber-based sextortion crimes.

14. Subsequently, the Committee also received a written submission from the Association of British Insurers on the challenges facing businesses in tackling cybercrime.

15. In the wake of the written and oral evidence received, the Committee wrote[iii] jointly to the Cabinet Secretary for Justice and Home Affairs ('the Cabinet Secretary') and the Minister for Business and Employment setting out the Committee's observations from its evidence taking and seeking a response to various questions raised. The Cabinet Secretary responded to the Committee on 3 September 2025.

16. The Committee also wrote to the Federation of Small Businesses Scotland[iv], the Scottish Chambers of Commerce[v] and the Scottish Council of Voluntary Organisations[vi] on challenges facing businesses and vulnerable individuals in Scotland from risks of cybercrime. The Committee sought information on how resilient the small-and-medium size business community, and the charity/third sector community in Scotland are to the growing cyber risks they face.

17. The Committee received written responses from the Federation of Small Businesses Scotland, the Scottish Chambers of Commerce and the Scottish Council of Voluntary Organisations. These set out the work undertaken to date across the SME and third/voluntary sector in Scotland as part of the Scottish Government's wider cyber resilience strategy.

Oral Evidence

18. On Wednesday 14 May 2025, the Criminal Justice Committee undertook an oral evidence session on cybercrime and its impact on businesses and vulnerable

---

iii Letter from the Convener of the Criminal Justice Committee to the Cabinet Secretary for Justice and Home Affairs and the Minister for Business and Employment on cybercrime (26 June 2025)

iv Letter from the Convener of the Criminal Justice Committee to the Federation of Small Businesses Scotland (26 June 2025)

v Letter from the Convener of the Criminal Justice Committee to the Scottish Chambers of Commerce (26 June 2025)

vi Letter from the Convener of the Criminal Justice Committee to the Scottish Council of Voluntary Organisations (26 June 2025)

individuals in Scotland.

19. The Committee heard from-

- Adam Stachura, Associate Director of Policy, Communications and External Affairs at Age Scotland
- David Keenan, Chief Information Officer with Arnold Clark
- Jude McCorry, Chief Executive of the Cyber and Fraud Centre Scotland
- Nicola Taylor, Partnership Member of the CyberScotland Partnership
- Miles Bonfield, Deputy Director of the National Crime Agency
- Chris Ulliott, Head of Cyber Security at NatWest Bank, and
- Assistant Chief Constable Stuart Houston, Head of Organised Crime and Counter Terrorism Intelligence at Police Scotland.

20. The Official Report of the evidence session on 14 May is available online.

21. Several of the witnesses set out the scale of the challenge facing business and vulnerable individuals from cyber risks. Chris Ulliott, Head of Cyber Security at NatWest Bank told us about the size of the challenge the banking sector faces. He said-

> As a big bank in the UK, we are targeted all the time. Some facts and data can perhaps give a sense of scale. As a bank, we analyse every single email that enters our estate, and we process it, looking for malicious content. We block about a third of the emails— which is millions a month—because they are believed to be the start of an attack against our staff. Looking outside our network at the attacks that are probing our estate, we average about 100 million attacks per month that try to break past the organisation's defences. As a result, we have to make a huge on-going investment. I am very fortunate in that our bank has resources that I can use to defend against those attacks. Hundreds of people, with costs of millions of pounds per year, are defending the bank and our customers' money. I am very alive to the fact that, when I look to my customers and other organisations across Scotland, they cannot make that scale of investment. That is the scale of the problem that we are trying to handle and manage.[vii]

22. Speaking about the challenges of investigating cybercrime and the complex nature of the crime, Assistant Chief Constable Stuart Houston of Police Scotland told us-

---

vii Criminal Justice Committee, Official Report 14 May 2025, (Col 6).

