www.gov.scot/cyberresilience

Scottish Government
Riaghaltas na h-Alba
gov.scot

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

Learning & Skills Action Plan for Cyber Resilience 2018-20

Produced by the National Cyber Resilience Leaders' Board
in partnership with the Scottish Government

FOREWORD

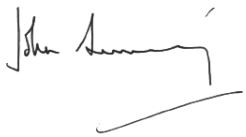
PEOPLE ARE AT THE HEART OF OUR VISION FOR SCOTLAND TO BE A WORLD LEADING NATION IN CYBER RESILIENCE

Fully realising the benefits of digital technology for Scotland, whether at home, at school, at work or at play, increasingly relies upon our ability to operate safely and confidently online.

This Cyber Resilience Learning and Skills Action Plan is the blueprint for government and its partners to work together to strengthen and further embed understanding of cyber resilience across our education and lifelong learning system. When implemented it will help ensure that people across Scotland, whether in early years, school, college or non-formal and workplace learning settings, have greater opportunities to develop the knowledge and behaviours they need to be safe and resilient in their online lives.

The plan also sets out our plans for ensuring that Scotland has a strong talent pipeline of individuals who are technically skilled in cyber security and cyber risk management, to help secure our businesses, charities and public services against current and future threats, and to develop and export innovative cyber security goods and services to the rest of the world. Supporting people to develop these specialist skills will be vital to the success of other action plans we are developing and implementing on cyber resilience, and which relate to the public, private and third sectors, as well as our forthcoming plan to help us to take advantage of the economic opportunities presented by our work on cyber security.

Our people's emerging skills and talents in this area are already setting us on the path to success. We must build on these strong foundations and support people from all backgrounds to become confident, digitally literate citizens, capable of fully realising their potential in Scotland's digital future. With the right mix of leadership and commitment from government, the education and skills sector, industry and academia, I am convinced that we can make this happen.



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

At the heart of this action plan is collaboration - both in terms of how it has been put together, how it will be delivered, and in its oversight. We now need as many organisations to buy in to the ambitions of this plan, and this includes policymakers – those people whose job it is to link agendas such as this so that we are improving people lives, public services and strengthening our communities and our economy in as coherent a way as possible.

We can no longer identify the digital world as a "separate space". Digital is integral to everything we do – especially for young people. Cyber resilience is crucial if we are to get the most out of digital. The cyber resilience agenda gives us the prospect

FOREWORD (CONTD.)

of focusing on equity of opportunity. Of course there will be the risk of some people in some groups being left behind; it's our aim to ensure that this does not happen. We see this as a chance for us to review the way that digital intersects with our lives and to make sure that everyone is included in reaping its rewards.

The rights-based agenda is key to achieving a cyber resilient population. The United Nations Convention on the Rights of the Child and the Sustainable Development Goals can really help us to drive forward opportunities for Scotland's young citizens to flourish in their use of digital technologies. This action plan is all the more timely for being launched early in Scotland's Year of Young People.

Finally, we want to really raise the profile of learning that takes place in informal and non-formal settings. Learning for cyber resilience (whether it's about being safe online as an individual, or learning technical cyber security skills) happens in community learning settings, in youth work and in third sector organisations, not just in schools and colleges. We want to make a plea for these organisations to get on board and to encourage their partners to come to the party too. Please do take the opportunity that this action plan offers on behalf of your learners and make sure that everyone in Scotland benefits as we become more cyber resilient and widen our horizons together.

Louise Macdonald, OBE
Chief Executive,
Young Scot & Co-chair of the Learning and Skills Steering Group, National Cyber Resilience Leaders' Board

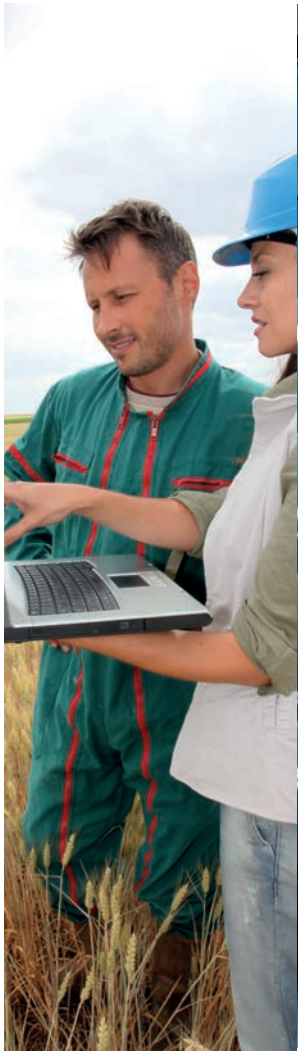
It's an exciting time to be progressing Scotland's digital future. Cyber resilience is such a crucial part of life so these skills are fundamental to the success and growth of Scotland's digital economy. As organisations are confronted with emerging digital security threats and risks, there is an increasing demand for specialist cyber security skills. This ambitious learning and skills action plan provides concrete steps to help grow a professional cyber security workforce that can protect our organisations from these threats. A key measure of success will be that cyber security is widely acknowledged as an established profession with clear career pathways and that more people are attracted to a career in cyber security.

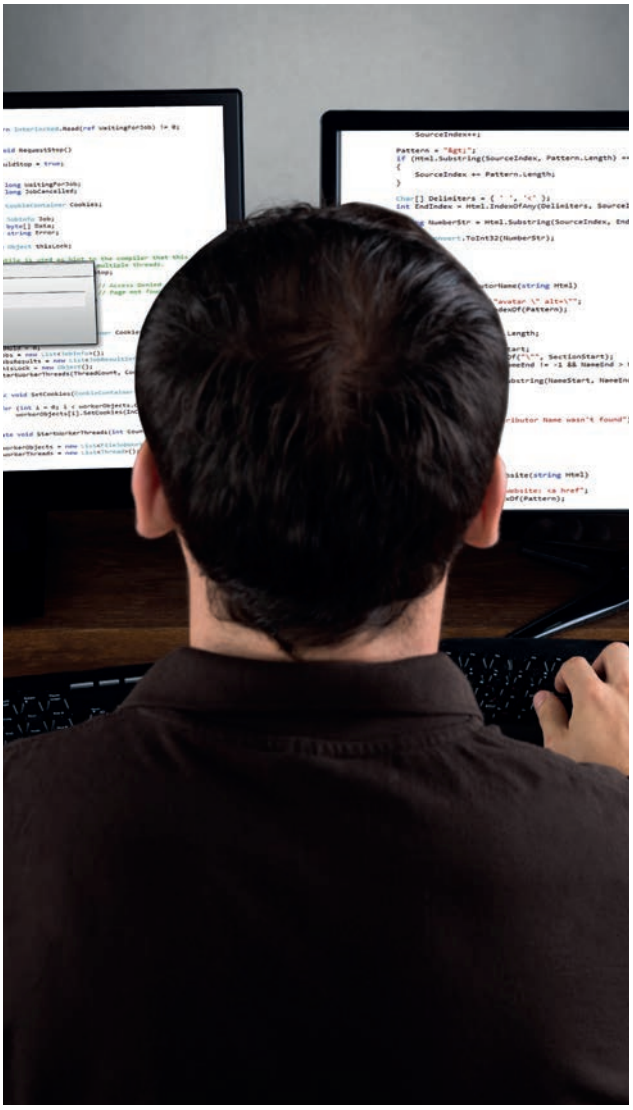
I have been delighted to support the development of this action plan. Skills Development Scotland will play a key role in helping people achieve career success in cyber security. However to extend the talent pool Scotland needs, a collaborative approach is critical, and stakeholders and industry need to work together. This will all contribute to Scotland becoming a leading nation in cyber resilience.

