Cabinet Secretary for Justice and Home Affairs
Angela Constance MSP

F/T: 0300 244 4000
E: scottish.ministers@gov.scot

Scottish Government
Riaghaltas na h-Alba

Audrey Nicoll MSP
Convener
Criminal Justice Committee
Scottish Parliament
Edinburgh
EH99 1SP

Justice.committee@parliament.scot

03 September 2025

Dear Convener,

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

Thank you for your letter of 26 June, following the Committee's evidence session held on the 14 May 2025. I am also responding on behalf of the Minister for Business and Employment.

The Committee's observations and questions have provided valuable insights and have been helpful in informing Ministerial reflections on this important issue.

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.

I trust that the responses set out in Annex A will provide the Committee with clarity on the work currently underway and planned as we refresh our Strategic Framework for a Cyber Resilient Scotland.

Once again, thank you for raising these important questions.

Yours sincerely,

ANGELA CONSTANCE

ANNEX A

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?

The increase in digital adoption across society brings with it additional risks. Both the 2023 Taking Stock Review and the End of Year Review (2024) highlight substantial progress in building Scotland's cyber resilience, particularly in terms of awareness raising, education and skills and public sector, but the cyber risk is still ever present and evolving e.g. cyber criminals using emerging technologies such as AI and quantum computing.

The cyber maturity of Scotland's **public sector** is steadily improving, driven by collaboration with the Scottish Government (SG), a stronger national eco-system and sector-wide initiatives. Key advancements include:

- Recognition of cyber risk as a core business risk, with increasing accountability at board level
- Enhanced use of threat intelligence from trusted sources such as the Scottish Cyber Coordination Centre (SC3) and the National Cyber Security Centre (NCSC), helping with cyber threat monitoring and defence
- Strengthened incident response planning and testing
- More regular staff awareness training

Despite this progress, the sector remains vulnerable and must continue to treat cyber resilience as a strategic priority. Priorities going forward include:

- **More Leadership and Accountability**: Cyber resilience must be embedded within organisational governance. Senior leaders must take ownership of cyber risk, integrating it into business risk management frameworks and foster a culture of awareness across all levels of the organisation.
- **Supply Chain Risk Management:** Supply chains represent a significant source of cyber risk in the public sector due to the services they supply and the access to data they are granted. Additionally, the globalisation of supply chains can add geopolitical dimensions to these risks. A dynamic, proportionate approach to supplier assurance is essential, including regular reviews throughout the lifecycle of contracts to ensure cyber security standards remain robust and appropriate. The SC3 will have a role to play in helping to understand the overall view of cyber risk and the dependencies between organisations and suppliers.
- **Cyber Assurance and Regulatory Compliance:** Public bodies are subject to varying levels of cyber regulation and assurance:
- **Regulated Entities** (such as health and water services) are regulated under the Network and Information Systems Regulations 2018, with oversight from Competent Authorities and audited against frameworks like the NCSC Cyber Assessment Framework (CAF).
- All public sector organisations should conduct **regular cyber risk assessments** and implement proportionate assurance mechanisms for internal systems and third-party suppliers.

- **Legacy systems:** Legacy technologies and systems pose significant resilience challenges. Many of these systems were not designed with modern cyber security threats in mind, making them vulnerable to attacks and difficult to update without disrupting services. The complexity of integrating new technologies with older infrastructure can put further strains on resources. Budget challenges can also hinder progress in modernisation and getting access to appropriately skilled staff.
- **A skilled public sector workforce:** A skilled cyber workforce is essential to protect data, maintain public trust and ensure the uninterrupted delivery of critical services. As cyber threats become more persistent, cyber security staff must be equipped with up-to-date knowledge and skills to defend against attacks. These include risk assessment and management, network security, incident response as well as understanding compliance and regulatory frameworks. Scotland's public sector is experiencing workforce challenges including:
- **Talent shortage**: Difficulty attracting and retaining skilled professionals due to competition with the private sector and from other countries
- **Professional pathways**: Limited progression opportunities within the public sector, both for entry level positions and for progressing into a more senior role
- **Budget constraints:** Limited funding for recruitment and training
- **Evolving threats**: Ongoing upskilling is required to stay ahead
- **Fragmented professional standards:** Inconsistent standards across public bodies. Addressing these challenges requires coordinated investment in professional development, standardisation of competencies and creation of clear career pathways.
- **Public-Private Collaboration:** Cross-sector collaboration offers opportunities to share tools, infrastructure and expertise – reducing costs and duplication of effort. There is an opportunity to strengthen collaboration between the public, private and third sectors. Sharing examples of good practice - particularly from the private sector - can help raise standards across the board. A coordinated approach could lead to common actions and solutions that benefit all sectors.