> ...these crimes are often borderless and are, on occasion, perpetrated outwith the UK. We have had cases of denial-of-service attacks that have been orchestrated by individuals within Scotland. Someone was convicted of that as recently as last year. Quite often, a network of people are involved in the larger ransomware attacks. In the past, organised crime groups would operate in networks of people who knew one another, but we need to be alive to the fact that people now often operate in networks where they have only seen someone through a screen.[viii]

23. ACC Houston went on to explain that the action the police take "is often to gather the threat intelligence and to find out the weaknesses in systems". Police look to "push out a prevention message" in response to various current forms of cyberattacks "to ensure that vulnerable people are not being taken in by anything that is happening or exploited in any way". He explained that the police are " there to investigate that and to get an outcome, but a big part of that involves helping businesses to recover" from cyberattacks.[ix]

24. David Keenan, Chief Information Officer with Arnold Clark, spoke to the Committee of the impact a major cyber-attack had on the business in December 2022. This took the form of a ransomware attack in which a large amount of sensitive customer and corporate/employee data was stolen. The criminals deliberately planned the timing of the attack over the Christmas period, when staffing levels in the organisation would be reduced, and thereby take longer for their staff to detect and respond to. The cyber-attack had an immediate impact on Arnold Clark customers, with Mr Keenan explaining that-

> In the days immediately after the attack on Arnold Clark, when we were unable to operate our systems for a period, more than 4,000 customers were expecting to come and make use of our services. More than 700 people who had bought a car were expecting to take delivery of that vehicle. Some 2,000 people who either had their car in for a service or had booked in to have their car serviced were unable to have that work done. We were unable to provide our rental service to more than 1,500 people who had planned to make use of it, many of whom were holidaymakers who were travelling from abroad. They expected to arrive at Glasgow or Edinburgh airport and to come to our local rental branch to collect the car that they had booked for rental. That was the direct impact on customers.[x]

25. However, the cyber-attack also had a major impact on the well-being of the staff of Arnold Clark and their ability to do their job. Mr Keenan explained how seriously Arnold Clark took cybersecurity before the attack saying that: "at the time of the incident, we had well over 200 members of staff in IT, with a multimillion-pound budget and 12 members of staff who were dedicated to cybersecurity, but that still was not enough to protect us". He pointed out that while a business of the size of Arnold Clark would not face the same ongoing scale of attack as a business the size of NatWest Bank, Mr Keenan added-

---

viii Criminal Justice Committee, Official Report 14 May 2025 (Col 5).
ix Criminal Justice Committee, Official Report 14 May 2025 (Cols 4 - 5).
x Criminal Justice Committee, Official Report 14 May 2025 (Col 5).

> What we face is not quite at that scale, but we are seeing similar things. Ultimately, a cybercriminal has to be lucky only once, but we have to be lucky against every single attack.[xi]

26. Jude McCorry, the Chief Executive of the Cyber and Fraud Centre Scotland, highlighted the value of stolen data to criminal groups. Contrasted the way the law treats the handling of stolen goods in the real world, as opposed to the handling of stolen data. Ms McCorry told us-

> If someone handles stolen physical goods, they commit a crime, but someone can share data and it can be sold from the dark web. The victim is the company that has been the subject of the cyberattack, but it is also the victim again six months or a year later, because solicitors are chasing its customers to tell them that they might have a case against the company or organisation because their data has been leaked. It is not good that people's data is out there, and another industry is thriving on that stolen data because it is not a criminal act to steal it. We need to look at things such as that.[xii]

27. Adam Stachura, Associate Director of Policy, Communications and External Affairs at Age Scotland spoke of research they had undertaken to understand how the changing shape and nature of cybercrime is impacting vulnerable groups like the elderly.

28. Initially, Age Scotland's research focused "on older people's attitudes to scamming and fraud" but recently they have begun to examine the impact cybercrime is having as it has become more prevalent. In their latest research on this issue, published in 2023, it showed that "between 2021 and 2023, there had been changes in the type of thing that people encountered" in relation to online crime. "Being targeted through email or text message was the most common method, and there will now be a lot more cases in which, because of developments in AI ... people will not be able to understand that some things are not real, as they will look very convincing". The development of AI-enhanced scams is posing a major problem and driving an increase in cyber-related crimes targeting vulnerable groups.

