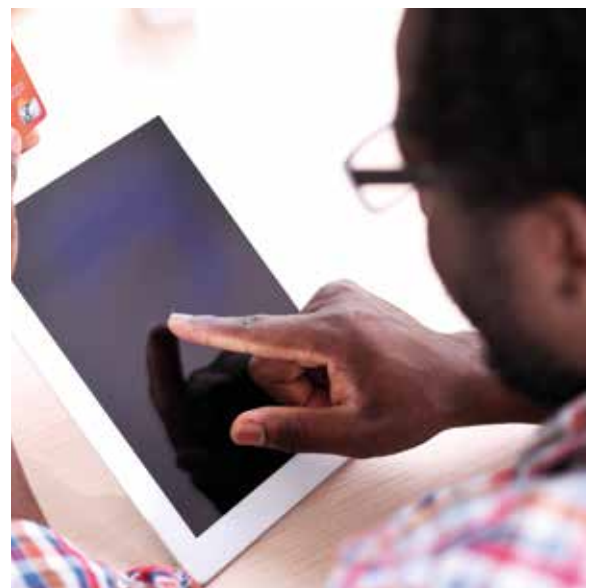




SAFE, SECURE AND PROSPEROUS: A CYBER RESILIENCE STRATEGY FOR SCOTLAND



CONTENTS

01 A MESSAGE FROM THE
DEPUTY FIRST MINISTER

02 SECTION 1 - THE IMPORTANCE
OF CYBER RESILIENCE

- WHAT IS CYBER RESILIENCE?
- WHO IS THE STRATEGY FOR?
- WHY DO WE NEED A CYBER RESILIENCE STRATEGY?

03 SECTION 2 - BECOMING CYBER
RESILIENT

- WHAT IS OUR VISION?
- WHAT ARE THE GUIDING PRINCIPLES OF THE STRATEGY?
- WHO NEEDS TO BE INVOLVED?
- HOW CAN WE BUILD CYBER RESILIENCE?

04 SECTION 3 - IMPLEMENTING
THE STRATEGY AND MEASURING
THE IMPACT

- HOW WILL WE IMPLEMENT THIS STRATEGY?
- HOW WILL WE KNOW IF WE ARE MAKING A DIFFERENCE?

ANNEXES

- A. STRATEGIC PRIORITIES
- B. STRATEGIC WORKING GROUP
- C. GETTING THE BASICS RIGHT



John Swinney MSP
Deputy First Minister

A message from the Deputy First Minister

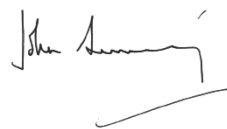
WE ALL WANT TO SEE A SCOTLAND WHERE PEOPLE – AT HOME AND AT WORK – BENEFIT FROM THE HUGE OPPORTUNITIES OFFERED BY DIGITAL TECHNOLOGIES. IN ‘SCOTLAND’S DIGITAL FUTURE: A STRATEGY FOR SCOTLAND’, THE SCOTTISH GOVERNMENT SET OUT HOW WE AIM TO DEVELOP DIGITAL PUBLIC SERVICES, GROW THE DIGITAL ECONOMY, RAISE LEVELS OF DIGITAL PARTICIPATION AND IMPROVE BROADBAND CONNECTIVITY SO THAT SCOTLAND CAN MAKE THE MOST OF THE DIGITAL AGE.

Our increasing reliance on digital technologies can make us more vulnerable to the criminals who seek to exploit them for malicious purposes. For example, digital technologies can help criminals to bully vulnerable people, sexually exploit children, steal intellectual property, or destroy critical infrastructure. I want us all to take steps to minimise these risks, so that Scotland becomes one of the safest countries in the world to live in and one of the most reliable places to do business with.

The 2014 *Programme for Government* signalled our intention to produce a strategy for building Scotland’s cyber resilience for the benefit of our people and our economy. We have listened to what you said in this summer’s public consultation and have worked with a range of experts to develop *Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland*. This strategy sets out the actions we need to take to make Scotland a cyber resilient place to live, work and do business.

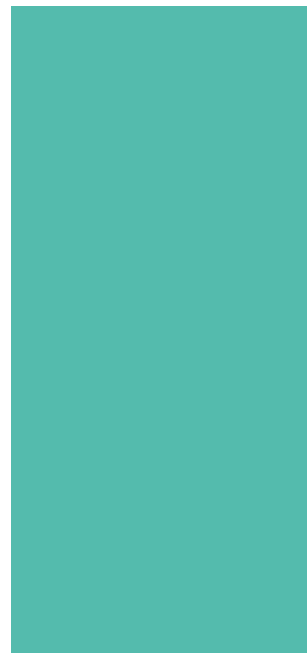
This government intends to lead from the front; building our own cyber resilience and working with other public sector organisations to make sure resilience is built in to digital public services. We will also be working with those who provide key services in the private and third sectors to encourage them to make sure they are cyber resilient.

We all have a stake in making Scotland one of the safest places in the world to live and do business, thus ensuring our economy and our people reap the rewards of expanding digital opportunities. I ask all leaders and educators across the public, private and third sectors to regard cyber resilience as vital to their success in our online world.



John Swinney MSP
Deputy First Minister

Cyber resilience is being able to prepare for, withstand, rapidly recover and learn from deliberate attacks or accidental events in the online world.



1

SECTION 1 – THE IMPORTANCE OF CYBER RESILIENCE

This section covers:

What is cyber resilience?

Who is the strategy for?

Why do we need a cyber resilience strategy?

What is cyber resilience?

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

Who is the strategy for?

Scotland's cyber resilience cannot be achieved by government alone. This strategy is for the Scottish nation – for leaders, educators and policy makers across the private, public and third sectors. It provides direction on how to recognise, manage and respond to the increasing threats we all face online. By doing this, we can safely reap the rich benefits offered by the digital age.

Why do we need a cyber resilience strategy?

Historically we have taken steps to secure our land, sea and airspace. In this modern world, the protection of digital networks such as the internet is becoming just as important. Many countries have put in place cyber security strategies, including [UK Cyber Security Strategy](#). Our strategy aims to build on this solid foundation and move Scotland to a stage where we all routinely recognise and manage cyber risks in the same way as we deal with other day-to-day risks to our health and prosperity.

Therefore, we need a cyber resilience strategy to support the development of a culture of cyber resilience and, at the same time, create the necessary environment to ensure Scotland becomes a leader in meeting the growing demand for cyber skills talent.