In terms of **comms messaging and cyber awareness**, we have increased the reach of communities through the strengthening of the CyberScotland Partnership, a collaborative of representative bodies that can spread cyber messaging to a range of diverse audiences. There are different parts of society that are particularly vulnerable to cyber risk including younger, older people, people with disabilities and who do not have English as a first language. We have been working closely with the organisations such as YoungScot, Youthlink, AgeScotland and LeadScotland to drive forward audience specific campaigns. For example, LeadScotland has produced cyber awareness messaging in a range of community languages, YoungScot has produced social media campaigns specifically targeting young people. We also now have a structured national awareness comms plan implemented, reaching more organisations and businesses. We have a plan of action in place to grow the CyberScotland Partnership so to expand reach into more people and businesses in Scotland. Recent new Partners include the Institute of Directors and AgeScotland.

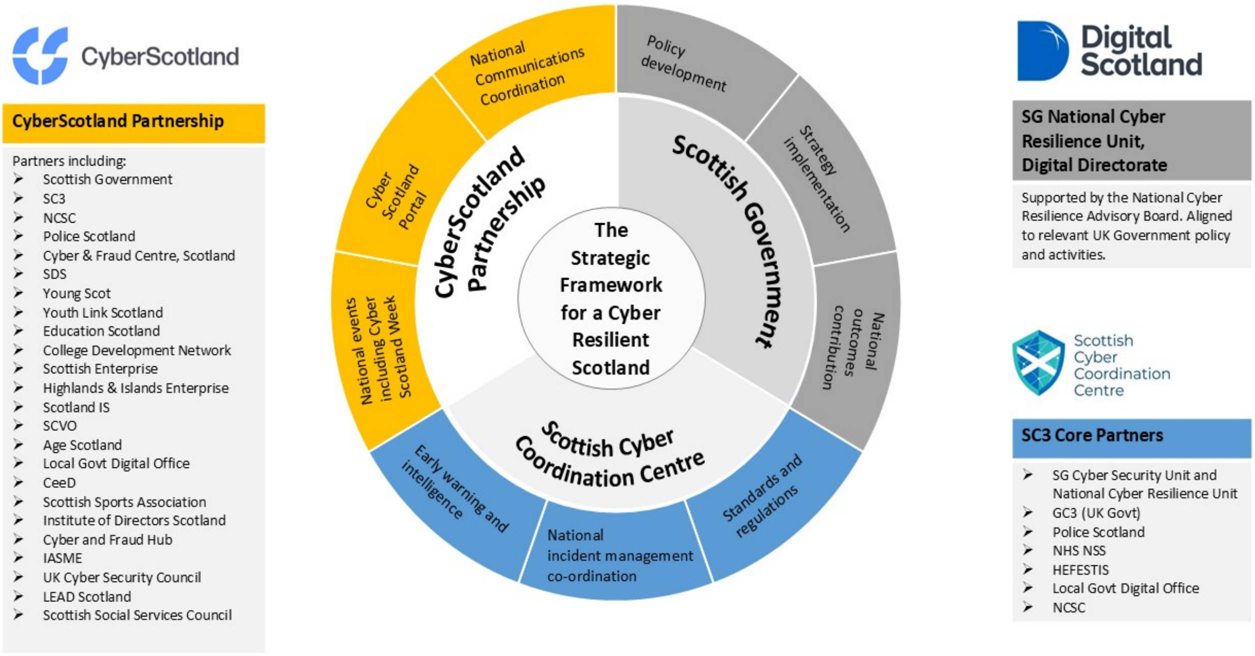
Across the **education and lifelong learning systems** we have developed cyber security qualifications in schools and colleges, increased the number of CyberFirst Schools and are slowly adding further cyber security learning into our colleges and universities. Education Scotland has been the key driver of the school initiative.

We continue our work with our partners to reach more businesses and organisations across the private, public and third sectors.

Q2: 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.

