Links to authoritative sources of advice and support can be found at the Scottish Government Cyber Resilience website: https://www.gov.scot/policies/cyber-resilience/

The NCSC's small business and charities guides can be found at the NCSC website (see: www.ncsc.gov.uk).

You can get a free digital health check and 1:1 support at Business Gateway's Digital Boost (see: www.bgateway.com/driving-growth/digitalboost).

If you're a Scottish SME, you can get a 0% interest, unsecured Digital Development Loan to help improve your cybersecurity (see: https://digitaldevelopmentloan.org/)

If you're a Scottish SME or 3rd sector organisation interested in working with the public sector, the Supplier Development Programme can provide expert training, support and information to help you grow your business. See: https://www.sdpscotland.co.uk

Scottish Government
Riaghaltas na h-Alba
gov.scot

SAFE, SECURE AND PROSPEROUS:
A CYBER RESILIENCE STRATEGY FOR SCOTLAND

PUBLIC SECTOR ACTION PLAN

Cyber Resilience Unit

Scottish Government

E-mail: cyberresilience@gov.scot

Scottish Public Sector

Supplier Cyber Security

The Cyber Threat

Cyber-attacks (such as phishing, ransomware, hacking, etc.) are becoming an increasing threat to our economy and society. No internet-connected organisation, however large or small, is immune.

Cyber-attacks may be targeted at specific organisations or individuals, or untargeted, where attackers indiscriminately attack as many vulnerable machines or users connected to the internet as possible.

These attacks are as real a risk to the small business that relies on a database of customers to distribute its goods as they are to multinational banking organisations.

According to the DCMS Cyber Security Breaches Survey (2018), 40% of all UK businesses suffered a cyber breach/attack in a 12 month period.

Nearly 7 in 10 medium/large businesses identified a breach or attack, while 42% of micro or small businesses identified a breach during the same period.

The Scottish Public Sector

Most Scottish public sector organisations rely on **3rd party suppliers** to deliver products, systems, and services, and require exchange of information to deliver those services effectively. Successful cyber attacks on these suppliers can be very damaging and disruptive, to both the 3rd party suppliers themselves and to the public bodies relying on their goods or services.

A series of high profile, very damaging attacks around the world has demonstrated that attackers increasingly have both the intent and ability to exploit vulnerabilities in supply chain security. There is a clear need for Scottish public sector organisations to understand the cyber threat to supply chain security and to work with suppliers to take appropriate, proportionate action to mitigate it.

As part of the **Scottish Public Sector Action Plan on Cyber Resilience**, Scotland's public sector organisations are encouraged to adopt a **common approach to supplier cyber security**.

A **guidance note** for Scottish public sector organisations is available at https://www.gov.scot/publications/cyber-resilience-supply-chain-guidance.

An **assessment tool** for suppliers (**The Cyber Security Procurement Support Tool)** is available at https://cyberassessment.gov.scot/.

What does this mean for your organisation?

Depending on the types of contract your organisation delivers, or wants to deliver, to Scottish public sector organisations, you may find that you are **asked for more information** about your organisation's arrangements to **defend against cyber threats** during procurement processes.

Public sector organisations and their suppliers can now use the **Cyber Security Procurement Support Tool** which supports public sector organisations to identify cyber risks and ask suppliers consistent questions about protection against cyber threats. A **voucher scheme** has also been introduced to support smaller businesses and charities to achieve the National Cyber Security Centre's (NCSC) **Cyber Essentials certification**. This can be accessed via the Scottish Enterprise and SCVO websites.

Organisations can help ensure they are ready for these changes, and protected against the most common forms of cyber threats generally, by **taking action now** to ensure they have appropriate protections in place. Doing so may help avoid damage and disruption due to cyber attacks, and position you better to win public and private sector contracts in the future. The reverse of this leaflet provides links to advice and support.).