- **The estimate of Scotland's total sales conducted over computer networks in 2012 was £38bn**
- **A third of businesses expect internet sales to make up at least 20% or more of their total sales over the next 2-3 years**
- **92% of businesses in Scotland have broadband**

SECTION 1 – THE IMPORTANCE OF CYBER RESILIENCE

The digital age is transforming Scotland

The growth of the internet and other digital networks has brought speed, agility, efficiency and access to technologies that have transformed the way we do business, socialise and provide key services.

As individuals we can more easily keep in touch with friends and family and obtain information, products and services from around the world – all thanks to increased access to the internet, facilitated by mobile technology and faster and more widespread broadband.

Enterprises – both the private and third sectors – increasingly use online technology to make connections with clients and customers and to deliver services. They rely more and more on online connectivity and reap the benefits, thanks to growing opportunities to work innovatively with partners across Scotland and around the world. This in turn helps to grow our economy.

Our public services are increasingly being provided online with the aim of improving access for all, reducing costs while enhancing operational performance. An example of an online platform for accessing public services is the Scottish Government's mygov.scot.

In terms of critical infrastructure, in both private and public sectors, Scotland increasingly relies on networked technologies to run the systems that heat our houses, provide fuel for our vehicles and ensure that our water is safe to drink.

Linking key elements of our infrastructure such as energy, telecommunications and transport systems to the internet brings considerable benefits in terms of efficiency and innovative practice.

Also, there is huge potential for Scotland to contribute to meeting the ever-growing global demand for **cyber resilience and security professionals, goods and services**. Cyber security is a high growth sector. In 2013 the global market was worth \$66bn and it is expected to grow to \$144.67bn by 2024 (Source: Visiongain, 2014).

The Scottish Government recognises the benefits of advances in technology to our economy and has committed to delivering digital connectivity across the whole of Scotland by 2020. Scotland's *Digital Future Strategy* outlines the steps required to ensure Scotland is well placed to take full advantage of the economic, social and environmental opportunities offered by the digital age.

The greatest cyber opportunity for Scotland and its people is for us to become one of the most cyber aware nations in the world – skilled and able to make the most of the digital technology as we enter the next wave of digital enablement. The 'Internet of Things' means that more of what we take for granted every day will be connected. From our personal and medical devices, through our domestic appliances and home automation systems, to the smart buildings and cities which form our built environment. This connectivity brings great opportunities, but is not without risks.

Scotland's Digital Economy

Digital technologies and capabilities are vital for Scotland's economic growth and to maintaining our international standing.

The Scottish Government and its partners in the public and private sector are working hard to deliver key components of a successful digital economy in Scotland. These include:

- accessible and reliable infrastructure so people and enterprises can get online
- improving opportunities for people to develop the skills needed to work in a digital economy
- citizens able to take advantage of the growing range of goods and services available online

Effective cyber resilience is vital if we are to maximise the opportunities for our citizens to benefit from the digital economy

The 'Internet of Things' refers to the way in which any device, which can be turned on and off, is connected to the internet, or to other devices. This includes everything from mobile phones, tablets, coffee makers, fridges, boilers, lamps, headphones, and other wearable devices. This also applies to components of machines, for example a jet engine of an aeroplane or the drill of an oil rig.

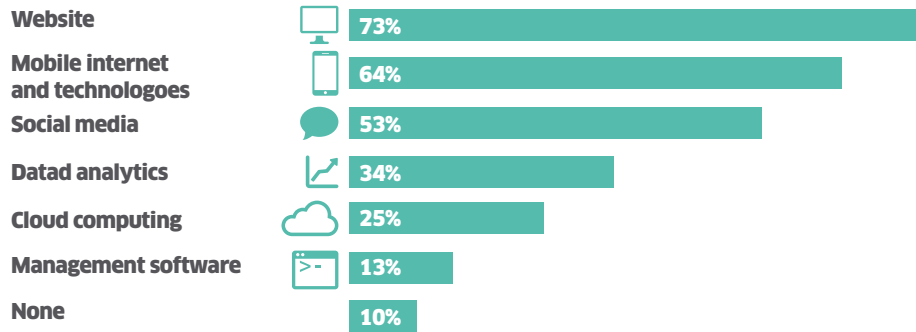




92%

of businesses
have broadband

Adoption of key technologies in Scotland:



6 out of 10 state that using mobile internet and technologies enables staff to work remotely



one third of exporters sell at least 20% of their international sales via their website

With new opportunities come new risks

Our increasing use of, and dependence on, the internet bring new risks. Just as we have seen the benefits of digital technology enabling and promoting legitimate economic activity, we are now experiencing cyber crime at an unprecedented rate. Every day we hear of new online vulnerabilities, attacks and incidents affecting parts of Scottish society – from individuals through to large organisations. Cyber crime is also under-reported. As a result, the scale of the problem is difficult to grasp, and at the moment we do not have a full understanding of the complex risks that cyber crime presents to Scotland.

There is no one type of cyber crime or criminal. Illegal users of the internet include:

- script-kiddies¹, testing their skills against the security of systems
- criminals committing traditional crimes, but online, either as individuals or organised crime gangs
- politically-motivated hackers
- government or commercially-sponsored spies

Cyber crime can include:

- bullying
- identity theft and fraud
- sexual exploitation
- the theft of intellectual property
- attacks against essential services or critical infrastructure

This strategy complements a number of strategies that seek to prevent and combat crime in Scotland. See page 15 for links to these strategies.

An ever-increasing global threat

There is currently a lack of data that calculates the economic cost of cyber crime in Scotland as most cyber crime goes unreported. This is most likely due to victims not being fully aware of the cyber crime itself or organisations' fear of reputational damage.

At a global level, [The Center for Strategic and International Studies \(CSIS\) report on the Global Cost of Cybercrime](#) estimates:

- the likely annual cost to the global economy from cybercrime is more than **\$445 billion**
- cyber crime is equal to between 15% and 20% of the value created by the internet

¹ An unskilled individual who uses scripts or programs developed by others to attack computer systems

What are the impacts of cyber attacks?

The internet and mobile technologies are now central to Scotland's economy and wellbeing. Risks exist at every level of our daily lives. The consequences of a cyber attack can vary from a minor inconvenience to a major disruption. The cost of cybercrime will continue to increase as more business functions move online and as more companies and consumers around the world connect to the internet.

For our economy

A major challenge for Scotland is the increasing number of online incidents that are causing harm to our economy. From intellectual property theft by competitors, to the destruction of corporate and national assets, the threats are outpacing our defensive efforts.