The *Taking Stock review* demonstrated both areas of progress but also those where more improvement is required. The cyber threat is not a government-only solution: it is vital that we have a strong national ecosystem to coordinate and cohere the steps we are taking. The SG has led on building a strong ecosystem of partners, with complementary strengths, capabilities and reach – united in their common goal of making Scotland a more cyber resilient. See Ecosystem diagram below:



CyberScotland

CyberScotland Partnership

Partners including:
- Scottish Government
- SC3
- NCSC
- Police Scotland
- Cyber & Fraud Centre, Scotland
- SDS
- Young Scot
- Youth Link Scotland
- Education Scotland
- College Development Network
- Scottish Enterprise
- Highlands & Islands Enterprise
- Scotland IS
- SCVO
- Age Scotland
- Local Govt Digital Office
- CeeD
- Scottish Sports Association
- Institute of Directors Scotland
- Cyber and Fraud Hub
- IASME
- UK Cyber Security Council
- LEAD Scotland
- Scottish Social Services Council

The Strategic Framework for a Cyber Resilient Scotland
CyberScotland Partnership
Scottish Government
Scottish Cyber Coordination Centre
National Communications Coordination
Cyber Scotland Portal
National events including Cyber Scotland Week
Policy development
Strategy implementation
National outcomes contribution
Early warning and intelligence
National incident management co-ordination
Standards and regulations

Digital Scotland

SG National Cyber Resilience Unit, Digital Directorate

Supported by the National Cyber Resilience Advisory Board. Aligned to relevant UK Government policy and activities.

Scottish Cyber Coordination Centre

SC3 Core Partners

- SG Cyber Security Unit and National Cyber Resilience Unit
- GC3 (UK Govt)
- Police Scotland
- NHS NSS
- HEFESTIS
- Local Govt Digital Office
- NCSC

Lessons are learned from almost every cyber incident and exercise that the Scottish SG is notified of. The SC3 routinely shares threat intelligence information, Indicators of Compromise and recommended mitigation measures across the public sector are shared at an operational level with the cyber/information security professionals to ensure that actions can be taken quickly to reduce risk and exposure to cyber threats. SG are working closely and regularly to build the cyber resilience of the public sector.

Q2. 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? [1]

Exercising is one of the most cost-effective ways an organisation can test its preparedness and ability to respond to cyber incidents. Scenario-based exercises establish how effective current defence and response mechanisms are, improve internal relationships and skills (specifically the ability to deal with an actual cyber attack), and identify areas for further improvement.

The SC3 has a specific Cyber Exercising workstream which aims to promote and improve the level of cyber exercising across the Scottish public sector including how we learn and share lessons from both incidents and exercises. During 2025 the SC3 has worked with a number of organisations to test their cyber incident response arrangements. These include SEPA, Social Security Scotland, Edinburgh City, North Lanarkshire and Scottish Borders councils.

One of the core functions of the SC3 is its national incident coordination service. This is where the SC3 steps in and activates a multi-agency response to major public sector incidents. This may also include the deployment of technical specialists to provide subject matter expertise and augment response efforts.

SG undertook a cyber exercise in March to test the coordination arrangements of the Scottish Cyber Incident Management Plan to ensure it remains fit for purpose, flexible and adaptable to meet the changing cyber environment. This multi-agency exercise had representation from 12 organisations including various departments within SG, Police Scotland, UK Government, NCSC, NHS, Local Authorities, Digital Office, Social Security Scotland, BT and Capita.

The scenario explored an escalating series linked cyber attacks impacting on the Scottish Public Sector service delivery and was intended to focus on the coordination of multiple of concurrent incidents during which time the Scottish Governments resilience coordination's were stood up to coordinate a severe storm weather event.

The main findings of the exercise were as follows:

- national cyber coordination arrangements remained flexible and match fit to meet the needs of the wider UK Cyber Incident Coordination

- SGoRR and SC3 have the capability to manage a number of serious concurrent events but this has clear resourcing limits.

[1] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 24-26

- Consideration should be given to ensuring there is a high degree of assurance and testing, akin to that applied to Critical National Infrastructure, around government IT infrastructure to provide confidence on its security and resilience. This should include external ‘red-team’ exercising.

Q3. 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)? [2]

SG expects all public bodies manage their risks, including cyber, in an appropriate and reasonable manner. It is up to each body how it manages its day-to-day business and decision-making processes. SC3 supports the public sector in doing this via a range of central services, advice and support mechanisms.