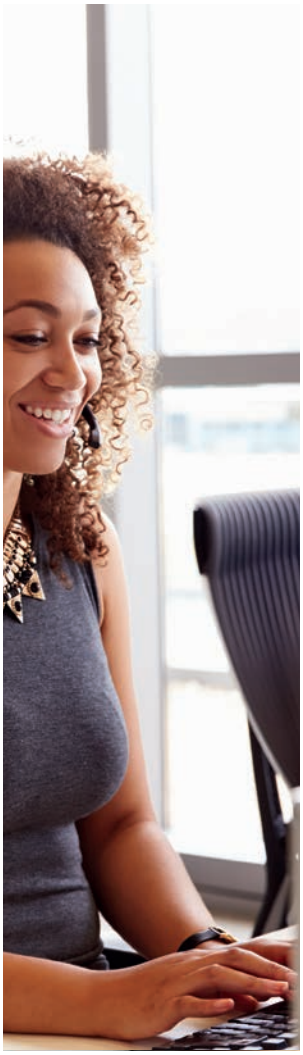
Gordon McGuinness,
Director of Industry & Enterprise Networks, Skills Development Scotland & Co-chair of the Learning and Skills Steering Group, National Cyber Resilience Leaders' Board

CONTENTS

INTRODUCTION AND BACKGROUND







INTRODUCTION AND BACKGROUND

Digital technologies bring enormous opportunities for individuals, families, businesses and communities. They also bring new threats and vulnerabilities that we must manage safely and securely. The Scottish Government's **Digital Strategy**[1] states that digital skills (including cyber resilience) are fundamental to the life chances of our people and the economic success of our country.

Safe, secure and prosperous: a cyber resilience strategy for Scotland[2] ("the strategy"), was published in 2015. It set out the Scottish Government's vision for cyber resilience:

> ***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 six outcomes are interdependent – progress towards one may underpin or drive progress towards others.

The strategy is closely aligned with the **UK National Cyber Security Strategy**[3] which sets out the UK Government's approach to making the UK secure in cyberspace. Cyber security is a reserved matter, but it has strong implications for the delivery and resilience of devolved services. As such, the Scottish Government works closely with the UK Government and the UK's National Cyber Security Centre (NCSC) to ensure alignment between work on cyber resilience at the UK wide and Scottish levels.

More recently in Scotland, the **Programme for Government**[4] sets out the commitment to develop and implement a range of action plans to improve cyber resilience in the public, private and third sectors. It also committed to developing this learning and skills action plan, and to help realise the economic opportunity resulting from the growth of our cyber security goods and services sector in Scotland. These plans will help steer Scotland towards our vision of being a world leading nation in cyber resilience by 2020.

The Cyber Resilience Learning and Skills Action Plan ("the action plan") has been produced jointly by the Scottish Government and the National Cyber Resilience Leaders' Board (NCRLB), drawing on the advice of partners from across key sectors. It sets out the

1 https://beta.gov.scot/publications/realising-scotlands-full-potential-digital-world-digital-strategy-scotland/
2 http://www.gov.scot/Publications/2015/11/2023/downloads
3 https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
4 http://www.gov.scot/Publications/2017/09/8468

actions the Scottish Government intends to take, working closely with the NCRLB and key partners from the public, private and third sectors, to build stronger learning and skills capabilities in cyber resilience and cyber security in Scotland.

The overarching aim of this action plan is to enable transformational cultural change through learning and skills in Scotland so that all sections of society and business benefit from being more cyber resilient. As the activities detailed are implemented, we must take account of the rapidly changing cyber security landscape, both in terms of technological advancement and the methods that criminals and hostile actors develop to exploit them. The Scottish Government will continue to work with delivery partners, supporting them to address new challenges and threats as they are identified.

Terms we use in this action plan

"Cyber resilience" and "cyber security"

As defined in the Strategy, **"cyber resilience"** refers to our ability to prepare for, withstand, rapidly recover and learn from deliberate attacks or accidental events in the online world. 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 online and rapidly recover from a cyber attack – and this is the concept of cyber resilience.

For the purposes of this action plan we are distinguishing between cyber resilience and cyber security, with **"cyber security"** referring mainly to the technical aspects that help protect equipment and electronic data from cyber attack, and that contribute to the wider outcome of **"cyber resilience"**.

"Learning" and "skills"

By **"learning"** we mean development of the knowledge, understanding and positive behaviours of all citizens. This includes workers in non-digital technology roles. Learning can take place:

- "informally" through awareness-raising and communications activity,
- "non-formally" in learning settings such as youth groups, community learning centres and local libraries, and
- "formally" in schools, colleges, universities or workplaces, through the delivery of courses and qualifications.

By **"skills"** we mean the development of cyber security specialist knowledge and skills to meet the demands of organisations in all sectors, now and in the future. Skills development generally takes place in formal settings, such as schools, colleges or universities, or through work-based training such as short courses or apprenticeships.

More effective learning and skills development will contribute to the achievement of all six outcomes of the strategy, with some examples of this contribution given below:

1. **Our people are informed and prepared to make the most of digital technologies safely.**

   Informal, non-formal and formal learning will equip people with the basic knowledge and understanding of the risks involved in using digital technologies. Learning will enable them to make the most of digital technologies and take effective steps to protect themselves and their families in their day-to-day and working lives. It may also help young people in particular to understand the risks of becoming involved in online crime, and steer them to make informed choices in relation to their online activity.

2. **Our businesses and organisations recognise the risks in the digital world and are well prepared to manage them.**

   Organisations in Scotland's public, private and third sectors will benefit from:

   - embedding cyber resilience learning into workplace training for people at all levels of an organisation, including senior managers and board members.
   - understanding the cyber security skills they need to draw on (whether by employing specialists or by procuring services) in order to be as cyber resilient as possible.
   - being able to employ workers who have learned the basics of cyber resilient practices during their education, as well as any more specialist skills as part of vocational training.

3. **We have confidence in, and trust, our digital public services.**

   The likelihood of damaging cyber security breaches affecting digital public services and the citizens and businesses they serve will be reduced if public bodies can improve their cyber resilience by drawing on the skills of cyber security professionals and ensuring their staff understand and use fundamental cyber resilient practices. Demonstrating that Scottish digital public services are cyber resilient is likely to become increasingly important to earning the trust of citizens and organisations in Scotland.

4. **We have a growing and renowned cyber resilience research community.**

   Our universities need knowledgeable and skilled individuals to undertake cyber security research, to spark and drive innovation and to retain and attract more talent to Scotland.

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

   By embedding cyber resilience into our education and lifelong learning system, and by ensuring an adequate supply of skilled professionals, we can strengthen Scotland's infrastructure, society and economy. Scotland can be recognised as a country of expertise and knowledge in cyber security, and one that is attractive to inward investors.

6. **We have an innovative cyber security, goods and services industry that can help meet global demand.**

   Our increased supply of home-grown talented and skilled professionals will meet the needs of employers in all sectors, address the recognised skills shortage, and also grow our cyber security goods and services industry.

The scope of this action plan

This action plan has a broad scope, stretching from basic informal learning (awareness raising), through to formal cyber security skills development. It also includes actions to build a thriving research community that can promote research, attract teaching talent and encourage investment to Scotland that will, in turn, build the knowledge and skills that drive innovation. Research and innovation will contribute to Scotland's ability to compete in a global cyber security goods and services market, which we expand upon in a separate action plan that focuses on the economic opportunity of cyber resilience for Scotland.

