www.gov.scot/cyberresilience

Scottish Government
Riaghaltas na h-Alba
gov.scot

FIRM FOUNDATIONS: PROGRESS REPORT ON SAFE, SECURE AND PROSPEROUS A CYBER RESILIENCE STRATEGY FOR SCOTLAND (2015–2020)

FOREWORD

In the five years since its launch, *Safe, secure and prosperous: a cyber resilience strategy for Scotland* has put in place many of the building blocks to strengthen Scotland's ability to prepare for, withstand and recover from cyber attacks.

Through an ambitious, proactive and hugely collaborative approach, our strategy and its associated action plans have helped to establish Scotland as a leading nation in cyber resilience good practice.

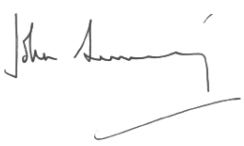
Other countries look to us as a model for many aspects of our approach, particularly in the ways we have enhanced the cyber security of our public sector and our work to embed cyber resilience and cyber security skills across our education and lifelong learning system.

This report sets out the progress we have made in Scotland, and the impact our interventions have had to date. Fundamentally, this report shows that the cyber resilience of our people and organisations and our cyber security skills base have grown since 2015. It also illustrates the early growth to date of our cyber security products and services industry, while demonstrating that there is room for further opportunity and expansion.

Our cross-societal approach and the role of partners have been key to the substantial progress made so far. Many achievements are due to fantastic public, third and private sector drive and collaboration. Positive collaboration between governments and with the National Cyber Security Centre (NCSC) – our trusted source of cyber security advice, guidance and support – have also been critical factors in the progress made in these first few years.

I want to thank every organisation and individual for the part they have played in getting us to this important stage. I also want to thank the National Cyber Resilience Advisory Board, which has shown great national leadership, first under the chairing of Hugh Aitken, and now under the chairing of David Ferbrache. Thank you to Hugh and David for your advice, determination and ambition on behalf of Scotland.

It is clear to me, however, that our task is not yet complete and will continue to challenge all of us, whether government, digital public services, businesses or individuals. The global landscape has changed significantly since the publication of this strategy. The technological and threat environment is constantly evolving and, as the ongoing COVID-19 pandemic has shown us, reliance upon digital technologies is central to the conduct of business and education activity. COVID-19 has required fundamental change, at pace, to how we work, how we do business and how we interact socially. We must look beyond 2020 and consider how we can sustain a long-term national response, ensuring that cyber resilience is seen as a fundamental and integral component of economic and societal recovery. Of course, we cannot do this alone. We need to work ever more closely with industry and wider society in Scotland, across the UK and internationally, to ensure that Scotland continues to be a safe, secure and resilient place to live, work and do business. This report is a critical component of that continued endeavour: a staging post from which we can reflect back to help us look forward.



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

REFLECTIONS FROM THE CHAIR OF THE NATIONAL CYBER RESILIENCE ADVISORY BOARD – DAVID FERBRACHE, OBE

Safe, secure and prosperous: a cyber resilience strategy for Scotland set out an ambitious vision for a digital society and economy remaining resilient in the face of a growing cyber threat.

In the five years since the strategy was published much has been achieved and the progress is a testament to the cyber resilience community in Scotland. Nowhere was this national effort clearer than in the response to the changing cyber threat we saw during COVID-19 with the Scottish Government, Police Scotland, the Scottish Council for Voluntary Organisations and the Scottish Business Resilience Centre working together to raise awareness and support the community in the face of a rapidly evolving cyber threat.

The five action plans put in place to deliver the cyber resilience strategy have made progress, in some cases exceptional, in others challenges remain.

The Learning and Skills Action Plan reached many young people through the work of Skills Development Scotland, Education Scotland, Young Scot, Police Scotland, Civic Digits, NCSC's CyberFirst programme and the Cyber Christmas Lectures. Cyber resilience is now a key part of the educational curriculum and national occupational standards; with National Progression Awards, HNC, HND and Professional Development Awards in Cyber Resilience and Cyber Security.

The Third Sector Action Plan saw over 250 organisations achieve Cyber Essentials, over 1,000 charities educated on cyber fundamentals, and 10,000 third sector organisations provided with regular cyber advice through the Scottish Charity Regulator, OSCR.

The Public Sector Action Plan has seen good progress in focusing public sector bodies on cyber security risks, raising board awareness, achieving Cyber Essentials certification, establishing incident management policies and ensuring the cyber security of supply chains is considered. There is more to do to fully embed cyber resilience into public sector digital strategies and investment plans, and to build confidence that Scotland can withstand a large scale cyber attack – but this is a good start.

The Private Sector and Economic Opportunity Action Plans have proved most challenging. While the Scottish Business Resilience Centre, ScotlandIS and Scottish Information Sharing Network/CISP have reached many hundreds of firms in Scotland, there is much to do working with Ministers, professional and trade bodies to scale these initiatives and achieve the impact we require, working closely with the NCSC. As a nation we need to have confidence in building our cyber resilience research and industry base, and in promoting Scotland's cyber security goods and services sector. We often underplay our achievements.

The cyber threat has grown, as has our dependency on cyberspace. Continuing Ministerial focus, increased investment and creativity are needed to drive the cyber resilience agenda. Without such investment we risk undermining the resilience of the digital economy which Scotland will depend on for its future, but we recognise that in these times of restraint we must also be disciplined in linking that investment to clear outcomes and metrics. The journey toward cyber resilience has begun, and that journey will be vital to the achievement of a safe, secure and prosperous Scotland.

David Ferbrache, OBE
Chair, National Cyber Resilience Advisory Board

CONTENTS

CREATING THE RIGHT CONDITIONS FOR SCOTLAND

1

1. CREATING THE RIGHT CONDITIONS FOR SCOTLAND

1.1 THE STRATEGY'S VISION

Safe, secure and prosperous: a cyber resilience strategy for Scotland (*the Strategy*) was published in November 2015[1]. It has, at its heart, the vision that Scotland could be a world leader in cyber resilience and be a nation that could claim, by 2020, to have achieved the following outcomes:

1. our people are informed and prepared to make the most of digital technologies safely
2. our businesses and organisations recognise the risks in the digital world and are well-prepared to manage them
3. we have confidence in and trust our digital public services
4. we have a growing and renowned cyber resilience research community
5. we have a global reputation for being a secure place to live and learn, and to set up and invest in business
6. we have an innovative cyber security goods and services industry that can help meet global demand

The Strategy's outcomes contribute to a number of national outcomes in Scotland's National Performance Framework (NPF). The figure on the next page shows how the Strategy contributes to the NPF, and how Scotland's NPF in turn contributes to the UN Sustainable Development Goals.

1 Throughout this report we reference a number of strategic documents, action plans, resources and toolkits. Where possible, a hyperlink has been included each time a document is mentioned for the first time.

Strategic Outcomes	Contributes to → National Performance Framework Outcomes	Contributes to → UN Sustainable Development Goals
Our people are informed and prepared to make the most of digital technologies safely	We tackle poverty by sharing opportunities, wealth and power more equally	1. No poverty 10. Reduced inequalities
	We are well educated, skilled and able to contribute to society	4. Quality education 10. Reduced inequalities
	We live in communities that are inclusive, empowered, resilient and safe	11. Sustainable cities and communities
Our businesses and organisations recognise the risks in the digital world and are well-prepared to manage them	We live in communities that are inclusive, empowered, resilient and safe	9. Industry, innovation and infrastructure 11. Sustainable cities and communities
	We have thriving and innovative businesses, with quality jobs and fair work for everyone	8. Decent work and economic growth 9. Industry, innovation and infrastructure
	We have a globally competitive, entrepreneurial, inclusive and sustainable economy	8. Decent work and economic growth 9. Industry, innovation and infrastructure
We have confidence in and trust our digital public services	We live in communities that are inclusive, empowered, resilient and safe	9. Industry, innovation and infrastructure 11. Sustainable cities and communities
	We respect, protect and fulfil human rights and live free from discrimination	16. Peace, justice and strong institutions
We have a growing and renowned cyber resilience research community	We are well educated, skilled and able to contribute to society	4. Quality education
	We have a globally competitive, entrepreneurial, inclusive and sustainable economy	8. Decent work and economic growth 9. Industry, innovation and infrastructure
We have a global reputation for being a secure place to live and learn, and to set up and invest in business	We live in communities that are inclusive, empowered, resilient and safe	9. Industry, innovation and infrastructure 11. Sustainable cities and communities
	We have a globally competitive, entrepreneurial, inclusive and sustainable economy	8. Decent work and economic growth 9. Industry, innovation and infrastructure
	We are open, connected and make a positive contribution internationally	17. Partnerships
We have an innovative cyber security, goods and services industry that can help meet global demand	We have thriving and innovative businesses, with quality jobs and fair work for everyone	8. Decent work and economic growth 9. Industry, innovation and infrastructure
	We have a globally competitive, entrepreneurial, inclusive and sustainable economy	8. Decent work and economic growth 9. Industry, innovation and infrastructure
	We are open, connected and make a positive contribution internationally	17. Partnerships

The Strategy also aligns to Scotland's Digital Strategy *Realising Scotland's Full Potential in a Digital World* which was published in March 2017. This had a number of ambitions, including our vision of Scotland as a country with a global reputation for being a secure place to work, learn and do business.

The actions delivered under the Strategy align closely and contribute to the objectives of the UK's National Cyber Security Strategy (2016-2021), which are to:

- defend our people, organisations and infrastructure
- deter our adversaries
- develop our research, skills and industry

Under the UK's National Cyber Security Funding Programme, funding was identified for delivering these objectives in Scotland amounting to £6.8 million between 2017 and 2021.

This funding, plus an additional £3.48 million from the Scottish Government (a total of £10.28 million), has enabled a number of programmes, projects and interventions to be delivered across the country. We detail these, and their outcomes, throughout this report.

1.2 LEADERSHIP AND PARTNERSHIP WORKING

Scotland's approach to policy development is collaborative. The Strategy and its linked action plans were developed with partners from a number of organisations across sectors. Organisations and individuals were able to have their voices heard through a public consultation. Individual governance structures were put in place to oversee the development and delivery of each action plan.

To provide strategic advice, challenge and support to Scottish Ministers, the National Cyber Resilience Leaders' Board was established in September 2016, chaired until December 2018 by Hugh Aitken CBE. In March 2019, David Ferbrache OBE became chair of a restructured Board, renamed the National Cyber Resilience Advisory Board. Bringing together leaders and influencers from across the private, public and third sectors, the Board has been an influential and important sounding-board for the Cyber Resilience Unit in the Scottish Government which has responsibility for coordinating the implementation of the strategy and action plans.

1.3 THE ACTION PLANS

Following the global "Wannacry" cyber attack in May 2017, Scottish Ministers asked the National Cyber Resilience Leaders' Board to work with the Scottish Government to put in place a suite of action plans which would accelerate the Strategy with the aims of improving cyber resilience across sectors, embedding cyber resilience in our education and lifelong learning system and driving the growth of our CyberSec products and services industry. Five actions plans were developed:

Public Sector Action Plan (2017-2018) aiming to:

- establish a common, effective, risk-based approach to cyber resilience across Scottish public bodies
- ensure that Scotland's Public Sector has technical measures in place to protect against cyber threats

- engage with the Public Sector to promote a consistent implementation of a risk-based supply chain cyber security policy
- ensure that the Public Sector is regarded as an exemplar in cyber resilience

Private Sector Action Plan (2018-2020) aiming to:

- strengthen awareness-raising and systems of advice and support
- strengthen incentives to improve cyber resilience in Scotland's Private Sector

Third Sector Action Plan 2018-2020) aiming to:

- strengthen communications, awareness-raising and systems of advice and support
- strengthen partnership working, leadership and knowledge sharing in Scotland's Third Sector
- strengthen incentives to improve cyber resilience in the Third Sector