29. Speaking about the reaction of older people to these crimes, Mr Stachura told us that-

> The last time that [Age Scotland] undertook research on the issue, we found that about 20 per cent of people who had been a victim of a fraud-related crime did not report it. They did not know where to go to report it, they did not think that it would be taken seriously and they did not think that anything could be done. I am not sure whether 20 per cent represents a lot of people or not very many, but, in the future, we will want people to become more confident in reporting what has happened to them.[xiii]

30. The evolving nature of the threat from cybercrime was also highlighted by witnesses. The 'traditional' concept of a cyber-based theft, such as to extort money from a victim or monetise the proceeds of the theft by selling on stolen data to other

---

xi Criminal Justice Committee, Official Report 14 May 2025 (Col 5).
xii Criminal Justice Committee, Official Report 14 May 2025 (Col 12).
xiii Criminal Justice Committee, Official Report 14 May 2025 (Cols 15 - 16).

networks of criminals, is still a major risk.

31. However, the evidence we received also highlights the growing interdependence of wider society on a complex web of interconnected digital networks from the public, private and commercial sectors. Many of the services on which modern society depends, such as online banking, electronic payments, retail and food shopping, travel and remote working can all be impacted by indirect cyberattacks on a service provider, or one of their supply-chain sub-contractors.

32. We heard about the wider societal and economic harm which a cyberattack on key public or commercial organisations can have. Such disruption may also be caused by a cyberattacks on a key supply-chain sub-contractor on whose IT systems the operations of a key organisations depend. Jude McCorry of the Cyber and Fraud Centre Scotland pointed out that, as a society-

> ...we need to think about the broader destruction and damage for organisations and not just the data element. Data exfiltration is very damaging, but we should also consider the broader impact of cybersecurity attacks. In Scotland, islanders have been left without food because Co-op stores have been empty. We are coming up to the high season for tourism in Scotland, so there will be further issues when people start to visit the islands and there is no food in the stores. We also have to consider the human impact of cybersecurity.[xiv]

33. Ms McCorry also pointed to the disruption to various local authorities around Scotland as a result of cyber-attacks on their systems. Both City of Edinburgh Council[xv] and West Lothian Council[xvi] were the victims of targeted cyber-attacks in mid-2025 which impacted the delivery of key services, like data held by schools.[xvii]

34. The increasing risk of cyber-attacks on public sector organisations like local authorities was also recently highlighted in an November 2025 by the Accounts Commission for Scotland report on a cyber-attack on Comhairle nan Eilean Siar which impacted the Council in November 2023.

Scottish Government

35. The Committee did not have an opportunity to take oral evidence directly from the Scottish Government on cybercrime owing to the pressure on its work programme with regards to the Stage 1/Stage 2 consideration of various bills. However, the Committee wrote to the Cabinet Secretary on various issues arising from the evidence it had received.

36. In a written response to the Committee on 3 September, the Cabinet Secretary stated-

---

xiv Criminal Justice Committee, Official Report 14 May 2025 (Cols 3 - 4).

xv City of Edinburgh Council press release (May 2025): https://www.edinburgh.gov.uk/news/article/14204/targeted-phishing-attack-on-schools-and-early-years-network.

xvi West Lothian Council press release (July 2025) https://www.westlothian.gov.uk/article/85686/Cyber-Attack-update.

xvii Criminal Justice Committee, Official Report 14 May 2025, (Col 3).

> The Scottish Government acknowledges the increasing cyber risks, particularly as our society becomes more digitally connected. We remain committed to strengthening cyber resilience across all sectors and at a national level. This work is being advanced through strategic partnership, notably via the CyberScotland Partnership and the Scottish Cyber Coordination Centre, which serve as key levers in our coordinated endeavours and the refresh of The Strategic Framework for a Cyber Resilient Scotland. We also continue to engage closely with UK Government and the National Cyber Security Centre on reserved security matters.

37. The Cabinet Secretary went on to outline the work the Scottish Government is undertaking to refresh its Strategic Framework for a Cyber Resilient Scotland.