The continuum diagram below illustrates a fundamental principle of this action plan: that we will not achieve a cyber resilient Scotland that benefits from economic opportunities in cyber resilience and digital more broadly, unless cyber resilience is embedded across our learning and skills system.

basic awareness → learning for all → skills development → economic opportunity

awareness raising	embedding cyber resilience in curricula	embedding cyber resilience in workplace learning	developing cyber security specialist skills	upskilling in cyber security	building research capability and capacity

An expanded version of this diagram is attached at **Annex A**.

This action plan also supports the delivery of action plans being developed to build cyber resilience and security within our public, private and third sectors. Cyber resilience forms a core part of wider digital ambitions for Scotland, and it is closely aligned to a range of Government ambitions such as increasing **internet safety**, **digital participation** and **digital skills** more broadly.

Our intention is not to create more layers of governance as a result of this action plan, but to seek ways to embed or integrate the actions set out in this plan within wider strategies and programmes.

This approach is already being implemented effectively in a number of key policy areas. For example, cyber resilience (in relation to learning and skills) forms a key part of the following recently-published strategies:

- **Realising Scotland's full potential in a digital world: A Digital Strategy for Scotland (March 2017)**[5]
- **Science, Technology, Engineering and Mathematics: education and training strategy**[6]
- **Enhancing Learning and Teaching Through the Use of Digital Technology (September 2016)**[7]

5 http://www.gov.scot/Publications/2017/03/7843

6 https://beta.gov.scot/publications/science-technology-engineering-mathematics-education-training-strategy-scotland/

7 http://www.gov.scot/Publications/2016/09/9494

The Scottish Government will continue to actively promote cyber resilience across relevant evolving policies, strategies and programmes.

Measuring the impact of this action plan

This action plan will be measured using a set of indicators that will be agreed with delivery partners. We will monitor progress using these indicators on a quarterly basis during the lifetime of the action plan.

Monitoring and measuring will be overseen by the National Cyber Resilience Leaders' Board.

Principles

The following **four principles** will underpin all our activities in relation to learning and skills:

Principle 1

Cyber resilience is enabling: it is about getting the most out of online digital technologies while mitigating risk in a proportionate way.

Principle 2

Creating a cyber resilient country requires a cultural shift: all providers and stakeholders in our education and lifelong learning system should commit to making cyber resilience an integral part of their work.

Principle 3

Cyber resilience is a dynamic area: we need to continually innovate and refresh our knowledge and communication to take account of changing technological and cyber crime challenges.

Principle 4

Cyber resilience learning opportunities should be inclusive of everyone.

AIMS AND ACTIONS

AIMS AND ACTIONS

This action plan sets out **4 overarching aims** to successfully grow Scotland's cyber resilience learning and skills landscape. These aims are to:

A. Increase people's cyber resilience through awareness raising and engagement

B. Explicitly embed cyber resilience throughout our education and lifelong learning system

C. Increase people's cyber resilience at work

D. Develop the cyber security workforce and profession to ensure that skills supply meets demand and that skilled individuals can find rewarding employment in Scotland.

The Scottish Government, the National Cyber Resilience Leaders, Board and its partners have identified **37 key actions** sitting under these aims, which we will take forward collectively during the period 2018-20. These actions are set out below.

AIM A: Increase people's cyber resilience through awareness raising and engagement

To get the most out of the online world, it is important that Scotland's citizens are enabled to get the "basics" right, and take a preventative approach to help themselves stay safe online. It is also vital that they know what to do if they are subject to an online attack so that they can get back up and running safely. We need therefore to encourage basic cyber awareness and readiness in people's everyday use of digital technologies.

The take-up of even simple measures to improve personal cyber resilience appears to be low in Scotland. According to recent research commissioned by the Scottish Government, just over half of adults interviewed claimed to regularly install software updates; fewer than 1 in 10 protected their mobile devices with a password; and only 13% checked that a website was secure before divulging personal data[8]. Simple measures can prevent or minimise threats.

Furthermore, research from 2017 by the Carnegie UK Trust[9] found that people living in the most deprived communities in Scotland were least likely to use a password, to turn off location services or use a different online name. This reminds us of the need to target people living with disadvantage.

There is a wealth of advice and guidance available from national campaigns, most of it useful. However there is so much of it, and from multiple sources, that for citizens it may feel confusing or overwhelming. We will work with national partners to ensure cyber resilience messages are communicated effectively in Scotland using actual experiences to make the most impact. Working with Scottish intermediary organisations will be vital, as they are often best placed to reach particular audiences. Messages will be communicated in a positive way through their channels, with cyber resilience understood as an **enabler**, to ensure that individuals are not deterred from engaging with digital online technologies. Evidence demonstrates that peer learning can also be useful for building shared knowledge and trust in raising awareness.

8 Ipsos MORI, 2015

9 Digitally Savvy Citizens https://www.carnegieuktrust.org.uk/publications/digital-savvy-citizens/

A number of ambassadors/champions' networks already exist to promote key messages to particular audiences, for example, the Scottish Government's Digital Champions Development Programme and Police Scotland's Web Constables network. Working closely with these and other networks we can identify opportunities to deliver targeted messages about cyber resilience in the communities where they have influence.

The actions to increase people's cyber resilience through awareness raising and engagement (Aim A) are as follows:

1. The Scottish Government will work with partners in Scotland and the wider UK (for example, Get Safe Online[10]) to disseminate general and targeted cyber awareness messages to key audiences including citizens, businesses and organisations. **Ongoing**.
2. The Scottish Government will offer communications support to its national partners to deliver their own cyber resilience messages for their audiences, and ensure those messages are aligned with authoritative sources of advice (i.e. Cyber Aware, NCSC). **Ongoing**.
3. The Scottish Government will work with key partners, including Police Scotland, to identify ambassadors and champions who can deliver cyber resilience messages. **Ongoing**.
4. The Scottish Government will work with partners, including the UK Government, to monitor changes and improvements in cyber resilience behaviours among the general Scottish population. **Ongoing**.

AIM B: Explicitly embed cyber resilience throughout our education and lifelong learning system

The need for individuals to be cyber resilient has never been greater. It is vital that everyone, whatever their age, whether they are working or not, is able to keep safe online and know what to do if they experience a cyber attack.

From Early Years education, children and young people need opportunities to develop appropriate knowledge, understanding and behaviours to become more cyber resilient, for their present and future lives. Parents, grandparents and carers also need opportunities to develop their own understanding so that they can support their children and those dependent on them. People in Scotland are increasingly relying on online services to maintain their independence, access services, connect with families and their communities and manage their health and wellbeing. Being resilient online is therefore becoming increasingly important.

Cyber resilience within formal learning

Formal learning is delivered in Early Years learning settings, in schools, colleges, third sector organisations, universities and through training providers. Learners work towards formal qualifications or credit.

Work is being taken forward by the Scottish Government and partners to ensure that cyber resilience is recognised as core to digital literacy and digital participation. This is already being reflected in policy, for example within Scotland's refreshed

10 www.getsafeonline.org

Digital Strategy[11] and **Enhancing Learning and Teaching Through the Use of Digital Technology**[12], as well as in projects to develop the digital capacity and resilience of schools. It is also reflected in the STEM: Education and Training strategy, published in October 2017, which sets out a comprehensive programme to drive improvement in STEM learning throughout the education and training landscape. This strategy recognises digital skills and the importance of cyber resilience as part of STEM.

At school level, cyber resilience is now embedded in Curriculum for Excellence, within Experiences and Outcomes (Es and Os) of Digital Literacy, alongside internet safety[13]. Whilst not a formal 'Responsibility of All' i.e. on the same footing as literacy, numeracy and health & wellbeing, curriculum guidance is clear that Digital Literacy should be placed at the heart of all learning and that outcomes can be delivered by staff in all curricular areas and at all levels. This guidance was published in March 2017 and Education Scotland has committed to providing support for implementation of the new statements.