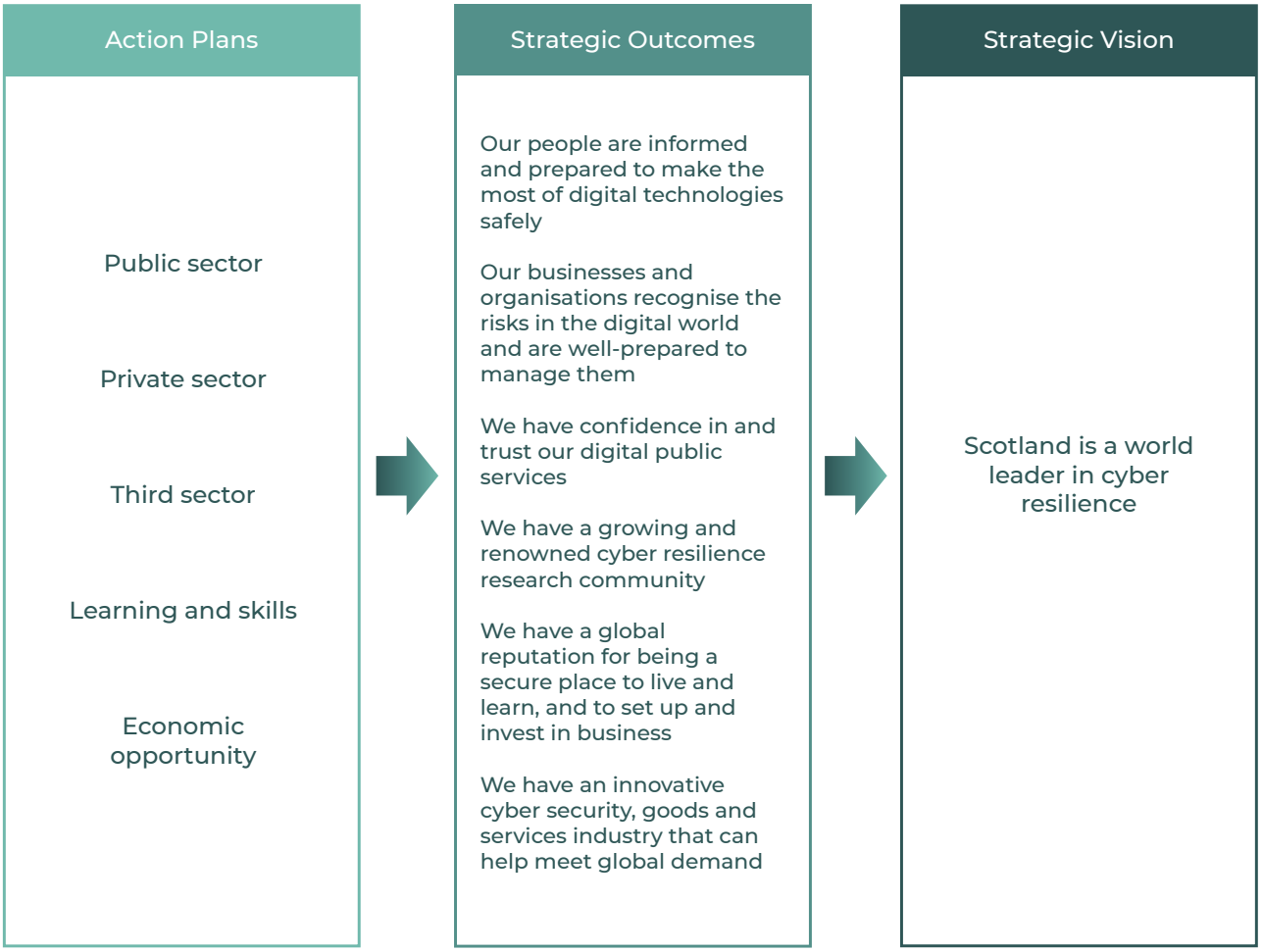
Learning and Skills Action Plan (2018-2020) aiming to:

- increase people's cyber resilience through awareness raising and engagement
- explicitly embed cyber resilience throughout our education and lifelong learning system
- increase people's cyber resilience at work
- develop the cyber security workforce and profession to ensure that skills supply meets demand and that skilled individuals can find rewarding employment in Scotland

Economic Opportunity Action Plan (2018-2021) aiming to:

- develop the right market conditions to encourage continued growth of the cyber cluster
- develop the right academic capability and capacity to grow business innovation
- develop the right cluster management arrangements to ensure coordination and increase impact
- develop the right supporting institutions to stimulate innovation and renewal within the cluster
- develop the right brand to promote Scotland's cyber cluster globally, grow exports, and reflect Scotland's position as the place to be for researching, developing and supplying cyber goods and services

The table below shows how the action plans contributed to the strategic outcomes.



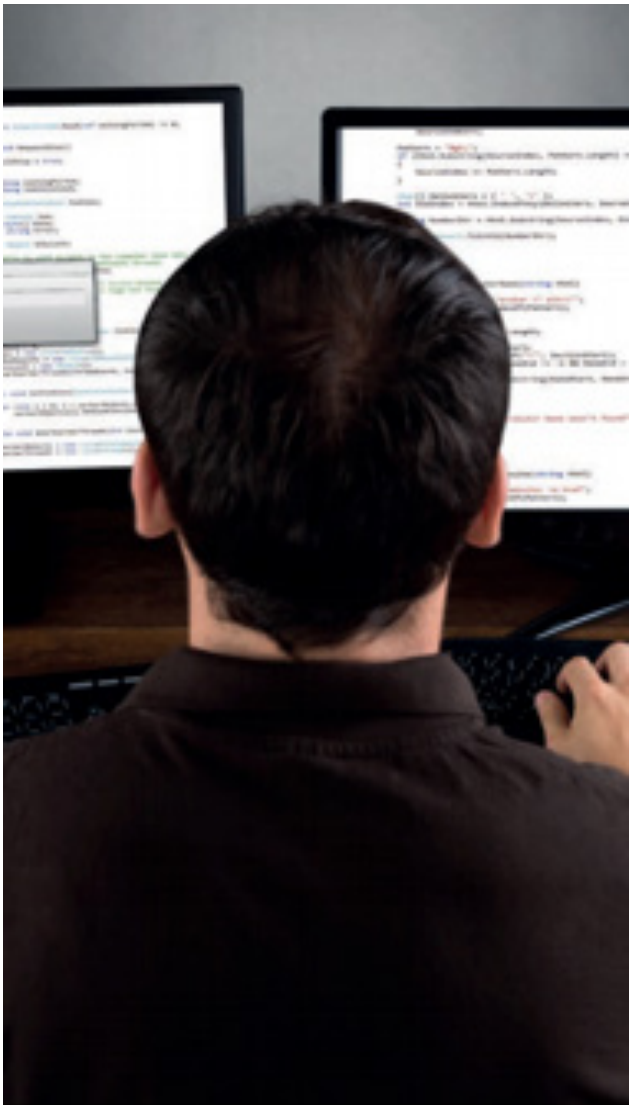
Partnership working

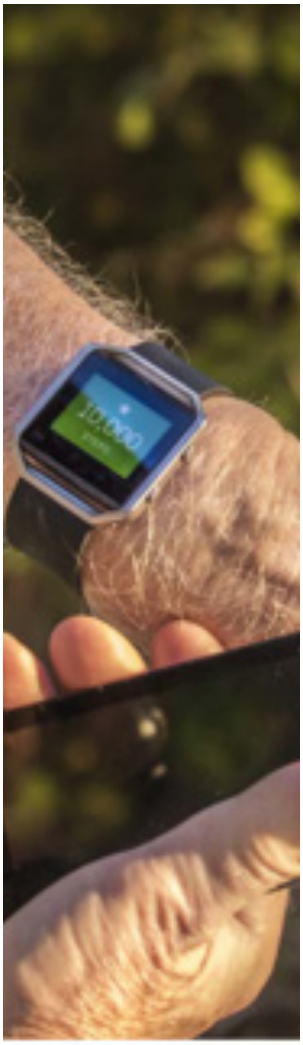
The following partners have been involved in developing, delivering and supporting the implementation of all aspects of the Strategy:

- The Scottish Government
- National Cyber Resilience Advisory Board
- National Cyber Security Centre
- Police Scotland
- UK Government

Our full list of partners involved in delivering the actions within the plans can be found in Annex A.

TIMELINE OF KEY MILESTONES





2

2015

November:
- Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland launched at the National Economic Forum.

2016

April:
- Learning and Skills Coordinator appointed.

July:
- Higher Education Integrator appointed.

September:
- National Board established; first meeting took place.

November:
- CiSP Coordinator appointed.

2017

March:
- Cyber resilience named within Scotland's 3 to 18 curriculum. (Curriculum for Excellence)

November:
- Cyber Resilience: Public Sector Action Plan 2017-2018 published.
- Third Sector Action Plan Cyber Resilience Steering Group established.

2018

March:
- Learning and Skills Action Plan for Cyber Resilience 2018-2020 published.

June:
- Cyber Resilience: Private Sector Action Plan 2018-2020 published.
- Cyber Resilience: Third Sector Action Plan 2018-2020 published.
- Third Sector Cyber Catalyst group established.
- HNC in Cyber Security validated by Scottish Qualifications Authority.

August:
- Workplace Coordinator appointed.

September:
- Economic Opportunity Action Plan published.
- Cyber Resilience Learning and Skills Steering Group established.

November:
- Dynamic purchasing scheme for Digital Services launched, to include cyber security services.

2019

April:
- CYBERUK 2019 Conference took place in Glasgow.
- Cyber Scotland Week took place for the first time.
- Safe, Secure and Empowered guidance and resources for non-formal learning workers published.
- Cyber Centre for Doctoral Training programme announced by EIT Digital.

June:
- Third Sector Cyber Resilience Coordinator appointed.

July:
- HND in Cyber Security validated by SQA.

August:
- Head of Cyber Cluster appointed.

October:
- Cyber Capability Toolkit launched.
- Cyber careers map published.

November:
- Internet of Things innovation challenge programme launched.
- Cluster Management Organisation officially launched.

December:
- Cyber capability database went online

2020

January:
- Public Sector Cyber Resilience Framework and self-assessment tool published.
- Supply Chain Cyber Security Policy published.
- Scottish Cyber Assessment Service launched.
- Number of learners completing the National Progression Awards in Cyber Security reached 1600.

February:
- 2nd Cyber Scotland Week
- Senior Leaders Public Sector Forum took place.
- Pilot of Cyber Advice Helpline launched.
- Scotland's cyber proposition for inward investors created.

March:
- Senior Leaders Public Sector Forum took place.

March onwards:
- COVID-19: community engagement and awareness raising to highlight the cyber threat related to COVID-19. Launch and distribution of weekly Bulletin, providing advice in relation to immediate cyber threats relating to COVID-19.

May:
- PDAs in Cyber Resilience validated by SQA.

August:
- Exercise in a Box delivery programme started.

September:
- Neurodiversity cyber security training fund launched.

November:
- End of strategy progress report published.

RISING TO THE CHALLENGES OF COVID-19

When the COVID-19 pandemic hit early in 2020, our everyday lives – including how we work, communicate and socialise – changed almost overnight. Suddenly all of Scottish business and society were relying like never before on digital and online technologies. The Scottish Government and its partners had to respond fast, in the certain knowledge that cyber criminals the world over would take advantage of the ensuing disruption. Indeed, very early on we were seeing examples of COVID-19-themed scams relating to PPE supplies, along with numerous other scams exploiting people's anxiety about money and health. We also saw examples of attempted cyber theft of research into COVID-19.

During this period, our relationships with the NCSC and Police Scotland have never proven more fruitful, especially in relation to our ability to share intelligence and respond quickly to incidents.

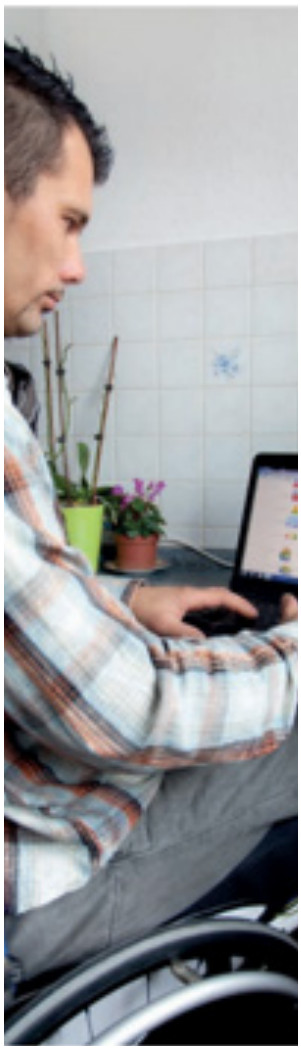
We quickly identified the need to provide, on an almost daily basis, clear, up-to-date and authoritative information, advice and guidance on cyber scams, threats and attacks that continue to emerge and evolve as the course of the pandemic develops.

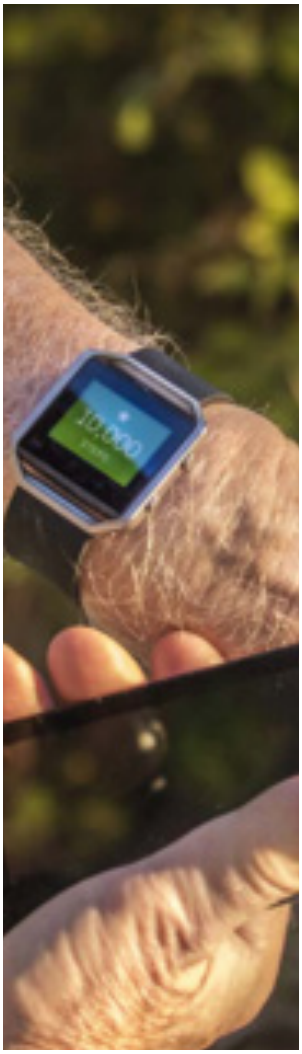
A small dedicated team of the Scottish Government, Police Scotland, SCVO and the SBRC met almost daily to identify and collate emerging threats and scams and provide appropriate advice and guidance organisations need to respond to these. The guidance took the form of a weekly Bulletin reaching stakeholders across the private, public and third sectors.

