Federation of Small Businesses

For support
For protection
For business

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

2 September 2025

By email: **justice.committee@parliament.scot**

Dear Audrey,

Many thanks for your letter of 26 June 2025, requesting our input to the Committee's scrutiny of the challenges facing businesses and vulnerable individuals in Scotland from the risks of cybercrime.

In December 2023, we published a report, ***Cracking the case: uncovering the cost of small business crime***. While predominantly focused on England and Wales, the survey conducted as part of the research included some findings from Scotland, which I have used to respond to the questions posed by the Committee.

Although the sample size for Scottish findings (67, unweighted) is lower than our usual statistical threshold of 100 responses, I hope the data is useful to the Committee in terms of providing a snapshot of cyber resilience and challenges among Scottish small businesses.

What is your view on the effectiveness of the Scottish Government cyber resilience policies and its most recent Private Sector Action Plan?
We do not have a position on this.

What is your view of the level of cyber operational resilience amongst SMEs and the business community across Scotland?
Our 2023 survey asked respondents:

> *What steps, if any, have you taken to protect your business against cybercrime and fraud?*

The Scottish findings were:

- Have anti-virus software on devices: 85.2%
- Regularly update software on IT systems: 64.9%
- Regularly back up data and IT systems and test them: 38.6%
- Use cloud computing: 35.6%
- Have security policies for the use of email, internet and mobile devices: 28.8%

T 0141 226 7913
E Scotland.Policy@fsb.org.uk
W fsb.org.uk

A Suite 8B,
58 Waterloo Street,
Glasgow, G2 7AD

Registered Office:
National Federation of Self Employed and Small Business Limited,
Sir Frank Whittle Way, Blackpool Business Park, Blackpool, FY4 2FE
Registered in England: 1263540

- Have implemented 2 Factor Authentication (2FA) or Multi Factor Authentication(MFA): 22.4%
- Regularly train staff in good IT security practices, including on anti-fraud and/or anti-bribery measures: 12.6%
- Take key or sensitive data offline: 16.9%
- Encrypt stored data, communications with customers and suppliers: 19.2%
- Insurance protection: 14.0%
- Regular security risk assessments to identify important information, systems and vulnerabilities: 16.7%
- Supplier background checks: 10.3%
- Written plan to deal with IT failure / attack by cyber criminals: 10.0%
- Sourced advice from a reliable source: 7.1%
- Monitoring the escape / loss of key credentials online (e.g. passwords / address / ID etc.): 5.7%
- Obtaining a recognised security standard: 3.4%
- Other: 2.4%
- Not applicable to my business / we have not taken any particular measure(s): 8.1%

What is your view on the levels of cybercrime across Scottish business and what it may be costing the Scottish economy? Do you have a view on the findings of the ABI's most recent report on cybercrime?

Our 2023 survey asked respondents:

Thinking about the period from January 2021 to January 2023, have any of the below cybercrimes been attempted / committed against your business?

The Scottish findings were:

- Phishing email (attempting to trick user to click on a link / attachment): 57.5%
- Malware attack (malicious software causing loss of data / damage to devices / servers): 5.9%
- Social media hacked: 4.1%
- Theft of money from business bank account(s) or alternative system of money storage: 12.2%
- Ransomware attack (preventing access to device or files, and demanding ransom): 5.0%
- Online platform hacked (not including your own website): 3.0%
- Own website hacked: 2.2%
- Denial of service attack (causing online service or website to be inaccessible): 1.2%
- Intellectual property (IP) theft: 2.9%
- Cryptocurrency related theft: 1.7%
- Theft by an external party of business data from a device, network, or system (outsider threat): 1.2%
- Other: 1.7%
- Don't know / not sure: 1.2%
- None of the above: 34.3%

Our 2023 survey also asked respondents:

Thinking about the most impactful cybercrime and / or fraud that you experienced in the last 2 years, how much would you estimate the cost to your business over the period is?

T 0141 226 7913
E Scotland.Policy@fsb.org.uk
W fsb.org.uk

A Suite 8B,
58 Waterloo Street,
Glasgow, G2 7AD

Registered Office:
National Federation of Self Employed and Small Business Limited,
Sir Frank Whittle Way, Blackpool Business Park, Blackpool, FY4 2FE
Registered in England: 1263540

The Scottish findings were:

- £1,000 or below: 43.1%
- £1,001- £25,000: 21.1%
- £25,001-£100,000: 3.0%
- Above £100,000: 2.5%

We note the publication of the ABI's most recent report on cybercrime and its contribution to the evidence base on cyber resilience and challenges among small businesses.