SQA is reviewing the ICT Core Skill framework, and this review is likely to highlight cyber resilience as a significant aspect. It is important that providers of education such as schools, colleges, community-based provision and others that support vocational learning, such as training providers, are equipped to support their learners to be more cyber resilient as well.

Cyber resilience within non-formal and informal learning

Non-formal and informal learning takes place in all of the settings mentioned above, for example in after-school clubs, but also in youth work, community learning settings and workplaces.

Cyber resilience learning is beginning to happen in some parts of this landscape such as digital youth work and work with disabled adults, and in training for practitioners in the non-formal learning sector. Examples include Young Scot's **Digital Academy**[14] including its work on **5Rights**[15] (which looks at supporting people to understand their rights in the digital world), Lead Scotland's **Getting Digital**[16] programme, and its formal learning module **Thinking Digitally**[17] (which is worth 12 credits at SCQF level 6), and the **Digitally Agile Community Learning and Development** project[18].

There are numerous learning resources available but they are not often packaged for or targeted at those working in non-formal learning settings. Practitioners in non-formal learning settings need access to appropriate guidance and training on how to build cyber resilience into their work with individuals and groups. Education Scotland, national youth and lifelong learning organisations have a role to play in contributing to the development of this guidance.

11 See footnote 5.

12 http://www.gov.scot/Publications/2016/09/9494/0

13 SG recently refreshed its *National Action Plan on Internet Safety for Children and Young People*, which makes reference to the cyber resilience strategy. **"Internet safety"** is about people being protected, safe and supported in the online world. **"Cyber resilience"** is about individuals and organisations being able to prepare for, withstand, rapidly recover and learn from deliberate attacks or accidental events in the online world. Internet safety is an important part of cyber resilience.

14 https://www.youngscot.net/what-we-do/digital-academy/

15 https://young.scot/5rights/

16 http://www.lead.org.uk/getting-digital/

17 http://www.getconnectedandlead.org.uk/show.php?contentid=160

18 a partnership between YouthLink Scotland, Learning Link Scotland and SCDC: https://www.digitallyagilecld.org/

The actions to explicitly embed cyber resilience throughout our education and lifelong learning system (AIM B) are as follows:

5. The Scottish Government will work with Education Scotland and other partners to look at ways to embed cyber resilience into Early Years education and will produce a plan of action by **autumn 2018**.

6. Education Scotland will work with education Regional Improvement Collaboratives to raise the profile of cyber resilience in regional planning for education, from **spring 2018** and **then on an ongoing basis**.

7. The Scottish Government will work with key partners to ensure that, when relevant skills frameworks are under review, cyber resilience is embedded appropriately. In the immediate term, this will include working with Scottish Qualifications Authority (SQA) on its review of the ICT Core Skill, by **summer 2018** and **then on an ongoing basis**.

8. Education Scotland will collate and disseminate existing learning and teaching resources to schools to support the learning of cyber resilience within the curriculum area of Digital Literacy. The Digital Skills Partnership[19] will support the dissemination of the resources. This will be done by **spring 2018** and resources will thereafter be refreshed as required.

9. The Scottish Government will work with organisations involved in non-formal learning, such as Scottish Council for Voluntary Organisations (SCVO), Young Scot, Lead Scotland, Youthlink Scotland, Learning Link Scotland and the Community Learning and Development (CLD) Standards Council, to develop and publish guidance for providers on the delivery of cyber resilience learning, by **spring 2019**.

10. The Scottish Government will work with appropriate teacher education institutions, Education Scotland, College Development Network and universities to plan how to strengthen the focus on cyber resilience in initial teacher education and career long professional learning in cyber resilience for teachers in schools and lecturers in colleges and universities, a plan to achieve this will be ready by **autumn 2018**.

11. The Scottish Government will work with Education Scotland to identify opportunities to embed cyber resilience into education inspection frameworks. In the first instance Education Scotland will embed cyber resilience in the reviewed quality framework for colleges, *How Good is Our College?*, within the principles of leadership, governance and curriculum, by **autumn 2018, and thereafter as opportunities arise**.

12. The Scottish Funding Council (SFC) will analyse colleges' and universities' steps towards embedding cyber resilience within their curricula and other activities in order to identify future activity required to support these institutions, by **summer 2018**.

13. College Development Network will explicitly identify knowledge, understanding and skills of cyber resilience as a key standard for lecturers within the upcoming review of the Professional Standards for Lecturers in Scotland's Colleges, by **summer 2018**.

19 The Digital Skills Partnership is a collaboration between universities, colleges and industry aimed at making the education system more responsive to changing skills requirements.

14. The Scottish Government will work with SDS and the Scottish Training Federation to identify options for engagement with independent training providers that can support their trainees' cyber resilience, by **winter 2018**.

15. The Scottish Government will work with the National Parent Forum of Scotland and other relevant organisations, to identify activity to develop parents' and guardians abilities to engage with their children's learning in order to ensure their children become more cyber resilient, by **winter 2018**.

16. The Scottish Government will work with public, third and private sector organisations involved in supporting the upbringing of children and young people to identify and implement measures to support children and young people to become more cyber resilient, by **winter 2019**.

17. The Scottish Government will work with care providers whose staff are well placed to support their clients to be more cyber resilient, by **winter 2019**.

AIM C: Increase people's cyber resilience at work

Workers who use digital technologies to perform their roles, often referred to as "digital end-users", are often the most important "link" in terms of cyber resilience for organisations.

A report[20] by the Federation of Small Businesses on skills and training has identified that over a fifth of small businesses are failing to take advantage of the digital world partly because their staff lack digital skills (22%) but also because of concerns about cyber security (21%). Guidance and training for employers is available from a number of trusted sources to help build their workforces' cyber resilience. In addition, there are a number of high quality self-learning programmes available, including e-learning modules – some are free, and others need to be bought under licensing arrangements.

Cyber resilience should be embedded in workplace practices and integrated into workplace learning and development, with as much emphasis as organisations place on health and safety. The role of unions is important too, as they often support workplace learning.

It is not, however, just the general workforce that need to build these capabilities. It is critical that senior managers understand the importance of having a cyber resilient workforce, and that they lead on embedding cyber resilience practice in the workplace. They themselves need to understand and be able to manage cyber risk, ensuring that it is part of risk registers, that it informs incident management and response plans, and is embedded within communication and organisational development workstreams.

We are beginning to see growing commitment and action being taken by employers, particularly in larger private sector organisations, in public bodies, and in some third sector organisations, to increase their workforces' cyber resilience. Employers have expressed an appetite for more national guidance on training programmes. For example, there has been significant demand from employers, unions and employees for the government funded Scottish Union Learning's programme of cyber security training for workers (which can be delivered in all sectors and not just for union members).The Scottish Business Resilience Centre has been working to drive up good cyber hygiene

20 Learning the Ropes: Skills and Training In Small Businesses (Dec 2017) http://www.fsb.org.uk/docs/default-source/fsb-org-uk/skills-and-training-report.pdf?sfvrsn=0

in Scottish private sector organisations, particularly within SMEs. This has included encouraging Cyber Essentials certification. Highlands and Islands Enterprise have reached over 130 businesses in 2017 to raise awareness of the importance of cyber resilience in the workplace. In the public sector, as part of the Public Sector Action Plan[21], there is a range of training programmes and materials being rolled out to support staff at all levels to become more cyber resilient.