The Bulletin has attracted very positive feedback and has been welcomed as an important resource during a very challenging time.

As we recover from COVID-19, we will continue to work in an agile way with our partners, including the NCSC and Police Scotland, to assess and respond to the ever-changing threat landscape.

MEASURING PROGRESS





3

3. MEASURING PROGRESS

Extensive analytical work has been carried out to measure the Strategy's impact, focusing on the strategic outcomes and the subsequent five connected action plans. See Annex B for a description of our approach to measuring impact.

3.1 KEY ACHIEVEMENTS OF THE ACTION PLANS

The following are key national achievements, however we acknowledge the many more areas of development and progress led by our partners and stakeholders across Scotland.

The Public Sector

> ***"The cyber resilience of our public sector is vital to ensure people have trust and confidence in our online services and the progress so far is helping Scotland fast become a global exemplar to other nations."***
>
> John Swinney MSP,
> Deputy First Minister and Cabinet Secretary for Education and Skills

Since 2017, the Scottish Government, in partnership with the UK Government's National Cyber Security Funding Programme, provided £1.285 million[2] to increase the cyber resilience of Scotland's public sector.

We have worked with our partners to deliver the Public Sector Action Plan to establish a common, effective, risk-based approach to cyber resilience across Scottish public bodies; ensuring that technical measures are in place to protect against cyber threats; promoting a consistent implementation of a risk-based supply chain cyber security policy and working towards the Scottish public sector being regarded as an exemplar in cyber resilience.

Key achievements

✔ Significant developments in cyber security measures of public bodies. As of May 2020:

- 76% of public sector bodies have placed cyber security on their risk register
- 96% of public sector bodies have designated a board member with responsibility for cyber security
- 60% of public sector bodies have put in place incident management policies.

✔ Increased uptake of NCSC's Active Cyber Defence measures as a result of active promotion in Scotland. As of May 2020:

- 73% of eligible public sector bodies are using the Protective DNS Service (or an alternative solution)[3]
- 68% of eligible public sector bodies are using Mail Check (or an alternative solution)
- 83% of eligible public sector bodies are using Webcheck (or an alternative solution)

2 financial figures given in relation to spending on the actions plans are to March 2020

3 Universities and colleges can access the MailCheck service, but are not eligible for the Protective DNS or Webcheck Services. Therefore, they have been removed from the sample.

✔ Significant take-up of Cyber Essentials as a result of Scottish Government's programme of grant funding. As of May 2020:

- 88% of public sector bodies have achieved Cyber Essentials or Cyber Essentials Plus
- 86% of public bodies agreed that the process of achieving (or working towards achieving) Cyber Essentials or alternative has helped to improve the overall cyber security of their organisation.

✔ Increased ability of public sector bodies to improve the effectiveness of their cyber resilience arrangements through the development and roll out of the Cyber Resilience Framework and the self-assessment tool (see diagram below) to help public sector organisations. This has been downloaded 766 times since its launch in January 2020. In addition, the framework has gathered significant interest and praise from governments across the globe, as well as other parts of the UK, in the months since its launch, demonstrating the strong innovation and leadership of Scotland's public sector in cyber resilience.

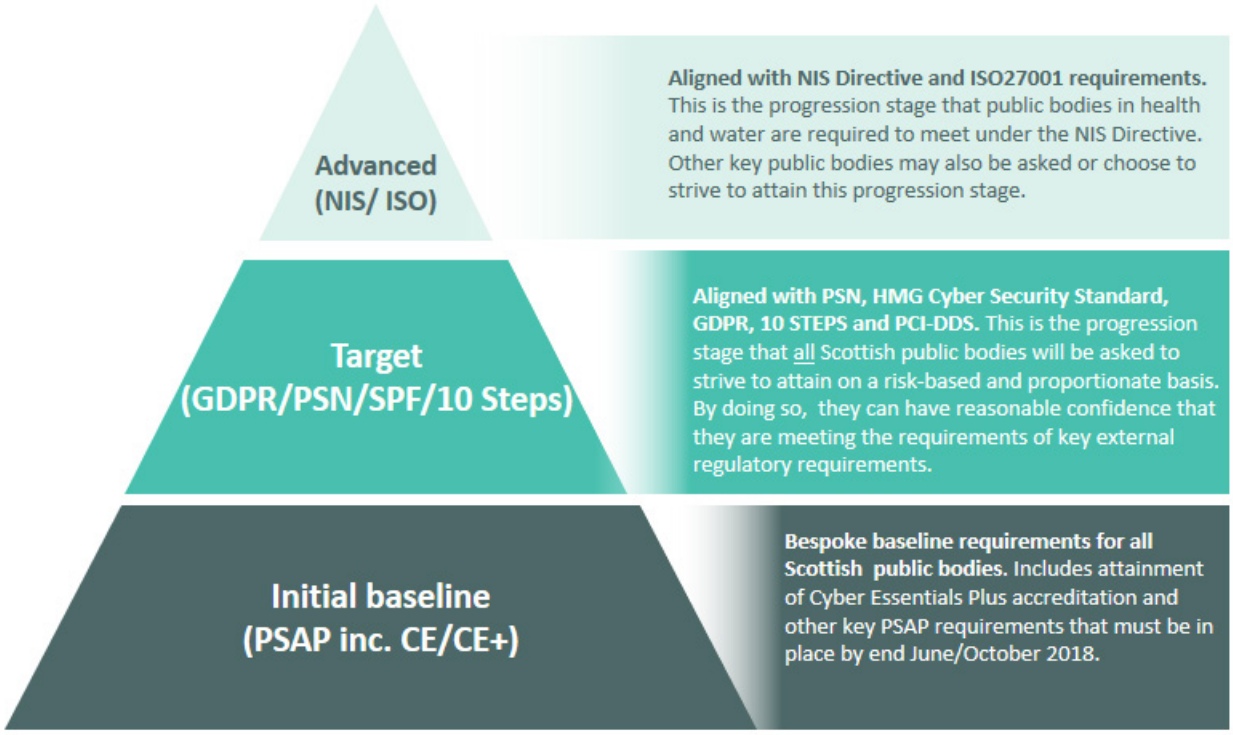


Diagram shows the three progression levels of cyber security as set out in the Scottish Public Sector Cyber Resilience Framework 2019-20

✔ The development of a programme with the Scottish Health Competent Authority to bring health boards, which are subject to the NIS Regulations, into alignment with the Cyber Resilience Framework. This will ensure a common cyber resilience framework across Health and Social Care sectors and remove historical barriers to sharing patient data in a secure and efficient way.

- ✔ The development and roll out of the Public Sector Implementation Toolkit to help public sector organisations implement the Scottish Public Sector Action Plan. This page has been visited 1,935 times since June 2018.
- ✔ The publication of a staff training guide that can be used to upskill workers in cyber resilience. This has been downloaded over 500 times since October 2019.
- ✔ The publication of the cyber capability toolkit to help organisations develop incident management plans for responding to the threat of cyber attacks.
- ✔ The publication of the Scottish Public Sector Supplier Cyber Security Guidance Note and a Scottish Procurement Policy Note in January 2020 to support Scottish public sector organisations to put in place consistent, proportionate, risk-based policies that effectively reduce the risk of Scottish public services being damaged or disrupted by cyber threats as a result of supplier cyber security issues. The Scottish Public Sector Supplier Cyber Security Guidance Note webpage has been viewed 1,045 times and the document has been downloaded 287 times since publication.
- ✔ The launch of the Scottish Cyber Assessment Service (SCAS) Beta Tool in January 2020 to support cyber assurance of potential suppliers during procurement. 221 users across 46 public sector organisations and 87 private sector organisations have registered on SCAS since the system launched, with the expectation of more registering as they become aware of its benefit.
- ✔ The development of the Dynamic Purchasing Scheme (DPS) for the provision of Digital Services, including Cyber Security Specialists, Cyber Security Services, Cyber Security Training, Security Testing and Digital Forensics. There are currently 92 cyber security services suppliers registered in the DPS and 23 cyber security-related contracts have been awarded through the DPS scheme, allowing the public sector expedited access to cyber security services and/or specialists.
- ✔ The establishment of the Public Sector Cyber Catalyst scheme, with 28 public sector bodies registered as Cyber Catalysts, to share knowledge and learning around public sector cyber resilience and identify common solutions to common problems.
- ✔ Increased membership and active usage of the Cyber Security Information Sharing Partnership (CiSP) across the public sector. As of 2020, 83% of public sector bodies in Scotland are CiSP members.

CASE STUDY

Cyber Essentials Plus in the Public Sector

Independent Living Fund (ILF) Scotland achieved Cyber Essentials Plus in October 2018. As a small organisation hosted within the Scottish Government's "SCOTS" network and only formed in 2015, this was a significant achievement, driven by the organisation's priority to ensure it provided safe and secure web services. For ILF Scotland, achieving the accreditation has raised the organisation's competence in understanding and protecting against common threats and vulnerabilities, as well as enabling it to articulate cyber risks to its board. All staff have been made aware of their role in supporting the organisation's cyber resilience, and are now more aware of the need to consider permissions and security of data, as well as access to data systems and their own personal cyber safety.

In August 2018, **West Lothian Council** achieved Cyber Essentials Plus across its entire network (which includes both its corporate and education services), covering over 17,000 end user devices. For the Council, achieving Cyber Essentials Plus helped reinforce the message that everybody has a part to play in cyber security, and why resilience is so important to the organisation.

Social Security Scotland, formed in September 2018, introduced a strong security culture at the outset in recognition that increased security awareness will lead to improved security behaviours and reduce exposure to threats and a greater understanding of security risks. A key component of their Security Strategy has seen them investing in and developing a bespoke security learning programme that not only reaches new starts but also ensures that security is embedded throughout the organisation. Social Security Scotland hosted an event to share their approach with other public sector organisations in recognition of the benefits of a collaborative approach and supported other organisations through the sharing of materials and expertise.

Following the framework publication in January 2020, **Accountant in Bankruptcy (AiB)** assessed the maturity of their cyber security using the framework and self-assessment tool. By using these, AiB were able to quickly form a two-year plan from the areas for improvement identified in the assessment and put in place a work programme to achieve broad alignment with the Target progression stage by the end of the 2021/22 financial year. They have also instigated an exercise and support programme to regularly test their most significant risks and to educate staff on the importance of cyber security and resilience.

The Private Sector

> ***"We have an ambitious Cyber Resilience Strategy, which at its core is about making Scotland a safe place to live, learn and do business. Developing robust technology, in Scotland, rooted in principles of quality and trust, goes hand in hand with that."***
>
> Kate Forbes MSP
> Cabinet Secretary for Finance

Since 2018, the Scottish Government, in partnership with the UK Government's National Cyber Security Programme provided £762,000 to increase the cyber resilience of the private sector.

We have worked with our partners to deliver the aims of the Private Sector Action Plan which are fundamentally to strengthen awareness of the cyber threat to businesses and improve cyber resilience across Scotland's private sector.

Key achievements

✔ 26 business and cyber advice events took place during Cyber Scotland Week 2020, promoting and sharing cyber resilience advice to businesses.

✔ The SBRC has engaged with SMEs across Scotland and since 2017 they have:

- delivered over 150 cyber presentations on various aspects of cyber resilience to business audiences across Scotland
- managed the Trusted Partner Network, endorsed by Police Scotland which includes 28 independent IT companies based or operating in Scotland accredited nationally as Cyber Essentials Certifying Bodies. They share their knowledge and experience by taking companies through the Cyber Essentials journey
- supported the Approved Practitioners Scheme, in collaboration with Police Scotland, which includes 18 independent IT companies based or operating in Scotland accredited nationally as Accredited Cyber Essentials (ACE) Practitioners, and able to provide advice, guidance and consultancy to organisations.

✔ The launch of the Cyber Essentials Voucher scheme fund (worth £544,000) in 2018 which has helped to secure Cyber Essentials Accreditation for nearly 300 SMEs.

✔ The establishment of the Scottish Information Sharing Network (SCiNET) – the Scottish regional membership group within the CiSP as a community for Scottish businesses to engage plus the recruitment of a Scottish CiSP Coordinator. As of summer 2020, there are 458 members, an increase of 275% since 2017. Since 2017, the CiSP Coordinator has delivered 110 events, together with bespoke engagement with individual organisations and membership bodies, in order to increase awareness of CiSP, Cyber Essentials and NCSC resources available to Scottish businesses.