For individuals and families

Online crime has a clear impact on the lives of families in Scotland. A recent Mori survey of 1,000 adults in Scotland showed that 1 in 10 had experienced unauthorised use of their personal data, a similar number had been exposed to upsetting or illegal images and 7% had experienced abusive or threatening behaviour online. As our use of online technology continues to grow, we are at an increasing risk of becoming victims of criminal or unscrupulous behaviour online. We can fall foul of fraud or extortion, disclosure of personal information, identity theft or being subject to forms of abuse including stalking, bullying and exploitation. These attacks may not be targeted at specific individuals, but can be indiscriminate mass campaigns often impacting hundreds or even thousands of people.

For businesses and organisations

Organisations of all sizes rely on crucial information assets, such as databases of client details or intellectual property, that are of value to competitors and cyber criminals. Cyber criminals often operate through stealth with some organisations seldom noticing cyber attacks until the effects of the attack start to impact. Businesses may be reluctant to share news or information about their attack for fear of a loss of reputation. Criminals focus on the easiest targets which means small and medium-sized enterprises (SMEs) can be particularly vulnerable. The direct and indirect costs of cleaning up from a cyber attack can be high and are often unplanned for. In many cases these costs may not be covered by conventional insurance policies.

Key statistics from the [BIS Information Security Breaches Survey 2015](#) show that:

- 50% of the worst breaches were caused by inadvertent human error – up from 31% in 2014
- 74% of small businesses had a security breach – up from 60% in 2014
- For SMEs, the most severe breaches can cost as much as £310,800 – up from £115,000 in 2014
- 90% of large organisations had a security breach – up from 81% in 2014

For public services

Our public services are reliant on digital systems. Digital networks make it possible to provide innovative and integrated public services that deliver to those in most need and promote growth. It crucial that cyber risk is planned and budgeted for when providing these services. In turn, this will help to keep citizens' confident in using digital public services.

For our national security and international reputation

This strategy will contribute to protecting Scotland from infrastructure attacks, hostile reconnaissance and thefts of intellectual property. This will ensure Scotland's reputation as a safe place to live, work, invest and trade.

Increasing our cyber resilience

Individuals and families will be

- more aware of how to protect themselves from online crime
- better able to protect their personal data
- less likely to suffer financial loss as the result of a cyber attack
- more confident online users

Businesses and organisations will have

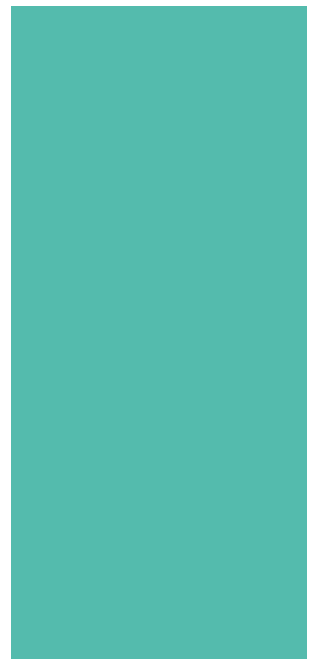
- online services that are more reliable
- protected intellectual property
- increased productivity
- stronger reputations

Digital public services will be

- effective in their systems and response arrangements
- more efficient in the delivery of key services
- better placed to provide continuous services
- trusted by the public with regard to data protection

Scotland's reputation will be

- enhanced and recognised as a safe, secure and resilient country in which to live and do business



SECTION 2 – BECOMING CYBER RESILIENT

This section covers:

What is our vision?

What are the guiding principles of the strategy?

Who needs to be involved?

How can we build cyber resilience?

Our vision

The Scottish Government has worked with a broad community² to develop this strategy and, having consulted widely, has concluded that **Scotland can be a world leader in cyber resilience and be a nation that can 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.**

Improving Scotland's cyber resilience will contribute to many of the outcomes in the [National Performance Framework](#), in particular:

- we live our lives safe from crime, disorder and danger
- we live in a Scotland that is the most attractive place for doing business in Europe
- our young people are successful learners, confident individuals, renowned for our research and innovation
- our public services are high quality, continually improving, efficient and responsive to local people's needs

Improvements in cyber resilience also play an important role in achieving the ambitions of [Scotland's Economic Strategy](#) by helping Scottish businesses increase their competitiveness, protect their intellectual property, succeed at a global level and tackle inequality through helping all people become resilient when using online digital technologies.

² See Annex B – Strategic Working Group

Guiding principles

This strategy is underpinned and inspired by the following guiding principles:

A respect for rights and values. Everything we do will enshrine the rights and values contained within the [European Convention on Human Rights](#) and the [Commonwealth Charter](#). We are committed to transparency and accountability in government, reducing inequality and promoting sustainable economic development.

National and local leadership. The scope and complexity of the cyber resilience challenge requires clear national and local leadership, coordination of capabilities and responsibilities. This should be aligned with a focus on:

- improving the welfare and safety of Scotland's people
- building our economy
- inspiring us all to benefit from digital connectivity

Personal and shared responsibilities. We are all users of technology and we all have a responsibility to take steps to protect ourselves, our families, our organisations, our customers and service users online. Working together we can create a safer online environment in which we are open to sharing knowledge, skills and effective practice.

Promoting digital inclusion. Activity to build cyber resilience should at the same time promote digital inclusion and ensure that vulnerable people currently excluded from these opportunities can make the most of technologies safely.

Contributing to global citizenship. Cyber threats are a global issue and tackling it is part of Scotland's efforts to contribute as a good global citizen. Our endeavours will be aligned with UK, European and international partners.

Who needs to be involved?

Government alone cannot build the cyber resilience of a nation. Cyber resilience is a shared responsibility. The Scottish Government intends to take the lead and will encourage and engage with all sectors to promote and build a cyber resilient nation.

Everyone has a responsibility to safeguard themselves and their families online, just as they would safeguard themselves, their homes and their businesses from traditional criminal threats.

Stakeholders within the public, private and third sectors are asked to consider this framework in the context of their own settings, and embed cyber resilience within their own strategic and operational plans.

