**Letter to Criminal Justice Committee on challenges facing businesses and vulnerable individuals in Scotland from the risks of cybercrime**

Audrey Nicoll MSP

Convener

Criminal Justice Committee

Scottish Parliament

19th September 2025

**Dear Convener,**

Thank you for your letter on 26th June 2025, seeking views on challenges facing businesses and vulnerable individuals in Scotland from the risks of cybercrime.

On behalf of the Scottish Chambers of Commerce Network, which represents more than 12,000 members across Scotland, we welcome the opportunity to share perspectives from the business community on the growing issue of cybercrime.

At the Committee's evidence session on 14th May 2025, it was noted by Chris Ulliott, Head of Cyber Security at NatWest Bank, that small businesses generally lack the resources to efficiently combat threats from cybercrime, especially when compared to larger firms.

Considering most of our members are SMEs, this is a sentiment that we often hear from businesses.

This can be due to a variety of factors, including but not limited to: limited financial resources, a lack of dedicated IT staff, lower awareness and risk-management in general, or more simply they continue to operate with outdated or insecure technology.

Considering the growing cost of doing business, our members have highlighted that the cost for business Cyber Essentials certification can be a barrier to achieving cybersecurity. Ranging from around £300 for the basic, self-assessed level for micro businesses, to over £1000 for more advanced support for more developed firms, this cost can prove prohibitive for businesses already operating on tight margins.

We also see small business reporting that the CE assessment reveals additional unknown costs required to progress any remedial actions to ensure their systems are secured

Certifying Bodies (CB's) are already trained and certified in the delivery of CE assessments, advice and training and have built up this expertise in recent years, however, the targeting of small business has stagnated. We recommend the government and other public bodies consider ways to reduce the cost barrier for SMEs: for example, by funding locally or regionally delivered training by CB's across the country.

We also have concerns of a growing 'cyber protection gap' for SMEs, echoed in the views shared by the Association of British Insurers in response to the Committee's inquiry.

While larger organisations and specific sectors exhibit relatively developed cyber security practices, smaller organisations and certain sectors typically cannot or do not, highlighting persistent disparities and vulnerabilities.

As identified in the 2025 Cyber security breaches survey, awareness of key government campaigns on cyber security, such as Cyber Aware, have seen a steady decline in recent years across the board. This has been particularly prevalent among micro and small business, as well as smaller charities.

This confirms the importance of continuing to reiterate key messages and better promote education and resources on cyber security via official sources.

The CyberScotland Partnership, which includes stakeholders like Police Scotland, ScotlandIS, and the National Cyber Security Centre, should be the key vehicle with which to drive forward awareness in Scotland.

Beyond incident response, these resources educate businesses on proactive steps, such as avoiding phishing attacks and using strong passwords, which can prevent many common cyber threats from occurring. They can also direct organisations to 24/7 cyber response helplines and cybersecurity specialists who provide technical knowledge and support during an incident.

Data on the specific impact of cybercrime to Scottish business in recent years is generally sparse, with UK-wide data being more readily available.

A recent survey published by Vodafone Business estimated that small businesses across Scotland are losing £386 million to cybercrime per annum. This means that on average, Scottish firms are losing £5,584 each year due to cyber-attacks.

The cyber security breaches survey estimates that at least 20% of businesses and 14% of charities have been the victim of at least one cybercrime in the last 12 months, accounting for approximately 283,000 businesses and 29,000 registered charities.

More reassuringly, the data does indicate that more SMEs are becoming more aware and vigilant of the risks of cybercrime. The same cyber security breaches survey shows that cyber security remained a high priority for around seven in ten businesses (72%) and charities (68%).

However, the sophistication of the threats posed by cybercrime also continues to rise. There are several high-profile examples of the damage that can be done, from the Marks and Spencer data breach, the Afghan refugee data leak, to the ransomware attacks on Scottish schools which took place earlier this year.

We have also seen evidence of the long-lasting impact it can have for an organisation. In 2020, the Scottish Environment Protection Agency (SEPA) suffered a sophisticated ransomware attack, which had a long-term impact on the organisation's delivery capacity.

The rise of AI is also another element that will pose another layer to the threat from cybercrime. As noted by the National Cyber Security Centre:

> ***"Artificial intelligence (AI) will almost certainly increase the volume and heighten the impact of cyber-attacks over the next two years…***
>
> ***"Moving towards 2025 and beyond, commoditisation of AI-enabled capability in criminal and commercial markets will almost certainly make improved capability available to cybercrime and state actors."***

It will be important that criminal law and cybersecurity policies can incorporate and manage the risks from AI in this space, to mitigate the risk to business, public bodies, charities, and society more generally.

There is also more necessity to consider the role of education in ensuring that cyber resilience is a part of the curriculum and qualifications space, as well as promoted within the workforce to build a more secure economy.

Recent reviews of the government's cyber resilience polices indicate advancements in the public sector through the Public Sector Cyber Resilience Framework, including increased training, and support for third sector organizations, better co-ordination across sectors in Scotland with the National Cyber Security Centre (NCSC), as well as the establishment of the CyberScotland Partnership (CSP) and the Scottish Cyber Coordination Centre (SC3).

The Private Sector Action Plan (2023-25) **has 6 key objectives:**

- Increase businesses' understanding of cyber risks that may affect them.
- Improve cyber resilient behaviours of the private sector workforce.
- Build the professional skills of IT and cyber security staff across the private sector.
- Embed cyber security standards, regulations, and compliance across the private sector.

- Raise awareness of the cyber security goods and services and expertise available to all organisations.
- Support businesses to prepare for, respond to and recover from cyber incidents.

These are all appropriate and sensible objectives to continue prioritising and supporting businesses with. We would advise that these are routinely monitored and updated where appropriate, to ensure their effectiveness and flexibility against ever evolving cyber threats.

Yours sincerely,

E. A. Cameron

**Dr Liz Cameron CBE**

**Chief Executive, Scottish Chambers of Commerce**