The Scottish Parliament
Pàrlamaid na h-Alba

Criminal Justice Committee

Angela Constance MSP
Cabinet Secretary for Justice and Home Affairs

and

Richard Lochhead MSP
Minister for Business and Employment
Scottish Government

Thursday, 26 June 2025

Dear Cabinet Secretary Constance and Minister Lochhead

Challenges facing businesses and vulnerable individuals in Scotland from the risks of cybercrime

I am writing jointly to both of you as various aspects related to the Scottish Government policies on cyber resilience, online/digital activity and the impact of cybercrime, fall across your respective portfolios.

At our meeting of Wednesday 14 May 2025 the Criminal Justice Committee took evidence on the challenges facing businesses and vulnerable individuals in Scotland from the risks of cybercrime.

We heard from witnesses representing Age Scotland, Arnold Clark, the Cyber and Fraud Centre Scotland, the CyberScotland Partnership, the National Crime Agency, NatWest Bank and Police Scotland.

The primary focus of the session was to gain an insight into the current impact of cybercrime in areas which, until recently, receive less debate in the public realm. For example, cybercrime's impact on the lives of individuals like the elderly, those in employment, and the wellbeing of the business community across Scotland.

This session was organised before public knowledge of recent high-profile cyber-attacks on large retail business, such as the Co-Op and Marks and Spencer. Those incidents are a timely reminder of how dependent society has become on the

security of online operations of various stakeholders across the private and public sector.

Following the evidence session, the Committee received a written submission from the Association of British Insurers (ABI), highlighting their concerns around cybercrime and the level of preparedness and resilience across Scotland's business community.

Cyber Resilient Scotland: strategic framework

The first cyber resilient strategy for Scotland was published by the Scottish Government back in November 2015.[1] In February 2021 the Government updated this strategy with the publication of the *Cyber Resilient Scotland: strategic framework*. The 2021 strategy states that it looks to build on the original 2015 strategy by "expanding on its achievements and addressing ongoing and new challenges."

In October 2023, the Scottish Government published the results of a review of the 2021 strategy, entitled *Taking Stock: report on progress towards a cyber resilient Scotland*. It set our future priorities through four action plans for: the public sector, the private sector, the third sector and a learning and skills action plan.

Update on progress and current issues

While some of the legislative and policy powers relating to cybercrime issues are devolved to Scotland, we recognise other key legislative and policy powers will remain reserved to the UK Government and Parliament.

The annex to this letter sets out a number of key issues which arose during our scrutiny on 14 May, along with a series of questions on which the Committee is seeking a joint written reply from you.

We have also written to the Scottish Chambers of Commerce, the Federation of Small Businesses (Scotland) and the Scottish Council on Voluntary Organisations seeking their views on some of the issues raised.

All of these letters are available on our website.

A response by **Friday 19 September 2025** would be much appreciated.

Best wishes,

Audrey Nicoll MSP
Convener

[1] Safe, secure and prosperous: a cyber resilience strategy for Scotland" (November 2015): Safe, secure and prosperous: a cyber resilience strategy for Scotland - gov.scot

ANNEX

ISSUES ARISING FROM EVIDENCE ON CYBERCRIME

Introduction

As highlighted by witnesses on 14 May, the Scottish Government and key public and private sector partners have already undertaken much good work in terms of Scotland's preparedness and resilience on defending against cyber threats. We acknowledge the Scottish Government's leadership in this area and recognise how seriously Ministers take this threat. We commend all those working hard to protect Scotland from cybercrime. [2]

The Criminal Justice Committee is thankful to the witnesses who provided written and oral evidence on the challenges currently facing Scotland from the risks of cybercrime. It is clear from what we have heard so far that this is a fast-evolving and complex threat, which requires constant vigilance and adaptation to combat.

Set out below are a number of key issues arising from the evidence we have received to date, and on which we are seeking a response from Scottish Ministers.

This includes issues where the Scottish Government has, or plans, to take action directly within its own devolved powers, as well as where it is seeking to liaise with the UK Government (and other devolved administrations) on addressing these issues.

Scottish Government policy on cyber resilience

The Scottish Government seeks to address the threat of cybercrime and cyber security through various initiatives, including the Scottish Cyber Coordination Centre (SC3) and the Public Sector Cyber Resilience Strategic Framework. (Feb 2021). The Strategic Framework has four main outcomes-

i. *People recognise the cyber risks and are well prepared to manage them,*

ii. *Businesses and organisations recognise the cyber risks and are well prepared to manage them,*

iii. *Digital public services are secure and cyber resilient, and*

iv. *National cyber incident response arrangements are effective.*

Q1. In light of the evidence the Committee as received to date, can the Scottish Government report on progress made in meeting its four outcomes since the publications of the 2023 *Taking Stock* review?