SG issued The Public Sector Cyber Resilience Framework, 2nd Edition (referred to as “PSCRF v2.0”) to Public Sector Organisations in June 2024 and formally published in December 2024. The PSCRF was created to support public bodies in understanding cyber/information security standards and highlights key policies which Public Sector Organisations may wish to have in place as well as specific controls that are aligned with industry best practice including the NCSC’s Cyber Assessment Framework (CAF) and ISO 27001.

SC3’s Public Sector Cyber Resilience Assessment (CRA) replaces both the Public Sector Cyber Resilience Survey and the PS-CRF for 2025, simplifying the process for public sector organisations. It is mapped to the CAF and will help organisations to better understand whether and to what extent they are meeting cyber resilience maturity levels. Organisations may, additionally, want to refer to CAF mapping resources to check alignment against standards such as ISO 27001.

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?

The PSCRF v2.0 currently outlines the basic cyber/information security standard (Tier 1) which the majority of public bodies should have in place. It also outlines additional controls that some more mature public bodies or those carrying additional cyber risk should consider having in place.

The PSCRF v2.0, builds on the NCSC Cyber Assessment Framework - this already provides a template for large scale organisations. For SMEs, smaller business and third sector/voluntary organisations, the NCSC backed Cyber Essentials certification scheme

[22] 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]

provides an appropriate baseline standard in terms of cyber security, with Cyber Essentials Plus ensuring a degree of independent verification of cyber maturity.
We are developing a process to better understand the cyber maturity levels of the public sector through the development of the Cyber Observatory.

Q4. 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?

The Public Sector Cyber Resilience Action Plan sets out actions for public bodies to ensure that they develop and test their incident development plans, include cyber risks on corporate risk registers and that each organisation has a designated board member with responsibility for cyber issues and were regularly discussed.

SG has supported the public bodies in meeting these actions through:

- Cyber Awareness sessions
- Public sector cyber awareness board training provided to 289 board members across the public sector during 2023 and 2024.
- A Cyber Incident Response Plan and a series of scenario specific playbooks published in 2019 and have been updated a number of times in response to lessons identified (latest update in December 2024) {https://www.gov.scot/publications/cyber-resilience-incident-management/}
- Organisational Cyber Testing and Exercising Regime: Guidance published in January 2025 to help organisations test their incident plans
- An Exercising Cadre has been developed to train a number of cyber and resilience professionals across the public sector to ensure that the sector could access the cyber exercise facilitation skills necessary to oversee strategic cyber exercises. So far, we have trained 40 exercising professionals.

Going forward, through our annual survey, we will be delving deeper into public sector organisations' maturity around board and senior management involvement in response planning and exercising.

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 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.[3]

Q5. 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?

SG is very clear, cyber is everyone's business - cyber security and resilience underpins and enables the safe and secure delivery of digital public services. However, current legislation, including at UK level, does not position cyber matters in a similar fashion to safety awareness as a legal requirement. Therefore, whilst we are keen to see cyber resilience considerations mainstreamed into all facets of public sector policy, there often remains a need for specialist cyber security and resilience advice which, given skills and resource challenges, cannot always be accessed locally. The upcoming UK Cyber Security and Resilience Bill will expand regulation to cover more digital service providers, strengthen security standards and improve incident reporting. It will likely empower regulators with greater oversight and enforcement capabilities.

Q6. Is mainstreaming of cyber resilience/safety (even on a statutory basis) an area the Scottish Government would liaise with the UK Government on?

SG liaises closely with the UK Government on all aspects of cyber security and resilience, including on UK Strategic direction and legislation, such as the upcoming Cyber Security and Resilience Bill which is likely to enhance the powers of cyber regulators and to extend the scope of the Network and Information Systems Regulations to cover more Operators of Essential Services.

Q7. 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?

This is a challenge, but we very much agree that changing at source is the way in which we can create systemic change. The SG are currently developing a roadmap for the mandating of key resilience elements for public sector organisations, which will define appropriate requirements and enforcement mechanisms depending on the nature of the organisation. The SG can explore the potential for expanding a similar approach to other sectors. The public sector also incentivises cyber/information certification in their supply chains as part of procurement processes, mandating certification where appropriate and proportionate or requiring certified suppliers to answer less cyber assurance questions during tender evaluation.

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

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.

