www.gov.scot/cyberresilience

Scottish Government
Riaghaltas na h-Alba
gov.scot

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

PRIVATE SECTOR ACTION PLAN 2018-20

FOREWORD

PRIVATE SECTOR ACTION PLAN

Digital technology offers huge opportunities for Scotland as a modern, progressive nation.

Our ability to inform and interact with citizens and consumers is being transformed by the digital world, and Scotland's private sector is developing ambitious plans to embrace these opportunities.

Scotland's digital strategy makes clear our determination to ensure that our businesses continue to prosper in an increasingly connected and competitive world.

But these opportunities also bring new threats and vulnerabilities that we must take decisive action to manage.

The cyber threat is growing. I regard it as vital to our ambitions as a modern, digital nation that our businesses, large and small, understand that threat, and are supported to take steps to protect themselves.

No organisation, however large or small, is immune. Cyber attacks are as real a risk to the small, rural bakery that relies on a database of customers to distribute its goods as they are to multinational banking organisations in our financial districts.

This action plan sets out how we will work in partnership with Scotland's private sector to help tackle the cyber threat. Key to success will be the willingness of Scotland's businesses, charities and public sector organisations to work in partnership to raise fundamental levels of cyber resilience across Scotland.

Alongside our action plans on Learning and Skills and Third and Public Sector Cyber Resilience, this plan represents an important step towards our ambition for Scotland to be a world-leading nation in cyber-resilience.

I look forward to working with Scotland's private sector, and our partners in the UK and internationally, to help make this a reality.

John Swinney MSP
Deputy First Minister and Cabinet Secretary for Education and Skills

CONTENTS

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

1. The importance of cyber resilience in Scotland's private sector has never been greater. Digital technologies bring significant opportunities for our businesses and our economy – but they also bring with them new threats and vulnerabilities that we must take decisive action to manage.

2. The cyber-threat is assessed as a Tier 1 threat to the UK's national security. The National Crime Agency describes it as a "major and growing threat" to UK businesses. Increasingly we have seen major cyber attacks affecting large numbers of businesses worldwide as a result of unintended consequences.

3. The National Cyber Security Centre notes that cyber criminals are becoming increasingly sophisticated, and are able to make judgements on "Return on Investment" when deciding who to target where – the harder the target, the smaller the ROI, the less incentive there is to invest time and money in an attack on those targets. Making Scotland overall, and individual sectors and businesses within Scotland, more cyber resilient may therefore help tip the balance around these judgements in the future, bringing economic advantage to Scottish companies through an ability to continue operations unaffected by common cyber attacks. Being able to demonstrate that cyber security is taken seriously – that services and customer data are protected and resilient – will become increasingly important to a business's reputation, which in turn may impact on overall performance.

4. To combat the threat, and to ensure Scotland's overall preparedness and resilience, businesses of all sizes must be supported to adopt a "when, not if" mindset in respect of future cyber attacks, and to take appropriate, proportionate preventative action.

5. This Private Sector Action Plan has been developed in partnership by the Scottish Government and the National Cyber Resilience Leaders Board (NCRLB). It has drawn heavily on the views and expertise of key private sector stakeholders, including representatives of the SME sector – a vital part of the Scottish economy. It sets out the key actions that the Scottish Government and key partners will take during 2018-20 to help make Scotland's private sector, and Scotland overall, more cyber resilient. It aims to realise the opportunities presented by Scotland's strong cyber resilience networks and communities of interest to position Scotland as a world leading nation in cyber resilience.

6. Delivery of the action plan will be coordinated and led by the Scottish Government's Cyber Resilience Unit, working in partnership with the NCRLB and Scottish private sector partners.

KEY ACTIONS

A. Developing a common approach to cyber resilience across the Scottish private sector

7. The Scottish Government and the NCRLB will work to ensure that the views of the Scottish private sector, including SMEs, help inform UK-level consideration of whether there is a case for extending regulatory requirements around cyber resilience more widely across parts of the private sector. This will include a particular focus on ensuring input from any sectors that are critical to the functioning and health of the Scottish economy, and key areas of competitive advantage. **(Key Action 1)**

8. The Scottish Government and the National Cyber Resilience Leaders Board will work with the NCSC and key partners to consider options for developing a Private Sector Cyber Resilience Framework or Pathway by spring 2019. This would aim to provide a simple, structured way for organisations in Scotland – particularly SMEs and those in currently unregulated sectors – to assess the cyber threat to their operations and select an appropriate set of controls or guidance to help them work progressively towards strengthening their cyber resilience. As part of this work, consideration will be given to making clear how such a framework or pathway could align with the core common supply chain cyber security requirements of public and larger private and third sector organisations. This should help drive greater consistency in the demands placed on SMEs in supply chains. **(Key Action 2)**

9. The Scottish Government will work with the NCRLB and private sector partners to explore the potential for a more joined up, integrated, national-level approach to cyber resilience across the Scottish private sector (and public and third sectors). This will include consideration of initiatives to improve cooperation and collaboration between key sub sectors of the Scottish economy that rely on one another for continued effective operation, with a view to strengthening the overall cyber resilience of Scotland. **(Key Action 3)**

B. Strengthening awareness-raising and systems of advice and support

10. The Scottish Government will work with the National Cyber Resilience Leaders Board, the NCSC and key partners to strengthen the promotion of good cyber resilience practice at all levels in the private sector. This work will include the strengthening of systems of advice and support for the private sector (and other sectors) in Scotland, and activity aimed at raising awareness of the economic importance of cyber resilience and effective ways of achieving it. An initial "target landscape" for advice and support will be identified with the goal of achieving this by spring 2019, and thereafter improved on an ongoing basis. **(Key Action 4)**

C. Strengthening partnership working, leadership and knowledge sharing in Scotland's private sector

11. The Scottish Government will work in partnership with the NCSC, UK Government and key Scottish private sector organisations to help catalyse better cyber resilience practice across Scotland's private sector. From summer 2018, a cross-sectoral group of private sector cyber catalyst organisations will work with the Scottish Government and the NCSC to develop and support implementation of practical solutions to key challenges on an ongoing basis, with an initial focus on:

- strengthening leadership for, and helping drive greater awareness and uptake of good cyber resilient behaviours in, the Scottish SME community, including through the use of supply chain measures;
- strengthening coordination and knowledge sharing in respect of cyber resilience across key organisations operating in Scotland;
- supporting and promoting uptake of key educational initiatives in Scotland, including cyber security apprenticeships;
- helping shape recommendations in respect of the potential for a more joined up, integrated, national-level approach to cyber resilience across the Scottish private sector.

Appropriate support will be offered to the private sector cyber catalysts to help achieve desired outcomes. The Scottish Government will play a leading role in supporting and driving forward the work of the group, and identifying avenues for delivery. **(Key Action 5)**

D. Supply chain cyber security – leveraging requirements to improve the cyber resilience of Scotland's SME community

12. The Scottish Government will work with private sector organisations and key partners to clarify the common core cyber resilience requirements that are currently placed on third party suppliers, and their relationship to wider standards and guidance. Thereafter, the potential for greater cross-sectoral alignment and cooperation in respect of common core supply chain requirements will be explored, with the goal of promoting greater coherence across Scotland's public, private and third sectors. A key aim of this alignment will be to improve the cyber resilience of Scotland's SME community as part of the supply chain of larger private sector organisations. **(Key Action 6)**

E. Strengthening incentives to improve cyber resilience in Scotland's private sector

13. The Scottish Government and the National Cyber Resilience Leaders Board will work with the UK Government and key private sector stakeholders to consider how best to strengthen incentives to support the uptake of cyber security standards/accreditation, and the adoption of good cyber resilience practice more generally. This will include the continuation of a modified voucher scheme to support the achievement of Cyber Essentials or Cyber Essentials Plus by Scottish SMEs. On the basis of activity across all action plans, we aim to at least double the number of organisations across the public, private and third sectors holding Cyber Essentials or Cyber Essentials Plus certification in Scotland during Financial Year 18-19. **(Key Action 7)**

F. Benchmarking, Monitoring and Evaluation

14. The Scottish Government will work with the NCRLB, the NCSC, Competent Authorities/ Regulatory Bodies and key partners to develop appropriate benchmarking, monitoring and evaluation arrangements for implementation by spring 2019. **(Key Action 8)**

A summary of these key actions, along with timelines, can be found at **Annex A** to this action plan.

INTRODUCTION AND BACKGROUND

1

1. INTRODUCTION AND BACKGROUND

1. **Safe, secure and prosperous: a cyber resilience strategy for Scotland**[1], was published in 2015. It set out the Scottish Government's vision for Cyber Resilience in Scotland:

Scotland can be a world leader in cyber resilience and be a nation that can claim, by 2020, to have achieved the following outcomes:

(i) Our people are informed and prepared to make the most of digital technologies safely.

(ii) Our businesses and organisations recognise the risks in the digital world and are well prepared to manage them.

(iii) We have confidence in, and trust, our digital public services.

(iv) We have a growing and renowned cyber resilience research community.

(v) We have a global reputation for being a secure place to live and learn, and to set up and invest in business.

(vi) We have an innovative cyber security, goods and services industry that can help meet global demand.

These outcomes are interdependent – progress towards one may underpin or drive progress towards others.

2. "Safe, secure and prosperous" is closely aligned with the UK National Cyber Security Strategy[2], which sets out the UK Government's strategic approach to making the UK secure and resilient in cyberspace. Cyber security is a reserved matter, but it has strong implications for the resilience and security of Scotland's economy. Scotland has unique partnerships and networks that support resilience across all sectors. As such, the Scottish Government works closely with key partners such as the UK National Cyber Security Centre to ensure appropriate alignment between work on cyber resilience at the UK and Scottish levels.

3. This action plan has been produced by the National Cyber Resilience Leaders Board (NCRLB) and its private sector representatives, in partnership with the Scottish Government. It has drawn heavily on the views and expertise of key private sector stakeholders, including representatives of the SME sector. It sets out the key actions that the Scottish Government and key partners in the private sector will take during 2018-20, in order to make progress particularly towards outcomes (ii) and (v) above:

> ***Our businesses and organisations recognise the risks in the digital world and are well prepared to manage them.***
>
> ***We have a global reputation for being a secure place to live and learn, and to set up and invest in business.***

It aims to realise the opportunities presented by Scotland's strong cyber resilience networks and communities of interest to position Scotland as a world leading nation in cyber resilience.

[1] http://www.gov.scot/Publications/2015/11/2023

[2] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

The goals of this action plan and its relationship to wider work on cyber resilience in Scotland

4. The specific goals of this action plan are to move Scotland closer to the above outcomes, and to our vision of being a world leading nation in cyber resilience, by:

- Driving greater levels of **good cyber resilience practice** across Scotland's wider private sector, particularly our **SME community**, thus helping to raise overall fundamental levels of cyber resilience in Scotland's private sector;
- developing greater **cross-sectoral coherence** of work on cyber resilience within Scotland's private sector, and exploring the potential for a more **integrated, joined-up, national-level approach** to the cyber resilience of Scotland's private sector as part of wider UK-level arrangements.

  This will be achieved in part by providing appropriate **support** to work on cyber resilience that is currently being undertaken at the UK and Scottish levels with private sector organisations that form part of the **critical infrastructure** of Scotland; and
- promoting **greater coherence and alignment** of work on cyber resilience across **the private sector and Scotland's public and third sectors**.

5. The Scottish Government and the NCRLB are developing and implementing complementary action plans for the **public and third sectors**. The first of these, the Public Sector Action Plan on Cyber Resilience, was published on 8 November 2017[3], and the Third Sector Action Plan is expected to be published alongside this Private Sector Action Plan. The aim is for all sectors in Scotland to adopt a broadly aligned approach to cyber resilience where possible. As such, development of this Private Sector Action Plan has had regard to the Public Sector Action Plan and the Third Sector Action Plan.