The actions to support employers and individuals to increase cyber resilience at work (AIM C) are as follows:

18. The Scottish Government will work with key partners to provide/signpost best practice guidance on how to build cyber resilience effectively into workplace learning, as identified in the public, private and third sector action plans, by **autumn 2018**.

19. The Scottish Government will work with SDS and industry partners to explore opportunities for strengthening cyber resilience across occupational standards[22], by **autumn 2018**.

20. Scottish Union Learning will measure and report back to the Scottish Government on the impact of its autumn 2017 – spring 2018 government-funded cross-sectional cyber resilience workshops, **by summer 2018, after which next steps will be decided.**

AIM D: Develop the cyber security workforce and profession to ensure that skills supply meets demand and that skilled individuals can find rewarding employment in Scotland.

The cyber security skills shortage

In common with other countries, cyber security skills supply in Scotland is currently not meeting demand. At a global level, the workforce gap has a projected shortage of 1.8 million professionals by 2022[23]. In Scotland, this gap in cyber security skills is one of the most critical[24] in the digital sector.

We can estimate that there were likely to be 360 – 480 unfilled vacancies in 2017. In the absence of positive interventions to increase skills supply, these figures are expected to rise by 20% per year in Scotland (in line with the rate of growth in demand for cyber skills UK-wide).

Based on these trends, a conservative estimate for unfilled (or contractor-filled) vacancies in Scottish cyber security jobs in the future is as follows:

Year 2018: 430 – 580

Year 2019: 516 – 700

Year 2020: 620 – 840

21 http://www.gov.scot/Publications/2017/11/6231

22 Occupational standards are standards of performance that people are expected to achieve in their work, and the knowledge and skills they need to perform effectively.

23 https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

24 http://www.gov.scot/Topics/Economy/digital/digitalservices/workforce/sgs

Reasons for cyber skills shortages

There are a number of reasons for current skills shortages:

- Not enough people are identifying cyber security as a career option (at school and for career transitioners and changers).
- Not enough school pupils (particularly girls) are choosing STEM subjects or are aware of cyber security careers.
- Not enough school leavers are pursuing relevant degrees (especially young women).
- The cyber security cluster in Scotland is at a relatively early stage of development.
- We are not retaining enough skilled individuals in Scotland, with many graduates moving to London or elsewhere upon completion of their degrees.

The need to actively promote cyber security as a career

Cyber security is a rapidly changing and expanding field. This expansion requires skilled workers to help organisations perform a range of cyber security functions. As organisations identify what is needed to adequately manage current and future cyber security risk, leaders need to consider their cyber security workforce capabilities and capacity as part of this. Cyber security should be regarded as an accessible and inclusive career option, open to people from all backgrounds.

The Scottish Government is keen to see more promotion of, and more pathways into, cyber security as a career option. This includes promoting the current range of pathways into cyber security which includes an Information Security Modern Apprenticeship and a Cyber Security Graduate Apprenticeship. Skills Development Scotland continue to actively promote cyber security as a career through their career channels and programmes.

There are some pockets of non-formal or extra-curricular activity aimed at promoting cyber security as a career to young people. These include the competitions and games promoted by Cyber Security Challenge UK, activity led as part of NCSC's CyberFirst programme, and the Cyber Christmas Lectures, aimed at engaging the interest of young people. More work is required to the Scottish curriculum and to make appropriate links with Scotland's schools and other learning providers.

Several schools now offer SQA's National Progression Awards (NPAs) in Cyber Security and a number of colleges offer introductory computing courses with a cyber security element as well as the NPAs. SQA's forthcoming HNC and HND (with linked Professional Development Awards (PDAs) in Cyber Security should increase delivery of cyber security learning opportunities in colleges.

We are keen to encourage engagement with schools and colleges by employers (both public and private sector), higher education institutions, professional associations such as (ISC)[2], ISACA and ISSA, as they can support the development of future cyber professionals. This support can include offering Foundation Apprenticeship work placements, engaging with schools, colleges and universities to develop/deliver course content, employing interns, mentoring of students, and sponsoring and supporting PhD and MSc students and undergraduates.

Skills development pathways

Scotland is steadily building a strong pipeline in cyber security qualifications. We have attached at **Annex B** a snapshot of qualifications that are available (or will soon be available) in Scotland for developing cyber security skills across our education system.

In our schools and colleges, there are currently low numbers of Computing Science teachers. To support the effective delivery of these new qualifications, we need teachers who are confident and able to teach cyber security and who are supported by high quality learning and teaching resources and best practice in cyber security techniques.

Some businesses look for a wide range of professional qualifications and accreditations, (see **Annex C** for a list). Others seek advanced-level academic study. It can be resource-intensive for individuals to maintain the range of accreditations/professional body memberships. There is a requirement to better understand, explain and promote the existing professional qualifications and accreditation landscape.

Skills and academic development in universities

Traditionally, cyber security has been embedded into computing science degree-level and postgraduate courses in the form of accredited modules. Over recent years, the increased demand for cyber security graduates and specialists has led to a growth of dedicated cyber security degree-level and postgraduate courses in our universities. Graduate level apprenticeships in cyber security are gaining momentum as a result of funding from Skills Development Scotland and the European Social Fund. A Graduate Level Apprenticeship in Cyber Security has been developed by Skills Development Scotland, and Napier University, for example, has recently launched its own BSc Graduate Level Apprenticeship in Cyber Security and Forensics.

As the demand for skilled professionals in cyber security increases, it is important that government, the private sector and academia work together to categorise and describe cyber security work. This would support academic institutions to standardise curricula and certification where appropriate, and employees, employers and employability services to best match skilled people to skilled jobs.

Our universities have a critical role in inspiring and supporting future cyber security professionals, through engagement with schools and colleges. There is also an opportunity for academia and the cyber security industry to work together to develop cyber security related curricula. For example the Palo Alto Cyber Networks Cyber Academy Programme provides technology and services for use in the classroom – at no cost – to any higher education institution. They work with academic partners to develop bespoke curricula and, so far, have worked in partnership with Abertay University, Glasgow Caledonian University and Glasgow Clyde College.

NCSC has a role to play in boosting the outcomes of our universities. Universities should be encouraged to achieve NCSC certification for their undergraduate or postgraduate degrees to raise their profile on the global stage. In addition, NCSC's CyberFirst Bursary scheme is available to fund studies at undergraduate level in any STEM subject.[25]

Cyber security research and innovation

Scotland is already home to five of the world's top universities and there is a pedigree and increasing depth of expertise in cyber security across our higher education institutions. The University of Edinburgh, for example, is an NCSC-accredited Academic Centre of Excellence in Cyber Security Research and other Scottish universities are working effectively to build their offer in respect of cyber security research. One method of boosting research activity would be to increase numbers of PhD students taking forward cyber security-related research that can contribute to innovation and inclusive growth in the Scottish economy. One potential step towards this would be to establish a Centre for Doctoral Training to link industry with researchers. This may also assist in attracting the best talent to our universities.

Scotland's cyber security goods and services industry is, in line with the rest of the world, growing at a significant rate. Expert technical skills are in demand, but so are the skills to drive innovation and research.

The role of cyber security has grown significantly in Scotland's financial sector, creating jobs and opportunities, particularly in relation to "fintech", and this growth is expected to continue as new technologies roll out and our businesses and people become even more digitally connected.

25 https://www.ncsc.gov.uk/articles/cyber-first-bursary-scheme

Cyber security skills – an integral part of digital and many other skills.

The Scottish Government is clear that cyber security skills must be clearly identified as a key aspect of the Scottish Government's Digital Technologies Skills Investment Plan, as well as all Skills Investment Plans across other industries. All future reviews of Skills Investment Plans in other industries will include cyber security skills, where appropriate.