Q8. 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?

While SC3 seeks as part of the lessons learned activities following significant cyber incidents, to evaluate the immediate financial impact as well as the scale of the disruption to public services, there is no formal project or modelling underway to estimate this at a national level. However, Department for Science, Innovation and Technology (DSIT) in UK Government are currently researching into the quantification of cyber attacks on businesses and the economy and SG are contributing to this developing research.

Q9. 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?

The Scottish Government expects that all public bodies manage their cyber risks in a responsible and proportionate manner. It is up to each body how it manages its day-to-day business, budgets and decision-making processes. However, it is also worth noting that many cyber risks cannot be mitigated by merely increasing budgets – major systemic vulnerabilities often have roots in legacy technologies and outdated practices, and so wider digital and cultural transformation is often required to tackle the underlying cause. For other risks, making the best use of the systems, services and support already in place is often more effective and better value for money than buying in advanced security solutions. It should also be noted that some cyber threats cannot realistically be fully mitigated regardless of how much preventative spending takes place, which is why SC3 also promotes effective detection and response processes as well.

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?

The Scottish Government itself provides the SCOTS Connect shared services platform - a secure, robust, scalable and fit for purpose ICT solution for the Scottish public sector.

This currently serves 21,000 customers over half of which are not core Scottish Government.

In addition to the above the Digital Directorate's Cloud Platform Service (CPS) provides a cloud environment in both AWS and Microsoft Azure where Scottish public sector organisations can host their applications. Whilst these solutions are still relatively new, they have 39 customers.

Both SCOTS and CPS have security services provided to them from the Scottish Government's own SOC. This enables us to provide a top-class SOC service to these customers but also create efficiencies of scale and cost effectiveness.

SG are currently considering the feasibility of a centralised SOC, as organisations are increasingly on Microsoft 365, but it is a significant challenge given the complexity of networks and data patterns.

SC3 recognises the importance of a coordinating function: it recognises the value of Defending as One. It works closely with other coordinating functions and, where appropriate, SOCs. For example, SC3 provides the Malware Information Sharing Platform (MISP) service which all subscribed public sector organisations benefit from, strengthening their existing cyber defence activities with curated, real-time technical threat data.

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?

Under the Verity House Agreement, Scottish Local Authorities are empowered as autonomous entities with significant control over their own funding and decision-making. The agreement establishes a "partnership of equals" between the Scottish Government and local councils, affirming that councils are best placed to determine how to serve their communities. It commits to reducing ring-fencing of funds, regularly reviewing powers and funding, and adopting the principle of "local by default, national by agreement." This means that local authorities have full and exclusive powers unless otherwise provided by law, and the Scottish Government cannot unilaterally direct or limit their actions

However, the Scottish Government is always willing to support and facilitate engagement on collaborative approaches to cyber security and resilience - this includes with local government and other key partners in the public and private sector.

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.[4]

Q10. Is there any modelling underway in Scotland of timing and methodology employed of those committing cyber attacks 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.

SC3 plans its support, including out-of-hours support to account for fluctuations in incident frequency. Cyber incidents are unpredictable by nature and therefore SC3 moves quickly to address challenges as they occur, mindful of any recruitment and other budgetary

[4] Criminal Justice Committee *Official Report, 14 May 2025*, Col 24

constraints. SC3 also works closely with other national partners, NCSC, Police Scotland, the UK Government and Devolved Administrations, to maintain a common view and understanding of threat actor methodologies.

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."***[5]

Q11. Are insurance sector representatives' part of the Scottish Government working groups on the review of the Cyber Resilient Scotland Framework?
No, however we acknowledge the value that cyber insurance can bring to organisations as one component of a broader risk mitigation approach, and that feedback has been received from a range of experts across the public and private sector on the framework review.

Q12. What is the Scottish Government's view of the findings of the ABI research in respect of the risks to SMEs from cybercrime?
Cyber crime poses a growing threat to Scotland's SMEs, and this report highlights that nearly half have experienced some kind of breach in 2024, yet many remain uninsured, lacking board understanding of risk and resilience. Appropriate mitigation action against the threat, of which insurance is a potential component.

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 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.[6]

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.

[5] *Cyber Resilience for SMEs: The Insurance Gap Exposed* (ABI, Jan 2025), page 5: abicyberresilienceforsmestheinsurancegapexploredjan2025.pdf
[6] Criminal Justice Committee *Official Report, 14 May 2025*, Col 27-28

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.