Do you have a view on the levels of cybercrime being reported by businesses to the police?
Our 2023 survey asked respondents:

Thinking about the most impactful crime that you have experienced in the last two years, to whom did you report it?

The Scottish findings were:

- The police in person / by phone: 20.2%
- My bank: 19.7%
- The IT / service provider: 20.4%
- Action Fraud: 9.8%
- The police via the single online home reporting platform: 2.3%
- The Information Commissioner's Office (ICO): 5.1%
- Other: 11.6%
- Don't know / not sure: 2.6%
- I did not report it: 32.0%

What is your view on the access of Scottish business to skilled IT/cyber staff? Does the Scottish business sector, especially SMEs, have timely access to specialist support to help them deal with, and recover from cyber-attacks?
Our **2025 Scotland Big Small Business Survey** identified 'Digital/AI' as being the area in which most SMEs feel there is a skills gap in their workforce, with 31.8% of the 233 respondents to this question identifying it as such.

Do you feel Scottish businesses have access to enough up-to-date information and intelligence on the cyber risks facing them?
Our 2023 survey asked respondents:

Please select any of the below statements which apply to you when you think about cyber security or anti-fraud measures for your business:

The Scottish findings were:

- The cost of a managed service provider is too high: 30.9%
- The cost of relevant software is too high: 12.5%
- I don't have the resources and / or skills to invest: 27.7%
- I cannot afford it due to other business costs rising: 17.2%
- I don't understand cyber security or have enough information to make a decision to invest: 21.8%
- I have never faced any issues with cybercrime and / or fraud: 18.2%
- I don't think there is a risk of cybercrime and / or fraud to my business: 6.9%
- Other: 5.1%
- Don't know / not sure: 18.1%
- None of the above / I don't think this is relevant to my business: 13.5%

T 0141 226 7913
E Scotland.Policy@fsb.org.uk
W fsb.org.uk

A Suite 8B,
58 Waterloo Street,
Glasgow, G2 7AD

Registered Office:
National Federation of Self Employed and Small Business Limited,
Sir Frank Whittle Way, Blackpool Business Park, Blackpool, FY4 2FE
Registered in England: 1263540

What is your view on whether the criminal law and public policy in Scotland is keeping pace with the developing risks from cybercrime?
We don't hold a position on this.

What is your view on the human cost to business owners and employees who are the victims of cybercrime? Is there enough support to help business deal with the ramifications of a cyber-attack on them?
Our 2023 survey asked respondents who had experienced business crime:

You've said that you have experienced crime in the last two years. What were the wider impacts of that/those crime/s on your business?

The Scottish findings were:

- Purchased replacement equipment, fixtures or fittings: 15.6%
- Lost stock: 8.8%
- The business's reputation was negatively impacted: 10.5%
- The payment provider "charged back" the cost of the fraud to my business: 6.3%
- Delivery of products/services to customers were delayed: 6.5%
- Full extent not known yet: 12.3%
- Lost business (existing or future or both): 10.2%
- Insurance premiums and / or excesses increased: 6.7%
- Did not proceed with existing business development plans: 6.3%
- Myself or others had to take time off to deal with the case as it progressed / went through court: 10.2%
- Myself or others had to take time off to recover from the physical and / or mental trauma: 4.7%
- Temporarily closed the business: 2.3%
- Permanently lost member(s) of the workforce or leadership team: 4.6%
- Personal damage / compensation claims against me from my employees: 2.6%
- Had to pay a fine to a regulator or the court: 2.3%
- Other: 37.1%
- Don't know / not sure: 17.4%

Any other views you may have on the impacts of cybercrime on businesses in Scotland?
N/A.

I trust this information is helpful to the Committee as part of its scrutiny work. However, if you have any additional questions, or would like to clarify any of the points contained above, please don't hesitate to get back in touch.

Best wishes,

Colin Borland
Director of Devolved Nations, Federation of Small Businesses (FSB)

T 0141 226 7913
E Scotland.Policy@fsb.org.uk
W fsb.org.uk

A Suite 8B,
58 Waterloo Street,
Glasgow, G2 7AD

Registered Office:
National Federation of Self Employed and Small Business Limited,
Sir Frank Whittle Way, Blackpool Business Park, Blackpool, FY4 2FE
Registered in England: 1263540