38. On 5 November 2025, the Scottish Government published its refreshed Cyber Resilient Scotland 2025 to 2030: strategic framework.

Evidence on cybercrime from the Committee's Pre-Budget Scrutiny 2026/27

39. As part of Pre-Budget Scrutiny in advance of the 2026/27 Scottish Budget, the Committee took written and oral evidence from numerous key stakeholders across the criminal justice sector. The Committee received 25 responses to its Pre-Budget Call for Views.

40. Various stakeholders highlighted not only the growing resource and capital funding required to investigate and prosecute cybercrime. They also pointed to the need to ensure cyber resilience as digitalisation plays an ever-growing part in how Scotland's criminal justice system operates and serves the public.

41. Police Scotland stated in their written evidence to the Committee that "looking forward, our analysis suggests AI will be increasingly used to generate images of child sexual abuse, other non-consensual sexual images and fraud and disinformation campaigns supported by “deepfake technology”, while cyber warfare will continue with significant financial implications and risk to human life".[xviii]

42. In her oral evidence to the Committee, the Chief Constable of Police Scotland, Jo Farrell told us-

> Poverty, geopolitics, cybercrime and civil unrest are driving a high level of demand, and the challenge for policing is evolving rapidly. That is illustrated by the increase in online harm and threat and in violence associated with organised crime, as well as a high level of protests. The threat is now.[xix]

43. Expanding on the issue, the Chief Constable told the Committee that "there has also been an increase in the use of cyber to commit crime, including fraud, and that has had an effect on the reach of such crime. Money laundering is on the rise, as

---

xviii Police Scotland Pre-Budget Scrutiny 20206/27 written submission to the Criminal Justice Committee.

xix Criminal Justice Committee, Official Report 5 November 2025, (Cols 25-26).

we know from our partnership work with banks, which highlight suspicious activity".[xx]

44. Other stakeholders such as the Crown Office and Procurator Fiscal Service (COPFS) and the Scottish Courts and Tribunal Service (SCTS) highlighted key technology modernisation projects such as the national roll-out of the Digital Evidence Sharing Capability (DESC) and other forensic technology projects, remote provision of evidence and body worn video camera. All of which, stakeholders told us, will require upfront capital and cybersecurity investment, as well as recurrent training costs for staff.

45. In its written evidence to the Committee, SCTS told us-

> The case management systems that underpin the work of the criminal justice system are largely unseen but absolutely critical. Developing and investing in a new system whilst maintaining the legacy system is not something SCTS is resourced for. Similar challenges exist for other justice organisations. There is an opportunity to work together – introducing newer technology that could design out many of the legacy risks and issues faced by current systems (data security, process complexity, lack of interoperability, cyber risk etc). At the same time, we have the potential to transform services, with simpler systems freeing up staff time, offering improved information sharing, analytics and more tailored public-facing services.[xxi]

46. In his oral evidence to the Committee, the Chief Executive of the SCTS, Malcolm Graham, told us that "increasing risk of cyber insecurity in the systems that [SCTS] have to continue running" requires a growing spend "to try to shore up those systems and keep them safe". He said that "it gets to a point at which the only answer is to replace those systems and build them into a network of interfacing digital justice modules that can be designed to be cyber safe for the world that we now live in". His colleague Yvette Greener, Chief Operating Officer of the STCS, added that the impact that cyber insecurity is having means it "features as one of the most serious risks on [the SCTS's] strategic risk register".[xxii]

---

xx Criminal Justice Committee, Official Report 5 November 2025, (Cols 27-28).
xxi Scottish Courts and Tribunal Service Pre-Budget Scrutiny 2026/27 written submission to the Criminal Justice Committee.
xxii Criminal Justice Committee, Official Report 12 November 2025, (Cols 11-12).

Conclusion

47. The Criminal Justice Committee draws the attention of the Parliament to the issues emerging from the scrutiny it has undertaken on the risks posed by cybercrime and cyber-insecurity to businesses and vulnerable individuals in Scotland.