Q13. 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?

The decision on how any Proceeds of Crime Act receipts are utilised in Scotland is a matter for the Scottish Ministers. Currently funds are primarily committed to fund the CashBack for Communities programme until April 2029.

Cashback for Communities is an early intervention justice programme. It is specifically aimed at supporting young people who may be at risk of becoming involved in antisocial behaviour, offending or reoffending. CashBack partners deliver projects that promote safe spaces, trusted adults and a range of positive diversionary and support activity for young people aged 10-25. CashBack for Communities early intervention work with young people also contributes to the preventative strand of Public Sector Reform strategy. Support and diversionary work with young people reduce the risk of engagement with police and the justice system. As a result, this enables public bodies to focus on other priorities. Since inception of the programme in 2008, Cashback has committed £156m to supporting around 1.4m young people across all 32 local authorities in Scotland.

Q14. 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?

Police Scotland's budget has been increased by £90 million this year. It is for the Chief Constable, under the oversight of the Scottish Police Authority, to allocate that money in accordance with her priorities.

Q15. 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?

Scottish Ministers announced a commitment to a further phase of CashBack in the 2025/26 Programme for Government. This next phase of the Programme will run from April 2026 to March 2029.

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.[7]

Over the last number of years, the Scottish Government has provided funding to various organisations as part of its 'Cyber Essentials Accreditation' initiative.[8]

Q16. 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?

SG continues to work with the National Cyber Security Centre (NCSC) and IASME to promote Cyber Essentials across the public, private and third sectors. The CyberScotland Partnership is growing from strength to strength in reaching more people and organisations across Scotland. SG has supported 3 rounds of the Public Sector Upskilling Fund, which has helped to provide over access to over 400 cyber security learning opportunities.

Q17. Does the Scottish Government have any dedicated "just-in-case"[9] 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.[10]

While there is no dedicated fund for this, we are actively exploring how best to grow the cyber industry and its skills base, as part of the updated Strategic Framework for a Cyber Resilient Scotland (published Nov 2025), in addition to public sector training such as the upskilling fund and exercising cadre. We are also exploring the possibility of extending the Modern Apprenticeships within the public sector.

Q18. 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?[11]

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.

[7] 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
[9] Criminal Justice Committee *Official Report, 14 May 2025*, Col 24
[10] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 41-42
[11] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 10 – 11, 13

Scottish Government through strategic partnerships look to share knowledge and information across the Public Sector and wider through extensive collaboration in the UK Cyber Networks.

While Police Scotland explores graduates and apprenticeships to support technical aspects of investigations, relationships with Academia allow Police Scotland's Research and Insights team to develop and participate in research studies which align with strategic priorities; ensuring an evidence-led approach is applied to decision making. In addition, Police Scotland is now a member of Abertay's Cyberquarter which will take advantage of collaboration opportunities and skills to support:

- Research and Development (R&D)
- Access to specialist resources, technology and infrastructure.
- Knowledge Transfer Partnership - Projects to address specific strategic challenges, where together new knowledge/expertise is created.

Police Scotland has a Data Science Centre of Excellence which has been set up within the Chief Data Office, bringing together the technical expertise of Data Scientists, Data Engineers and Data Analysts to focus on releasing efficiencies and delivering operational capability across the organisation. This unit is the product of extensive engagement and will harness the opportunities present within Artificial Intelligence (AI) to deliver material improvement to policing in Scotland. Any solutions built will be done so in a way that is secure, ethical, and transparent, making full use of the mature Rights-Based Pathway and Data Ethics Triage process already in place.

Q19. 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?

SG recognises the challenges as well as the opportunities of new and emerging technologies and will look at every opportunity to join up AI progress with tackling cyber crime.

Currently we are working with UKG's DSIT's cyber security and AI team, and we promote the relevant codes of practice relating to AI and cyber security. The CyberScotland Partnership and through the Cyberscotland.com portal provides links to this information.

NCSC maintain a list of assured companies providing incident response, training and other cyber services, some of which are using AI as part of their service offer.

ScotlandIS, a CyberScotland partner, manage and maintain the cyber directory which highlights Scottish cyber companies and their areas of expertise.