[2] Criminal Justice Committee *Official Report, 14 May 2025* (Col 26): Nicola Taylor, CyberScotland Partnership https://www.parliament.scot/api/sitecore/CustomMedia/OfficialReport?meetingId=16432

Q2. What lessons have been learned from the *Taking Stock* review in order to better enhance Scotland's cyber resilience and build upon the efforts of government and stakeholders to date?

In the Taking Stock review, the Scottish Government "committed to delivering at least one national cyber exercise per year" in Scotland.

Q3. Can the Scottish Government outline the extent of its most recent cyber exercises? When did these take place, who took part in them and what learning was achieved?

The evidence we took highlighted the need for a greater understanding of what level of cyber defence and preparedness is required in 2025, and how the whole Scottish public sector needs more effective integration around their common cyber defence interests.

Witnesses spoke of the recent cyber-attacks on various public bodies like SEPA, and on Scottish local authorities. This posed the question as to whether expecting every public body or agency to have its own complete response package to cyber-attacks is economically and practically feasible in this day and age? [3]

Q4. Do the current Scottish Government frameworks ensure public sector bodies meet the current international standards on cyber security and information security management such as those set by the International Standards Organisation (ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27032)? [4]

Q5. Is the Scottish Government looking to develop guidelines around a basic standard of cyber preparedness that all Scottish public sector bodies should be required to meet? If not, would the development of such basic standards for the public sector provide a template for large-scale Scottish businesses and SMEs, as well as third sector/voluntary organisations across Scotland to meet, in terms of a basic cyber preparedness?

Q6. Does Scottish Government cyber policy require all Scottish public sector bodies to have an up-to-date cyber response plan in place, or to have dedicated cyber-attack drills? Do such policies require all public bodies to have a management lead responsible for responding to cyber protection? Are boards of Scottish public bodies required to have regular discussions on their cyber security and preparedness plans?

Developing operational resilience as standard

Witnesses pointed out that there are multiple benefits to developing operational resilience around loss of access to an organisation's IT/data systems as a result of a

[3] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 24-26
[44] International Standards Organisation. [ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection] [ISO/IEC 27002: 2022 Information security controls] [ISO/IEC 27032:2023 Cybersecurity, Guidelines for Internet security]

cyberattack, such as a malware or ransomware attack that encrypts or deletes vital corporate systems.

Developing operational resilience around cybercrime is beneficial not only when responding to cyberattacks, but for other forms of emergency planning where vital organisational systems are disrupted (such as weather emergencies or loss of public utilities etc).

Witnesses referenced the fact that organisations are required by law to carry out fire testing and drills several times a year. It was felt that public sector organisations should also move to that model for cybersecurity, "rather than just doing one exercise every so often and then forgetting about it." This, it was felt, is needed because things like "supply chain, staffing and organisation all change". So, there is a need to make sure that businesses and organisations not only have cyber response plans, but that staff routinely carry out testing of these plans.[5]

Q7. What is the Scottish Government's view that cyber resilience and safety awareness, arrangements and preparedness should be mainstreamed across public, private and third sector organisations similar to our approach to fire safety?

Q8. Is mainstreaming of cyber resilience/safety (even on a statutory basis) an area the Scottish Government would liaise with the UK Government on?

Q9. In lieu of any necessary statutory or policy power being reserved, would the Scottish Government look to use existing devolved powers like business supports/grants etc, to encourage Scottish SMEs and third sector organisations to develop and engage in meeting a basic standard of cyber preparedness?

What is cybercrime costing Scotland?

It is clear to the Committee from the evidence we have received, one of the most difficult aspects of cybercrime is to try to quantify how much it is costing the Scottish economy, or its impact on public expenditure, now and into the future?

This element is likely to be a crucial piece of the jigsaw when it comes to deciding what level of public resource and budgetary spending will be required, going forward, to combat the risk of cyber harm.

Q10. Is there any financial and budget modelling underway of the costs of cyber-attacks on the Scottish public sector, and what the wider impact is on businesses and the Scottish economy?

Q11. Cyber disruption to private/third sector organisations in Scotland may inevitably have a knock-on impact on public spending in terms of the need for the Scottish Government and public bodies to respond to the disruption they cause to the public. Is the Scottish Government looking to assess the benefit of enhanced public spending on cyber resilience, on the grounds of preventative spending?