The key actions to develop the cyber security workforce and profession to ensure that skills supply meets demand and that skilled individuals can find rewarding employment in Scotland (AIM D) are as follows:

21. The Scottish Government will work with SDS to include cyber security within future skills planning, including through their work with the Enterprise and Skills Strategic Board. **Ongoing**.

22. The Scottish Government will work with SDS and the Digital Technologies Skills Group – the group responsible for advising on the Digital Technologies Skills Investment Plan - to ensure there is a robust evidence base to underpin future decision making on the development of cyber security skills in Scotland. This work will also include an ongoing review of other countries' approaches to developing cyber security skills, **Plan produced by summer 2018 and implementation throughout 2018 and 2019**.

23. SDS will work with partners in the Digital Technologies Skills Group, and with wider industry, to produce a cyber security career framework that will support employers and individuals from all backgrounds to understand education and career pathways into and through the cyber security industry. This will also provide guidance for digital technology professionals who wish to develop their cyber security skills. The framework will include information about professional qualifications and accreditation, and will be finalised by **autumn 2018**.

24. SQA will support the delivery of current and new cyber security qualifications by developing teaching, learning and assessment materials. With Education Scotland and College Development Network, SQA will continue to support the professional learning of teachers and lecturers to deliver these qualifications. **Roll out throughout 2018 and 2019**.

25. The Scottish Government will work with SDS to consider options to support career changers or unemployed people to develop skills for cyber security roles. **An options paper to achieve this will be produced by autumn 2018**.

26. The Scottish Government, with lead partner Education Scotland, will work with the UK Government to identify opportunities to shape the UK national schools cyber security programme (called Cyber Discovery) for appropriate implementation in Scotland. **A plan to do so will be produced by summer 2018**.

27. The Scottish Government, in partnership with ScotlandIS, the cyber security industry, academia/SICSA and the Digital Skills Partnership, will aim to categorise and describe cyber security work. This could be used by academic institutions to standardise curricula and certification, and by employees, employers and employability services to best match skilled people to skilled jobs. **This work will be completed by spring 2019**.

28. The Scottish Government, ScotlandIS and representatives from the cyber security sector in Scotland will work with the UK Government and wider UK industry to develop the UK Royal Chartered Professional Body for Cyber Security, with the aim of it having a strong Scottish presence and benefiting Scotland's cyber security sector, by **summer 2018 and then ongoing**.

29. SDS will work alongside industry partners to review National Occupational Standards for cyber security with a view to embedding cyber resilience competences appropriately in professional roles by **spring 2019**.

30. The Scottish Government, Education Scotland and SDS will work with partners at the UK level to ensure appropriate alignment of cyber skills development plans, ensuring that Scotland can benefit fully from UK-wide initiatives. **Ongoing**.

31. The Scottish Government will work with SDS and Industry Leadership Skills Groups to promote the importance of cyber security to all sectors, and ensure that cyber security is embedded appropriately into Skills Investment Plans where appropriate. **Ongoing**.

32. The Scottish Government will work with SQA to strengthen its portfolio of cyber security qualifications, through filling in gaps in the portfolio and keeping existing qualifications relevant. **Ongoing**.

33. Scottish Informatics and Computer Science Alliance (SICSA) will lead work with universities and colleges to build capacity for cyber security courses (including cyber security within IT courses) at under- and post-graduate levels, as well as research opportunities. This will include working with the Scottish Government to consider establishing a forum for bringing together industry with researchers, such as a Centre for Doctoral Training. **Throughout 2018 and 2019**.

34. SICSA and College Development Network will increase levels of engagement with schools and communities aimed at inspiring young people to consider cyber security as a career. **Ongoing**.

35. The National Parent Forum for Scotland (NPFS) will continue work with SDS to disseminate existing resources that seek to promote cyber security careers to parents/families. NPFS and SDS will review the need for new resources in this area and develop them if required. **Throughout 2018 and 2019**.

36. SDS will identify opportunities to further integrate cyber security skills into the Apprenticeships Family, and work with industry and employer groups to ensure widespread awareness and adoption of work-based learning pathways within the cyber security industry. **Ongoing**.

37. The Scottish Government will work with SDS and others to ensure a coordinated approach to develop a pipeline of future cyber professionals. This will include supporting Digital World and My World of Work careers campaigns; promotion of e-placement Scotland and other internship, placement and mentoring opportunities; and creating opportunities for industry to enhance the delivery of curriculum. The Scottish Government will produce a coordination plan by **summer 2018**.

ANNEXES

Annex A – continuum of cyber resilience learning and skills

activity →	awareness raising	embedding cyber resilience in curricula	embedding cyber resilience in workplace learning	developing cyber security specialist skills	upskilling in cyber security	building research capability and capacity
section of population targeted	general population	people, particularly children and young people, in education system, and in youth work and community learning; families	digital end-users in workplaces, employers, including boards	future cyber security specialists (currently in education or seeking retraining)	existing digital technology specialists who need to increase their knowledge and skills in cyber security	research specialists
outputs from this activity	campaigns, signposting, communications, ambassadors/ champions	curriculum guidance for professionals, learning materials, session plans, training, qualifications, ambassadors/ champions and families	guidance for employers on effective learning programmes, training for trainers and learning & development leads, ambassadors/ champions	national career framework; careers advice in schools, colleges and universities; families; specialist learning programmes including qualifications; retraining programmes; talent spotting/ nurturing activities; better engagement between industry and education, ambassadors/ champions	guidance for employers and employees on upskilling opportunities; better engagement between industry and skills providers (for example so that colleges and universities can provide bespoke training for employers) membership of professional body, ambassadors/ champions; qualifications and accreditation	research activity; establishment of an industry/ research forum (e.g. Centre for Doctoral Training); start-ups and spin-outs from universities, expertise to meet industry needs
delivers on the aim from this action plan:	A. increase people's cyber resilience through awareness raising and engagement	B. explicitly embed cyber resilience throughout our education system	C. increase people's cyber resilience at work	D. develop the cyber security workforce and profession to ensure that skills supply meets demand and that skilled individuals can find rewarding employment in Scotland	D. develop the cyber security workforce and profession to ensure that skills supply meets demand and that skilled individuals can find rewarding employment in Scotland	D. develop the cyber security workforce and profession to ensure that skills supply meets demand and that skilled individuals can find rewarding employment in Scotland

Annex B – Qualifications and courses that develop cyber security skills, levelled against the Scottish Credit and Qualifications Framework (SCQF)

This table provides a snapshot overview (at February 2018) of learning programmes (qualifications and courses) available in Scotland at the time of publication of this action plan, including those which are planned for launch in the near future.

Several computing science courses at undergraduate and postgraduate level may also include cyber security modules.