This strategy is for:

- **Policy makers - at local and national government level.**

The strategy demonstrates the importance of cyber resilience across all policy areas. It is dependent on and, in turn, supports many other national strategies and programmes, including:

- [Scotland's Economic Strategy](#)
- [Scotland's Digital Future](#)
- [Scotland's Serious Organised Crime Strategy](#)
- [Digital Justice Strategy](#)
- [Curriculum for Excellence](#)
- [e-Health Strategy](#)
- [Equally Safe](#)
- The forthcoming Resilience Strategy

Cyber risks will continue to grow across all parts of society, and therefore policy makers should refer to this strategy when developing, implementing and reviewing policies, strategies and initiatives of their own.

The Scottish Government is responsible for driving forward this strategy. Policy makers are responsible for ensuring that all relevant stakeholders are included in, and can actively contribute to, the implementation of measures within the strategy.

Who needs to be involved

- **Public sector partners such as:**

- Education Scotland
- Highlands and Islands Enterprise
- local authorities
- NHS Scotland
- Police Scotland
- Scottish Enterprise
- Scotland's colleges
- Scotland's universities
- Skills Development Scotland

These and other public sector organisations play central roles in reaching individuals, families and businesses. They are essential partners in leading education and prevention activity to ensure our collective cyber resilience.

- **Representative bodies of business and industry** such as Chambers of Commerce, Federation of Small Businesses, Scottish Council for Development and Industry and The Confederation of British Industry Scotland have an important role to play to ensure businesses and employees are cyber resilient.
- **Private sector organisations** play a crucial role in ensuring that the cyber risk is regarded as being as important as any other business risk.
- **Third sector organisations** are well placed to support families and communities to become more cyber resilient and can often reach the most vulnerable in our society. Third sector organisations are increasingly providing digital services and can themselves be vulnerable online, so there is a need to build their own cyber resilience.

How can we build cyber resilience?

Strategic priorities

Achievement of the desired outcomes of the strategy will require effective leadership at national and local levels. With its partners the Scottish Government commits to advancing research and innovation, developing education and skills and providing clear communication and public awareness.

The Scottish Government, its agencies and partners, will work together to implement this strategy, focusing on four strategic themes:

- 1. Leadership and Partnership Working**
- 2. Awareness Raising and Communication**
- 3. Education, Skills and Professional Development**
- 4. Research and Innovation**

Theme 1: Leadership and Partnership Working

Becoming more cyber resilient requires a sustained and collaborative effort. The Scottish Government will provide a framework that it and its partners can use to coordinate and evaluate the implementation of the strategy. It will encourage stakeholders to embed cyber resilience in their strategic and operational plans. It will continue to work closely with the UK and other governments on cyber resilience and security matters.

Cyber resilience must be regarded as a crucial aspect of business operation and continuity. Public, private and third sector leaders play a vital role in embedding cyber resilience within their own settings.

The Scottish Government intends to demonstrate its commitment to cyber resilience and to lead by example. It will implement cyber resilience arrangements within its own systems to build trust with citizens and businesses. It will work in partnership with the public sector to develop cyber resilience as part of a shared responsibility. The transformation involved in moving to a “digital first” approach for public services goes far beyond the technology which supports these services. Resilience needs to apply to people, processes and technology in every business function and needs to be factored in to all aspects of the design of new digital services.

The high-level priority actions under Leadership and Partnership Working are:

| Priority Actions | Scottish Government | Public Sector | Private Sector | Third Sector |
|---|---------------------|---------------|----------------|--------------|
| 1. Establish a strategic governance group under Scottish Ministers to oversee the effective implementation and evaluation of the strategy | ✓ | | | |
| 2. Incorporate cyber resilience into all national and local government policies | ✓ | ✓ | | |
| 3. Ensure board/executive level commitment to cyber resilience | ✓ | ✓ | ✓ | ✓ |
| 4. Develop cyber incident reporting measures and link to wider ICT/digital and business continuity plans | ✓ | ✓ | ✓ | ✓ |
| 5. Define the standards relating to cyber resilience for public sector procurement of goods and services | ✓ | ✓ | | |
| 6. Ensure the safety and security of online shared services systems | ✓ | ✓ | ✓ | ✓ |
| 7. Embed cyber risk and resilience assessments when developing new products, services and processes | ✓ | ✓ | ✓ | ✓ |
| 8. Consider shared development or procurement of cyber resilient systems and tools for public sector | ✓ | ✓ | | |

Leading by example

The Scottish Government: Cyber Resilience in the Public Sector

To achieve outcome 3: *We have confidence in and trust our digital public services*, the Scottish Government, in collaboration with key public sector partners, has begun the process of preparing an action plan.

A working group has been established and is using the strategy to begin developing specific actions that the public sector can take forward.

The Scottish Government is committed to implementing cyber resilience arrangements within its own systems with the aim of building trust with citizens and businesses and working in partnership with the public sector, to develop cyber resilience across all our public services as part of a shared responsibility.

Anne Moises, Scottish Government's Chief Information Officer is leading the public sector towards this transformation:

"It is clear that the transformation involved in moving to a digital first approach for public services goes far beyond the technology which supports those services. It is vital that the people, processes and technology within the public sector become more resilient."

"Resilience needs to apply to the essential infrastructure in nearly every business function and we need to ensure that resilience is factored into all aspects of the design of new digital services. The infallible prevention against cyber threat is not achievable and so the focus moves to detection, rapid response and recovery. We need to imagine the unexpected, plan for it and practise our response. We will do this by ensuring that cyber resilience scenarios and cyber incident response plans are regularly reviewed, tested and exercised."

Digital Champions

The Digital Champions Development Programme has been developed by the Scottish Government to inspire leaders about the transformational potential of digital tools and technology, and to give them the confidence to take action to release that potential. The programme includes aspects of cyber resilience. More information on: <http://www.gov.scot/Topics/Economy/digital/digitalservices/workforce/dgp>

Theme 2: Awareness Raising and Communication

What we do online has the potential to affect everyone – at home, at work and around the world. Taking a preventative approach and getting the cyber basics right goes a long way towards being safe and secure online and getting the most from being online. It is important that we foster a culture of cyber awareness and readiness among individuals, families, communities and organisations across Scotland, so that they can protect themselves online.

The take-up of even relatively simple measures to improve personal cyber resilience is low in Scotland. Just 1 in 12 claim to regularly install software updates; fewer than 1 in 10 password protect their mobile devices; and only 13% check that a website is secure (e.g. closed padlock symbol) before divulging information. Simple measures can prevent or minimise threats. See Annex C on getting the basics rights for individuals and enterprises.

