Audrey Nicoll MSP

Convener
Criminal Justice Committee
Scottish Parliament, Edinburgh
EH99 1SP
Justice.committee@parliament.scot

17/09/2025

Dear Convener,

The Scottish Council for Voluntary Organisations (SCVO) appreciates the opportunity to respond to your letter on 26th June 2025 as part of the work the Criminal Justice Committee is undertaking on the challenges facing businesses and vulnerable individuals in Scotland from the risks of cybercrime.

SCVO is the national body representing the voluntary sector (charities, social enterprises, and voluntary groups, aka third sector) in Scotland, with a membership of 3,000+ organisations. Our mission is to champion the sector's social and economic contributions, provide essential services and debate big issues. The sector in all its diversity is a powerful force for positive change across Scotland and a significant part of our economy, with over 46,500 voluntary organisations and over 800,000 volunteers. For further information please refer to SCVO's State of the Sector 2025.

SCVO has been actively involved in the CyberScotland Partnership since its inception and has delivered a number of programmes, including supporting around 200 charities to attain Cyber Essentials (between 2018 and 2020), and more recently, supporting dozens of organisations to use the IASME Cyber Readiness Tool to benchmark their cyber security controls. SCVO currently employs a Cyber Resilience Co-ordinator to manage implementation of the Third Sector Cyber Resilience Action Plan (2023-35), in collaboration with Scottish Government. This work sees us supporting the sector on their journey to becoming more cyber resilient, guiding a programme of work to help them prioritise cyber risk, protect against common threats and prepare for cyber incidents. For further information please refer to SCVO's Cyber Resilience page.

Below is SCVO's response to the questions you directed to us, providing our views on the level of cyber preparedness and resilience amongst the charity/third sector community in Scotland.

If you have any further questions please let us know.

Regards,

Alison Brogan

Third Sector Cyber Resilience Co-ordinator

Scottish Council for Voluntary Organisations (SCVO)

What is your view on the effectiveness of the Scottish Government cyber resilience policies and its most recent Third Sector Action Plan?

SCVO has been actively involved in the recent review of Scottish Government's cyber resilience strategy to ensure that it is relevant and realistic for the third sector. We will subsequently be involved in the creation of the new third sector action plan over the coming months, which will then be used as a baseline for our ongoing cyber resilience programme of work.

These documents are useful in providing direction and focusing alignment across government policies and different sectors to help us achieve our goal of improving cyber resilience across Scotland as a whole. Having a clear framework and effective partnership sin place is crucial in ensuring that investment and efforts from key partners is relevant to the needs of the third sector and delivers impactful change.

What is your view of the level of cyber operational resilience amongst the third sector community across Scotland?

SCVO are seeing steady progress when it comes to cyber resilience within Scotland's third sector, however there is still work to be done to ensure organisations are operating safely online as the cyber threat continues to grow.

In autumn last year SCVO added some cyber risk and resilience questions to our [Third Sector Tracker](), a growing research community made up of representatives from third sector organisations across Scotland. Of 372 respondents, only 41% reported a high understanding of cyber resilience. However, 60% felt confident about their cyber protection measures. The most common measures being anti-virus software, software updates and regular backups.

SCVO also provide a free [digital checkup service](), allowing third sector organisations to assess their current digital maturity and plot a route ahead, which includes some questions on cyber security. Through this we can see that the majority of voluntary organisations in Scotland see cyber security as a business priority however very few have a cyber incident response plan and/or adequate staff/volunteer cyber training in place.

The above appears to align with the figures seen within the [annual cyber security breaches survey]() more broadly for UK charities. SCVO have used this information to help focus their cyber resilience programme of work with the intention of starting to address some of these gaps as a priority.

What is your view on the levels of cybercrime across Scottish third sector organisations 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?