Key:

PDA = Professional Development Award

HNC = Higher National Certificate

HND = Higher National Diploma

NPA = National Progression Award

SCQF Level	Institution or Awarding Body	Award
11	Abertay University	MSc/PGDiP Ethical Hacking and Cyber Security
	Edinburgh Napier University	MSc Advanced Networking
		MSc Advanced Security and Cybercrime
	Glasgow Caledonian University	Graduate Level Apprenticeship in Cyber Security
		MSc Network Security
	Glasgow University	Introduction to Computer Forensics and E-Discovery
	Heriot-Watt University	MSc Network Security
	Open University	Digital Forensics module
		Graduate Level Apprenticeship in Cyber Security
	Robert Gordon University	MSc Information and Network Security
	UHI Perth	Managing Cyber Risk (Forthcoming)
	University of Edinburgh	Blockchains and Distributed Ledgers
	University of Glasgow	MSc Information Security
		IntM Security, Intelligence and Strategic Studies
	University of the West of Scotland	MSc Information and Network Security
10	Abertay University	BSc (Hons) Ethical Hacking
	Edinburgh Napier University	BEng (Hons) Computer Security & Forensics
		Graduate Level Apprenticeship in Cyber Security
	Glasgow Caledonian University	BSc (Hons) Cyber Security & Networks
		BEng (Hons) Networked Systems Engineering
		BEng (Hons) Digital Security, Forensics and Ethical Hacking
		Graduate Level Apprenticeship in Cyber Security
	Robert Gordon University	BSc (Hons) Cyber Security
	University of the West of Scotland	BSc Cyber Security

9	SQA	PDA: Cyber Security (due summer 2019)

8	SQA	Diploma for Information Security Professionals (forms the qualification element of the Modern Apprenticeship Framework)
		HND Cyber Security (due winter 2018/19)
		PDA: Cyber Security (due winter 2018/19)

7	SQA	HNC: Cyber Security (due summer 2018)
		PDA: Cyber Security (due summer 2018)

6	SQA	NPA: Cyber Security
		Diploma for Information Security Professionals (forms the qualification element of the Modern Apprenticeship Framework)

5	BCS/ECDL	IT Security 2.0
	SQA	NPA: Cyber Security

4	SQA	NPA Cyber Security
		Cyber Security Fundamentals
	West College Scotland	eSafety unit

Annex C – Professional accreditation for cyber security professionals

Professional accreditation for cyber security professionals (snapshot, as of Feb 2018)

CONVENER	ACCREDITATION	TARGET AUDIENCE
ISACA	Certified Information Systems Auditor	CISO, CTO, ISO and associated IT & Cyber security personnel
ISACA	Certified Information Security Manager	CISO, CTO, ISO and associated IT & Cyber security personnel
ISACA	Certified in the Governance of Enterprise IT	CISO, CTO, ISO and associated IT & Cyber security personnel
ISACA	Certified in Risk and Information Systems Control	CISO, CTO, ISO and associated IT & Cyber security personnel
ISACA	CSX Fundamentals Certificate	
ISACA	CSX Practitioner Certification	
ID Cyber	Cyber Ethical Hacker	CISO, CTO, ISO and associated IT & Cyber security personnel
CESG	CESG Certified Professional	CISO, CTO, ISO and associated IT & Cyber security personnel
$(ISC)^2$	Systems Security Certified Practitioner	CISO, CTO, ISO and associated IT & Cyber security personnel
$(ISC)^2$	Certified Secure Software Lifecycle Professional	CISO, CTO, ISO and associated IT & Cyber security personnel
$(ISC)^2$	Certified Cloud Security Professional	CISO, CTO, ISO and associated IT & Cyber security personnel
$(ISC)^2$	Certified Authorization Professional	
$(ISC)^2$	Certified Information Security & Systems Professional	CISO, CTO, ISO and associated IT & Cyber security personnel
$(ISC)^2$	HealthCare Information Security and Privacy Practitioner	
IACIS	Certified Forensic Computer Examiner	CISO, CTO, ISO and associated IT & Cyber security personnel
IACIS	Certified Advanced Windows Forensic Examiner	
IACIS	IACIS Certified Mobile Device Examiner	
CYBARY	IR, Forensics, Network, Pentesting, management	CISO, CTO, ISO and associated IT & Cyber security personnel
SANS	IR, Forensics, Network, Pentesting, management	CISO, CTO, ISO and associated IT & Cyber security personnel
CompTIA	Certified Information Security Management Principles	Support Engineer, Maintenance Engineer, Desktop Engineer, Computer Administrator or PC Support Analyst
MICROSOFT	Various	CISO, CTO, ISO and associated IT & Cyber security personnel
CISCO	Various	CISO, CTO, ISO and associated IT & Cyber security personnel
CREST	Various	CISO, CTO, ISO and associated IT & Cyber security personnel

Annex D – Cyber Resilience Awareness Raising programmes

National Cyber Security Centre
a part of GCHQ

The National Cyber Security Centre (NCSC) is intended to be the authoritative voice and centre of expertise on cyber security for the UK as a whole. It has a key role in managing significant national cyber security incidents. NCSC is a relatively new organisation – just over a year old – and continues to develop its advice and support offering.

Cyber Essentials Scheme is a certification scheme run by the National Cyber Security Centre (NCSC) aimed at encouraging all UK organisations to protect themselves against the most common forms of cyber-attack. Developed by the UK Government in partnership with industry, the scheme sets out a simple set of five technical controls to help keep internet connected systems and the data they hold safe: www.cyberessentials.ncsc.gov.uk

CYBER ESSENTIALS

CYBER AWARE
Protecting your device
Protecting your data
Protecting your business

Cyber Aware is a cross-government awareness and behaviour change campaign delivered by the Home Office in conjunction with Department of Culture, Media & Sport alongside the National Cyber Security Centre, and funded by the National Cyber Security Programme in the Cabinet Office (https://www.cyberaware.gov.uk/).

Cyber Aware has a wide range of communications and marketing campaigns which focus on three key pillars:

Action Fraud is the fraud and cybercrime reporting centre for England and Wales (https://www.actionfraud.police.uk/). It recently launched a 24/7 helpline to combat cyber-attacks against businesses, charities and organisations, under which businesses can speak to specially trained advisors who can offer advice and support during cyber-attacks (see: https://actionfraud.police.uk/news-action-fraud-launches-24-7-helpline-to-combat-cyber-attacks-dec17).

NB: Despite the fact that Police Scotland currently does not formally participate in the scheme, the website does not state that if you live in Scotland you should report cybercrime to Police Scotland.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

TAKE FIVE TO STOP FRAUD

Take 5, a national awareness campaign led by FFA UK (part of UK Finance), backed by UK Government and delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector, to help tackle financial fraud (https://takefive-stopfraud.org.uk/).

Protecting your computer

Protecting yourself

Smartphone and Tablets

Shopping, banking and payments

Safeguarding children

Social networking

Business

Get Safe Online (GSO) is a UK Government-funded free resource providing practical advice to individuals and businesses on how to protect themselves while on their computers and mobiles device and against fraud, identity theft, viruses and many other problems encountered online. Their website (https://www.getsafeonline.org/) contains a dense library of content that comes under the following headings:

Annex E – Cyber Resilience Learning and Skills Action Plan

Aims and actions

AIMS

A. Increase people's cyber resilience through awareness raising and engagement

B. Explicitly embed cyber resilience throughout our education and lifelong learning system

C. Increase people's cyber resilience at work

D. Develop the cyber security workforce and profession to ensure that skills supply meets demand and that skilled individuals can find rewarding employment in Scotland.