There is a wealth of well-intended advice and guidance available, so much so that it can be confusing. It is important that cyber resilience messages are communicated in the right way for different audiences. For example, we may talk in terms of “online” and “mobiles”, rather than “cyber”. Different organisations are well placed to develop specific messages and use the most appropriate language to reach different parts of society, including children and the most vulnerable.

Sharing information on cyber threats and vulnerabilities across sectors will also help us to better manage, respond to and move on from cyber incidents. For example larger industry leads can share their knowledge and expertise with SMEs. The [Scottish Business Resilience Centre](#) is a leading organisation providing innovative approaches to building cyber resilience amongst the SME community.

The high-level priority actions under Awareness Raising and Communication are:

| Priority Actions | Scottish Government | Public Sector | Private Sector | Third Sector |
|---|---------------------|---------------|----------------|--------------|
| 1. Assess existing awareness raising programmes and identify whether there are gaps that should be addressed by further campaigns | ✓ | | | |
| 2. Develop specific and appropriate awareness-raising activity for a range of audiences | ✓ | ✓ | ✓ | ✓ |
| 3. Establish a cyber resilience network to share evidence of what works | ✓ | | | |
| 4. Establish a central gateway for trusted advice and guidance to citizens and businesses | ✓ | | | |
| 5. Assure the public around the safe use of digital public services | ✓ | ✓ | | |
| 6. Encourage the sharing of information relating to cyber incidents, threats and vulnerabilities across sectors | ✓ | ✓ | ✓ | ✓ |
| 7. Develop methods on how to measure impact | ✓ | ✓ | ✓ | ✓ |



Scottish Cyber Information Network (SCiNET)

SCiNET is a secure online information sharing platform and a joint collaboration between industry and government to share cyber threat and vulnerability information and to raise awareness of how to respond to a cyber incident.

Owned by Cert UK*, Scottish businesses can:

- obtain early warning of cyber threats
- learn from the experiences, mistakes and successes of other users without fear of exposing organisation sensitivities
- engage with industry, government and law enforcement counterparts in a secure environment
- seek advice from other members
- participate in the building of pooled knowledge with access to UK wide fusion cell outputs/information

“With the ever evolving cyber threat landscape, SCiNET provides Scottish businesses with an online resource to share threat information in real time and with key partners in business and academia. This kind of partnership has the ability to turn the ever-evolving cyber security landscape into a significant opportunity, not only to protect but to grow an industry sector that can be of major benefit to the Scottish economy and the people of Scotland.”

DCC Iain Livingstone, Police Scotland

* CERT UK: the UK National Computer Emergency Response Team, formed in March 2014 in response to the UK's National Cyber Security Strategy.

Theme 3: Education, Skills and Professional Development

Education and training, alongside activity to raise awareness, are critical to changing behaviour and making us more effective in the way we engage with digital technologies. They are also key to having enough cyber professionals to effectively prevent or deal with cyber crime.

Every child, young person and adult must have the cyber resilience skills for learning, life and work – to be able to protect themselves online and achieve the full benefits of a digital economy.

In learning settings, relevant curricula should drive the development of skills which will help learners to become more cyber resilient.

Most jobs require knowledge, understanding and skills in digital technology, and this will only continue to grow. Training in all vocational areas, not just digital occupations, must include learning outcomes related to cyber resilience.

If we are to succeed in integrating cyber resilience at all ages and stages of education, from pre-school to post-employment, we need to ensure that our teachers and trainers have the skills, knowledge and understanding to teach cyber resilience. Appropriate learning materials and guidance are required for educators, in both formal and non-formal learning contexts.

It is crucial that we continue to develop and retain cyber expertise in Scotland to ensure we continue to prosper.

The high-level priority actions under Education, Skills and Professional Development are:

| Priority Actions | Scottish Government | Public Sector | Private Sector | Third Sector |
|--|---------------------|---------------|----------------|--------------|
| 1. Map existing cyber resilience skills across learning settings to identify gaps | ✓ | ✓ | | |
| 2. Explore opportunities to embed cyber resilience into curricula in all learning settings | ✓ | ✓ | ✓ | ✓ |
| 3. Introduce cyber resilience into workplace learning and development | ✓ | ✓ | ✓ | ✓ |
| 4. Explore ways to embed cyber resilience into teacher training | ✓ | ✓ | | |
| 5. Grow the number of apprenticeships in cyber security and resilience | ✓ | ✓ | ✓ | ✓ |
| 6. Explore ways to develop and retain cyber expertise in Scotland | ✓ | ✓ | ✓ | |



National Progression Awards in Cyber Security

The first school-based national qualifications in cyber security have been developed by the Scottish Qualifications Authority. The National Progression Awards in Cyber Security at SCQF levels 4, 5 and 6 provide foundation knowledge and skills in data security, digital forensics and ethical hacking – and provide a skills pipeline into the cyber security industry.

The aim of the awards is to produce knowledgeable and skilled individuals who are aware of the potential misuses of, and unauthorised access to, computer systems but who use these competences for legal and ethical purposes.

The qualification is available through schools, colleges and training providers. More information is available at – <http://www.sqa.org.uk/sqa/74738.html>

Schools and Police Scotland working together for a safe online experience

First year pupils at Kyle Academy in Ayr piloted The Cyber Badge – a 12-week course on cyber security.

The Cyber Badge, developed with Police Scotland and Scottish Universities, focused on:

- password security
- online bullying
- grooming
- computer crime
- social networking

Learners get the chance to take their knowledge home, discovering how much (or little!) their parents and carers know about online security and then helping them to become more cyber resilient.

The Cyber Badge, with support from Education Scotland, is now being promoted to schools throughout Scotland.



Theme 4: Research and Innovation

Effective coordinated research will ensure Scotland's place at the forefront of cyber resilience.

There is currently limited information on cyber resilience in Scotland, including the cost of cyber crime. First and foremost, we need to establish a baseline from which we can measure progress in cyber resilience. Researchers should consider how they can boost existing UK and global data for Scotland's needs and interests.

Ongoing commitment to research will ensure our knowledge and understanding remains fit for purpose. Collaborative research and sharing effective practice across Scotland and other countries will help us stay at the forefront of this rapidly evolving issue. In turn, this will help inform the development of new and innovative technologies and practices. The Higher Education sector has a key role to play in this effort.

Innovation is in Scotland's DNA and there is a real opportunity for us to be global innovators in this field. Universities are producing outstanding graduates in the digital design, ethical-hacking and forensic fields, and it is vital that we grow, nurture and keep these skills in Scotland.