- ✔ The creation and dissemination of a number of cyber resilience toolkits for businesses to improve their online security, protect against cyber threats and manage their cyber incident response, available on the Cyber Resilience Guidance and the Cyber Resilience Incident Management web pages, which have been visited over 2,300 times since October 2019.
- ✔ The circulation of the Napier Meridian newsletter to share cyber security knowledge and information, with a current reach of 6,800 individuals, up from 4,140 in 2014.
- ✔ The circulation of the weekly Cyber Bulletin to key stakeholders, which has raised awareness of the cyber threats related to COVID-19.
- ✔ The development of draft guidance for SMEs and smaller third sector organisations on the supply chain cyber security requirements of organisations in Scotland.

CASE STUDY

Cyber Essentials Voucher Scheme

To support SMEs and the third sector defend against the most common cyber attacks, the Scottish Government made available £544,000 to organisations to achieve Cyber Essentials certification. Managed through Scottish Enterprise, vouchers of up to £1000 were made available. In addition the scheme was designed to build awareness, providing a first step for many towards improving cyber security through a recognised cyber security standard.

The scheme ran between October 2019 and April 2020 with a target set to achieve at least 360 new certifications. Whilst there was significant interest in the voucher scheme, the take up of vouchers among SMEs was more problematic than it was in the third sector.

The COVID-19 pandemic affected the latter part of the scheme, when a number of businesses were still working towards achieving Certification. As of July 2020, 282 SMEs and 120 third sector organisations had successfully achieved Cyber Essentials certification, with a further 85 SMEs and 126 third sector organisations in the process of completing and are expected to achieve Cyber Essentials.

The Third Sector

> ***"The third sector position is largely positive … we have witnessed considerable community engagement from charities through the catalyst programme and a strong uptake of our cyber essentials voucher scheme."***
>
> David Ferbrache OBE
> Chair, National Cyber Resilience Advisory Board

Since 2018, the Scottish Government, in partnership with the UK Government's National Cyber Security Programme, has provided £434,000 in funding to increase cyber resilience across the Third Sector.

We have worked with our partners to deliver the aims of the Third Sector Action Plan, to strengthen partnership working, leadership, communications, awareness raising and knowledge sharing across Scotland's Third Sector.

Key Achievements

- ✔ The establishment of a Third Sector Cyber Catalyst Group as a trusted authoritative source to provide communication channels out to the sector. 17 third sector CEOs have committed their organisations to become Cyber Catalyst members. A Third Sector Cyber Catalyst Group report was published in March 2020, which sets out the group's role, achievements to date and plans to support cyber resilience.
- ✔ Since 2018, approximately £250,000 has been made available to support 250 third sector organisations achieve Cyber Essentials, with the Scottish Council for Voluntary Organisations (SCVO) managing the voucher scheme, on behalf of Scottish Government.
- ✔ The delivery of Cyber Essentials education events to over 100 charities across Scotland by SCVO.
- ✔ Engagement with over 5,000 people working in the third sector took place during Cyber Scotland Week 2020, including those attending SCVO's The Gathering event.
- ✔ The delivery of cyber fundamentals education sessions to over 1,000 charities across Scotland through key trusted partners including our Third Sector Cyber Catalysts (SCVO), Scottish Government, NCSC and Police Scotland.
- ✔ The appointment of Scotland's first national third sector cyber resilience coordinator, based within SCVO, to directly support catalyst projects and the wider third sector around communications and awareness raising.
- ✔ The dissemination of cyber advice to over 10,000 charities through the Scottish Charity Regulator via its OSCR monthly e-bulletin.
- ✔ Good press coverage of cyber resilience across the third sector including Third Force News, which has a mailing out audience of 30,000 third sector professionals and SCVO's website which has 80,000 page views per month.
- ✔ The delivery of a pilot cyber exchange programme to support peer learning across key issues managed by the Association of Chief Officers of Scottish Voluntary Organisations (ACOSVO).

✔ The creation of a cyber best practice guide for CEOs, Chairs and Trustees, published on ACOSVO's website, potentially reaching their full member audience of over 500 voluntary sector leaders and senior staff.

✔ The issue of a Ministerial-endorsed cyber support resource pack by the Scottish Sports Association to all Scottish Governing Bodies of Sport.

CASE STUDY

Cyber Leadership Exchange Programme

A cross-sectoral leadership exchange programme is being piloted by ACOSVO, the membership organisation for voluntary sector leaders and senior staff in Scotland. The programme, which is funded by the Scottish Government, is modelled on ACOSVO's long-running successful leadership exchange programme, but with a specific cyber resilience theme.

The pilot was launched in January 2020, and aims to pair individuals in cyber-related roles from organisations in all sectors. The programme's participants take part in exchange activities to learn about their respective organisations' systems, issues and solutions, and generally to share and develop best practice.

Examples of exchanges taking place include: a head of IT from a public body working with a head of IT from a third sector organisation; a digital innovation lead from a third sector representative body working with an IT manager from another third sector body; and a cyber security manager in a public body working with a cyber resilience officer in a third sector organisation.

An important focus so far has been on how different organisations have resolved digital issues arising from the pandemic and the need to continue to function and deliver services online, remotely and securely.

For further information click here.

CASE STUDY

Scottish Sports Association: supporting Scotland's sports organisations to be cyber resilient

The Scottish Sports Association (the SSA) is the independent membership body for Scottish governing bodies of sport (SBGs). SGBs represent around 13,000 sports clubs across the country between them.

The SSA supports Scotland's cyber resilience strategy as a catalyst organisation, promoting cyber resilience in the third sector. As an organisation driven by partnership working, the SSA has greatly valued the support of key partners including the Scottish Government's Cyber Resilience Unit, Scottish Government's Active Scotland Division, sportscotland and SCVO.

In February 2019, the SSA joined the Scottish Government and SCVO in disseminating a survey across the third sector, to gauge organisations' knowledge of cyber resilience practices and how to counteract cyber risk. The responses to these questions showed that while over half of the SSA's members said that cyber resilience was a priority for them, many were not sure how to improve, while others did not feel the clubs they represented had sufficient awareness. Members also felt that while there were strengths in some areas (for example, in using encryption and undertaking penetration testing), others could put in place better cyber resilience practices (for example, around advising staff on how to respond to the most common types of cyber attacks). The findings also suggested that training was an issue: including where to find it, what to focus on, and how to roll it out, including to Scotland's 200,000+ sports volunteers.

On the back of the survey, the SSA created a Focus Group of individuals from among its membership to consider the findings and to plan actions that would make a difference to sports organisations in Scotland.

One action resulting from the work of this Focus Group has been the regular sharing of "top tips" in the SSA's fortnightly Member Update; a second action has been the development of a Cyber Resilience Resource Pack, endorsed by Kate Forbes MSP (Cabinet Secretary for Finance) and Joe FitzPatrick MSP (Minister for Public Health, Sport and Wellbeing). The pack is a one-stop-shop, with helpful links to guidance and training materials.

Kim Atkinson, the SSA's CEO says: "We launched the Cyber Resilience Resource Pack just after the NCSC had published new data suggesting that at least 70% of sports associations had suffered a cyber breach, so the timing couldn't have been more appropriate."

Next steps for the SSA and its members include: rolling out the Resource Pack and offering tailored support for members, especially during changed ways of work throughout COVID-19; and then seeking ways to support members to cascade the guidance to Scotland's sports clubs.

SCOTTISH SPORTS ASSOCIATION

Learning and Skills

"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…"

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

Since 2018, the Scottish Government, in partnership with the UK Government's National Cyber Security Programme, allocated £1.3 million of funding to support the Learning and Skills Action Plan.

We have worked with our partners to deliver the aims in the Learning and Skills Action Plan to increase people's cyber resilience at home and at work through a programme of awareness raising and engagement. We have embedded cyber resilience throughout our education and lifelong learning system and have developed our cyber security skills pipeline.

Key achievements

✔ The creation of a communications toolkit that partners can use to tailor cyber awareness messaging for their audiences. The Scottish Government's cyber resilience blog has received over 15,000 views since January 2016, and our Tweets have reached over 2,000,000 impressions.

✔ The publication of a weekly Cyber Bulletin to highlight current cyber threats and prevention measures relating to COVID-19.

✔ Through Young Scot's DigiAye and DigiKnow programmes young people have accessed awareness messages on online safety. Cyber security careers have also been promoted to young people from disadvantaged backgrounds, or who face barriers to participation, with information on the different routes to cyber security jobs:

- The Young Scot DigiAye webpage (online since November 2017), and DigiKnow webpage (online since December 2018) and associated social media content have received more than 82,000 impressions on platforms that young people use, and more than 200,000 impressions via Twitter
- Since February 2019, Young Scot's DigiKnow programme has directly reached 201 young people and 95 adults (support workers, teachers, youth workers, parents) and enabled 156 young people to achieve an SCQF level 3 certificate in Internet Safety

✔ Sustained the continuation of the Cyber Christmas Lectures, which have reached over 9,500 young people since 2015, promoting cyber security careers and basic cyber awareness.

✔ Police Scotland has provided training and support on cyber resilience for a range of young people and adults across our education and lifelong learning system, while also advising on a number of learning and skills projects across Scotland. Since 2015 they have provided training to:

- 679 web constables and other police colleagues
- 200 school teachers

- 400 youth workers
- 50 adult learning workers

✔ The delivery of training for educators in all parts of our education and lifelong learning system on how to build cyber resilience into their learning and teaching. Since 2016, 2,000 youth workers and 3,000 school teachers have had access to training in cyber resilience learning and teaching.

✔ Cyber resilience is now included in the benchmarks and Experiences and Outcomes of Curriculum for Excellence.

✔ The appointment of a new cyber resilience development post within Education Scotland to roll out national support and resources for teachers in schools.

✔ The launch of the Digital Schools Special Recognition Badge for schools for Cyber Resilience and Internet Safety. To date sixteen schools have achieved the Special Recognition Award in Cyber Resilience and Internet Safety, with several more registered to achieve it.

✔ Guidance for non-formal learning workers on how to lead learning activities in cyber resilience. 2,000 sets of guidance and learning resources have been provided to non-formal learning workers, including youth workers, adult learning workers and other community workers.

✔ Cyber resilience is now named in the revised National Occupational Standards for Youth Work.

✔ Cyber resilience is now identified in the revised Professional Standards for Lecturers in Scotland's Colleges.

✔ Cyber resilience is now prioritised in the learning outcomes of the SQA's new Digital Literacy units.

✔ SDS developed National Occupational Standards for Cyber Resilience that will assist in embedding cyber resilience competences across multiple occupations.

✔ Civic Digits theatre company developed The Big Data Show, an interactive performance to teach young people about cyber resilience, digital citizenship and cyber security careers, performing to over 2,500 young people since autumn 2018.

✔ The delivery of training to workplaces, including face-to-face, resources and webinars, has included:

- the roll out of a staff training guide in cyber resilience, which has been downloaded over 500 times
- eight webinars organised by SBRC, attended by 517 people; with subsequent views on YouTube, standing at 1,300 as of July 2020
- over 8 workplace learning sessions have been delivered, including train the trainer sessions to Citizens Advice Bureau, National Lottery and Scottish Training Federation
- Scottish Union Learning has delivered training for trainers and for union learning reps, collaborating with 19 unions to deliver training to over 2,000 members and non-members across dozens of Scottish workplaces

- ✔ The Scottish Social Services Council has developed bite-sized digital learning resources for carers. SSSC's Staying Secure Online resource has been used 870 times by care staff across Scotland since summer 2019.
- ✔ SDS commissioned research into international skills policy, relating to reskilling and upskilling; and also into the cyber security labour market to help their skills development programme of work.
- ✔ The delivery of a reskilling programme for veterans and unemployed people, with 27 veterans having begun a reskilling programme delivered by SaluteMyJob and the University of Abertay in 2020.
- ✔ A pilot with Edinburgh Napier University to support people with neurodiverse conditions into cyber security training and employment, with a larger work programme starting in the autumn of 2020.
- ✔ The publication of the cyber security career map and guidance on qualifications and certification, which has been viewed almost 4,000 times since October 2019 on SDS' Digital World website.
- ✔ SDS's careers promotion programme called Discover Cyber Skills, aimed at 12-14 year-olds has had over 80,000 young people taking part since 2017.
- ✔ SQA developed learning and teaching materials to support the National Progression Awards (NPA) in Cyber Security and more than 1,600 people have completed NPAs in Cyber Security in schools and colleges since 2015.
- ✔ SQA developed an HNC and HND in Cyber Security, and also Professional Development Awards in Cyber Resilience. Over 300 college students have registered for the HNC so far, and 57 students have completed it, with many using their HNC credit to move on to the HND in Cyber Security.
- ✔ NCSC's CyberFirst learning and development opportunities and the UK Government's Cyber Discovery programme have been brought to Scotland. More than 300 young people have taken part in CyberFirst opportunities since 2015 and more than 3,600 young people from Scotland have taken part in the UK-wide Cyber Discovery programme.
- ✔ SDS has promoted the Modern and Graduate Apprenticeships in Cyber Security: 152 starts on the Modern Apprenticeships in Information Security and 87 people have registered for the Graduate Apprenticeships in Cyber Security.
- ✔ Increased capacity and activity in universities in relation to teaching and research in cyber security. Nearly all universities in Scotland now offer cyber security courses. Edinburgh University is an Academic Centre of Excellence in Cyber Security research.