AIM A: Increase people's cyber resilience through awareness raising and engagement

No	Action	Timescales
1	The Scottish Government will work with partners in Scotland and the wider UK to disseminate general and targeted cyber awareness messages to key audiences including citizens, businesses and organisations.	Ongoing
2	The Scottish Government will offer communications support to its national partners to deliver their own cyber resilience messages for their audiences, and ensure those messages are aligned with authoritative sources of advice (i.e. Cyber Aware, NCSC.	Ongoing
3	The Scottish Government will work with key partners, including Police Scotland, to identify ambassadors and champions who can deliver cyber resilience messages.	Ongoing
4	The Scottish Government will work with partners, including the UK Government, to monitor changes and improvements in cyber resilience behaviours among the general Scottish population.	Ongoing

AIM B: Explicitly embed cyber resilience throughout our education and lifelong learning system

No	Action	Timescales
5	The Scottish Government will work with Education Scotland and other partners to look at ways to embed cyber resilience into Early Years education and will produce a plan of action.	Plan ready autumn 2018
6	Education Scotland will work with education Regional Improvement Collaboratives to raise the profile of cyber resilience in regional planning for education.	Spring 2018 and then ongoing basis
7	The Scottish Government will work with key partners to ensure that, when relevant skills frameworks are under review, cyber resilience is embedded appropriately. In the immediate term, this will include working with Scottish Qualifications Authority (SQA) on its review of the ICT Core Skill.	Summer 2018 and then ongoing basis

8	Education Scotland will collate and disseminate existing learning and teaching resources to schools to support the learning of cyber resilience within the curriculum area of Digital Literacy.	Spring 2018 and resources thereafter refreshed as required
9	The Scottish Government will work with organisations involved in non-formal learning, such as Scottish Council for Voluntary Organisations (SCVO), Young Scot, Lead Scotland, Youthlink Scotland, Learning Link Scotland and the Community Learning and Development (CLD) Standards Council, to develop and publish guidance for providers on the delivery of cyber resilience learning.	Spring 2019
10	The Scottish Government will work with appropriate teacher education institutions, Education Scotland, College Development Network and universities to plan how to strengthen the focus on cyber resilience in initial teacher education and career long professional learning in cyber resilience for teachers in schools and lecturers in colleges and universities.	Plan to achieve this ready by autumn 2018.
11	The Scottish Government will work with Education Scotland to identify opportunities to embed cyber resilience into education inspection frameworks. In the first instance Education Scotland will embed cyber resilience in the reviewed quality framework for colleges, How Good is Our College?, within the principles of leadership, governance and curriculum.	By autumn 2018, and thereafter as opportunities arise.
12	The Scottish Funding Council (SFC) will analyse colleges' and universities' steps towards embedding cyber resilience within their curricula and other activities in order to identify future activity required to support these institutions, by summer 2018.	Summer 2018
13	College Development Network College Development Network will explicitly identify knowledge, understanding and skills of cyber resilience as a key standard for lecturers within the upcoming review of the Professional Standards for Lecturers in Scotland's Colleges.	Summer 2018
14	The Scottish Government will work with SDS and the Scottish Training Federation to identify options for engagement with independent training providers that can support their trainees' cyber resilience.	Winter 2018
15	The Scottish Government will work with the National Parent Forum of Scotland and other relevant organisations, to identify activity to develop parents' abilities to engage with their children's learning in order to ensure their children become more cyber resilient.	Winter 2018
16	The Scottish Government will work with public, third and private sector organisations involved in supporting the upbringing of children and young people to identify and implement measures to support children and young people to become more cyber resilient.	Winter 2019
17	The Scottish Government will work with care providers whose staff are well placed to support their clients to be more cyber resilient.	Winter 2019

AIM C: Increase people's cyber resilience at work

No	Action	Timescales
18	The Scottish Government will work with key partners to provide/signpost best practice guidance on how to build cyber resilience effectively into workplace learning, as identified in the public, private and third sector action plans.	Autumn 2018
19	The Scottish Government will work with SDS and industry partners to explore opportunities for strengthening cyber resilience across occupational standards.	Autumn 2018
20	Scottish Union Learning will measure and report back to the Scottish Government on the impact of its government funded programme of cyber resilience workshops delivered in multiple sectors between autumn of 2017 and spring 2018, after which next steps will be decided.	Autumn 2018

AIM D: Develop the cyber security workforce and profession to ensure that skills supply meets demand and that skilled individuals can find rewarding employment in Scotland

No	Action	Timescales
21	The Scottish Government will work with SDS to include cyber security within future skills planning, including through their work with the Enterprise and Skills Strategic Board.	Ongoing
22	The Scottish Government will work with SDS and the Digital Technologies Skills Group – the group responsible for advising on the Digital Technologies Skills Investment Plan - to ensure there is a robust evidence base to underpin future decision making on the development of cyber security skills in Scotland. This work will also include an ongoing review of other countries' approaches to developing cyber security skills.	Plan produced by summer 2018. Implementation throughout 2018 and 2019.
23	SDS will work with partners in the Digital Technologies Skills Group, and wither industry, to produce a cyber security career framework that will support employers and individuals from all backgrounds to understand education and career pathways into and through the cyber security industry. This will also provide guidance for ICT professionals who wish to develop their cyber security skills. The framework will include information about professional qualifications and accreditation.	Autumn 2018
24	SQA will support the delivery of current and new cyber security qualifications by developing teaching, learning and assessment materials. With Education Scotland and College Development Network, SQA will continue to support the professional learning of teachers and lecturers to deliver these qualifications.	Roll out throughout 2018 and 2019.
25	The Scottish Government will work with SDS to consider options to support career changers or unemployed people to develop skills for cyber security roles.	Options paper produced by autumn 2018.
26	The Scottish Government, with lead partner Education Scotland, will work with the UK Government to identify opportunities to shape the UK national schools cyber security programme (called Cyber Discovery) for appropriate implementation in Scotland.	Plan produced by summer 2018.

27	The Scottish Government, in partnership with ScotlandIS, the cyber security industry and academia, will aim to categorise and describe cyber security work. This could be used by academic institutions to standardise curricula and certification, and by employees, employers and employability services to best match skilled people to skilled jobs.	Spring 2019
28	The Scottish Government, ScotlandIS and representatives from the cyber security sector in Scotland will work with the UK Government and wider UK industry to develop the UK Royal Chartered Professional Body for Cyber Security, with the aim of it having a strong Scottish presence and benefiting Scotland's cyber security sector.	Ongoing
29	SDS will work alongside industry partners to review National Occupational Standards for cyber security with a view to embedding cyber resilience competences appropriately in professional roles.	Spring 2019
30	The Scottish Government, Education Scotland and SDS will work with partners at the UK level to ensure appropriate alignment of cyber skills development plans, ensuring that Scotland can benefit fully from UK-wide initiatives.	Ongoing
31	The Scottish Government will work with SDS and Industry Leadership Skills Groups to promote the importance of cyber security to all sectors, and ensure that cyber security is embedded appropriately into Skills Investment Plans.	Ongoing
32	The Scottish Government will work with SQA to strengthen its portfolio of cyber security qualifications, through filling in gaps in the portfolio and keeping existing qualifications relevant.	Ongoing
33	Scottish Informatics and Computer Science Alliance (SICSA) will lead work with universities and colleges to build capacity for cyber security courses (including cyber security within IT courses) at under- and post-graduate levels, as well as research opportunities. This will include working with the Scottish Government to consider establishing a forum for bringing together industry with researchers, such as a Centre for Doctoral Training.	Throughout 2018 and 2019
34	SICSA and College Development Network will increase levels of engagement with schools and communities aimed at inspiring young people to consider cyber security as a career.	Ongoing
35	The National Parent Forum for Scotland (NPFS) will continue work with SDS to disseminate existing resources that seek to promote cyber security careers to parents/families. NPFS and SDS will review the need for new resources in this area and develop them if required.	Throughout 2018 and 2019
36	SDS will identify opportunities to further integrate cyber security skills into the Apprenticeship Family, and work with industry and employer groups to ensure widespread awareness and adoption of work-based learning pathways within the cyber security industry.	Ongoin
37	The Scottish Government will work with SDS and others to ensure a coordinated approach to develop a pipeline of future cyber professionals. This will include supporting Digital World and My World of Work careers campaigns; promotion of e-placement Scotland and other internship, placement and mentoring opportunities; and creating opportunities for industry to enhance the delivery of curriculum. SG will produce a coordination plan.	Coordination plan ready by summer 2018

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: 978-1-78851-688-4

Published by The Scottish Government, March 2018

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS350986 (3/18)