The SC3 promotes a range of tools and partnerships to help the Scottish Public Sector defend itself against cyber attack. NCSC's free Active Cyber Defence services are good examples of tools available to a broad customer base – including the private sector for the Early Warning tool.

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.[12]

Q20. 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?

Incident response will generally always require the victim organisation to engage a trusted Cyber Incident Response provider, partly as organisations rarely have the skills to carry out forensic investigations and uncover the root cause of incident, but also partly to ensure that a recognised third-party can provide attestations that the victim organisation no longer poses a threat to its stakeholders.

NCSC maintains and publishes a list of assured CIR companies - mainly of which are global companies with deep resource pools which ensures access even in the event of multiple concurrent attacks.

SC3 was created in the wake of the cyber attack on the Scottish Environmental Protection Agency (SEPA) to address this very challenge and is building its capacity to work with public sector organisations with their cyber security and resilience.

Q21. 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?

We are aware of that risk and that this is true more broadly of modern technology solutions in general - effective security always represents a balance of factors, and the optimal landscape would represent a mix of international leaders and local providers.

SC3 works with many partners and vendors to encourage and motivate the development of robust cyber security services. Cyber resilience requires international cooperation, and, subject to robust procurement, use of tools from beyond Scotland and the UK. We are supportive of UK Government efforts to improve market incentives for cyber and data-focused businesses here.

<u>Effective intelligence sharing</u>

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

[12] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 37-38

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.[13]

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?

SC3 already facilitates the sharing of threat intelligence across many different partners, including via our MISP. We are currently developing improved intel sharing practices and would be happy to connect more closely with the data science sector.

Public bodies must be clear on the cyber and information security requirements when procuring goods and services, and this includes ensuring that requirements are cascaded down to second and third order suppliers as part of robust supply chains.

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.[14]

Q22. 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?

The Framework encourages organisations to secure supply chains appropriately and this would include ensuring that suppliers secure any data shared with them under contract. Organisations should seek assurances, up to and including audits, around the level of protection and operational maturity of supplier controls and process; this should extend to their own suppliers further down the chain and should be enforced by appropriate contractual clauses.

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. [15]

[13] Criminal Justice Committee *Official Report, 14 May 2025*, Col 17-18

[14] Criminal Justice Committee *Official Report, 14 May 2025*, Col 18-19

[15] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 5 - 6

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.
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.[16]

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.

Q23. 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?

NCSC's Takedown Service, which is available to all UK organisations, allows for a quick and easy route to removal of malicious websites and material. Where more direct action is required, the Scottish Government liaises with NCSC, Police Scotland and the NCA, who have clear track record of coordinating international law enforcement operations against criminal platforms.

Q24. How is the Scottish Government, and key partners, tailoring their messaging on cyber threats to reach older people?

The Scottish Government works with CyberScotland Partner organisations including Police Scotland and the National Cyber Security Centre as technical authority to produce messaging to all audiences with older people being a priority group.

AgeScotland joined the CyberScotland Partnership in 2025 and is working with the Scottish Government to explore ways to better tailor messaging, guidance, advice and support to older people.

[16] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 3 - 4

SG has also funded initiatives including a print magazine containing advice on cyber threats which was distributed to community centres and doctors' waiting rooms; as well as free cyber resilience community workshops for older people covering online scams, protecting information and building confidence in technology.

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. [17]

***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*.**

Q25. 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?

Cyber Security and Legislative Measures in the United Kingdom

The primary legislation governing personal data is the **Data Protection Act 2018**, which operates alongside the **UK General Data Protection Regulation (UK GDPR)**. Under this framework, section 170 makes it unlawful to obtain, disclose, or retain personal data without the consent of the data controller, including in cases involving stolen data.

The Scottish Government is consulted on any proposed legislative changes and acknowledges that the Home Office is actively exploring legislative options to better address the handling of stolen data, particularly in the context of ransomware, where data theft is a common tactic

In addition, the Computer Misuse Act 1990 remains a key legal instrument for prosecuting offences related to unauthorised access and data theft. Recognising its limitations, the UK Government has conducted a review to modernise the Act and ensure it aligns with today's cyber threat landscape.

To mitigate the impact of ransomware, the Home Office has proposed several measures following a public consultation including:

- **A targeted ban on ransomware payments** for critical national infrastructure (CNI) and public sector organisations.
- **A ransomware payment prevention regime**, potentially economy-wide or threshold-based, with possible exemptions for individuals.
- **A mandatory ransomware incident reporting regime**, based on thresholds, requiring suspected victims to report incidents.