The NCRLB is of the view that the Scottish and UK Governments should support Scotland's private, public and third sectors to work together as partners, ensuring strong leadership around cyber resilience and digital enablement for the benefit of all citizens and businesses. Many private and third sector organisations are both the supply chain and the purchasers of public sector services, thus increasing the importance of commonality and coherence. In simple terms, the more our citizens and organisations speak a "common language" around cyber resilience, the more likely it is that we will be able to work in partnership to make progress. Identifying common core cyber resilience requirements across more sectors, and encouraging sharing of good practice around cyber resilience, is also expected to help promote greater levels of cyber resilience and potentially reduce compliance burdens.

6. The Programme for Government 2017-18 also committed the Scottish Government and key partners to develop action plans in the following key areas:

- **Learning and Skills**, focused on how to ensure that (i) our citizens have the appropriate understanding, knowledge and behaviour to live and work safely and securely in the digital world; and (ii) our cyber specialist workforce have the appropriate skills. The success of this action plan, which was published on 7 March 2018, will be vital to establishing a genuine **culture of cyber resilience** in Scotland (including amongst private sector organisations), and to the longer term success of the private, public and third sector action plans.

[3] https://beta.gov.scot/policies/cyber-resilience/

- **Economic opportunity**, focused on how to seize fully the economic opportunities presented by the achievement of fundamental cyber resilience, and take a visible, global role in thought-leadership, research, development and innovation relating to cyber resilience. We expect this action plan to be published in Q3 2018.

7. To ensure efficiency and maintain momentum, these plans are being developed to differing timelines. Work to identify and take account of the strong interrelationships between the actions set out in this plan and other action plans is being undertaken on a regular basis by the Scottish Government and the NCRLB. In the future, our expectation is that this private sector action plan will be merged with other action plans to constitute a single action plan focused on Scotland's cyber resilience, as part of work on our overall security and resilience.

8. While the focus of this action plan is on cyber resilience, the actions set out in this plan will also help ensure that Scottish private sector organisations are meeting key requirements in respect of **protecting personal data**, which will be strengthened by the General Data Protection Regulation (GDPR)[4] from May 2018. The Information Commissioner has, for example, noted publicly that achieving Cyber Essentials accreditation can assist with preparing for GDPR. Private sector organisations should in general consider how work on cyber resilience aligns with wider work on GDPR compliance.

9. The action plan recognises that the private sector in Scotland is of considerable scale and complexity. SMEs account for 99.4% of Scottish private sector organisations and 55% of private sector employment[5], but Scotland is also home to a number of large, multinational companies, who have reporting structures and regulatory calls on them from outwith Scotland. Some companies are of significant technical sophistication, or handle significant amounts of personal data, while others operate only very basic IT systems and may be concerned with delivery of goods or services on a small scale. One of the biggest challenges in developing this action plan has been the need to take account of these significant differences in scale and risk profile. The NCRLB private sector lead representatives and other key private sector partners have offered advice to help ensure the action plan meets multiple needs.

The importance of cyber resilience to Scotland's private sector

10. "Cyber resilience" means being able to prepare for, withstand, and rapidly recover and learn from deliberate attacks or accidental events that have a disruptive effect on interconnected technologies. Cyber security is a key element of being resilient, but cyber resilient people and organisations recognise that being safe online goes far beyond just technical measures. By building understanding of cyber risks and threats, they are able to take the appropriate measures to stay safe and get the most from being online.

[4] https://ico.org.uk/for-organisations/data-protection-reform/

[5] See: http://www.gov.scot/Topics/Statistics/Browse/Business/Corporate/KeyFacts

11. The importance of ensuring cyber resilience in Scotland's private sector has never been greater. In the view of the NCRLB, there are compelling arguments for Scotland's private sector to work together to improve overall levels of cyber resilience now, supported by the Scottish Government. A number of factors make this so. They include:

(i) The scale and nature of the cyber threat to the digital systems upon which our economy increasingly relies, and the risks this presents to: our ambitions for Scotland's digital economy; our overall security and resilience; and the success of individual businesses in Scotland: Scotland's refreshed digital strategy[6] emphasises that the Scottish Government and its partners are fully committed to harnessing the benefits of digital technology across our economy, in order to deliver a step-change in productivity. Digital connectivity offers significant opportunities for innovation and inclusive economic growth. However, with these opportunities come new threats and vulnerabilities, and it is imperative that we take these seriously and take action to address them and minimise their disruptive effects. Much of our prosperity now depends on our ability to secure our technology, data and networks from the threats we face. Yet cyber attacks are growing more frequent, sophisticated and damaging when they succeed.

The National Crime Agency describes the cyber threat as a "major and growing threat" to UK businesses. It assesses that the cost of cybercrime to the UK economy is billions of pounds per annum, and that the accelerating pace of technology and criminal cyber capability development currently outpaces the UK's collective response to cybercrime. It is assessed that the number and severity of cyber incidents affecting private sector organisations will **continue to increase** at a significant rate. These threats come from a variety of sources, including hostile state actors, cyber criminals, political activists, opportunists and others. The rise of internet connected devices gives attackers more opportunity. The National Crime Agency reported that 2017-18 was "punctuated by cyber attacks on a scale and boldness not seen before".[7]

Our SME and micro-business community is particularly at risk. Cyber attackers increasingly understand that SMEs typically have more digital assets than an individual, but less security than a large corporation. This can effectively put small businesses in cyber attackers' "sweet spot", leaving them at higher than average risk for attack. Many of Scotland's c. 340,000 micro businesses[8] operate on mobile devices, the security of which may be fundamental to those businesses' continued operation.

The threat can be **targeted or indiscriminate**. Even where cyber criminals attempt to target specific organisations, the nature of the cyber threat is such that there can be significant unintended wider consequences. Businesses of all sizes in Scotland need to understand the risks they face, and be confident they can take proportionate action to mitigate it. The nature of the cyber threat is such that this action is most likely to be effective if private sector organisations commit to **working together**, both within the private sector and across the public and third sectors, to mitigate the cyber threat across Scotland. The greater the "herd immunity" to the cyber threat in Scotland, the more secure all businesses are likely to be.

[6] http://www.gov.scot/Resource/0051/00515583.pdf

[7] http://www.nationalcrimeagency.gov.uk/publications/785-the-cyber-threat-to-uk-business/file

[8] Businesses with fewer than 10 employees and sole traders – see: http://www.gov.scot/Topics/Statistics/Browse/Business/Corporate/alltables

(ii) Legislative changes and their potential legal, financial and reputational impact: The new GDPR and the Security of Network and Information Systems (NIS) Directive both come into force in May 2018, and in combination place new duties on private (and public and third) sector organisations to ensure the protection of personal data and the continuity of essential services reliant on network and information systems, and to report personal data/cyber security breaches. Private sector organisations subject to these provisions could face significantly increased administrative fines of up to £17 million for data breaches or cyber security failures leading to service failure. These legislative changes should drive greater awareness of the importance of cyber resilience and the need to have appropriate technical protections for personal data in place. The actions set out in this plan are aimed at supporting businesses to understand how better to comply with the cyber aspects of such legislative duties.

(iii) Economic opportunity. The flip side of these threats is that there is a significant economic opportunity for Scottish businesses, whether collectively or at an individual level, in working to become more cyber resilient. These opportunities include:

- **Avoidance of cost and disruption to business**: We cannot fully evaluate the likely impacts of a large, global scale attack across public, private and third sectors but it is widely anticipated that there will be an attempt to achieve this in the near future. Available evidence suggests there would be significant short and longer term disruption across critical digital infrastructure and, as a result, serious disturbance to business activity which would affect us all. The NCSC has indicated publicly that the UK is likely to face its first major "category one" cyber incident in the next few years. (For the purposes of comparison, the WannaCry ransomware attack in May 2017 was a category two incident.) Lloyd's of London has reportedly assessed that a serious cyber-attack could cost the global economy more than £92bn, which is as much as catastrophic natural disasters such as Hurricanes Katrina and Sandy. This risk adds to the urgency with which all sectors need to review and address their security.

  Recent research by DCMS[9] found that four in ten of all UK businesses suffered a cyber breach or attack in a 12 month period. Nearly seven in ten medium/large businesses identified a breach or attack, while 42% of micro or small businesses identified a breach during the same period[10]. The research also showed that businesses holding electronic personal data on customers, and those that have staff using personal devices for work (BYOD) were more likely to have experienced cyber breaches than those that do not. Small businesses may face failure or bankruptcy as a result of ransomware attacks if they have not taken appropriate cyber security precautions. Insurers may also increase or reduce insurance costs depending on their assessment of a business' vulnerability to cyber-attack.

  NCSC note that cyber criminals are becoming increasingly sophisticated, and are able to make judgements on "Return on Investment" when deciding who to target where – the harder the target, the smaller the ROI, the less incentive there is to invest time and money in an attack on those targets. Making Scotland overall, and individual sectors and businesses within Scotland, more cyber resilient may therefore help tip the balance around these judgements in the future. This may be expected to bring economic advantage to Scottish companies through an ability to continue operations unaffected by common cyber attacks.

[9] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018

[10] Ibid.

- **Productivity and business growth**: As the digital economy matures, it is expected to lead to increased productivity and increased online trading. However, to take advantage of digital innovation, businesses and their employees must be able to operate confidently and safely in the digital world. Cyber resilience is fundamental to productivity and business growth – it supports companies to take calculated risks and should be at the forefront of new business development.
- **Reputation**: As citizens' understanding of the cyber threat increases, and as the profile of cyber attacks and data breaches continues to rise, the importance that consumers, investors, insurers and others place on cyber resilience is likely to increase. Being able to demonstrate that cyber security is taken seriously – that services and customer data are protected and resilient – will become increasingly important to a business' reputation, which in turn may impact on overall performance.
- **Inward investment and exporting**: More broadly, Scotland has an ambition to become a world leading nation in cyber resilience. An ability to demonstrate that Scotland has strong levels of overall cyber resilience across its private, public and third sectors could become an increasingly important factor in attracting international investment and the development of a cyber security cluster in Scotland. The presence of a vibrant cyber security cluster within Scotland should be to the benefit of all businesses in Scotland, and will assist in keeping in-demand talent and skills close to home and producing the goods and services that Scottish businesses and public bodies need to be cyber resilient. Demand in the world wide security service industry is currently outstripping supply, providing Scotland with an opportunity also to sell goods and services worldwide. Our **learning and skills** action plan has set out proposals to ensure a strong talent pipeline is in place in Scotland.
- **Seizing the economic opportunity**: The IT Security industry is fast moving and dynamic. Other countries are already moving to seize the economic opportunity that an increased focus on cyber resilience offers, and major operators are currently exploring a range of potential bases to locate future developments. The NCRLB private sector lead representatives have made clear their view that if Scotland does not move at pace to realise the economic opportunities presented by work on cyber resilience, it risks losing out to competitors. This only adds to the urgency for implementation of this action plan, the need for momentum to be maintained, and appropriate support (including funding) from government and industry.

  As noted earlier in this plan, a separate **economic opportunity** action plan focused on how to seize fully the economic opportunities presented by the achievement of fundamental cyber resilience, and take a visible, global role in thought-leadership, research, development and innovation relating to cyber resilience, is under development and will be published later in the year.

12. Against this background, the NCRLB has articulated its view that Scotland's private sector must make demonstrable progress towards establishing fundamental standards of cyber resilience that are in line with world-leading nations. Cyber resilience should be seen as just as fundamental to business practice standards in Scotland as health and safety currently is.

13. The NCRLB emphasises that cyber resilience is as much a **cultural** issue as a technical one. They view it as vital that Scotland's private sector organisations understand and manage the cyber threat at **Board/owner level**, and take action to promote a culture of cyber security at all levels of the organisation (the Cyber Resilience Learning and Skills Action Plan sets out the actions we will take to achieve this transformational cultural change through our systems of formal and informal learning in Scotland). The NCRLB views it as being vitally important that smaller businesses are supported to understand and manage the threat in an appropriate and proportionate way – a one-size-fits-all approach to cyber resilience in Scotland's private sector is not desirable.