CASE STUDY

Cyber security careers, qualifications and professional certification

As we support the growth of cyber security skills talent in Scotland, it is important that we engage and inform potential students, trainees and job applicants about the range of careers in cyber security and the training pathways available in Scotland.

To this end, SDS worked with partners to create a career "map", a qualifications framework and information about professional certification that might be required by employers and industry.

Career map

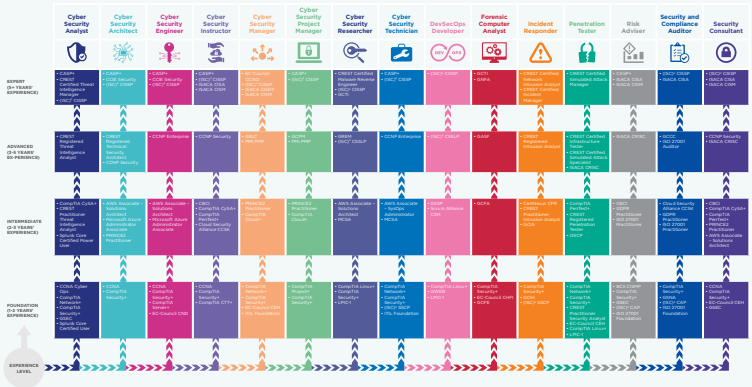
The interactive cyber security career map provides information about fifteen typical cyber security roles, suggesting likely duties, qualifications likely to be required by employers, and a salary range.

Qualifications framework

The cyber security qualifications framework provides information on qualifications in cyber security that can be taken in Scotland at school, at college and at university. Qualifications are available from Scottish Credit and Qualifications Framework (SCQF) level 4 to 11, with PhDs available at SCQF level 12.

Professional certification

The guide to cyber security professional certification provides an overview of a number of certifications available from different accrediting bodies for people with varying levels of professional experience.



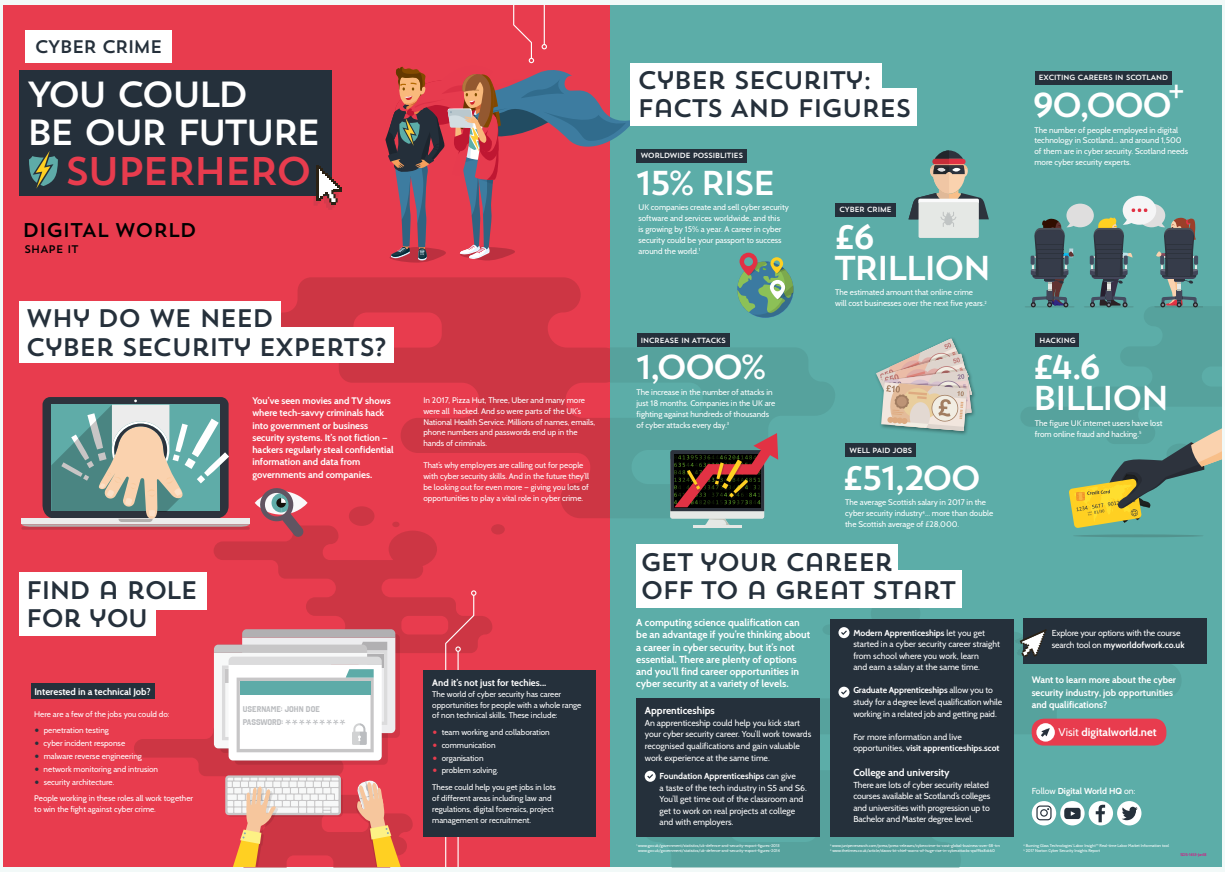
CASE STUDY

Discover Cyber Skills

The Discover Cyber Skills programme was created by SDS to inspire a new generation of "cyber security superheroes". Blending real-world and online events, this government-funded, industry-backed programme enhances the cyber security skills and interest of young people, ensuring there is a pipeline of talent to fill Scottish cyber security jobs.

The four-year funded programme of activity showcases what can be achieved when government, education and industry collaborate. It has delivered high quality, industry-relevant cyber security learning experiences which map directly to the school curriculum and are fully inclusive by being offered online for all Scottish S1-S3 pupils.

By the end of the third year of delivery, the programme has now engaged with 80,000 learners, far exceeding its original target of 3,000 pupils over 4 years.



CASE STUDY

CyberFirst in Scotland

The NCSC's CyberFirst education programme is actively engaged in Scotland, providing a range of opportunities tailored to meet the needs of Scottish students.

These opportunities include:

- CyberFirst Adventurers/Trailblazers (11-13 year-olds)
- CyberFirst Girls' Competition (Aimed at S2 girls)
- CyberFirst Defenders Summer Courses (15 year-olds)
- CyberFirst Futures Summer Courses (16 year-olds)
- CyberFirst Advanced Summer Courses (17 year-olds)
- CyberFirst Bursaries and Degree Apprenticeship scheme

To date, over 300 students aged 11-17 from Scotland have attended a CyberFirst course.

80 CyberFirst bursary students are attending 12 different Scottish universities.

Many of these courses have been SCQF credit-rated by the SQA. Young Scot points are also available.

For more information visit www.ncsc.gov.uk/new-talent

CASE STUDY

Personal Cyber Security at Work

Nicola is a union activist at the RMT Union. She works as a Ticket Examiner for ScotRail, where her duties include inspecting, checking and selling tickets to passengers, providing them with information, and assisting travellers with reduced mobility.

Aware of the importance of cyber security in both her personal and working life, Nicola attended a personal cyber security workshop and a personal cyber 'Train the Trainer' workshop delivered by Digital Skills Education Ltd at the STUC, in October 2018. At the workshop, Nicola found out how to set secure passwords, spot fake websites and keep data safe online. During the 'Train the Trainer' workshop, Nicola learned the tutoring skills to deliver "bite-sized" cyber security modules on how to choose safe passwords and safer web browsing to colleagues.

Shortly after attending both workshops, Nicola delivered a two hour cyber security training session with RMT members in her workplace. The session covered how to create strong passwords and use password managers such as 1Password, Dashlane and iCloud Keychain. Nicola discovered that the learners really enjoyed testing the strength of their current passwords against an online password checker, and completing the interactive 'Diceware' random password generator exercise to create more secure passwords.

Nicola thought that taking part in the 'Train the Trainer' workshop made her feel more confident about sharing her knowledge with others, and gave her the best tips to deliver a session herself. She suggested incorporating role-play into future workshops, but would definitely recommend it to other colleagues. Nicola was impressed with what she learned on both workshops and has been sharing this information with others.

CASE STUDY

The Big Data Show – cyber resilience takes to the Stage

The Big Data Show is a creative learning experience aimed at 11-13 year olds. Created by Civic Digits theatre company, it weaves together digital magic, games and live performance to inspire the next generation to consider their own cyber resilience, and to pursue careers in digital technology, including cyber security.

Civic Digits developed the concept with pupils from Perth Academy. They toured a 60 minute version of the show to fifteen schools, reaching approximately 2,000 pupils in 2018-19, including 7 shows for Cyber Scotland Week in April 2019. Research during this period demonstrated that the project improves the participants' digital literacy. It showed that girls valued their data more and boys were more concerned about the risk of data breaches.

In 2019-20, Civic Digits continued to develop the project as an SQA accredited course. The course comprises of two in-school workshops and a 90-minute live show in a traditional theatre (such as Perth Theatre and the Lyceum in Edinburgh). Civic Digits aimed to reach approximately 6,000 participants in this phase of the project. They proved there is a huge appetite for creative, engaging learning about cyber resilience and digital technology. The project has attracted a significant amount of international attention, with plans to license the project to the Victoria State Government, present the project at the Australian National University and talks are in progress with producers in North America.

The Cyber Resilience Strategy and the Learning and Skills Action Plan have helped to support and guide the project significantly. The Scottish Government has supported the project with funding and by assisting with making connections with youth work, the police, the NCSC and overseas.

The COVID-19 pandemic has inspired Civic Digits to re-shape the project as a live, online experience. The show's producers believe that in this moment of crisis, the message of cyber resilience embedded in cyber creativity is even more relevant than ever.

The Big Data Show by Clare Duffy and Rupert Goodwins is produced by Suzy Glass and Robyn Jancovich-Brown for Civic Digits, with co-producers Perth Theatre at Horsecross Arts and Unlimited Theatre. It is funded by Creative Scotland, Scottish Government, Digital Xtra and the Garfield Weston Foundation.

Civic Digits
Theatre Company

Economic Opportunity

> ***"Scotland is a thriving centre of cyber security research, talent and assets. We are attracting the best academics and innovators that help make Scotland a safe, secure and prosperous country to do business and invest."***
>
> Nicola Sturgeon MSP
> First Minister

The Scottish Government, in partnership with the UK Government's National Cyber Security Programme has provided £1.2 million in funding to support the growth of the cyber security goods and services industry in Scotland.

Since 2018, we have worked with our partners to deliver the aims of the Economic Opportunity Action Plan, which are to: develop the right market conditions to encourage growth of the cyber security goods and services industry; establish a cyber security cluster to ensure coordination and increase impact; develop the right academic capability and capacity to grow business innovation and develop the right brand to support Scotland's cyber cluster globally, grow exports and reflect Scotland's position as "the place to be" for researching, developing and supplying cyber security goods and services.

Key achievements

✔ The establishment of the Cluster Management Organisation (CMO) for CyberSec within ScotlandIS. The CMO has achieved silver European Secretariat for Cluster Analysis (ESCA) accreditation and so far has:

- built industry connections and organised a series of events to promote the benefits of being part of the Cluster with almost 300 professionals in attendance
- established an industry cluster advisory group to support the direction and growth of the cluster
- produced the first publicly available capability database, which captures information on all of the cyber companies operating in Scotland. There are currently 230 cyber security companies identified
- increased engagement with UK Government, especially DCMS which leads on UK-wide cyber security industry growth
- become an active participant in UK's Cyber Cluster Advisory group, in the Cyber Growth Partnership Working Group (which brings together UK Government and all the main UK cyber clusters), and in the UK's 5G security sub-working group helping to open up doors to the opportunities that 5G brings

✔ 350 people from 200 cyber security businesses attended the Scot Secure 2020 private sector event as part of Cyber Scotland Week 2020.

✔ Scottish Development International (SDI) publication of an international proposition to promote Scotland's growing cyber security goods and services sector.