The high-level priority actions under Research and Innovation are:

| Priority Actions | Scottish Government | Public Sector | Private Sector | Third Sector |
|---|---------------------|---------------|----------------|--------------|
| 1. Establish a coherent and sustainable approach to research | ✓ | ✓ | ✓ | ✓ |
| 2. Establish a baseline to identify the economic, societal and individual impacts of cyber crime | ✓ | ✓ | | |
| 3. Improve the sharing of research to develop our knowledge and understanding to help us become more effective in building cyber resilience | ✓ | ✓ | ✓ | ✓ |
| 4. Establish a baseline to identify current levels of trust and confidence in digital public services | ✓ | ✓ | | |
| 5. Develop new and innovative ways to help businesses and organisations become more cyber resilient | ✓ | ✓ | ✓ | ✓ |
| 6. Learn from other nations and share information to combat cyber crime | ✓ | | | |



Cyber Academy

The Cyber Academy at Napier University is a partnership between academia, law enforcement, industry and the public sector. It aims to integrate academic and professional practice, support innovation in cyber security, and provide access to members to an advanced and virtualized training infrastructure for both evaluation and training.

Royal Academy of Engineering (RAE) Industrial Secondment Scheme

The consequence of being a one-person business is often not having the expertise to adequately secure business information. Sole traders are less likely to have the capacity to employ someone to take care of their digital security. Often, reliance on smartphones means that the long-term survival of their business depends on a portable device that needs to be secure and resilient.

Funded by the RAE, Karen Renaud of the University of Glasgow will spend a year working with the Scottish Business Resilience Centre and strategic partners on a collaborative research project to:

- a) understand the particular needs of solo-SMEs with respect to security in their businesses
- b) develop an information security pack for solo-SMEs, to support them in improving their cyber security
- c) put in place measures to support the launch of a support community

CASE STUDY 1

INDIVIDUAL: ONLINE SHOPPING FRAUD

One of the most popular online auction and shopping websites offers people and businesses a virtual marketplace to buy and sell a broad variety of goods and services worldwide. The website is free to use for buyers, but sellers can be charged for listing items and again when those items are sold.

The issue

A man from Stirling was searching for a motorhome on the site when he found a listing that fitted his criteria located in Aberdeenshire. The listing had five days to run so the user sent a message to the seller asking if he could arrange to view the motorhome. The seller claimed to be working away from home and as a result this would not be possible before the auction ended. The listing only offered a few photographs of the van but during a message exchange through the system more details of it were given.

The buyer was cautious as the seller did not have any online selling history but he had stated he'd only joined the site to sell the item on behalf of an aging relative who was uncomfortable with technology. Although the buyer had stated they preferred to use cash, the seller indicated that he would prefer a deposit by bank transfer to secure the deal. The seller provided bank details which showed a London bank and an Eastern European name as the account holder. After doing some research the buyer found some identical photos of the motorhome in a trade magazine. It quickly became apparent that the seller had set up a fraudulent transaction.

The consequences and being cyber resilient

The lack of the seller's trading history, their unwillingness to allow a view before the sale, and the unusual bank details made the buyer cautious which subsequently saved them a huge loss of money.

CASE STUDY 2

SMALL BUSINESS

This hairdresser uses specifically designed software that holds clients details, appointments and marketing information.

The issue

When the manager started his computer, he was confronted with a poorly written ransom note in the form of an electronic notepad document left by hackers saying that they had encrypted “all your important data” and that if they wanted data back, they needed pay a ransom.

Ransomware is a type of virus that prevents or limits users from accessing their system. The victims are then forced to pay the ransom through certain online payment methods in order grant access to their systems, or get their data back. The business paid the 1,000 Euro ransom and were given a keycode to unlock his information, only to find that the majority of information was corrupted.

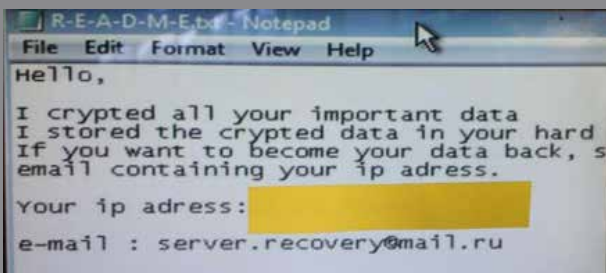
The consequences

A full year’s worth of data and information which was critical to the business was lost. The attacked systems contained appointments, salary information, customer history, shares information and marketing data. As the appointment details had been lost, the hairdresser wasn’t able to plan effectively: they didn’t know which clients were coming in nor had they their contact details.

Becoming cyber resilient

The hairdresser is now looking into backing up all data, including using removable back up devices.

The salon is approaching the developer and supplier of the software to ask them to investigate if there are any vulnerabilities in their software.



CASE STUDY 3

MEDIUM-SIZED BUSINESS: CYBER AND DATA BREACH IN A LEGAL PRACTICE

The issue

This practice operated with three Microsoft Windows servers that were not fully managed by their external contractor for cost reasons. All business data was backed up to an old tape drive on a daily basis but there had been no testing of the ability to recover the data. The business had limited spare capacity within their IT service architecture. Whilst anti-virus software was installed, this was not centrally managed and all users had administrative access to their computers allowing them control over the installed solution. There was no perimeter firewall appliance on the network and there was no content filtering on internet and email activity. The business had looked at business continuity but had not addressed the risks from IT believing that the risk and impact to the practice was low on IT dependency.

Becoming cyber resilient

Following a data breach, the practice recognised the need to address data security and business continuity risks due to the impact this had on the practice. The data breach was socially engineered and took advantage of a weak password policy and unnecessarily elevated operating permissions of users. The data breach itself cost the practice over £250,000 in immediate remedial activities and addressing the disclosure of data. The practice was heavily disrupted operationally for five days whilst systems were made secure ahead of the longer-term planned security measures. The practice

implemented the following to reduce the chance of this happening again:

- trained staff on cyber security
- installed and maintained a managed firewall appliance
- installed a fully managed anti-virus solution
- content filtered Internet and email activity
- implemented password policies for all users
- removed administrative access from all users
- implemented change management processes to reduce security principle failures
- implemented data backup procedures that tested recovery
- implemented business continuity for loss of access to IT systems
- implemented a process of carrying out external and internal penetration testing

The cost to the practice for the remedial work and the follow up actions was in the region of £100,000.

The benefits of being cyber resilient

The work carried out provided higher levels of confidence of their data systems. It also built up the confidence of both the practice and clients in that the business would be able to handle most unplanned situations whilst managing cyber and data security.