Current levels of cyber resilience in Scotland's private sector

14. Currently, we do not have a comprehensive picture of the state of cyber resilience across the Scottish private sector. Work is ongoing to build a strong understanding of the cyber resilience of private sector Critical National Infrastructure (CNI), in support of UK-level work on CNI. Achieving a greater understanding of private sector cyber resilience beyond CNI areas will be important to our ability to establish a baseline and measure progress over time. Key Action 3 in this action plan proposes work that may include improved mapping of the cyber-specific interdependencies between strategic companies in Scotland and other parts of the private, third and public sectors, with a specific focus on identifying ways of strengthening the overall cyber resilience of Scotland at a systemic level. Key Action 8 sets out a commitment to develop appropriate monitoring arrangements on the basis of existing and future information sources, to improve our understanding of the extent to which good cyber resilient behaviour is being adhered to across the Scottish private sector.

15. Many larger companies operating in Scotland are already compliant with the highest levels of cyber security and regularly report on this to shareholders and regulators (e.g. the FCA). There is important work being done by the UK and Scottish Governments, and regulatory bodies, to improve the cyber resilience of key private sector Critical National Infrastructure in areas such as energy, civil nuclear, finance, transport and communications. Scottish Local Authorities and Business Gateway have also been undertaking work to improve the fundamental cyber resilience of mainstream companies, although anecdotally there is significant work to do to ensure even some of Scotland's largest private sector organisations meet appropriate standards of cyber resilience. The introduction of UK legislation to implement the EU NIS Directive from May 2018 will see the establishment of Competent Authorities to oversee the cyber resilience of Operators of Essential Services in some key sectors, adding further weight to these efforts.

This plan proposes further work on a cross-sectoral basis to help support and complement these activities, by working in partnership with key private sector companies in a "cyber catalyst" group (see Key Action 5).

16. At the SME level, there is wide variation in the ability of Scottish companies to ensure their own cyber resilience, although it is clear that the majority do not have access to the resources or expertise that larger corporates can draw on. Federation of Small Business (FSB) representatives have noted that SMEs struggle to understand and implement the very wide variety of advice currently available on what to do to become more cyber resilient. This plan proposes work to improve systems of advice and support, which will include promotion of simple, straightforward, authoritative messages that are relevant to small businesses, helping raise awareness and promote better cyber resilience practice across Scotland's private sector (see Key Action 4).

There has been financial encouragement (£1,500 grants) through the Digital Scotland Business Excellence Partnership for 200 SMEs to become Cyber Essential certified – in 2016 Scotland was the only part of the UK providing this initiative. Key Action 6 sets out proposals for a modified version of this scheme to be continued, drawing on learning from the initial phase.

17. A number of mechanisms exist to encourage the sharing of threat intelligence across the Scottish and wider UK private sector. The financial sector has relatively well developed forums for sharing such intelligence with trusted partners. The NCSC has worked with industry to set up the Cyber Security Information Sharing Partnership (CiSP) to provide a secure environment in which to share cyber threat intelligence, increasing situational awareness and reducing the impact on businesses across Scotland and the rest of the UK. The Scottish Government has used National Cyber Security Programme funding to support a CiSP (and Cyber Essentials) coordinator role, located within the Scottish Business Resilience Centre (SBRC), to promote membership of CiSP, including in the private sector. Since the coordinator was appointed in November 2016, active membership of SciNet (the Scotland-specific area of CiSP) has increased from 122 to 307, an increase of 152%. This makes SciNet the largest geographical group on CiSP within the UK, and the second largest private membership group overall at the time of writing. Activity to promote increased active Scottish private sector membership of CiSP, with a goal of ensuring our businesses are better informed around the cyber threat, will be supported by this plan.

18. There is only limited information at present on the levels of cyber security accreditation achieved across different sectors in Scotland. Some larger companies are accredited to relatively sophisticated standards such as ISO 27001/2, although there is no publicly available central registry to make clear which companies have achieved this, and to which parts of their networks such accreditation applies (companies holding such accreditation often choose to advertise their compliance for business/reputational purposes). Uptake of the NCSC-endorsed Cyber Essentials[11] scheme in Scotland's private sector is improving. As of May 2018, 426 live Cyber Essentials certificates and 62 live Cyber Essential Plus certificates have been issued in Scotland. Those figures represent a 78% and 265% increase over the 12 months from May 2017 (a total 91% increase for both types of certificate combined). The number of Cyber Essentials certifying bodies in Scotland is increasing.[12] These figures suggest growing awareness of the scheme and the importance of the good practice it promotes amongst organisations in Scotland.

[11] The Cyber Essentials scheme offers a mechanism, endorsed by the National Cyber Security Centre, for organisations to demonstrate to customers, investors, insurers and others that they have adopted five critical network controls to guard against the most common forms of cyber-attack. taken essential precautions. See: https://www.cyberessentials.ncsc.gov.uk/ for further details.

[12] A list of certifying bodies operating in Scotland is available at the SBRC website: https://www.sbrcentre.co.uk/services/cyber-services/cisp-and-cyber-essentials/trusted-partners/

Scottish public sector organisations do not currently require the adoption of certification such as Cyber Essentials by private and third sector organisations wishing to do business with them (the UK Government currently mandates this only if bidding for central government contracts which involve handling of sensitive and personal information and provision of certain technical products and services). The practice of private sector organisations with extensive supply chains in Scotland varies significantly, with no consistent approach currently in place (although there is effectively much commonality of approach). Implementation of the NIS Directive, and NCSC technical guidance in respect of supply chain security, may assist with developing greater consistency in the key sectors it covers.

Both this plan and the Public Sector Action Plan on Cyber Resilience[13] propose work to help improve the uptake of appropriate cyber security accreditation/certification across Scotland's private sector, particularly in respect of Cyber Essentials and Cyber Essentials Plus. These include proposals to develop appropriate, proportionate, more aligned supply chain procurement policies in respect of cyber security accreditation/certification.

On the basis of all this activity, we aim to at least double the number of organisations across the public, private and third sectors holding Cyber Essentials or Cyber Essentials Plus certification in Scotland during Financial Year 18-19. (See Key Actions 2, and 4 to 6)

19. There is currently a lack of a clear **framework or pathway** for Scottish private (and public and third) sector organisations to work within and towards when managing the cyber risk, providing assurance and opportunities for benchmarking. Feedback suggests this is particularly problematic for SMEs, who lack the resources that large companies have to make sense of the many different existing standards. Cyber Essentials and Cyber Essentials Plus offer a clear entrance point – however, even these may be beyond the initial reach of some micro businesses who have yet to achieve even a basic understanding of the cyber threat. Scottish private sector organisations have indicated that achieving greater clarity on a progressive cyber threat management model beyond Cyber Essentials, towards more sophisticated measures thereafter, would be helpful.

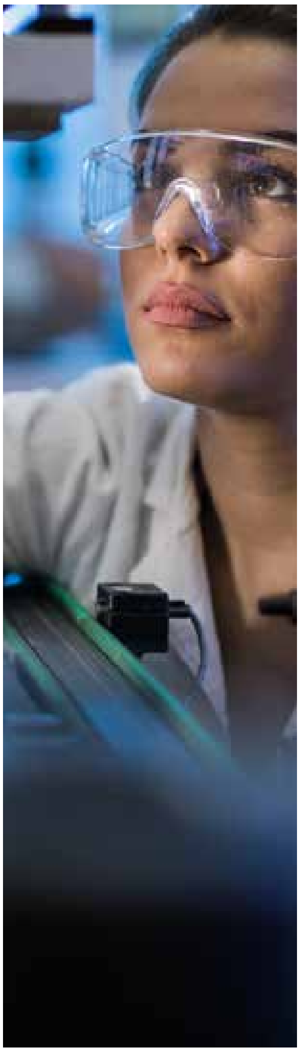
Such a framework or pathway would need to have a particular emphasis on supporting SMEs to understand the cyber risk and what options they have to manage it on a progressive basis. It must encompass standards or guidance that, at more sophisticated levels, ensure a robust, holistic, effective approach to cyber resilience, avoiding "checklists" and encouraging the management of cyber security with a multi-layered approach that encompasses people, processes and technology. It must also be adaptable to ensure it keeps up with fast-paced technological change and emerging threat. This action plan sets out proposals for the Scottish Government and the NCRLB to work with key private sector organisations, and key partners such as the NCSC, to explore the potential for the development and endorsement of such a framework or pathway, making it easier for our businesses (especially SMEs) to understand the cyber threat and work progressively towards more sophisticated ways of managing it. (See Key Action 2)

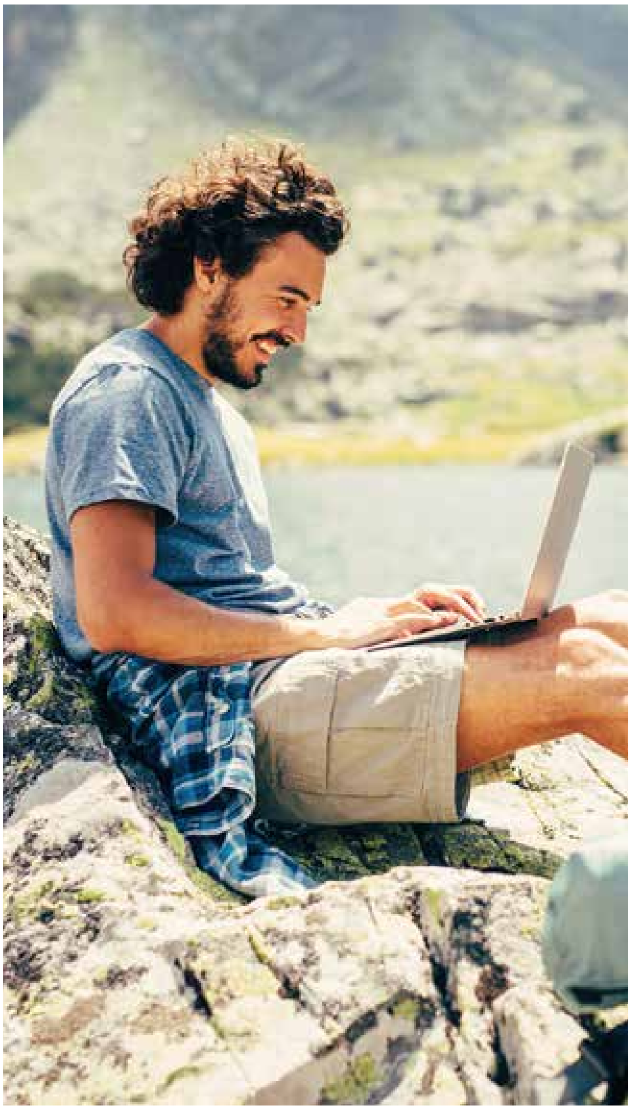
[13] See: https://beta.gov.scot/policies/cyber-resilience/cyber-resilience-action-plans/

20. Some private sector partners have argued there is currently a need for a more integrated, joined-up, national level approach to the cyber resilience of Scotland's private sector. This action plan proposes that consideration of this issue be undertaken in partnership with private sector cyber catalyst organisations, with a view to shaping recommendations to the Scottish and/or UK Governments. (See Key Actions 4 and 5)

21. Other private sector partners have argued that in the longer term a more fundamental approach to cyber security is required, treating digital communications services similarly to the way in which other utilities in Scotland and the rest of the UK are treated. Consideration will be given to undertaking initial research into this area through the SICSA Cyber Nexus and/or alternative expert groups, and identifying any resulting potential opportunities for Scotland.

KEY ACTIONS





2

2. KEY ACTIONS

Introduction

22. This section provides detail on the key actions that the Scottish Government and its partners will take during 2018-20 to help address these issues and ensure greater confidence in standards of cyber resilience in Scotland's private sector.

23. Delivery of the action plan will be coordinated and led by the Scottish Government's Cyber Resilience Unit, working as close partners with the NCRLB, the NCSC, the UK Government and key Scottish private sector partners.

