CYBER AND FRAUD CENTRE SCOTLAND (for businesses) and the Cyber and Fraud Hub (for Individuals)

www.cyberfraudcentre.com – supports organisations

www.cyberfraudhub.org – supports individuals.

Written Submission to Parliamentary session on Cyber Crime in Scotland

The Cyber and Fraud Centre – Scotland rebranded from the Scottish Business Resilience Centre in response to the growing threat of cyber and fraud. As Scotland's only cyber security social enterprise, our mission is to deliver accessible, affordable, and relevant services, focusing on the human side of security and victim support.

With a small team of 12, we support organisations across Scotland through incident response, training, services and community engagement. We are entirely self-funded and receive no direct funding from Scottish Government or any other agency. Generating £1m annually and reinvesting surplus to support the Cyber and Fraud Hub, which aids individuals and families affected by fraud.

We have supported organisations like SEPA, Western Isles, SAMH, Arnold Clark and Scullion law during their Cyber-attacks.

To support the Victims of the cyber attacks with a number of trusted Scottish technical and legal incident response organisation's, who go above and beyond for the victims.

Key Achievements (Past 5 years)

- Delivered NCSC 'Exercise in a Box' sessions to 2,500+ organisations, including those on Scottish remote islands.
- Trained 1,000+ business leaders via our Cyber Executive Education Program days.
- Provided free cyber training and services to small business and charities and guides for parents and older adults.
- Over 800 calls on our Incident Response line - In the last 12 months alone, we have received over 400 calls on our IR line across diverse cybercrimes including ransomware and business email compromise and other scams.

We had a huge increase in calls from individuals in relation to individual victims of fraud, so had to look at how we handled these, including a multimillion gold investment scam on an elderly lady in Scotland.

We spoke to Eddie Hawthorne from Arnold Clark, who also wanted to do something to support victims of cyber and fraud, about the idea of setting up a charity to support individuals working in partnership with the banks and policing, and he agreed to fund

a charity for two years during startup phase. We set up the charity – The Cyber and Fraud Hub

Cyber and Fraud Hub Impact in year 1.

- Supported 280+ individuals
- Actively working on cases worth over £9.5m, including scams targeting vulnerable elderly victims, we have recovered or prevented nearly 800k of fraud too.

Key Challenges and Trends

Fraud is growing at a phenomenal rate; and we are only seeing the reported figures. People are reluctant to report fraud crimes because of the shame they feel and because they have been so badly affected, they then don't know who to trust.

Also, when we do support victims, they are reluctant to tell their stories for fear of retribution or people thinking they were 'stupid' – so the stories go untold, and it is difficult for people to understand the real threats.
Other areas of note:

- Ransomware remains a growing threat, cyber-attack incidents like SEPA and Arnold Clark highlighted gaps in coordinated support during holiday periods, and over the last few weeks we have seen large retail organisaiton's impacted which in turn has now impacted residents in our remote island communities.
  Additionally:
    - There is still a feeling that 'it will never happen to me'. The hardest part of our job is to get individuals and organisation's to spend the time making themselves more resilient and preparing for an incident.
    - In Scotland, there is a real community effort around the 'good people' in cyber to pull together to help the victim in times of crisis, we have seen this on all the high profile attacks, but we do have a concern around capacity across the organisations and agencies if we had 2-3 high profile attacks at the same time, which is a huge possibility. (we have seen this with the 3 large retailers attack down south over the last few weeks)
    - We have a dependence around threat intelligence from private organisations and also law enforcement outside of Scotland – who are now under budgetary pressure or geo-political changes and challenges to keep supporting their own entities. We may not receive the same level of support going forward as we did historically.

- AI and data tools will likely enhance attacker capabilities. Cyber should be underpinning all our efforts around growing the economy and should be part of AI and start up investments, we are generating more and more data and complex modelling and IP, but we are not doing enough if sometimes anything to protect it.

- We are not investing enough in proactive areas to prevent cybercrime, or around innovation and Cyber and Fraud seems to be a forgotten entity.

- Smaller organisations see cyber security as too expensive, but there are lots of things organisations can do to make themselves more resilient in a cost-effective way, and we want to continue our work as a social enterprise to ensure that they do this – and by doing this we are making Scotland more secure.

- We need to learn from the past few years of Cyber attacks and build a more secure future

Policy Considerations

- Greater investment is needed in proactive cyber prevention and innovation.

- Laws around stolen data sharing should be modernised. Data taken or shared from the dark web after a cyber-attack **is** stolen data. The sharing or distribution of it should be a criminal offence. We also need to look at how we can arrange injunctions against the sharing of data across countries and jurisdictions.

- I know this is outside the remit of the Scottish Justice System, but we really need to raise this conversation and ensure our laws are in line with the way technology and crime exists

- Proceeds of crime should help fund prevention and victim support. Scotland have made some significant seizures around proceeds of crime, but this money is not going back into policing in Scotland or into organisation's like ours to help prevent the crime. Proceeds of Crime can be used by Police Forces down south.

- Cryptocurrency scams are a growing concern for us all, and we need to invest in very expensive technology, training and licensing to be able to look at this, disrupt the criminals, provide evidence and get arrests. We don't have a budget for this in Scotland and this is heavily invested in other law enforcement agencies down south.

- Elderly victims are particularly vulnerable. Systems must be more accessible and supportive. We created a dedicated resource to support information sharing, which is freely available - A Guide to Avoiding Fraud and Scams for Older People — CyberandFraudHub.

Call for Collaboration, ownership and funding.

At Cyber UK this week in Manchester – Richard Horne the CEO of NCSC has said that “Britain’s intelligence services are seeing a “direct connection between Russian Cyber attacks and physical threats to our security” Malign actors in Moscow are “waging acts of sabotage, often using criminal proxies in their plots, he also said that domestic security service MI5 were seeing the hacking threat from Russia manifesting “on the streets of the UK against our industries and our business, putting lives, critical services and infrastructure and national security at risk”

He told the CYBERUK audience that the role of the information security community was not just about protecting systems, it’s about protecting our people, our economy and our society from harm”

Scotland will not be immune to these threats, and we should see them as very real, we need to see cyber security as an inclusive movement with international collaboration to protect our nation.

Cyber and fraud prevention in Scotland benefits from strong collaboration across policing and other law enforcement government and industry. This co-operation is unique and worth celebrating but needs continued support, ownership and investment to thrive. We can all do much more to prevent and protect and stand out even more as a nation around the good things we are already doing. Cyber and Fraud Centre and the hub will continue to work alongside key partners and stakeholders to continue to support organisations and individuals.