✔ The development of targeted cyber campaigns/online content/webinars aimed at inward investors. SDI continue to develop and deliver an ongoing programme of activity and engagement to promote Scotland's cyber capabilities and attract inward investment, but we are in the early stages.

✔ Through support from the Scottish Funding Council (SFC), cyber security appears in college and university outcome agreements.

✔ Growth in cyber security research and knowledge sharing, both nationally and internationally, through funding to build research capacity via Scottish Informatics and Computer Science Alliance (SICSA) Cyber Nexus activities, including:

- the appointment of an academic cyber network integrator
- the publication of 100 academic papers on cyber security by a sample of eight leading Nexus academics across Scottish universities in 2019 and 2020
- 16 workshops, conferences and meetings between 2017 and 2019, aimed at bringing together academics, researchers, industry professionals, and students
- supported ten international visits/exchanges to promote international research collaboration and knowledge exchange between 2018 and 2020

✔ The steady growth in the number of PhDs in cyber security. EIT Digital have two Doctoral training programmes in cyber security at Edinburgh Napier University and University of Edinburgh and are anticipating around ten industrial PhDs to be created by the end of 2020. The University of Edinburgh is an Academic Centre of Excellence in Cyber Security Research, and Scotland has the only Bachelor's degree and two Master's degrees fully certified by the NCSC. Abertay University's postgraduate course in ethical hacking was awarded full certification from NCSC in August 2020.

✔ The launch of a two-year Secure IoT innovation programme in conjunction with the Centre of Excellence for sensing, imaging and Internet of Things (IoT) technologies (CENSIS). The programme is aimed at:

- supporting the private sector to develop innovative solutions to IoT security
- helping us understand current levels of awareness, challenges and opportunities for IoT security, and target future activity to improve this
- creating IoT testing capability to inform best practice guidance

In year one (2020/21), the programme will deliver:

- an IoT accelerator competition
- a series of IoT industry workshops
- an IoT vulnerability pilot

CASE STUDY

Scotland's CyberSec industry – the development of a Cyber Cluster

Scotland is home to the only silver accredited cluster management organisation (CMO) in the UK with ScotlandIS having gained silver accreditation in early 2020.

Clusters are regional concentrations of traded industries, shown to have higher average wage and employment increases and inhabit a higher number of innovative and high-growth firms and start-ups. ScotlandIS's CMO currently manages three clusters – CyberSec, Data and MaaS (mobility as a service which is a partnership with Technology Scotland).

The CMO's aim is to support and grow the sectors, covered by the respective clusters, through focusing on innovation, collaboration and networking. The CyberSec cluster has been running for a year and has around 230 cyber security companies with many more ecosystem organisations also part of the cluster.

Jane Morrison-Ross, Chief Executive of ScotlandIS, said: "Being the first organisation in Scotland – and one of the first in the UK – to achieve silver accreditation is a major achievement. Evidence points to cluster membership helping to make organisations more resilient to economic difficulties, such as during the COVID-19 crisis, building ecosystems that help organisations to share resources and help each other."

The CMO has created a cyber directory to allow local cyber companies to be easily found, organised a number of cluster events across Scotland and online, set up a cluster advisory group, created a website and posted numerous articles and blogs promoting the cluster.

SCOTLANDIS

3.2 MEASURING PROGRESS AGAINST THE STRATEGIC OUTCOMES

The Strategy's vision incorporated six outcomes. Below we present progress towards the outcomes using a range of national-level indicators.

Outcome 1: Our people are informed and prepared to make the most of digital technologies safely

Summary of progress

People feel more confident about controlling their privacy online and assessing the trustworthiness of websites, compared to 2015; while people's reported use of a number of cyber security measures has increased. However, data suggests that people may feel less confident using the internet compared to 2015, and new data shows that in 2018/19 one-in-five people experienced cyber crime. While almost three quarters of 12 year-olds in 2017/18 said they knew a great deal about protecting themselves online and about protecting their personal information online, just over half of their parents felt as knowledgeable.

There is a growing pipeline of cyber security courses from secondary schools through to universities with increasing numbers of students enrolling in cyber security courses at Scotland's colleges and universities.

The Scottish Household Survey found that, between 2015 and 2019, there was a significant increase in the percentage of people who reported feeling more confident about their ability to control their privacy settings online (76% to 80%) and about being able to tell what websites to trust (81% to 84%). The same survey found that the percentage of people adopting a number of key cyber security measures increased significantly between 2015 and 2019 for the following:

- Avoid opening emails or attachments from unknown people – 66% to 70%
- Change passwords for online accounts regularly – 31% to 35%
- Avoid giving personal information online – 65% to 68%
- Make sure mobile phone has up-to-date anti-virus software – 32% to 48%
- Make sure home wi-fi is protected with a username and password – 58% to 63%
- Back-up important information – 40% to 51%

Notwithstanding these positive developments, the Scottish Household Survey also found that a small but potentially growing proportion of the population may have less confidence using the internet due to privacy concerns (2% in 2015 to 5% in 2017).

Furthermore, the latest findings from the Scottish Crime and Justice Survey 2018/19 show that one-in-five adults who use the internet said they had experienced one or more types of online fraud and computer misuse. The majority of victims of most types of cyber fraud and computer misuse did not report the incident to the police. Credit card fraud was reported to the bank but victims rarely reported the crime to the police, because they dealt with it themselves, or because they felt that it was too trivial and not worth reporting.

For younger people, 2017-18 data from the Growing Up in Scotland (GUS) study shows that most 12-year-olds stated that they knew a great deal about protecting themselves online and about protecting their personal information online (70% and 72% respectively). Of the remainder, most said they knew quite a lot about protecting themselves and their personal information online (27% and 26% respectively). On the other hand, only 30% of parents indicated they knew a great deal about protecting themselves/their children online and about protecting their personal information online, with most parents saying they knew quite a lot about both (52% and 53% respectively).

Finally, at our universities, Higher Education Statistics Agency (HESA) data shows that the number of students graduating from cyber security courses at Scottish higher education institutions has increased steadily, from an estimated 230 in 2014/2015 to around 320 in 2018/19. Furthermore, the number of enrolments to courses that relate to cyber security at Scotland's colleges has increased considerably, from an estimated 11 in 2015/16 to around 714 in 2018/19.

Outcome 2: We have confidence in, and trust, our digital public services

Summary of progress

People are generally satisfied with the quality of online public services, and feel confident using them. However, we currently do not know whether, and how, this satisfaction relates to the quality of the cyber security of such services.

The Scottish Household Survey found that the proportion of people satisfied with the overall quality of online public services remained stable at over 80% between 2015 and 2018. Similarly, the percentage of people who say they feel confident using online public services has remained stable at around 85% between 2015 and 2019.

However, an identified issue with this outcome is that it does not seek to measure the actual quality of the cyber security of public services. It only focuses on the public's perception of public services, which is a separate factor influenced by a number of issues. Furthermore, we do not know where people's lack of trust and confidence in digital public services may come from – is it due to their lack of awareness of the importance of good cyber hygiene, or is it due to a (perceived) lack of security of online public services?

We can see through the Public Sector Action Plan that substantial progress has been made in building the resilience of our public sector bodies, but it has been difficult to demonstrate the correlation between this progress and measuring people's confidence and trust in digital public services.

Outcome 3: Our businesses and organisations recognise the risks in the digital world and are well prepared to manage them

Summary of progress

In 2017, most Scottish businesses said they were equipped with the cyber skills to protect against cyber threats, but only 10% of businesses had obtained a form of cyber security accreditation. As of 2020, 88% of public sector bodies have achieved Cyber Essentials or alternative, but fewer than 1% of charities in Scotland have. To note, the vast majority of third sector organisations surveyed by ACOSVO say they view cyber security as a priority, with 45% saying they want (or already have) Cyber Essentials. SCVO's data suggests more work needs to be done to improve the cyber resilience of smaller and medium-sized third sector organisations.

When it comes to private businesses the most recent information comes from the 2017 Digital Economy Business Survey, which found that more than 75% of businesses surveyed said they were fully or somewhat equipped with the relevant skills to protect against and deal with cyber security threats. This included 87% of businesses saying they used malware protection (i.e. anti-virus software); 73% saying they used boundary firewalls (i.e. preventing unauthorised access); and 51% saying they used patch management (i.e. updating software). to improve cyber security. However, the same survey found that in 2017, only 10% of Scottish businesses had obtained a form of cyber security accreditation. Amongst those who did not have a cyber security accreditation, only 8% were planning to obtain one in the next 12 months.

When it comes to the Scottish public sector, data from the first quarter of 2020 shows that 88% of public sector bodies have achieved Cyber Essentials or alternative/equivalent technical controls.

Finally, there currently are 24,977 registered charities in Scotland according to OSCR records. Research by ACOSVO in 2018 found that, out of 102 third sector organisations surveyed, 88% believe their organisation views cyber security as a priority, 65% say they have sought information, advice or guidance on cyber security in the previous year, and 45% say they want (or already have) Cyber Essentials accreditation.

Over 300 third sector organisations have taken part in SCVO's online digital checkup, which has been running since 2018. The checkup provides an overview of digital capability; with two questions specific to cyber resilience, related to organisational governance and training. SCVO findings from 2019-20 showed the strong correlation between an organisation's size and their overall cyber resilience (i.e. the larger the organisation, the more cyber resilient it is likely to be). This highlights and reinforces the continued need for sector support, particularly for potentially digitally vulnerable small and medium-sized charities.

We have invested a significant amount of funding to support third sector organisations to build their cyber resilience through awareness raising and training, and supported 120 third sector organisations in achieving Cyber Essentials, achieving our target commitment within the Third Sector Action Plan, with a further 126 in the process of obtaining the accreditation. However, this still amounts to less than 1% of all charities in Scotland. It is recognised the sector in Scotland is predominantly made up of small to medium-sized charities, therefore any cyber measures should be considered and implemented on a risk-based and proportionate basis.

Outcome 4: We have a growing and renowned cyber resilience research community

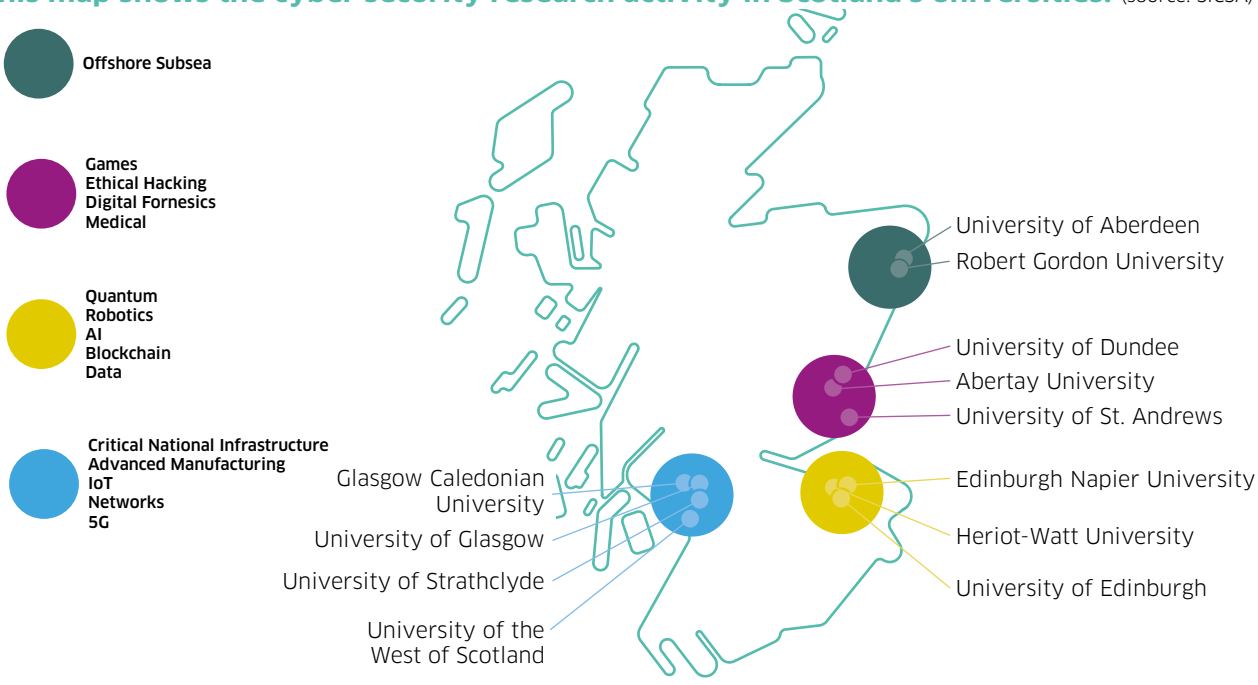
Summary of progress

While specific data about cyber security research in Scottish universities is not available yet, we know that investment in computer science research has grown by 8% since 2015, with full-time staff growing by 10%. Furthermore, the University of Edinburgh is an Academic Centre of Excellence in Cyber Security Research, and Scotland has the only Bachelor's degree and two Master's degrees fully certified by the NCSC.