24. The Scottish Government is clear that it cannot achieve a strong, cyber resilient private sector in Scotland by taking action on its own. While the Scottish Government will offer targeted funding, support and direction where it is able to do so (as outlined in this action plan), achieving a world leading cyber resilient private sector will also require leadership, commitment and resource from private sector organisations of all sizes in Scotland. As work is taken forward to drive higher levels of cyber resilience in Scotland's public and third sectors, potential links or opportunities for cross-sectoral knowledge-sharing will also be identified.

25. Action to promote cyber resilience in Scotland's private sector will of course continue beyond 2018-20. This action plan will be refreshed at the end of this period, to take stock of progress to date and ensure continued progress.

Collaborative working, levers and influence

26. The Scottish Government's preferred approach to driving up levels of cyber resilience in Scotland's private sector is one of **collaborative working** with partners – to that end, this action plan sets out proposals to work in close partnership with the private sector, based on a shared understanding of the importance and benefits of strong cyber resilience across the sector.

27. There are, nevertheless, some areas in which more direct levers of influence may be used to influence private sector partners in different sectors and of different sizes to take action in respect of cyber resilience. These levers sit at different levels (UK, Scottish, local) and with different organisations. The key actions set out in this action plan seek to maximise use of these levers, which include:

- **Legislation and regulation**: Cyber security is a reserved issue. As part of the "Defend" strand of the National Cyber Security Strategy, the UK Government is working with international partners to make sure the right regulatory framework is in place in the UK and Europe – one that incentivises better cyber security but avoids unnecessary burdens on business. This work includes implementation of the **Security of Network and Information Systems (NIS) Directive** into UK law from May 2018, which will place requirements on operators of essential services, including in key areas of the private sector, to improve certain aspects of cyber security. Some areas of the private sector (e.g. finance and civil nuclear) are effectively covered by other regulations. The **General Data Protection Regulation** (GDPR) will also come into force from May 2018, and will apply to all private sector organisations handling personal data. Both pieces of law will effectively require private sector organisations to ensure they have appropriate cyber security arrangements in place, either to ensure continuity of essential services or to protect personal data. Significant **fines** will be able to be levied by the Information Commissioner or Competent Authorities in the event of breaches.

- **Existing regulatory and advisory practice (inc. Critical National Infrastructure)**: Regulators in different sectors already have responsibility for ensuring and advising on the security and resilience of some private sector organisations in Scotland. This is particularly the case for Critical National Infrastructure, where cyber security is an area of increasing focus. The UK's NCSC is taking forward a significant programme of work to improve levels of cyber resilience in Critical National Infrastructure. The Scottish Government has also made progress in integrating consideration of cyber resilience into already embedded strategies and processes in respect of critical infrastructure, including the 2011 Critical Infrastructure Resilience Strategy and its associated work programme.
- **Supply chain requirements**: Whilst large companies account for only a small percentage of total business numbers, they represent a significant share of output, and they operate materiel, service and information supply chains that reach deep into Scottish and wider UK and international economic structures at all levels. SME supply chain scope is often smaller and there may not be as many chain partner relationships to manage, but they often form part of more complex business chain activity. The NCSC notes[14] that cyber criminals can identify the organisation with the weakest cyber security within the supply chain, and use the vulnerabilities present in their systems to gain access to other members of the supply chain, including large corporates.

  Large firms are both suppliers and contractors and there is an interdependency between the public and private sectors. The public sector in Scotland is a significant purchaser of private sector goods and services. Similarly, larger Scottish private sector organisations have extensive supply chain arrangements, within and outside Scotland. By placing proportionate requirements on private sector organisations in respect of cyber security, both to ensure their own cyber security and to drive up overall levels of cyber resilience in Scotland, public sector organisations can potentially raise awareness of the importance of cyber resilience and wield significant influence over the uptake of good practice and accreditation, not only in the private sector but also in the third sector. The Public Sector Action Plan on Cyber Resilience[15] sets out a proposal to develop a policy on supply chain cyber security for the public sector, which is expected to align with NCSC guidance on supply chain security (including requirements in respect of Cyber Essentials certification, based on management of risk). This private sector action plan includes proposals on supply chain cyber security at Key Action 6.

[14] https://www.ncsc.gov.uk/guidance/supply-chain-security

[15] Available at https://beta.gov.scot/policies/cyber-resilience/cyber-resilience-action-plans/

- **Financial and other incentives**: While the public sector (in common with other sectors) at all levels is currently operating under significant resource constraints, there is the potential for targeted financial and other incentives to be offered to private sector operators (particularly SMEs) to drive a greater focus on cyber resilient behaviour. These could conceivably include, for example, subsidies for organisations achieving or seeking to achieve certain levels of cyber security accreditation, or reductions in insurance premiums.

On this latter point, members of the NCRLB steering group have noted that **cyber insurance** is an increasingly popular method of transferring risk associated with cyber security. However, the cyber insurance sector is immature. The limitations of cover offered, especially for SMEs, are currently being tested by sizeable cross-industry claims, which may prompt insurers to re-evaluate the scope of policies offered. Discussions with the insurance industry, which include a focus on the comprehensive nature of cover and how implementation of standard security measures (such as Cyber Essentials) should reduce premiums/extend cover, are ongoing.

28. In developing this action plan, the Scottish Government and the NCRLB have sought the views of the UK Government (including the NCSC) and key regulatory bodies. These partners will also play a vital role in the implementation of the plan, and arrangements will be put in place to ensure continued collaboration and coordination as the actions outlined below are taken forward.

KEY ACTIONS

A: Develop a common approach to cyber resilience across the Scottish private sector

Key Action 1

The Scottish Government and the NCRLB will work to ensure that the views of the Scottish private sector, including SMEs, help inform UK-level consideration of whether there is a case for extending regulatory requirements around cyber resilience more widely across parts of the private sector. This will include a particular focus on ensuring input from any sectors that are critical to the functioning and health of the Scottish economy, and key areas of competitive advantage. (Timing: on an ongoing basis.)

29. The legislative and regulatory framework around cyber security in the UK is currently relatively under-developed. The Scottish Government welcomes the introduction of UK-wide legislation to implement the EU NIS Directive from May 2018, which will place requirements on operators of essential services to ensure they have appropriate arrangements in place to withstand, recover and learn from cyber attacks and other disruptive events. The GDPR will also place general requirements on organisations to ensure the security of systems dealing with personal data.

30. The NIS legislation will only cover operators of essential services in a limited number of sectors of the Scottish economy, namely:

- Electricity (electricity suppliers and generators, Single Electricity Market operators, transmission, distribution)
- Oil (upstream and downstream oil transmission, oil production, refining and treatment and storage)
- Gas (consumer supply, transmission, distribution, storage, upstream petroleum pipeline operators, LNG supply/storage, gas processing operations)
- Transport (air, maritime, rail, road)
- Water (supply of potable water to households)
- Health (NHS Boards in Scotland)
- Digital infrastructure (top level domain name registries, domain name services providers, Internet Exchange Point Operators)
- Digital service providers (online marketplaces, online search engines, cloud computing services)

Some sectors are exempt from some aspects of the Directive where there are provisions within existing regulations which are, or will be, at least equivalent to those the NIS Directive specifies (e.g. finance and civil nuclear sectors). However, many of the principles and technical guidance that the NCSC has produced to support implementation of the NIS Directive are sector-neutral with wide relevance.

31. The UK Government is expected to undertake a post-implementation review of the NIS Directive in due course, to take stock of its effectiveness and take further decisions on scope.

32. The Scottish Government strongly believes that a **partnership approach** with industry in Scotland will be key to success in driving higher standards of cyber resilience. The Scottish Government will work with the NCRLB and private sector partners (including the private sector cyber catalysts – see Key Action 5) to ensure that the views of the Scottish private sector are factored into UK Government consideration of whether there is a case for the requirements of the NIS legislation or other regulations to be extended, over time, to other key sectors of the economy. Any such decision should include consideration of the specific resilience requirements, and the relative importance of, key sectors of the Scottish economy, as well as the requirement to avoid placing undue burdens on the SME community. This will help ensure that any decision taken to extend UK-level legislation in the future (e.g. in the event that insufficient progress is being made in specific sectors on an issue that is vital to the overall resilience of the UK) can be rolled out as effectively as possible across Scotland.

In particular, the Scottish Government will support effective consideration of whether there is a case for extending regulatory requirements around cyber resilience to those sectors of the Scottish private sector where Scotland enjoys a **comparative advantage** that can be maintained and strengthened through active, safe participation in the international digital economy. Key sectors for consideration (which include reserved and devolved sectors) may include:

- Food and drink (including agriculture and fisheries)
- Creative industries
- Sustainable tourism
- Professional services (including legal services and accountancy)[16]
- Life sciences
- Manufacturing/engineering
- Communications (telecoms, internet and broadcast)[17]
- Space
- Chemicals
- Major retailers

33. This work will be undertaken on an **ongoing basis**, in line with the timetable set by the UK Government for consideration of potential extension of regulatory requirements around cyber resilience.

[16] In line with Article 1 (7) of the Directive, the banking and financial market infrastructures sectors within scope of the Directive will be exempt from aspects of the Directive where provisions at least equivalent to those specified in the Directive will already exist by the time the Directive comes into force. Firms and financial market infrastructure within these sectors must continue to adhere to requirements and standards as set by the Bank of England and/or the Financial Conduct Authority.

[17] Some operators in this area will already be subject to the new NIS requirements.

Key Action 2

The Scottish Government and the National Cyber Resilience Leaders Board will work with the NCSC and key partners to consider options for developing a Private Sector Cyber Resilience Framework or Pathway. This would aim to provide a simple, structured way for organisations in Scotland – particularly SMEs and those in currently unregulated sectors – to assess the cyber threat to their operations and select an appropriate set of controls or guidance to help them work progressively towards strengthening their cyber resilience.

As part of this work, consideration will be given to making clear how such a framework or pathway could align with the core common supply chain cyber security requirements of public and larger private and third sector organisations. This should help drive greater consistency in the demands placed on SMEs in supply chains.

Private sector organisations in Scotland – particularly SMEs and those in currently unregulated sectors – will then be encouraged, incentivised and supported to work towards implementing the most appropriate cyber resilience approach, based on the cyber threat to their operations. (Timing: by spring 2019, and thereafter on an ongoing basis dependent on confirmation of viability)

34. There exists a wide range of standards, guidance and accreditation schemes within the UK and internationally that can help provide assurance to private sector organisations and their customers with regard to managing the cyber threat. However, Scotland and the wider UK currently lack a clear, graduated hierarchy of such measures that can assist private sector organisations (particularly smaller or micro businesses) to identify the most appropriate outcomes, standards or accreditations to work towards in order to manage progressively higher levels of cyber threat, and to offer a way of benchmarking themselves against other private sector organisations.

35. Key private sector partners have indicated their support for the development of an easily recognisable Private Sector Cyber Resilience Framework or Pathway, with the aim of increasing awareness of the core common cyber resilience measures (via guidance, standards or accreditation schemes) that they should be considering implementing dependent on the cyber threat to their operations.

36. Feedback from private sector stakeholders has identified that any such Framework or Pathway must be informed by:

- **Existing standards or guidance**, particularly those endorsed by the National Cyber Security Centre such as Cyber Essentials, the 10 Steps to Cyber Security and NIS Technical Guidance. Unless particular gaps are identified in the landscape, there is no appetite to create fresh standards for the private sector – rather, the aim is to help make sense of existing ones;
- **Existing and planned practice in respect of supply chain cyber security** amongst larger public, private and third sector organisations – as set out later in this action plan, a key goal should be to promote greater awareness and alignment across different sectors in respect of the core common cyber security requirements they place on SME suppliers, and to enhance understanding amongst SMEs of those core requirements (see Key Action 6); and

- **The views of the Scottish SME community** on the types of guidance or support that are most likely to help them begin and sustain their journey towards greater cyber resilience.