[5] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 25-26

Q12. Is there any estimate of how much preventative spending could be achieved by a joined-up approach to cyber defence: for example, the provision of a common or shared Security Operation Centre (SOC) for public sector bodies in Scotland?

Q13. Is the Scottish Government looking to work with the Scottish local government sector, and other key partners in the public and private sector, on joint funding approaches to cyber defence?

We heard from witnesses like Arnold Clark and NatWest Bank of the complex and sophisticated methods used by cyber criminals to target business in terms of the timing of attacks, the methods used and the black-market ecosphere which supports cybercrime.[6]

Q14. Is there any modelling underway in Scotland of timing and methodology employed of those committing cyberattacks in terms of how instance response organisations should marshal their time and resources to support victims of cyber-attacks? For example, businesses being targeted when staff leave absences will be higher, like Christmas or school holidays.

The ABI submitted evidence to the Committee on the work the insurance industry is doing in terms of identifying severe cyber protection gaps for small and medium-sized enterprises. For businesses at such risk, ABI research shows that many SMEs think they are too small to present a target to cyber-criminals. Yet, the ABI highlighted a 2024 survey which found that 50% of UK businesses suffered some form of cyber security breach or attack.

In a major report published in January of this year, the ABI reported that, "many SMEs expressed that-

- *they felt that their risks from cyber-attacks were low;*
- *they did not require insurance or were already covered for such risks in other policies they held; and*
- *that the insurance product was too expensive or complicated to suit their modest requirements*."[7]

Q15. Are insurance sector representatives' part of the Scottish Government working groups on the review of the Cyber Resilient Scotland Framework?

Q16. What is the Scottish Government's view of the findings of the ABI research in respect of the risks to SMEs from cybercrime?

Policing resources and the Proceeds of Crime Act 2022

Police Scotland told us of the ability of police forces in England and Wales, and in Northern Ireland, to access proceeds of crime funding, recovered from criminal activity. Police use this to enhance their staffing, equipment, and other capabilities in the fight against cybercrime. This has become an especially effective funding option

[6] Criminal Justice Committee *Official Report, 14 May 2025*, Col 24
[7] *Cyber Resilience for SMEs: The Insurance Gap Exposed* (ABI, Jan 2025), page 5: abicyberresilienceforsmestheinsurancegapexploredjan2025.pdf

for police given the rise of the use of cryptocurrency by criminals, which forms part of the proceeds of crime recovered by police, and the potential value such cryptocurrency may have.[8]

For example, the work of Regional Organised Crime Units in England and Wales or the work of the PSNI in Northern Ireland in tackling financial crimes like online fraud. Those forces have benefitted from being allowed to access proceeds of crime to support their policing activities.

However, Police Scotland witnesses confirmed to us that police in Scotland currently have no such access to proceeds of crime recovered here, unlike their colleagues in England, Wales and Northern Ireland.

Q17. At a time when public sector funding, including Police Scotland's budget continues to be under pressure, why does the Scottish Government not provide access to some of the revenues recovered under the Proceeds of Crime Act 2002 in Scotland to support Police Scotland's efforts to combat cybercrime?

Q18. Would the use of proceeds of crime resources not allow Police Scotland to further strengthen and enhance their response to cybercrime, over and above the annual budget settlement they receive through the Scottish Police Authority?

Q19. As part of the planning for the 2026/27 Scottish Budget, will the Scottish Government consider using such recovered revenues to further enhance Police Scotland's response to Serious Organised Crime Groups cyber activities?

Cyber skills and resourcing across Scottish life

Witnesses highlighted the urgent need to increase the volume of cyber-skilled personnel across Scottish society, not only those available in the public sector and large-scale private sectors, but also those available to SMEs and the third sector.

There was an acknowledgement from witnesses that no Government, and no one sector of Scottish life "has all the answers" or can provide the level of resources needed to properly combat ever-growing cyber-threats. But that cross-sector coordination and cooperation on upskilling, resources, intelligence-sharing and joint assistance/action is the most effective way to respond.[9]

Over the last number of years, the Scottish Government has provided funding to various organisations as part of its 'Cyber Essentials Accreditation' initiative.[10]

Q20. Will the Cyber Essentials Accreditation initiative be continued and build upon? Is the Scottish Government looking to provide other methods of resourcing upskilling and shared learning on cybercrime and cyber threats across various sectors of Scottish society?