The majority of cyber-attacks are untargeted and opportunistic making it just as likely for third sector organisations to be impacted by cybercrime as other types of organisations. With the scale, range and sophistication of cyber threats continuing to grow each year, like every sector, it is a case of when rather than if a cyber-attack will occur. Third sector organisations in Scotland provide a wide range of essential services including those that support social care, health care and community, economic and social development. Disruption to services caused by a significant cyber-attack could potentially result in loss of life, funds and/or sensitive information.

Through SCVO's digital check-up we have previously asked about experiences with cyber-attacks and phishing remains to be the top threat which aligns with the data in the annual cyber security breaches survey. The figures in here are also useful to see more broadly for UK charities level of cybercrime and cost to economy.

ABI's most recent report on cybercrime specifically relates to SMEs; a number of the findings are not transferable to the third sector however there are some that are. Lack of awareness is definitely a key issue and something SCVO's cyber resilience programme is actively working on.

It is worth highlighting that the report does not appear to cover the work that the Scottish Government has been doing in this space with the CyberScotland Partnership. The [CyberScotland portal](#) has been created to provide a single source of truth for individuals and organisations, signposting to relevant information and support from across the UK.

Do you have a view on the levels of cybercrime being reported by third sector organisations to the police?

It is hard to obtain a clear view of the exact levels of cybercrime across Scottish third sector organisations as, like other sectors, it often relies on them reporting cyber incidents to the relevant authorities. As part of the CyberScotland Partnership SCVO work closely with the Scottish Cyber Coordination Centre (SC3) and Police Scotland however do not receive exact figures on a regular basis.

What is your view on the access of third sector organisations to skilled IT/cyber staff? Do third sector organisations have timely access to specialist support to help them deal with, and recover from cyber-attacks?

Third sector organisations have access to a range of IT support, depending on their size and resources. 77% of third sector organisations have a turnover of less than £100k per year – which means they typically won't have IT specialists as part of their staff team and may only have ad hoc access to professional IT expertise.

Larger voluntary organisations tend to have established digital teams in-house or outsource their IT support. The Scottish Third Sector Tracker highlights the major financial issues that these voluntary organisations are experiencing and the recruitment/retention issues that they face, in particular in relation to skilled roles like IT.

One of the biggest challenges when it comes to cyber resilience within the third sector is limited cyber capability at an operational level. Even in instances with established digital teams or external IT providers access to cyber expertise remains restricted, staff/volunteers dedicated to cyber security are rare within the sector, resulting in many organisations relying on external support. Procuring skilled cyber staff can be costly and not a viable option, at the moment there are no specific services providing free support although this is something that SCVO's cyber resilience programme is actively work on.

Through the CyberScotland Partnership there is a free Cyber Incident Response and Recovery Helpline that Scottish organisations can contact for support during an incident, which is referenced in SCVO's easy-to-use incident response template.

Do you feel Scottish third sector organisations have access to enough up-to-date information and intelligence on cyber risks facing them?

There is no lack of up-to-date information and intelligence on cyber risks facing the sector, e.g. via CyberScotland website and/or quarterly third sector bulletins. There does, however, appear to be limited awareness of the support that is available. Given the range of financial and other pressures facing voluntary organisations, it seems likely that the biggest barrier to accessing this support is time, with many third sector organisations spending much of their time firefighting and not having time to consider risks that aren't immediately facing them. A big part of SCVO's cyber resilience programme is to raise awareness of the work we're doing and all of the free best practice guidance and support that is available to help guide voluntary organisations in overcoming their cyber resilience challenges.

What is your view on whether the criminal law and public policy in Scotland is keeping pace with the developing risks from cybercrime?

No view on this.

What is your view on the human cost to third sector organisations and their employees who are the victims of cybercrime? Is there enough support to help third sector organisations deal with the ramifications of a cyber-attack on them?

The human cost of a cyber-attack can be significant to both staff and volunteers involved in the response and recovery, at the moment there is limited support to deal with this. Given the financial and other pressures facing voluntary organisations, falling victim to cybercrime may be the final straw for some and additional sources of support at such a difficult time would be very welcome.

Any other views you may have on the impacts of cybercrime on third sector organisations in Scotland?

No further views on this.