37. In undertaking this work, the Scottish Government, the NCRLB, the NCSC and key private sector partners (including the private sector cyber catalysts) will work together to:

- develop a stronger understanding of the **core cyber resilience requirements** that are currently encompassed by NCSC schemes and guidance, other common standards and key supply chain policies as they apply to the Scottish private sector (particularly SMEs), and how these relate to **progressively higher levels of cyber threat**;
- consider the development of **strengthened guidance** on the basis of this work where necessary, including in respect of public and private sector organisations' supply chain requirements (see Key Action 6), and the dissemination of such guidance appropriately via key partners, with a view to driving greater consistency in the messages going to private sector organisations (especially SMEs); and
- building on this work, consider options for the development of a **Private Sector Cyber Resilience Framework or Pathway**, with a particular focus on supporting SMEs and organisations in currently unregulated sectors to assess the cyber threat to their operations and select an appropriate set of core controls (via guidance, standards or accreditation schemes) to improve their cyber resilience.

38. In view of the fact that many strategic companies operating in Scotland will already be working to a range of UK and international regulatory requirements, it is expected that any such Framework or Pathway is most likely to be of use for smaller organisations (especially SMEs) in terms of assessing their own organisational cyber resilience. However, larger organisations in key sectors of the Scottish economy that are not currently subject to cyber security regulation may also find such a tool useful in identifying the levels of cyber resilience they should be aiming for in their organisations and networks based on the cyber threat to their operations. Such a framework, if appropriately aligned with common core supply chain requirements, could also drive benefits for larger companies seeking to manage supply chain cyber threats.

39. A **broad initial concept** for the development of a Private Sector Cyber Resilience Framework or Pathway is at **Annex B**. The potential for a pilot of this approach (or similar) is currently under discussion with the National Cyber Security Centre, the Federation of Small Businesses and other key partners.

One potentially key factor in securing greater awareness and take-up of any such Framework or Pathway will be an understanding of how **supply chain cyber security policies** in the public, private and third sectors broadly align with its contents. Key Action 6 in this action plan and Annex C set out how a clear understanding of the alignment of these policies could help ensure the success of any Framework or Pathway.

Developments in this area at the UK level, including in respect of NIS/NCSC guidance around supply chain cyber security, will be influential. The EU is also considering the development of a framework to govern European cybersecurity certification schemes, allowing schemes to be established and recognised across the EU in order to address market fragmentation. The current EU proposal outlines the minimum content of what would be required under such schemes. Ensuring alignment with this EU-level framework will be key.

40. The Scottish Public Sector Action Plan[18] sets out a commitment to develop a Scottish Public Sector Cyber Resilience Framework. Alignment between this and any Private Sector Cyber Risk Management Framework or Pathway will be carefully considered once both have been finalised.

41. The NCRLB emphasises that accreditation, while a helpful way of assessing and demonstrating good practice, does not offer a "silver bullet" to improving cyber security. Guidance will ensure that private sector organisations and their customers are aware that, ultimately, good cyber resilience is a **cultural issue**. Organisations should take care not to reduce cyber resilience to a "tick box" exercise.

Key Action 3

The Scottish Government will work with the NCRLB and private sector organisations to explore the potential for a more joined up, integrated, national-level approach to cyber resilience across the Scottish private sector (and public and third sectors).

This will include consideration of initiatives to improve cooperation and collaboration between key sectors of the Scottish economy that rely on one another for continued effective operation, with a view to strengthening the overall cyber resilience of Scotland.

42. It is vitally important that individual private sector organisations take appropriate action to ensure their own cyber resilience, including the presence of appropriate business continuity plans.

43. However, there are strong interdependencies between different organisations in Scotland's private sector (and public and third sectors). Companies and organisations that form part of the critical infrastructure of Scotland may rely on one another to be able to continue to operate effectively. This means that if one sector of the Scottish economy experiences a significant cyber incident, other sectors may be adversely affected also. Some private sector partners have argued that there is a need for a more integrated, joined-up, national level approach to the cyber resilience of the Scottish private sector (appropriately aligned with arrangements at the UK level), to ensure the continued functioning of the Scottish economy in the event of a major cyber incident. This might, for example, involve shared resilience arrangements across strategic companies in the Scottish private sector, supported by national level activity.

[18] See: www.gov.scot/cyberresilience

44. The Scottish Government will work with the NCRLB, the private sector cyber catalysts (see Key Action 5), the NCSC and UK Government partners to explore the potential for a more joined up, integrated, national-level approach to cyber resilience across the Scottish private sector (and public and third sectors). This work may include:

- Improving understanding of the cyber-specific **interdependencies** between strategic companies in Scotland and other parts of the private, third and public sectors, through a process of **mapping** key relationships and potential points of failure, with a specific focus on identifying ways of strengthening the overall cyber resilience of Scotland at a systemic level;
- Exploring ways of driving greater **threat-intelligence sharing across different sectors**, including through active membership of the Cybersecurity Information Sharing Partnership (CiSP); and
- Exploring the potential to strengthen **cross-sector incident response capability and protocols** when critical infrastructure in Scotland is at risk. These should ensure the appropriate involvement of the UK Government and NCSC, regulators, Police Scotland and Scottish Government Resilience (SGOR) arrangements.

45. This work will have a specific focus on key sectors of the Scottish private sector that are critical to the successful functioning of our economy.

46. The aim of this work will be to help shape recommendations to the Scottish and UK Governments as to the potential for future action by government and industry acting in partnership.

47. In the event that requirements for **technical innovation** are identified as a result of this work, and these requirements would align with the goals of public sector innovation funding schemes (e.g. benefit to the wider security and resilience of Scotland as a whole), consideration will be given to the potential for use of the **Can Do Innovation Challenge Fund**[19] to support the development of innovative solutions in this area. In the event that specialist academic expertise is required to explore specific issues raised by this area of work, consideration will be given to applying for funding for a collaborative industry/academia project or fellowship placement under the **SICSA Cyber Nexus Programme**.[20]

[19] See: https://www.scottish-enterprise.com/knowledge-hub/articles/insight/can-do-innovation-challenge-fund

[20] See: http://www.sicsa.ac.uk/funding/sicsa-cyber-nexus-industrial-public-sector-fellowships/

B. Strengthening awareness-raising and systems of advice and support

Key Action 4

The Scottish Government will work with the National Cyber Resilience Leaders Board, the NCSC and key private sector partners to strengthen the promotion of good cyber resilience practice at all levels in the private sector.

This work will include the strengthening of systems of advice and support for the private sector in Scotland, and communications activity aimed at raising awareness of the importance of cyber resilience and effective ways of achieving it. An initial "target landscape" for advice and support will be identified with the goal of achieving this by spring 2019, and thereafter improved on an ongoing basis.

48. It is vital that organisations across the Scottish private sector are aware of the importance of the cyber threat, know where to go to find trusted advice and support, and can take action to enhance their own cyber resilience.

49. The NCRLB have identified that there is a need to "declutter" and simplify the landscape in Scotland with respect to advice and support on cyber resilience for private sector organisations. Businesses of all sizes in Scotland should be able to discover the best official sources of advice and support in respect of cyber resilience, and be provided with high quality, consistent and easy-to-understand messages and advice products to support this. They should also understand where to go to find high quality, independent private sector expertise on cyber security.

50. To help achieve this, the Scottish Government and the NCRLB will work with key public and private sector partners to:

- finalise **analysis** on the cyber resilience advice and support landscape in Scotland, to identify the key strengths and weaknesses in current arrangements;
- develop and implement proposals to **promote easier access to trusted sources of advice and support on cyber security** for the private sector, with a focus on "decluttering" and simplifying the landscape. An initial "target landscape" for advice and support will be identified with the goal of achieving this by spring 2019, and thereafter improved on an ongoing basis; and
- build on this work to ensure businesses are provided with **high quality, consistent, and easy-to-understand messages and advice products** through key partners to help raise awareness and support organisations' progress in respect of cyber resilience. These communications and awareness raising activities will be delivered through a range of key partners where possible. These may include:
  - Business representative organisations and the Scottish Business Resilience Centre;
  - The Scottish Government, local authorities and other government bodies or agencies, including Skills Development Scotland, Business Gateway and Companies House;
  - Regulatory bodies;
  - Legal, accountancy and banking partners;
  - Private sector cyber catalyst organisations (see Key Action 5).
  - Specific industry bodies.

Awareness raising activities will have a particular focus on:

- Increasing **understanding of the cyber threat**, its importance to businesses of all sizes, and the **business arguments** for adopting good practice (including the introduction of the GDPR and the NIS Directive). The SBRC will undertake work with key partners to review the not for profit advice it provides to small and micro businesses in Scotland, to ensure it aligns with NCSC best practice.
- Raising awareness of the proposed **Private Sector Cyber Resilience Framework or Pathway** (if developed successfully – see Key Action 2), and the commercial benefits of managing the cyber threat more effectively (including meeting the requirements of Scottish public sector procurement policies and those of private and third sector cyber catalysts).
- Providing/signposting best practice guidance on how to build cyber resilience effectively into **workplace learning**, and opportunities to benefit from **educational initiatives/apprenticeships** and **retraining and upskilling programmes**, in line with the Learning and Skills action plan.
- Publicising widely any **incentives** that exist or that have been developed (see Key Action 7) to support the achievement of standards/accreditation schemes.
- Promoting and encouraging uptake of **free, reputable services** aimed at strengthening cyber security in the private sector.
- Promoting and encouraging **active**[21] **membership of the Cybersecurity Information Sharing Partnership (CiSP)** by eligible organisations, including any sectoral communities of trust within CiSP.
- Promoting and encouraging SMEs to **access key NCSC resources** available from the NCSC website, including Cyber Alerts, Advisory and Guidance reports, incident management guidance.
- Encouraging the private sector to **notify the NCSC and Police Scotland of cyber incidents** in line with official guidance on reporting cyber incidents.
- Promoting and encouraging uptake of the **Cross Sector Security Communications Network (CSSC)** managed by Police Scotland team within SBRC, to enable rapid alerts on key cyber security issues and to provide education and advice to business.

51. The role of the NCSC as a trusted source of advice is expected to be central to this work. Account will also be taken of the Scottish Government's ongoing Enterprise and Skills review.

[21] Proportionate to the size and resources of the member company.

C. Strengthening partnership working, leadership and knowledge sharing in Scotland's private sector

Key Action 5

The Scottish Government will work in partnership with the NCSC, UK Government and key Scottish private sector organisations to help catalyse better cyber resilience practice across Scotland's private sector.

From summer 2018, a cross-sectoral group of private sector cyber catalyst organisations will work with the Scottish Government and the NCSC to develop and implement practical solutions to key challenges on an ongoing basis, with an initial focus on:

- **strengthening leadership for, and helping drive greater awareness and uptake of good cyber resilient behaviours in, the Scottish SME community, including through the use of supply chain measures;**
- **strengthening coordination and knowledge sharing in respect of cyber resilience across key private sector companies operating in Scotland;**
- **supporting and promoting uptake of key educational initiatives in Scotland, including cyber security apprenticeships; and**
- **helping shape recommendations in respect of the potential for a more joined up, integrated, national-level approach to cyber resilience across the Scottish private sector (and public and third sectors).**

52. Discussions with key Scottish private sector organisations have made clear that they fully understand the leadership role they can play in respect of cyber resilience in their sector. If we are to succeed in our shared goal of raising standards of cyber resilience across the whole of the Scottish private sector, it will be vital that influential Scottish private sector organisations commit to wielding their influence to encourage others to adopt good cyber resilience practice.

53. Many key private sector organisations in Scotland are already working collaboratively within their own more specific sectors, and with regulatory bodies, to improve cyber resilience. This is particularly so in respect of key areas of Critical National Infrastructure in the private sector. Valuable work is being done by the NCSC and other lead departments in the UK Government to ensure companies across the UK are implementing best practice. This is complemented by the Scottish Government's programme of work on Critical Infrastructure, including the Stakeholder Impact Assessment process, under which Scottish Government officials meet with companies that are part of Scotland's critical infrastructure and support them to explore their own resilience (including cyber resilience) and preparedness.