---

[8] Criminal Justice Committee *Official Report, 14 May 2025*, Col 27-28
[9] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 10, 14, 16, 24, 26, 40-41
Criminal Justice Committee *Official Report, 14 May 2025*, Col 26

Q21. Does the Scottish Government have any dedicated "just-in-case"[11] funding to allow the development of a broader cyber skills base in Scotland which would allow us to be less reliant on partners based outside Scotland for help during a serious cyberattack?

Police Scotland and the National Crime Agency spoke of the need to find new ways of recruiting cyber-skilled staff into policing, rather than expecting people to undergo the "traditional" police training route. We were told of the need for the proper skills mix in policing, such as civilian investigators, and of the need to make policing an attractive career path for specialist cyber sector graduates to choose.[12]

Q22. Would the Scottish Government consider looking at new ways in which Police Scotland could employ "ethical hacking graduates" as part of the police, without having them go through the "traditional" police recruitment and training route?[13]

Other witnesses highlighted the need for a positive approach to the development of Artificial Intelligence (AI) tools. And for stronger co-working between the data science sector, universities and specialist academia, IT/cyber-resilient graduates, police and law enforcement, the Government and public, private and third sector partners.

Q23. Will Scottish Government cyber-resilient strategy look to join up policy and development between the data science sector and cyber security sector in the development of AI tools to protect data from cybercrime? Will Scottish Government cyber-resilient policy look to combat the various forms of data theft and protect individuals and businesses by providing a network of partners who can provide, or signpost cost effective tools to help defend against cyber threats?

Witnesses told us that Scotland needs to be mindful that budgetary pressures outside Scotland (such as in the rest of the UK, the EU and the US etc.) is impacting on the key stakeholders Scotland would normally call upon for assistance. When a major cyberattack(s) is underway in their jurisdiction, this resource squeeze may impact the assistance they can give Scotland when we require it.[14]

Q24. Does the Scottish Government believe we have enough specialist skilled people within Scotland to respond to a scenario where two or more major cyber-attacks take place on key Scottish organisations, especially where key partners outside Scotland do not have the capacity to assist us at the time?

Q25. What plans does the Scottish Government have to build on Scotland's data science industries to take a lead in developing the AI-based tools we need to defend our critical data systems in the future? Is there an assessment of the current risk Scotland may face in relying too heavily on international players to develop and provide cyber defence solutions at a time when other countries may be cutting back spending on cyber defence?

---

[11] Criminal Justice Committee *Official Report, 14 May 2025*, Col 24
[12] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 41-42
[13] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 10 – 11, 13
[14] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 37-38

Effective intelligence sharing

Witnesses explained the nature of the large, complex and borderless ecosystem of cyber criminality which supports and develops cybercrime. Yet, they felt, we are lacking a structure to allow those stakeholders in Scotland and the UK with intelligence and knowledge of this complex threat, (like major business, academia, and the police) to share that intelligence and knowledge where it is needed.

Such intelligence sharing systems could provide SMEs, and others who don't have the same resources to bring to bear on their own cyber defence, with important tools to help improve their cyber resilience.[15]

Q26. Will Scottish Government cyber-resilient policy look to facilitate the sharing of intelligence between the data science sector, cyber security community in Scotland and those key public and private stakeholders already involved our cyber security framework?

Another key aspect witnesses told us of is the need for SMEs to have a better understanding of the need for them to interact with responsible and secure data custodians along the whole supply chain they depend upon.[16]

Q27. Does the Scottish Government's Framework consider the issue of developing 'responsible and secure data custodians' along the whole supply chain with which businesses, eps. SMEs, must interact in the course of their work?

Law and policy keeping pace with developments

Witnesses highlighted areas where they believe both the criminal law, and wider public cyber policy, need to be updated in order to keep pace with emerging cyber threats. Police witnesses told us of the standard 4P's response model to cybercrime: "pursue, prevent, prepare and protect".

We learned that while many individuals who commit cybercrimes in Scotland are based here, many other are not Scottish based, with many being based elsewhere in the UK, or overseas. [17]

Witnesses highlighted that many vulnerable individuals, like the elderly, are falling prey to cyber-enabled fraud and scams. We were told that 95% of all fraud committed in Scotland is now cyber-enabled fraud committed online.

While we heard about a lot of the good work being done by the police, or groups like Age Scotland to protect older people, the COVID pandemic demonstrated that many older people in Scotland may have no direct human contact in their day to day lives. This makes them especially vulnerable to online/cyber-related crime.