CASE STUDY 4

LARGE COMPANY

The company designs, manufactures and installs building steelwork framework for the building industry. The company uses Computer Numerical Control (CNC) operated cutting, drill and punching equipment as part of the manufacturing process. The CNC equipment is connected directly to the drawing office through the business network which prepares the models using the latest in 2D and 3D software to ensure maximum efficiency and accuracy in their business process.

The issue

The business suffered a minor security breach in the office that resulted in multiple drawing model files being corrupted before being transmitted to a CNC drilling machine. The corruption resulted in major project delay as it was not identified until the steelwork was onsite and being assembled. The required secondary fabrication cost the business over £1,250,000 for manufacturing, crane rental and missed contract deadlines with clients.

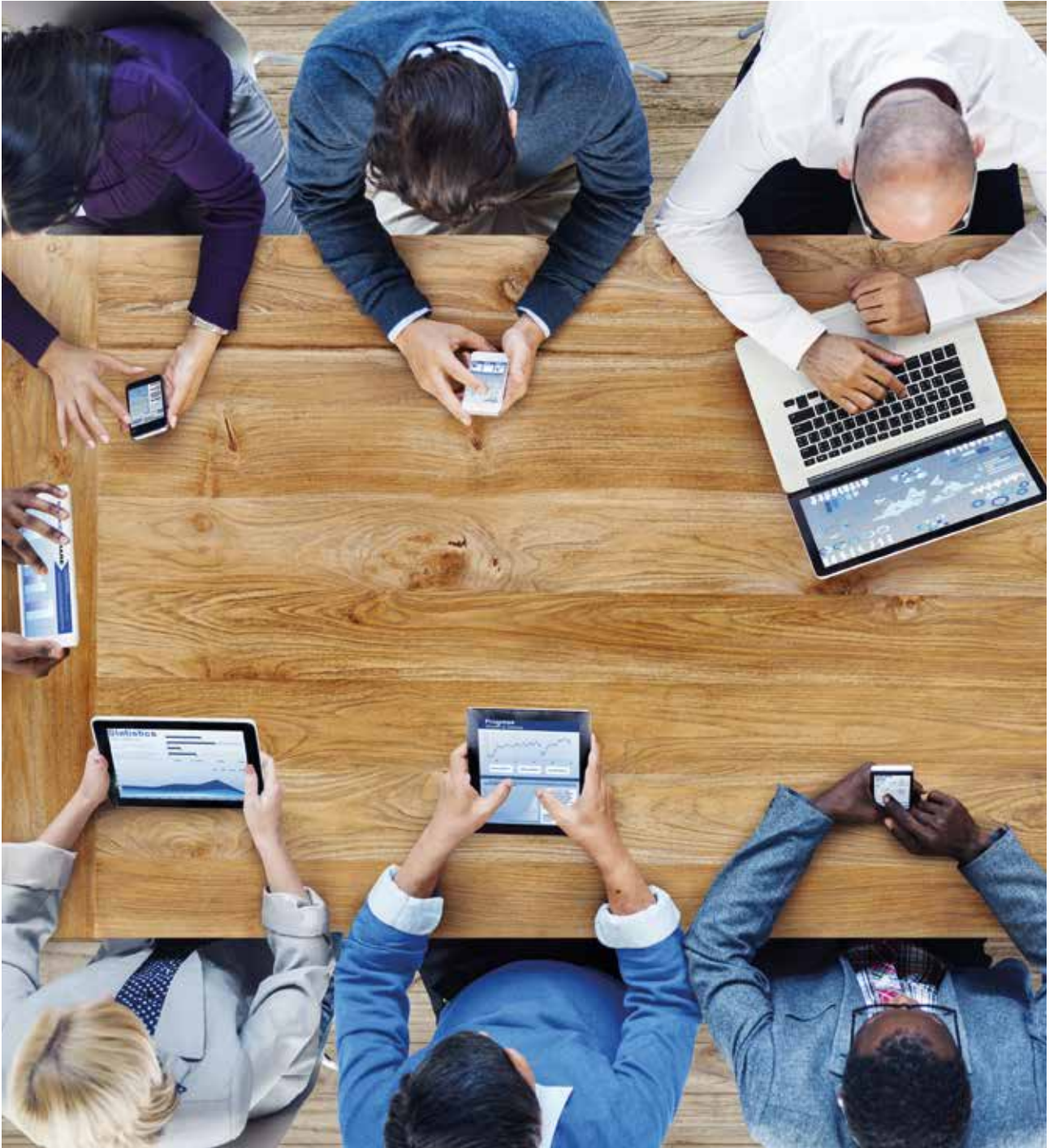
The root cause of the failure was down to weak security policies between the drawing office and the shop floor. It was also identified that poor patch management¹ by the CNC equipment manufacturer left a number of risks open.

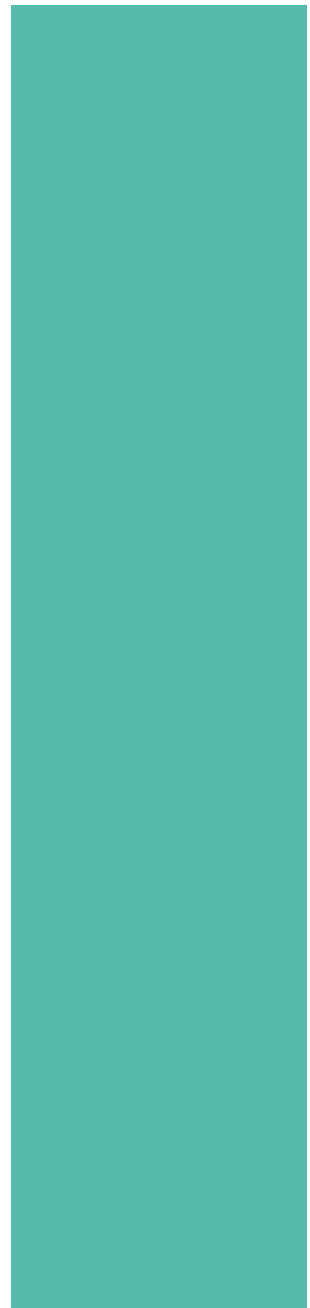
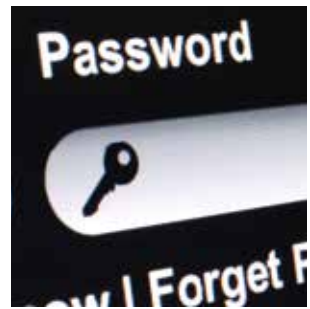
¹ Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system

Becoming cyber resilient

The business put new processes in place. It implemented an internal firewall appliance to isolate the shop floor equipment from each other to mitigate the risks of poor patch management by the manufacturers. The firewall appliance was also used to isolate the shop floor from all but authorised traffic from the drawing office with the security software installed on the office computers reconfigured to control the network traffic on the network as a whole. Change control processes were put in place to ensure that any change in the network configuration did not break the security principles of the network design.