This work will be bolstered by the introduction of NIS legislation from May 2018, which should help drive greater uniformity across the sectors to which it applies. Competent Authorities will be charged with ensuring compliance with the legislation, and will be working closely with individual companies to assist them in assessing levels of cyber resilience and taking action to improve areas of weakness.

54. There remains a clear need:

- to continue the support offered by the Scottish Government and other partners to NCSC/CPNI/the UK Government sectoral work on the cyber resilience of critical infrastructure in Scotland;
- to extend the focus of work on cyber resilience beyond these sectors;
- to ensure greater cross-sectoral cooperation, in both regulated and un-regulated sectors; and
- to catalyse good cyber resilience practice across the whole of the Scottish private sector.

55. To help achieve this, from summer 2018 the Scottish Government will begin work in partnership with the NCSC, UK Government and a cross-sectoral working group of **private sector "cyber catalyst" organisations** to develop and support implementation of **practical solutions** to key cyber resilience challenges in the Scottish private sector on an ongoing basis.

The Scottish Government will play a leading role in supporting and driving forward the work of the group, and identifying avenues for delivery.

Membership of this working group will be refreshed on a regular basis, in line with the key areas of focus that are identified through the ongoing work of the group. An up-to-date list of private sector cyber catalyst organisations will be placed on the Scottish Government Cyber Resilience website. These organisations will commit at board level to working with the Scottish Government and the NCSC to undertake the following broad initial programme of work:

(i) Strengthening leadership for, and helping drive greater awareness and uptake of good cyber resilient behaviours in, the Scottish SME community, including by making use of supply chain levers.

Where appropriate, private sector cyber catalyst organisations will be asked and supported to:

- Promote **public messaging** around the importance that should be attached to cyber resilience by all parts of the Scottish private sector, including by helping to develop and support a more consistent, joined-up programme of **awareness raising activities** aimed at the SME and third sector customer and client community in Scotland (see Key Action 4); and
- Support work (set out in more detail at Key Action 6) to **enhance cross-sectoral understanding and alignment of supply chain policies**. A key aim of this work will be to examine whether more consistent "core" cyber resilience requirements can be identified in respect of the Scottish SME and third sector community that form part of influential organisations' supply chains, thus improving the ability of SMEs to anticipate the likely cyber resilience demands that will be placed on them if they wish to win contracts.

(ii) Strengthening coordination and knowledge sharing in respect of cyber resilience across key organisations operating in Scotland.

Where appropriate, private sector cyber catalyst organisations will be asked and supported to share best practice knowledge gained from their own organisational activity on cyber resilience (including in respect of implementation of the NIS legislation or other regulations) **across sectors**, with a view to driving **greater cross-sectoral alignment and best practice**. This will include sharing learning with:

- one another, including in respect of any challenges or difficulties they have encountered, or any innovative solutions they have identified to overcome barriers and ensure an effective understanding of the cyber threat and implementation of effective cyber resilience measures;
- other Scottish private, public and third sector organisations – including, where appropriate, SMEs and charities – in order to help drive best practice in respect of cyber resilience, and develop a more coherent, aligned cross-sectoral approach across Scotland; and
- the NCSC and the UK Government Cabinet Office, as well as NIS competent authorities, to help inform the future development of the NIS standards and guidelines and other relevant requirements. Over time, the expectation is that these standards and guidelines will mature and improve to take account of experience in implementing them and technological developments.

Catalysts may be asked to facilitate wider engagement, beyond the membership of the working group, between government and key organisations in their sub-sector in Scotland in appropriate circumstances.

(iii) Supporting and promoting uptake of key educational initiatives in Scotland, including cyber security apprenticeships.

Where appropriate, private sector cyber catalyst organisations will be asked and supported to:

- **make use of key educational initiatives in Scotland**, including cyber security apprenticeships and Cyber First work placements, with a view to ensuring they have the right skills available to them to build organisational cyber resilience, and to support talent development in this area;
- **promote awareness** of these initiatives as part of wider work on public messaging; and
- **help inform the development of future initiatives**, to ensure they meet the needs of the Scottish private sector.

Further details of relevant initiatives and proposals in this area can be found in the Learning and Skills action plan.

(iv) Helping shape recommendations in respect of the potential for a more joined up, integrated, national-level approach to cyber resilience across the Scottish private sector (and public and third sectors).

Where appropriate, private sector cyber catalyst organisations will be asked and supported to contribute to work under Key Action 3 of this action plan, which aims to explore the potential for a more joined up, integrated, national-level approach to cyber resilience across the Scottish private sector (and public and third sectors).

56. A Scottish public sector cyber catalyst group has already been instituted, and it is intended that a similar group be established for Scotland's third sector. The Scottish Government will work to support the sharing of knowledge and learning across all 3 sectoral cyber catalyst groups, and to help drive greater alignment across all sectors.

57. The Scottish Government's existing work to support the overall resilience of critical infrastructure, including the Stakeholder Impact Assessment process, is being strengthened to take account of the NIS Directive. It is expected that through this, and similar activities, Private Sector Cyber Catalyst organisations that form part of the critical infrastructure of Scotland and the UK overall should experience greater consistency in respect of the audit/regulatory questions asked of them by the UK and Scottish Governments, regulators and competent authorities.

D. Supply chain cyber security – leveraging requirements to improve the cyber resilience of Scotland's SME community

Key Action 6

The Scottish Government will work with private sector organisations and key partners to clarify the common core cyber resilience requirements that are currently placed on third party suppliers, and their relationship to wider standards and guidance, by spring 2019.

Thereafter, the potential for greater cross-sectoral alignment and cooperation in respect of common core supply chain requirements will be explored, with the goal of promoting greater coherence across Scotland's public, private and third sectors.

A key aim of this alignment will be to improve the cyber resilience of Scotland's SME community as part of the supply chain of larger private sector organisations.

58. Supply chain cyber security is a vital part of organisational cyber resilience. Cyber criminals often attack the organisation with the weakest cyber security within the supply chain, and use the vulnerabilities present in their systems to gain access to other members of the supply chain, including large corporates.

59. Many large corporates in Scotland already require their supply chains to have appropriate cyber resilience measures in place, and make those requirements public. While the requirements they place on their supply chains are often similar, there is currently no agreed common practice or "core question set" either within or across sub-sectors (with the notable exception of the defence sector, where the Defence Cyber Protection Partnership have worked with industry to develop a Cyber Security Model for procurement[22]. This model is supported by an online tool called Octavian, which includes a short questionnaire to determine the Cyber Risk Profile for a contract or sub-contract).

Work is currently under way in the banking sector to explore the potential for greater alignment and cooperation between key organisations in respect of third party supply chain cyber security and assurance.

60. The NIS legislation and associated guidance will formalise requirements in respect of supply chain cyber security for private sector organisations who are subject to it – this may help ensure greater consistency in the approach taken across operators of essential services.

61. The Public Sector Action Plan commits the Scottish Government to working with key partners to develop a proportionate, risk-based policy in respect of supply chain cyber security, to be applied by public bodies in all relevant procurement processes. The views of Scottish business organisations have been sought on a draft policy early in 2018, with a view to implementation as part of the Scottish Public Sector Cyber Resilience Framework. This policy is expected to result in specific, proportionate, risk-based requirements being placed on private and third sector suppliers to the Scottish public sector in respect of cyber resilience.

The Scottish Government will make explicit how the public sector supply chain cyber security policy aligns with GDPR and NIS requirements.

[22] See: https://www.gov.uk/government/publications/defence-cyber-protection-partnership-cyber-risk-profiles

62. To help: (a) ensure the SME supply chain cyber security of private sector organisations that form part of the critical infrastructure of Scotland, and (b) improve the cyber resilience of Scotland's SME community, the Scottish Government will work with the NCSC and key private sector partners, including private sector cyber catalyst organisations, on the following programme of activity:

- Seeking views from the private sector to help **inform the development of the draft public sector supply chain cyber security policy** in early 2018, so that it takes account of existing good practice in the private sector;
- Identifying the current **common core supply chain cyber resilience requirements** that are placed on SME suppliers in key sectors of the Scottish economy, with a view to **improving sectoral guidance** for the SME community on what they need to do to strengthen their cyber resilience to position themselves to win contracts[23]. This work should include a focus on progressive management of cyber threats and risks. Initial mapping of some key sector requirements should be undertaken by spring 2019.
- Building on this analysis, considering the potential for **greater cross-sectoral alignment of core supply chain cyber resilience requirements** over time. Such alignment should have a particular focus on SME (and third sector) suppliers, and be informed by regulatory requirements (e.g. in respect of the finance sector or the NIS Directive) and existing good practice in the public, private and third sectors. It may include a focus on alignment with NCSC-endorsed guidance or schemes (including Cyber Essentials, the 10 Steps to Cyber Security, NCSC Supply Chain Guidance) and other widely recognised standards (e.g. ISO and IASME), and help inform the development of the proposed Private Sector Cyber Resilience Framework or Pathway (see Key Action 2); and
- Building on any such alignment work, exploring the potential for cross-sectoral **pooling or accessing of information** to support supply chain security across Scotland's strategic companies. This may include ways of accessing consistent information on which SME supply chain organisations have been assessed as capable of managing different levels of cyber risk in line with a Private Sector Cyber Resilience Framework or Pathway. This work will aim to reduce the burdens placed on both purchasers and suppliers in managing cyber risk in the supply chain.

63. While there will inevitably be a requirement for individual private sector organisations to include "bespoke" conditions around cyber security for specific contracts, identifying common core requirements should help provide a common starting point for consideration of the requirements that key private sector organisations (including the cyber catalyst organisations) will generally expect to see in place in their supply chains to manage the cyber risk in specific circumstances.

64. It is expected that this work will result in greater consistency in the incentives and requirements placed on Scotland's SMEs that form part of the public, private and third sector supply chain (or that wish to do so). That greater consistency of messaging, centred around a widely disseminated Private Sector Cyber Resilience Framework or Pathway, should help drive greater awareness in the SME community of what good practice in respect of cyber risk management looks like. **Annex C** gives a visual representation of what this might look like.

[23] This may, for example, take the form of guidance on "Supplying Scotland's [Finance/Energy/Pharmaceutical] Sector: Common Core Cyber Resilience Requirements" or "Supplying Scotland's larger companies: Common Core Cyber Resilience Requirements".

65. Private sector organisations that make use of Cyber Essentials in their supply chain, either now or as a result of the alignment work described above, will also be encouraged to promote the use of a voucher scheme to support SMEs in their supply chains to achieve accreditation to Cyber Essentials or Cyber Essentials Plus level (see Key Action 7).

66. Of course, not all SMEs in Scotland form part of the supply chain of the public sector and larger private and third sector organisations. Wider awareness raising work will be required to ensure greater uptake of good cyber resilient behaviour. This is covered in Key Action 4.

E. Strengthening incentives to improve cyber resilience in Scotland's private sector

Key Action 7

The Scottish Government and the National Cyber Resilience Leaders Board will work with the UK Government and key private sector stakeholders to consider how best to strengthen incentives to support the uptake of cyber security standards/ accreditation, and the adoption of good cyber resilience practice more generally.

This will include the continuation of a modified voucher scheme to support the achievement of Cyber Essentials or Cyber Essentials Plus certification by Scottish SMEs. We aim to at least double the number of public, private and third sector organisations holding Cyber Essentials or Cyber Essentials Plus certification in total in Scotland during Financial Year 18-19.

67. Private sector partners have put forward arguments that **incentives** will be key to promoting the adoption of cyber security standards/accreditation and the adoption of good cyber resilience practice more generally.

68. The Scottish Government is particularly keen to support SMEs and microbusinesses, who will often be starting from a relatively low base of knowledge or experience, to begin their journey towards greater cyber resilience. One way of doing so is to support uptake of Cyber Essentials/Plus certification. The Cyber Essentials scheme offers a mechanism, endorsed by the National Cyber Security Centre, for organisations to demonstrate to customers, investors, insurers and others that they have in place critical technical controls that protect against the most common internet-borne cyber attacks.