It has proven challenging to find exact figures around cyber research activity in Scotland. While coding improvements will be made in future years to start measuring cyber security research directly, data is currently only available for computer science as a whole. Most cyber security research sits in this field, and strong computer science, especially strong artificial intelligence and data science capacities, are important for cyber security progress. In 2018/19, the most recent year for which data exists, Scotland ranked second within the UK for for computer science research income. This income has grown by 8% since 2015/16, with computer science academic full-time-equivalent staff, many of whom are our research leaders, growing by 10%. Scotland's research income is growing more slowly than in the rest of the UK, suggesting more can be done to promote investment this field.

There is a range of cyber security under and post-graduate programmes across our universities. The University of Edinburgh is recognised as an Academic Centre of Excellence in Cyber Security Research by the National Cyber Security Centre (NCSC) and by the Engineering and Physical Sciences Research Council (EPSRC). Scotland has the only Bachelor's degree and two Master's degrees fully certified by the NCSC. Furthermore, EIT Digital have launched two Doctoral training programmes (at Edinburgh Napier University and Edinburgh University) in cyber security and are anticipating that ten industrial PhDs might be created by the end of 2020.

This map shows the cyber security research activity in Scotland's universities. (source: SICSA)



Outcomes 5 and 6: We have a global reputation for being a secure place to live and learn, and to set up and invest in business; and we have an innovative cyber security goods and services industry that can help meet global demand

Summary of progress

The number of cyber security companies in Scotland has been increasing steadily since 2015. Edinburgh is fourth in the UK for the absolute number of cyber security jobs postings, and the demand for core cyber security employees in Edinburgh is twice the UK average. Furthermore, the UK ranks first in the world for commitment to cyber security according to the Global Cyber Security Index (GCI). A number of activities have been undertaken to promote Scotland's CyberSec industry internationally, and Scotland's Cluster Management Organisation has achieved Silver accreditation. Finally, the number of foreign students graduating from cyber security university courses in Scotland has increased considerably since 2014/15.

We have decided to present Outcomes 5 and 6 together as they are deeply interconnected, both aimed at boosting and promoting Scotland's CyberSec industry in order to enhance Scotland's reputation internationally.

On a national level, we know that Scotland plays a central role in the UK CyberSec industry. We estimate that the number of cyber security companies in Scotland has increased from 50 to about 230 companies since 2015. However, official data on this is not available at this time as there is currently no Standard Industrial Classification code for cyber security businesses. Recent data from the Cyber security skills in the UK labour market 2020 shows that Edinburgh is fourth in the UK for the absolute number of cyber security jobs postings, and Glasgow is number 10, making Scotland one of the UK regions with the highest mean salary offers for core cyber security job postings (fourth region in the UK). Furthermore, the Edinburgh is third in the UK in terms of Location Quotients, with a Location Quotient of 2.0. This measure shows how concentrated labour market demand is within a geographic area. The average demand is set at 1.0, so a Location Quotient of 2.0 indicates that the demand for core cyber security employees in Edinburgh is twice the UK average.

It has proven more challenging to find specific evidence of the Scottish CyberSec industry's global reputation. While we do not have Scotland-specific data yet, we know that in 2018 the UK ranked as the country with the highest level of commitment to national cyber security, with a Global Cybersecurity Index (GCI) score of 0.931. This was up from 5th place in 2015, and from 12th place in 2017. The UK's absolute score has been increasing steadily since 2015. While lacking hard figures, we also have evidence of a number of targeted activities which have been undertaken with the specific purpose of reaching Scotland's international audience through Scottish Enterprise, ScotlandIS and SDI. These included presenting at the UK-NL Cyber & Fintech Summit in the Hague, and working with SDI to develop an international proposition as a tool to promote Scotland's cyber capabilities and attract inward investment in this space. Furthermore, our Cluster Management Organisation based within ScotlandIS has been awarded "Silver" accreditation by the European Secretariat for Cluster Analysis – a globally recognised standard demonstrating excellence and professionalism in our approach to cluster management.

We also estimate that the number of foreign-domiciled students graduating from cyber security courses in Scotland has increased since 2015, suggesting that Scotland's cyber security higher education is becoming more recognised internationally. Between 2014/15 and 2018/19, the total estimated number of non-EU and EU students qualifying with a degree in cyber security in Scotland quadrupled and more than tripled respectively, increasing from 4% to 13% of all cyber security graduates for non-EU and from 4% to 11% for EU students.

AWARENESS RAISING ACROSS OUR COMMUNITIES – CYBER SCOTLAND WEEK

In April 2019, we launched the first ever **Cyber Scotland Week**. This week evolved from Cyber UK, UK Government's annual cyber security event, held in Scotland for the first time.

Cyber Scotland Week is a week-long festival of events on cyber awareness, innovation and skills and careers. Coordinated by the Scottish Government and ScotlandIS, the week consisted of events raising awareness of good cyber resilience, showcasing the innovative work that is happening across Scotland's cyber industry as well as promoting a career in cyber security.

"The cyber security industry is an important contributor to our economic growth and Cyber Scotland Week is the perfect opportunity to showcase the innovative and exciting work that is happening across the sector."

Deputy First Minister

Cyber Scotland Week aims:

- Protection: improving cyber resilience knowledge, behaviours, awareness and practice (e.g. how to spot fake emails, choose better passwords etc.)
- Innovation: Showcasing innovative work happening across the sector
- Skills and Careers: Promoting skills development and a career in cyber security (e.g inspiring the younger generation to consider this as a career, or reskill existing staff)

Events took place all around the country and by a wide variety of stakeholders including:

CYBER SCOTLAND WEEK 2020

In 2020, 3 national conferences took place for the public, private and third sectors

1. Holyrood Connect – Public Sector Cyber Security Conference
2. The Gathering – Scotland's largest third sector conference
3. Scot Secure 2020 – Scotland's largest private sector conference

CEED Awards – First ever cyber resilience awards for the national engineering & manufacturing community in Scotland

We delivered 8 podcasts in collaboration with Police Scotland, SCVO, Young Scot, Safer Internet Day, Neon Circle and Tech Force sharing top tips to keep safe online. These have been played over 234 times

The UK Government's flagship cyber event, CYBERUK 2019, brought leading international cyber intelligence and security experts together and provided a platform for business leaders to learn how to protect and secure their organisations' information, finances and reputation

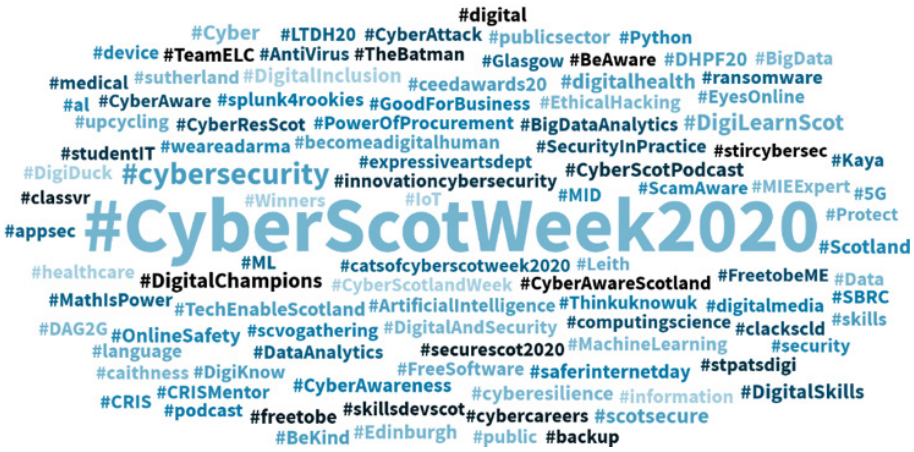
Cyber awareness raising stalls across Scottish workplaces, colleges and universities

Europe's largest annual digital health hackathon. Over 300 health professionals, entrepreneurs, designers and technology specialists spent 75 hours developing new digital health products and services with a stream in cyber security

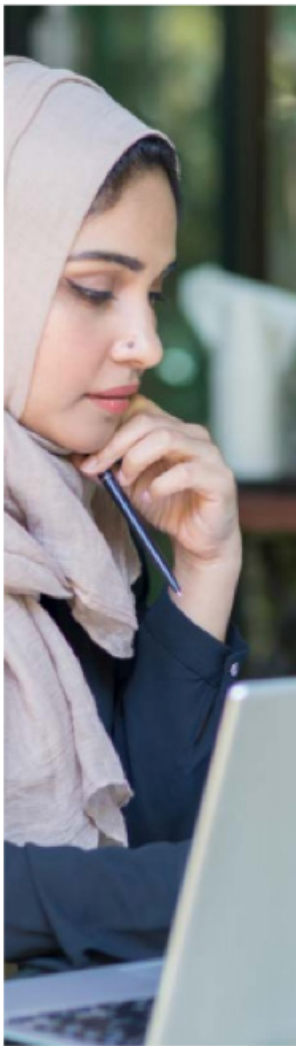
A cyber-themed event for 500 school children at the Glasgow Science Centre offering three floors of interactive exhibits, hands on workshops, including a Cryptography and DIY Gamer workshop, with opportunities to 'meet the expert' and learn about cyber career paths and opportunities

LEAD Scotland hosted cyber resilience workshops for people with disabilities, carers and volunteers with the aim of encouraging those who attend to pass their learning on to others

Large social media campaigns by a wide range of stakeholders across the public, private and third sectors. On **Social Media** #CyberScotWeek20 was used in over **1,900 conversations** by key stakeholders and influencers including Police Scotland, Education Scotland and Local Authorities.



CONCLUSIONS



4

4. CONCLUSIONS

4.1 LESSONS LEARNED AND CONTINUING CHALLENGES

We present some of our reflections in this section, as lessons learned and as priorities for future strategic and action planning.

There is evidence from across different types of organisations in different sectors that progress in cyber resilience is taking place and there is cause for optimism. The Scottish Government and partners have succeeded in delivering many of the aims of the action plans, which have contributed to the outcomes of the Strategy, particularly around learning and skills, and for the public and third sectors. We are in the very early stages of impact for the private sector and we expect a substantial growth in CyberSec products and services beyond 2021.

During COVID-19, organisations have had to deliver services and operate their businesses in a more digitally-dependent way and will most probably continue to do so. With this comes increased cyber risk. Particular areas of concern are around video conferencing, online fraud and security barriers to the use of different digital platforms.

Since the launch of the Strategy, we have identified and learned new and improved ways better some outcomes in ways that made them more measurable, or in ways that were more time-bound.

There needs to be a whole-of-government approach to cyber resilience. We have also identified opportunities to better embed cyber resilience in other Scottish Government policy areas. It is already identified in a number of policies and strategies, but we want to see better integration and alignment of cyber resilience outcomes; for example, rather than having cyber resilience as a stand-alone theme within the refreshed Digital Strategy, we intend for cyber resilience to be a fundamental principle of that strategy.

The primary task moving forward, and within the backdrop of response and recovery of COVID-19, is to consolidate our success and momentum, support organisations, communities and individuals to best utilise digital technologies on the one hand, while developing a culture of cyber resilience on the other. The Scottish Government will continue to work with the NCSC to understand the cyber risks in relation to those areas that most test our resilience.

Challenges in measuring the outcomes of the Strategy

It is difficult to measure the outcomes of any strategy that is not tied to a “control” group. We can never say, for example, that a strategic intervention is solely responsible for an observed change. The nearest we can come to linking interventions to outcomes is to write outcomes that are underpinned by clear indicators, so that the strategy is as measurable as possible, and can be said to have contributed to any observed changes.

We propose that future strategic planning should:

- Be more evidence-based, drawing on up-to-date local and international evidence. Where sources of evidence and/or measurement tools do not appear to exist, a plan should be put in place for introducing these. One example of this could relate to Scotland’s global reputation. Currently, we have access to UK-wide data, but no data that is Scotland-specific.

- Be outcome-focused, with logic models (or "theories of change") produced: creating one for the overall Strategy, and then one for each individual action plan. These logic models should be linked to measurable indicators that identify sources of evidence, data sets and measurement tools where possible. We created these for this Strategy, but retrospectively, in order to "unearth" evidence of impact. In future we will take a more "architectural" approach to impact measurement, whereby we will embed indicators that can evidence impact during the design of our strategy, rather than using an "archaeological", retrospective approach.

Challenges in delivering the action plans

Below, we identify some of the challenges or gaps we encountered in the delivery of the individual action plans. We have identified some emerging priorities that we consider will need attention in future strategic and action planning.