[15] Criminal Justice Committee *Official Report, 14 May 2025*, Col 17-18
[16] Criminal Justice Committee *Official Report, 14 May 2025*, Col 18-19
[17] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 5 - 6

Witnesses told us that the Scottish Government cybercrime campaigns reaching out through social media are not an effective way of reaching these vulnerable demographic groups.[18]

Witnesses highlighted the growth of fraudsters targeting older people through crimes like scam gold investment schemes, or the targeting of individuals through romance fraud. These, we learned, are currently the two biggest areas for targeting of older people in the last two years.

Regarding businesses and SMEs, witnesses told us that ransomware attacks are the single biggest threat to businesses across the UK, including in Scotland. Cyber-dependent crime, such as attacks with malware and ransomware, are undergoing a surge thanks to the new AI tools being used by criminals to fake everything from official looking documents, to faking online video calls where criminals can change the way they appear and sound. Such AI-enhanced scams can be carried out, in real time, to convince a victim they are taking to someone totally different from the real person targeting them.

Q28. In light of these sophisticated threats, what discussions are the Scottish Government having with the UK Government on efforts to work with authorities in other jurisdictions to block and take down the platforms that cause harm by enabling this type of cybercrime fraud to thrive?

Q29. How is the Scottish Government, and key partners, tailoring their messaging on cyber threats to reach older people?

Witnesses also highlighted a potential loophole in the criminal law in terms of the handling of stolen data, such as personal, medical or customer financial data etc. They pointed out that anyone handling physical stolen property could be charged with a criminal offence. However, the handling of stolen data/digital property is not currently an offence. [19]

We were told there is a "thriving" stolen data industry in terms of criminals using such data or dumping it onto the internet so others can continue to make use of it over and over. This perpetuates the damage to victims. And, in terms of cybercrime on business, this practice can continue to damage their good name or business operations long after the data has been stolen.

Q30. Is the Scottish Government undertaking any consultation with the UK Government making the handling of stolen data by anyone in the UK a criminal offence?

Q31. Is the Scottish Government looking to liaise with the UK Government on working with other jurisdictions to ensure best international practice in the criminalisation of the handling of stolen data is implemented in Scots law?

Witnesses also told us that the use of Serious Crime Prevention Orders (SCPO), which were extended to Scotland in 2015 following an amendment to the Serious

[18] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 3 - 4
[19] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 12 - 13

Crime Act 2007, could be used more effectively to target those involved in utilising stolen data, or using encrypted system to share stolen data. [20]

Q32. Does the Scottish Government have any plans to review the effectiveness of SCPOs in Scotland in terms of how they are used to combat those convicted of cybercrimes, or the misuse of encrypted communication platforms in the context of cybercrimes?

Human cost of cybercrimes

Witnesses spoke of the profound impact of cybercrime on individuals, such as vulnerable groups like older people. Many, it was felt, may not report such crimes to the police for fear it will not be taken seriously, or because of shame or embarrassment at having fallen victim to a fraud. [21] This could mean that there is a huge level of underreporting of the true extent of cybercrime across Scotland.

For businesses, witnesses said, the human impact of cybercrime on their employees is not well understood. We were told that when companies fall victim to cybercrime often the public/media focus is on the exfiltration (loss or theft) of personal data held by them, like customer data. But, as a result, there is little or no focus on the damage to the companies in question, and the impact on their staff. There is a pressing need to look at the 'human impact' of cyber security we were told.[22]

Business witnesses like Arnold Clark told us that, following a cyberattack on them they had done "the responsible thing—reported the crime to the police and the Information Commissioner's Office". This meant they were subject to an investigation over the loss of the data stolen from them.

But what was missing from their experience of seeking help in response to the cyber-attack on them was "an organisation to support them as a victim of a crime".[23] We heard about the long lasting psychological and personal impact the attack has on them and their staff. This included the shock and stress felt in the initial days. The need to deal with the frustration of their customers due to the disruption caused by the attack to the service they provide in terms of car sales, maintenance and rental. And the ongoing issues around the reuse of the stolen data.

While they were extremely complimentary of the response of Police Scotland, Arnold Clark pointed out that there was no entity in the Scottish criminal justice landscape that could support and guide them "as a victim" of crime.[24]

Q33. As part of the Review of the Cyber Resilient Scotland: strategic framework, does the Scottish Government have plans to establish some form of business victim support service, to support Scottish-based businesses through the aftermath of a cybercrime perpetrated upon them?

---

[20] Criminal Justice Committee *Official Report, 14 May 2025*, Col 12
[21] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 15 - 16
[22] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 3 – 4, and 9 – 10
[23] Criminal Justice Committee *Official Report, 14 May 2025*, Col 14
[24] Criminal Justice Committee *Official Report, 14 May 2025*, Col 14, 34-35