69. The Digital Scotland Business Excellence Partnership supported a voucher scheme that ran from summer 2016 until end 2017 to help Scottish SMEs achieve Cyber Essentials or Cyber Essentials Plus certification. The scheme provided funding to SMEs to allow them to secure the services of an industry expert to advise them on how to approach securing Cyber Essentials certification. The voucher was of the value of up to £1,500 per company. An evaluation of this scheme found that it had a positive effect on take-up and achievement of Cyber Essentials amongst SMEs.

70. The Scottish Government will build on the success of this scheme by funding a modified voucher scheme to support Scottish SMEs (and third sector organisations) to achieve Cyber Essentials or Cyber Essentials Plus. This scheme is expected to be operational from autumn 2018. We aim to at least double the number of public, private and third sector organisations holding Cyber Essentials or Cyber Essentials Plus certification in total in Scotland during Financial Year 18-19.

71. Private sector organisations will be encouraged to publicise this scheme to their supply chain companies and customers/clients, in order to drive greater take up of Cyber Essentials and Cyber Essentials Plus. The scheme will also be publicised through key partners (including business representative organisations) as part of the awareness raising activities set out under Key Action 4.

72. Beyond this, the Scottish Government, the NCRLB, the UK Government and key partners will work together to explore what additional incentives are already in place or could be developed further to promote good practice in the Scottish private sector in respect of cyber resilience. Areas for consideration will include work with the insurance industry around cyber insurance incentives. High level proposals on additional incentive schemes will be considered by the NCRLB by spring 2019, with decisions on subsequent action taken thereafter.

F. Benchmarking, Monitoring and evaluation

Key Action 8

The Scottish Government will work with the NCRLB and key partners to develop appropriate benchmarking, monitoring and evaluation arrangements, for implementation by spring 2019.

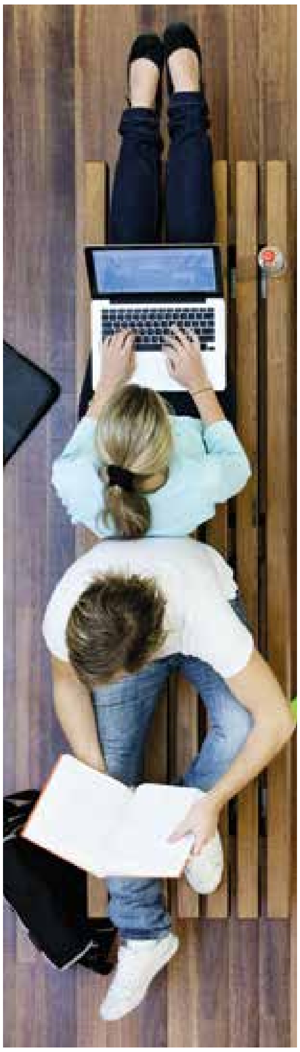
73. In order to understand what progress is being made towards the vision of Scotland as a world leading nation in cyber resilience, it will be important to have in place arrangements to achieve a regularly refreshed picture of the extent of good cyber resilience practice in Scotland's private sector. The benefits of this are expected to include:

- The provision of greater assurance to **members of the public** with regard to the cyber resilience of Scotland's private sector as a whole and the cyber resilience of specific sub-sectors.
- The provision of greater assurance to **investors** with regard to the cyber resilience of Scotland's private sector, thus contributing to the attractiveness of Scotland as a destination for **inward investment**.
- The provision of useful **benchmarking information** for private sector organisations, to assist them in making judgements around what level of standards/accreditation they should be aiming to achieve in light of industry benchmarks.
- The provision of greater assurance to **Government, Parliament** and **Regulatory Bodies** with regard to levels of cyber resilience across key areas of Scotland's private sector.

74. To help achieve this, the Scottish Government will work with the NCRLB, the NCSC, Competent Authorities/Regulatory Bodies and key partners to develop appropriate benchmarking, monitoring and evaluation arrangements by spring 2019. Key measures that may form part of these arrangements include:

- Working with Competent Authorities to monitor the extent to which key Scottish private sector companies are complying with the requirements of the NIS security principles (e.g. by making use of appropriate aggregated and anonymised information, broken down by sector);
- Working with the NCSC to monitor and report on the number of businesses achieving Cyber Essentials and Cyber Essentials Plus;
- Working with accreditation bodies and external audit companies to understand levels of take-up of private certification schemes and "attestation" in Scotland, where possible;
- Working with key partners to monitor and report on the uptake of free, reputable cyber security tools amongst Scotland's private sector (e.g. the Global Cyber Alliance's DMARC and Protected DNS services);
- Working with the NCSC to monitor and report on membership of the SciNet grouping on the CiSP; and
- Inclusion of appropriate questions focused on cyber resilience in Scottish-based surveys (e.g. the Scottish Crime and Justice Survey).

ANNEXES



A

Annex A. Key Actions and Timelines – Summary

Key action no.	Action required of:	Requirements	Deadline	Page no. action plan
1	SG, NCRLB, private sector partners.	■ Seek private sector views (including SME sector) on whether there is a case for extending regulatory requirements around cyber resilience more widely across the Scottish private sector.	Ongoing basis	23
	SG	■ Communicate findings to UK Government to inform consideration of the need for greater regulation of cyber resilience across whole of UK.	Ongoing basis	
2	SG, NCRLB, private sector partners	■ Consider options for developing a Private Sector Cyber Resilience Framework or Pathway, with a particular focus on unregulated sectors and SMEs. To include:	Spring 2019	25
	SG, NCRLB, private sector partners	– Work to develop a stronger understanding of core cyber resilience requirements currently encompassed by NCSC schemes and guidance, other common standards and key supply chain policies as they apply to the Scottish private sector (particularly SMEs), and how these relate to progressive levels of cyber risk.	Spring 2019	
3	SG, private sector cyber catalysts	■ Explore potential for a more joined up, integrated, national-level approach to cyber resilience across the Scottish private sector (and public and third sectors).	Ongoing	27
		■ Develop and put forward recommendations to the Scottish and/or UK Governments on the basis of this work, and/or align recommendations/ proposals with initiatives such as the Can Do Innovation Funding Challenge and the SICSA Cyber Nexus.	Ongoing	
4	SG, NCRLB, NCSC and key private sector partners	■ Undertake work to strengthen systems of advice and support and awareness raising activities – initial "target landscape" identified and achieved.	Spring 2019	29

Key action no.	Action required of:	Requirements	Deadline	Page no. action plan
5	SG and NCRLB	■ Begin work with NCSC and key private sector partners in a Private Sector Cyber Catalyst Working Group, with initial focus on:	From summer 2018	31
	SG, NCRLB and private sector cyber catalysts	– strengthening leadership for, and helping drive greater awareness and uptake of good cyber resilient behaviours in, the Scottish SME community, including through the use of supply chain measures;	Ongoing	
		– strengthening coordination and knowledge sharing in respect of cyber resilience across key private sector companies operating in Scotland;	Ongoing	
		– supporting and promoting uptake of key educational initiatives in Scotland, including cyber security apprenticeships; and	Ongoing	
		– helping shape recommendations in respect of the potential for a more joined up, integrated, national-level approach to cyber resilience across the Scottish private sector (and public and third sectors).	Ongoing	
6	SG, NCRLB and private sector cyber catalysts	■ Seek views from the private sector to help inform the development of the draft public sector supply chain cyber security policy in 2018, so that it takes account of existing good practice in the private sector.	First half of 2018	35
		■ Identify current common core supply chain cyber resilience requirements that are placed on SME suppliers in key sectors of the Scottish economy, with a view to improving sectoral guidance for the SME community on what they need to do to strengthen their cyber resilience to position themselves to win contracts.	Spring 2019	
		■ Building on this analysis, consider the potential for greater cross-sectoral alignment of core supply chain cyber resilience requirements over time.	From spring 2019	
		■ Building on any such alignment work, explore the potential for cross-sectoral pooling or accessing of information to support supply chain security across Scotland's strategic companies.	From spring 2019	
7	SG/SE	■ Continuation of modified voucher scheme for Cyber Essentials	Autumn 2018	37
	SG, NCRLB and key private sector partners	■ Explore greater use of incentives and put forward for consideration by NCRLB	By spring 2019	
8	SG	■ Work with NCRLB, NCSC, CAs/Regulatory bodies and key partners to develop benchmarking, monitoring and evaluation arrangements.	By spring 2019	38

Annex B – Scottish Private Sector Cyber Resilience Framework or Pathway – Concept

1. This annex sets out a broad concept for the development of a Scottish Private Sector Cyber Resilience Framework or "Pathway".

2. The concept has been developed by the Scottish Government and members of the National Cyber Resilience Leaders Board, in consultation with the NCSC and key private sector partners.

In line with Key Action 2 in the action plan, work will be undertaken to finalise and pilot this Framework or Pathway (on the condition that further work confirms its feasibility) on the basis of initial analytical work to develop a stronger understanding of the **core cyber resilience requirements** that are currently encompassed by NCSC schemes and guidance, other common standards and key supply chain policies as they apply to the Scottish private sector (particularly SMEs), and how these relate to **progressive levels of cyber threat**.

Aims

3. The Framework or Pathway would aim to provide a **common point of departure** for Scottish private sector organisations to **assess the cyber threat** to their assets, and **identify the key measures** they should consider implementing to help manage these threats in view of the impact on their operations.

The Framework or Pathway could be used by SMEs and other organisations to **benchmark** themselves against progressively more demanding or holistic approaches to cyber threat management. It would also provide a way for organisations in the early stages of their cyber resilience journey to identify key sources of guidance and assurance in order to **improve their capacity to manage progressively more targeted and sophisticated cyber threats**.

4. In view of the fact that many strategic companies operating in Scotland will already be working to a range of UK and international regulatory requirements, it is expected that any such Framework or Pathway would most likely be of use for smaller organisations (especially SMEs). However, larger organisations in key sectors of the Scottish economy that are not currently subject to cyber security regulation may also find such a tool useful in identifying the levels of cyber resilience they should be aiming for based on the likely cyber threat to their assets.

5. Work would be undertaken to align any Framework or Pathway with similar frameworks under development as part of the **public and third sector action plans on cyber resilience** by the Scottish Government and the NCRLB.

Overview of key potential features

6. The starting point for any potential Framework or Pathway would be **an agreed common way of assessing the broad cyber threat to an organisation's networks and assets**, either in general or in the context of specific contracts or undertakings.

7. These cyber threat profiles should be organised in a **progressive hierarchy**, based on broadly defined increases in the expected targeting and sophistication of cyber threats. It should also take into account the likely organisational impact of breaches.

8. There should then be a clear **hierarchy of guidance, standards or controls** that is "mapped" directly to the relevant threat level, thus ensuring greater consistency of application of appropriate standards and controls.

9. These cyber threat profiles and the hierarchy of standards or controls should, to the greatest extent possible, be aligned with or incorporate the following key existing or planned measures:

- **Existing standards, guidance or initiatives**, particularly those endorsed by the National Cyber Security Centre such as **Cyber Essentials**, the **10 Steps to Cyber Security**, **NIS Directive Technical Guidance**, **NCSC Supply Chain Guidance**, the **NCSC's cloud security principles**, the **NCSC's Cyber Security Information Sharing Partnership**, and **ICO guidance on protecting personal data**; and
- **Existing and planned practice in respect of supply chain cyber security** amongst larger public, private and third sector organisations.

10. The potential for development of a **freely accessible online tool** to support SMEs, in particular, to undertake a cyber threat assessment against the Framework or Pathway, and be directed to appropriate guidance or standards, would likely be key to the success of this work.