Public Sector

The Scottish public sector has made substantial progress in increasing its cyber resilience over the last few years with the majority of organisations achieving, and in some cases surpassing, the Public Sector Action Plan baseline cyber resilience requirements. There is a developing skills base across the public sector and an enthusiastic network of individuals helping to improve cyber security and resilience across the sector. However, there are a number of areas where further progress and improvements could be made as follows:

- **Cyber security standards:** 20 public sector organisations have yet to achieve Cyber Essentials or equivalent[4]. Some organisations have been unable to achieve accreditation until they replace legacy hardware. This has required significant investment in new hardware and careful consideration during digital transformation programmes, but these programmes will take time to complete.
- **Education and awareness raising:** 96% of Scotland's public sector bodies have a designated senior manager or board member responsible for cyber resilience matters, but many are not fully cognisant with what this responsibility entails. A range of resources have been developed since the Action Plan was published, but organisations still report that their staff are not adequately trained on cyber security issues. More engagement and education are required.
- **Intelligence-sharing:** 86% of public sector bodies are members of CiSP. Of those on CiSP, most do not share information with others. More work needs to be done on understanding the reasons behind low contributions and improving intelligence-sharing.

4 These 20 organisations have not indicated to us that Cyber Essentials should not apply to them. There are currently between 30 and 40 organisations that do not have Cyber Essentials for a good reason (for example, they either do not have a network of their own or they have outsourced management of it).

Private Sector

We know that in 2017, only 10% of Scottish businesses had obtained a form of cyber security accreditation, such as Cyber Essentials or Cyber Essentials Plus. Amongst those who did not have cyber security accreditation, only 8% were planning to obtain accreditation in the next 12 months. We do not believe that this position has improved greatly, and remain concerned for SMEs in particular. To that end there remains a pressing need to focus on supporting businesses get the cyber basics right so that they can be prepared for, prevent and, where necessary, respond and recover from cyber attacks.

- **Awareness and education:** There still appears to be confusion about how businesses access advice, guidance, resources, training and cyber security support services. Businesses struggle to know where to go to access the information they need and many have called for a One Stop Shop to address this gap. We are currently working with our national partners to improve this position.
- **Stronger collaboration with business representative bodies**: Identifying and working with the primary stakeholder groups, including the IT Managed Services Sector, who are trusted and have influence, is also recognised as key to gaining better traction with the private sector and in particularly with SMEs as we move forward. We have funded ScotlandIS to map the managed Services Sector in Scotland as a starting point for this work.
- **Front-line incident response for SMEs:** With funding support from the Scottish Government, the SBRC has responded to a demand to provide a cyber First Responder service providing a free and impartial single point of contact triage. This service will allow any business in Scotland to call for initial vendor agnostic advice and guidance immediately following a cyber incident. In addition, the SBRC will lead a programme of work to facilitate the delivery of NCSC's Exercise in a Box toolkit to organisations across the public, private, and third sectors between September 2020 and April 2021.

Third Sector

The provision of cyber resilience support across our Third Sector appears active, attuned to the needs of the sector, and there is evidence to suggest the key actions around communications and awareness raising have been successful. There is a vibrant network of actors engaged in developing the cyber resilience of the sector as a whole, who are energised and motivated to develop this work in partnership with the Scottish Government and other organisations, and are enthusiastic about the developments in cyber resilience over the past five years and going forward.

- **Sectoral reach:** The Third Sector encompasses an estimated 45,000 organisations (including charities, social enterprises and voluntary groups), therefore the potential reach to our communities is significant, particularly reaching organisations and individuals who may be more vulnerable to cyber crime. Given that the sector is mostly made up of a huge number of small to medium-sized charities, any support or intervention measures need to be implemented on a risk-based and proportionate basis.
- **Cyber Health Check:** An improved picture of the state of cyber resilience across the sector is required and further exploratory discussions with partners are planned for the development of a Cyber Health Check for the Third Sector.

Learning and Skills

There are clearly substantial developments across our cyber security skills pipeline, and a high degree of buy-in and leadership from our national education and skills partners.

- **Continued and further reaching awareness raising and education:** There is a need to increase awareness raising of basic cyber hygiene across the general population, with messages tailored for particular audiences and in alternative and accessible formats. We have begun work to develop an awareness raising programme aimed at carers (both kinship and looked-after children) and are currently working on accessible formats.
- **Robust Scottish research and data:** We have struggled to obtain robust data in relation to cyber security research activity in Scotland. The data available at the moment is only partial and high level. Access to more robust and relevant metrics relating to changes (and the drivers of changes) in individuals' awareness and behaviours to improve targeted interventions is required.
- **Teacher training:** We have only scraped the surface in terms of teacher training in cyber security and cyber resilience. Ideally we want to see cyber resilience embedded into initial teacher training to ensure that all educators (especially in schools but also in colleges) can build cyber resilience into teaching and learning across the curriculum.

Economic Opportunity

The CyberSec products and services industry is in its first phase in Scotland and the Economic Opportunity Action Plan is a key initial document to support the integration of cyber into broader economic development planning of the tech-ecosystem – linking cyber and digital, and cyber and fintech.

- **Growth of the Cluster Management Organisation**
  The CMO is in its infancy. We now understand the ecosystem and have laid the foundations of supporting the growth of a CyberSec products and services community in Scotland. Substantial effort will be required to build momentum going forward.
- **Public sector demand for CyberSec products and services**
  It was anticipated that there would be a significant increase in public sector demand for CyberSec products and services, but Scotland's cyber security companies report that this market still feels "hard to crack". The recently-introduced Dynamic Purchasing Scheme (DPS) procurement tool may generate more demand, and we may need to do more to influence the use of this through awareness raising with public sector customers. Additionally, we may need to work with other parts of the tech sector (fintech, data, AI etc.) to build collaboration across different areas of digital expertise so that they are better positioned to sell "total" digital solutions which may be easier for public sector buyers to understand.
- **Innovation**
  Again in relation to the public sector, we anticipated public sector-led innovation challenges. It has, though, proven virtually impossible to identify a public sector "owner" for such a challenge. We have taken an alternative approach and worked with CENSIS to develop an Internet of Things innovation programme. We expect that in the future Scottish Enterprise and the likes of CENSIS will continue to catalyse innovation.

- **Academic – Industry collaboration**
  The need to harness economic opportunities arising from research is critical, however this area needs to be concentrated on. We understand that the number of university cyber security spin outs in Scotland is low. We do not have many indigenous companies of scale (they tend to either remain small or be acquired). If we draw comparison with Northern Ireland, they seem to do this better than Scotland. We believe that a cyber innovation centre or cyber-specific accelerator working at scale may make a difference here and this should be explored further. The new Cyber Quarter in Tayside might address this to an extent, however we need to get better at addressing the challenge of how to identify and nurture the great ideas and innovation, and how to grow (and retain) cyber companies that can scale up beyond micro/small business level. There also needs to be closer connections with other tech industry developments coming out from the Scottish and UK Governments, so that the cyber security industry benefits from broader links and initiatives.
- **Attracting Investment**
  Looking at DCMS figures, levels of investment in Scotland seem disproportionately low (again – Northern Ireland provides a good comparator where they seem to do better). Scottish Development International is leading on international cyber campaigns to attract inward investment, so this might just need time to start generating impact. In the future we expect to give more focus to equip Scottish entrepreneurs to attract investment.

4.2 GOING FORWARD

This report has set out our progress against the Strategy we published in 2015.

Overall, there has been some good progress made across the outcomes of this first Strategy for Scotland, with clear strengths in how we have developed the cyber resilience of the public and third sectors, and in learning and skills. We have made some progress to better secure our private sector, but substantially more remains to be done, particularly around SMEs. Furthermore, we have only just begun to establish a thriving CyberSec industry and to position Scotland as a safe and secure place in which to live and work, and in which to do business and invest.

The risk of cyber attacks will not go away; indeed, as the COVID-19 pandemic has reminded us, cyber criminals will see opportunities in fast-changing situations and quickly adapt to take advantage of any vulnerabilities they perceive. We need to redouble our efforts to keep abreast of the criminal threat, working alongside law enforcement and our allies to help protect our people, our organisations and our infrastructure.

We are moving towards our strategic vision to make Scotland a world leading country for cyber resilience: one that people will want to live and work in, and one that businesses will want to invest in. Our current focus must be on how we can be as agile and adaptable as possible as we recover from the pandemic. We aim to publish a new Strategic Framework for Cyber Resilience in Scotland. during Cyber Scotland Week 2021.

ANNEX A

Partners involved in delivering or supporting the delivery of the action plans, many of whom are Cyber Catalysts, include:

Public Sector	Private Sector	Third Sector	Learning and Skills	Economic Opportunity
Aberdeenshire Council	BT	Aberlour Child Care Trust	Civic Digits	CENSIS
City of Edinburgh Council	CENSIS	Alzheimer Scotland	College Development Network	Highlands and Islands Enterprise
Cyber Security Scotland & 55 North Network Ltd	CGI Inc	Association of Chief Officers of Scottish Voluntary Organisations (ACOSVO)	Colleges across Scotland	NCSC
Disclosure Scotland	Charles River	Citizens Advice Scotland	Education Scotland	ScotlandIS
Dumfries and Galloway Council	Edinburgh Airport	Enable Scotland (The Piper Group)	Glasgow Science Centre	Scottish Development International
Fife College	Federation of Small Businesses	Fife Voluntary Action	Lead Scotland	Scottish Enterprise
Forth Valley College	Institute of Chartered Accountants of Scotland	Food Train	Mersyber	SICSA
Gartner Consulting	Institute of Directors Scotland	Housing Options Scotland	NCSC	Universities across Scotland
HE/FE Shared Technology & Information Services (HEFESTIS)	Konica Minolta	Learning Link Scotland	Scottish Informatics and Computing Science Alliance (SICSA)	UK Government
Higher Education Information Directors Scotland (HEIDS)	KPMG	NCSC	Scottish Funding Council	
Highlands and Islands Enterprise	KubeNet	Police Scotland	Scottish Qualifications Authority	
Independent Living Fund Scotland	Kyowa Kirin	Royal Blind	Scottish Social Services Council	
	Law Society of Scotland	Scottish Council for Voluntary Organisations (SCVO)	Scottish Union Learning	
	Leonardo	Scottish Federation of Housing Associations (SFHA)	Skills Development Scotland	
	NCSC	Scottish Sports Association	UK Government	
	NorthLink Ferries		Universities across Scotland	
	Pinsent Masons		Young Scot	
	Police Scotland			
	PwC			
	Royal Bank of Scotland			
	Scottish Business Resilience Centre (SBRC)			

Public Sector	Private Sector	Third Sector	Learning and Skills	Economic Opportunity
Local Government Digital Office	SBRC Trusted Partners	The Health and Social Care Alliance Scotland (The ALLIANCE)	YouthLink Scotland	
NCC Group	Scottish Chambers of Commerce	British Red Cross		
NCSC	Scott-Moncrieff	The National Lottery Community Fund		
NHS Lanarkshire	Scottish Power	The Wise Group		
NHS Lothian	SPP Energy Networks	UK Government		
NHS Scotland	Subsea 7			
NQC Ltd	Tesco Bank			
Information Security Forum	UK Government			
Police Scotland	William Grant & Sons			
Revenue Scotland				
Scottish Ambulance Service				
Scottish Canals				
Scottish Enterprise				
Scottish Environmental Protection Agency				
Scottish Fire and Rescue Service				
Scottish Government				
Scottish Local Authority Information Security Group (SLAISG)				

Public Sector	Private Sector	Third Sector	Learning and Skills	Economic Opportunity
Scottish Public Pensions Agency				
Scottish Water				
Skills Development Scotland				
Social Security Scotland				
sportscotland				
Student Awards Agency Scotland				
Transport Scotland				
UK Government				
University of Aberdeen				
University of Edinburgh				
University of St Andrews				
VisitScotland				
West Lothian Council				

ANNEX B

Measuring impact

Metrics from a number of sources show that progress to varying degrees has been made in Scotland.

The analysis of the progress of the Strategy comes with a number of limitations:

- in the absence of a control group, any observed changes in the strategic outcomes cannot be conclusively attributed to the Strategy's and Action Plans' interventions
- the strategic outcomes are not as robust as we would want them to be, as limited measurement indicators were available initially
- some of the outcome measures were identified retrospectively and may only provide a partial picture of the Strategy's progress
- there are some gaps in consistent data collection, especially when it comes to allowing comparisons with 2015

For these reasons, and recognising that this was the first Cyber Resilience Strategy for Scotland, we decided to focus on measuring the success of the strategic outcomes alongside identifying metrics which could evidence the progress of the associated action plans.

We will continue to work with partners to improve our evidence base for the next Strategy. As we set out in Section 4.1: Lessons learned and continuing challenges, we will develop our future strategic direction using more established measurement indicators to support more defined outcomes. This approach will enable us to monitor progress effectively towards the achievement of our vision.

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: 978-1-80004-218-6

Published by The Scottish Government, November 2020

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS731686 (11/20)