[17] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 12 - 13

These proposals aim to reduce financial incentives for cybercriminals, enhance law enforcement oversight, and improve national resilience against ransomware attacks. We are in close contact as these are developed.

Q26. 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 Crime Act 2007, could be used more effectively to target those involved in utilising stolen data, or using encrypted system to share stolen data. [18]

The Scottish Government regularly engages internationally on policy development matters, both through Uk-wide engagement opportunities and through direct links with international partners. While there has been no specific international engagement around the potential criminalisation of stolen data, Scottish justice operational partners such as COPFS and Police Scotland are active in their engagement through cooperation platforms such as Eurojust, Europol and Interpol, sharing international best practice on the changing nature of crime.

On the issue of using SCPOs to address cybercrime-related offences, the decision to apply to the court and the conditions sought is one for the Crown Office in consultation with police. It is for the court to determine whether to grant a SCPO and what conditions should be attached. The aim of a SCPO is to protect the public by preventing, restricting or disrupting involvement by the person in serious crime. Qualifying offences are set out in Schedule 1A of the Serious Crime Act 2007 and include offences under the Computer Misuse Act 1990 such as unauthorised access to computer material.

Q27. 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?

There are recommendations on the use of SCPOs set out in David Gauke's independent review of sentencing. The Scottish Government will consider the implications of these on the future use of SCPOs in Scotland in consultation with the appropriate authorities.

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. [19] ***This could mean that there is a huge level of underreporting of the true extent of cybercrime across Scotland.***

[18] Criminal Justice Committee *Official Report, 14 May 2025*, Col 12

[19] Criminal Justice Committee *Official Report, 14 May 2025*, Cols 15 - 16

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.[20]

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".[21] 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.[22]

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?

Scottish Government does not plan to establish a business Victim Support Service. Through Police Scotland and partners the following advice, guidance and support is available for victims of crime:

- Police Scotland encourages businesses to report cybercrime incidents. Doing so not only supports investigations but also contributes to a broader understanding of emerging threats. Businesses should report cybercrime to Police Scotland directly.
- Cybercrime Investigations within Police Scotland support victims of ransomware incidents from the initial report through to resolution. This includes offering early advice on risk-based decisions and recommending engagement with professional services such as Cyber Incident Response Companies, legal advisors, and media consultants.
- Cyber Harm Prevention Protect Officers engage with businesses and Critical National Infrastructure across all sectors—such as food, energy, telecoms, and transport—to understand the impact of cybercrime and promote a culture of cybersecurity. They help organisations plan for, respond to, and recover from cyberattacks, offering tailored guidance to minimise disruption and financial loss. Officers also advise on compliance with ICO requirements and national legislation and deliver cyber awareness and resilience training to Police Scotland staff. They work with partners to

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

develop educational resources that “target harden” organisations, children, adults, and vulnerable groups against online harms.

- Police CyberAlarm is available to businesses across Scotland, including SMEs, charities, educational institutions, and local government. Participating organisations receive regular reports on potentially malicious cyber activity targeting their firewalls and internet gateways, helping them identify vulnerabilities and strengthen their defences.
- Victim Support Scotland (VSS) is the primary victim support service to which Police Scotland refers victims and witnesses for assistance. When a victim or witness requests a referral to VSS, this must be recorded using the VSS field on the divisional crime system. Each local policing division has a designated coordinator responsible for extracting VSS data from the system.
  Every victim of crime—whether an adult or a child—must be provided with a Victim Care Card at the time of reporting the crime or as soon as reasonably practicable. The card records basic details of the crime or offence and includes relevant information for the victim, such as the investigating officer’s contact details and how to reach VSS.

The Scottish Government with support from Police Scotland funds the Cyber and Fraud Centre Scotland to manage the Incident Response Helpline support victims of cyber crime. They will help businesses to resume operations and to advise them on their next steps to recovery.

Police Scotland recognises the wide range of agencies involved in cyber-enabled and cyber-dependent crime, including response, investigation, and intelligence. Key partners include the Cyber Scotland Partnership (CSP), Scottish Cyber Coordination Centre (SC3), and the Cyber and Fraud Centre Scotland (CFCS). Continued collaboration across the cyber sector is essential to maximise collective resources and impact.