11. A basic visual representation of this proposed approach is set out on the following page. **It should be noted that the contents of this proposed framework or pathway will be subject to further work and discussion, and are included only for illustrative purposes at this stage.**

Annex B – Scottish Private Sector Cyber Resilience Framework or Pathway – Basic Concept (indicative draft only)

Private Sector Cyber Resilience Pathway (illustrative draft)

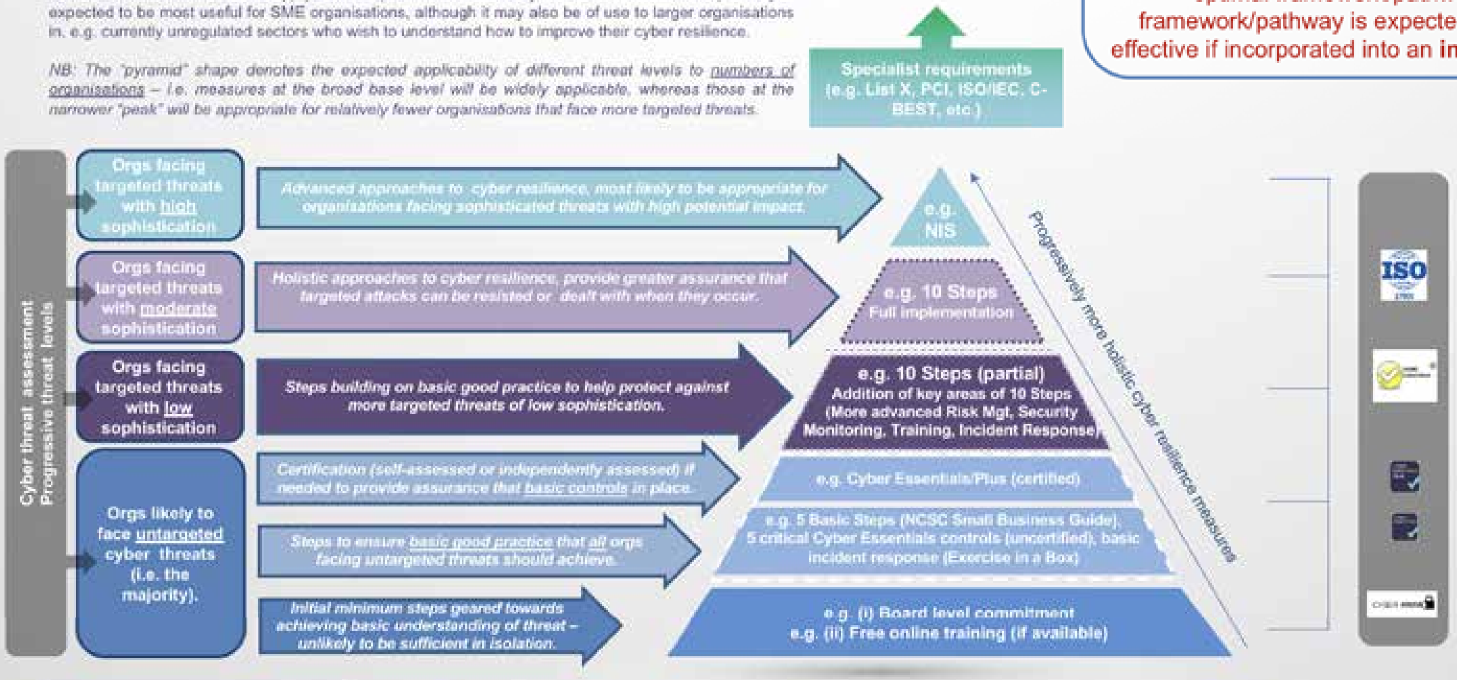
The Cyber Resilience Framework/Pathway would aim to provide a flexible pathway to help organisations to understand the broad cyber threat levels they may face, to factor in their own risk appetite and circumstances, and to guide them towards implementing progressively more sophisticated approaches to cyber resilience as appropriate.

Organisations using the Framework/Pathway could opt to amend or combine the controls and approaches set out at different levels to achieve optimal results based on the specific cyber threat profile they faced – the approach would not be prescriptive. The framework/pathway would aim to provide a common starting point for consideration of the best way to manage progressively higher cyber threat profiles. Work would be undertaken to understand how measures that are likely to be useful for managing different threat levels are aligned with NCSC-endorsed standards/guidance, widely recognised standards, and common core supply chain requirements across key sectors. The framework/pathway is expected to be most useful for SME organisations, although it may also be of use to larger organisations in, e.g. currently unregulated sectors who wish to understand how to improve their cyber resilience.

NB: The "pyramid" shape denotes the expected applicability of different threat levels to numbers of organisations – i.e. measures at the broad base level will be widely applicable, whereas those at the narrower "peak" will be appropriate for relatively fewer organisations that face more targeted threats.

NB: The contents of this framework/pathway are for **illustrative purposes** only.

Further work will be undertaken as part of implementation of the action plan to improve our understanding of the options for developing an optimal framework/pathway. The framework/pathway is expected to be most effective if incorporated into an **interactive tool**.



Specialist requirements (e.g. List X, PCI, ISO/IEC, C-BEST, etc.)

Cyber threat assessment
Progressive threat levels

Orgs facing targeted threats with high sophistication

Advanced approaches to cyber resilience, most likely to be appropriate for organisations facing sophisticated threats with high potential impact.

e.g. NIS

Orgs facing targeted threats with moderate sophistication

Holistic approaches to cyber resilience, provide greater assurance that targeted attacks can be resisted or dealt with when they occur.

e.g. 10 Steps
Full implementation

Orgs facing targeted threats with low sophistication

Steps building on basic good practice to help protect against more targeted threats of low sophistication.

e.g. 10 Steps (partial)
Addition of key areas of 10 Steps
(More advanced Risk Mgt, Security Monitoring, Training, Incident Response)

Orgs likely to face untargeted cyber threats (i.e. the majority).

Certification (self-assessed or independently assessed) if needed to provide assurance that basic controls in place.

e.g. Cyber Essentials/Plus (certified)

Steps to ensure basic good practice that all orgs facing untargeted threats should achieve.

e.g. 5 Basic Steps (NCSC Small Business Guide), 5 critical Cyber Essentials controls (uncertified), basic incident response (Exercise in a Box)

Initial minimum steps geared towards achieving basic understanding of threat – unlikely to be sufficient in isolation.

e.g. (i) Board level commitment
e.g. (ii) Free online training (if available)

Progressively more holistic cyber resilience measures

Measures in hierarchy/ pathway aimed at managing different risk levels would ideally be mapped against NCSC-endorsed standards/guidance, widely recognised standards (see box to left), and common core supply chain requirements across key sectors.

CiSP

Membership of the Cyber Security Information Sharing Partnership (CiSP) also forms a key aspect of the Scottish Private Sector Cyber Resilience Framework, to ensure active threat intelligence sharing.

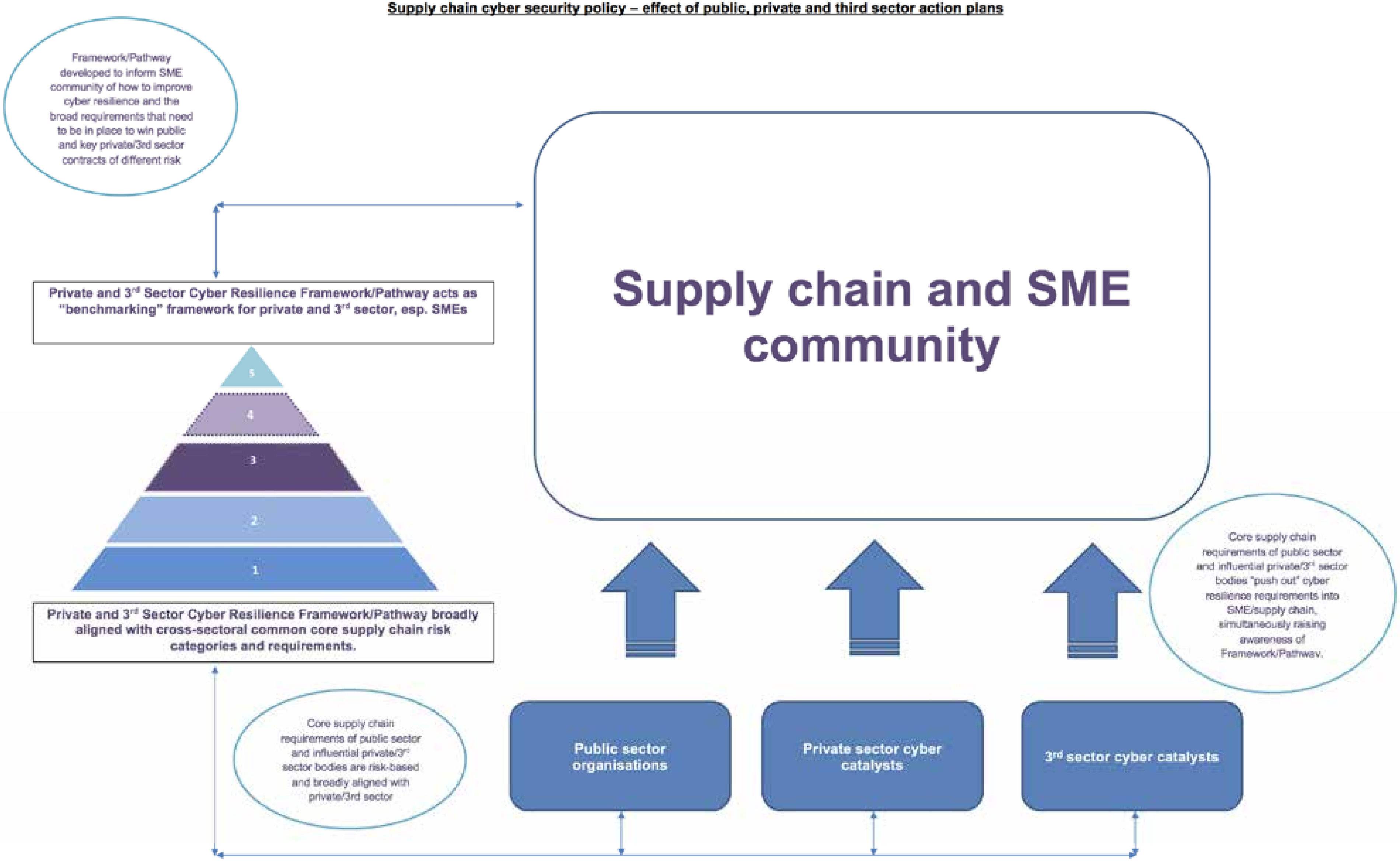
Where organisations are using cloud services or cloud - enabled products, they should follow the **NCSC Cloud Security Principles and Guidance on Managing the Risk of Cloud-Enabled Products.**

Where personal information is processed, organisations should consider ICO guidance for protecting and offshoring personal data, and NCSC guidance on protecting bulk personal data.

Significant cyber incidents should be **reported** to NCSC and Police Scotland, and to appropriate authorities dependent on status (e.g. NIS Competent Authorities, ICO, etc.)

Annex C – Supply chain cyber security policies – driving good practice through Scotland’s SME community (concept)

Supply chain cyber security policy – effect of public, private and third sector action plans



Framework/Pathway developed to inform SME community of how to improve cyber resilience and the broad requirements that need to be in place to win public and key private/3rd sector contracts of different risk

Private and 3rd Sector Cyber Resilience Framework/Pathway acts as "benchmarking" framework for private and 3rd sector, esp. SMEs

Private and 3rd Sector Cyber Resilience Framework/Pathway broadly aligned with cross-sectoral common core supply chain risk categories and requirements.

Core supply chain requirements of public sector and influential private/3rd sector bodies are risk-based and broadly aligned with private/3rd sector

Supply chain and SME community

Public sector organisations

Private sector cyber catalysts

3rd sector cyber catalysts

Core supply chain requirements of public sector and influential private/3rd sector bodies "push out" cyber resilience requirements into SME/supply chain, simultaneously raising awareness of Framework/Pathway.

Scottish Government
Riaghaltas na h-Alba
gov.scot

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at
The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-78781-039-6

Published by The Scottish Government, June 2018

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS421446 (06/18)