Whilst the insurance company underwrote the costs of the claim for the data breach and the associated ongoing costs as a result of the breach, insurance premiums where increased considerably. In addition to this increased premium, the business needed to invest an unplanned £28,000 to complete forensic analysis and secure their network.





SECTION 3 – IMPLEMENTING THE STRATEGY AND MEASURING THE IMPACT

This section covers:

How will we implement this strategy?

How will we know if we are making a difference?

How will we implement this strategy?

This strategy is the initial framework to help build a cyber resilient Scotland. It sets out high level actions which we will develop into a set of action plans post-publication. These plans will evolve to keep up with the pace of rapid and emerging digital change and the associated risks.

The Scottish Government will work with partners to use this strategic framework to set out detailed action plans that align to the themes.

We need your help to make Scotland more cyber resilient.

It is essential that we commit to implementing the strategy and associated action plans. Effective implementation of this strategy will require the input and action from every part of Scottish society – from communities, small businesses, large organisations, local authorities, third sector organisations, academia, law enforcement and central government and, of course, citizens themselves.

How will we know if we are making a difference?

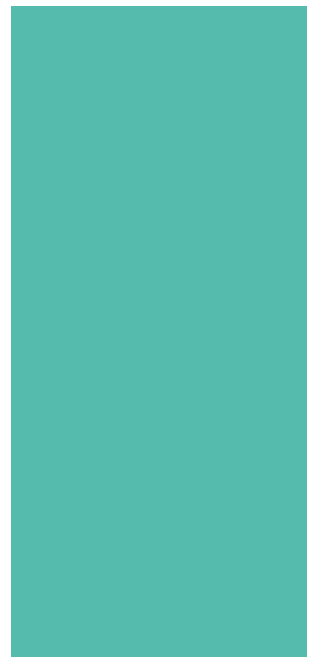
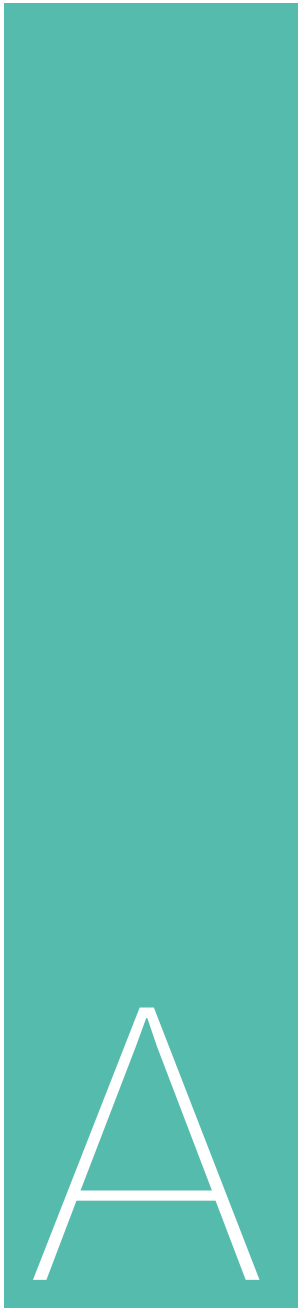
The Scottish Government will ask partners to share their own action plans and keep track of milestones and progress on an annual basis. There will be regular annual updates on progress to a national governance group. There will be some flexibility to reporting depending on the urgency of the task the stakeholder is responsible for, the rapid rate of development of threats and the developing skills and knowledge of the stakeholder.

The strategy will be reviewed in two years' time; however we may review some elements within the strategy more frequently (due to the rapidly changing nature of cyber).

How will we know we're making a difference?

We will know if we are succeeding if we are able to see a step-change in the cyber resilience of our citizens, businesses, public services and government. Our initial plan to measure success under each of the outcomes is as follows:

- 1. our people are informed and prepared to make the most of digital technologies safely**
Evidence example: public opinion surveys; number of young people undertaking cyber-based activity within the curriculum; number of cyber crimes committed against individuals.
- 2. our businesses and organisations recognise the risks in the digital world and are well-prepared to manage them**
Evidence example: business research; number of reports to Scottish Cyber Information Network (SCiNET); numbers of cyber crimes committed against SMEs.
- 3. we have confidence in and trust our digital public services**
Evidence example: number of public servants trained in cyber resilience; information of data breaches recorded by public sector organisations.
- 4. we have a growing and renowned cyber resilience research community**
Evidence example: number of post-graduate researchers; numbers of Scottish universities recognised as Academic Centres of Excellence in cyber security and cyber resilience; local and global recognition of research findings.
- 5. we have a global reputation for being a secure place to live and learn, and to set up and invest in business**
Evidence example: Scottish Enterprise investment data; international economic comparison research such as OECD.
- 6. we have an innovative cyber security, goods and services industry that can help meet global demand.**
Evidence example: number of staff employed within the cyber security goods and services sector; number of Scottish enterprises with recognised cyber security kite marks; take up of Scottish-based cyber security services; number of cyber resilience spin-off companies linked to Scottish universities and colleges.



ANNEX A

Scotland can be a world leader in cyber resilience and achieved the following outcomes

OUTCOMES

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

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

We have confidence in and trust our digital public services

PRIORITY ACTIONS

LEADERSHIP & PARTNERSHIP

1. Establish a strategic governance group
2. Incorporate cyber resilience into national and local government policies
3. Ensure board/executive level commitment to cyber resilience
4. Develop cyber incident reporting measures and link to wider ICT/digital and business continuity plans
5. Define the standards of cyber resilience for public sector procurement
6. Ensure the safety and security of online shared services systems
7. Embed cyber resilience assessments for new products, services and processes
8. Consider shared development or procurement of cyber resilient systems

AWARENESS RAISING

1. Assess existing awareness campaigns
2. Develop specific awareness-raising & communication activity for a range of audiences
3. Establish a cyber resilience network to share evidence of what works
4. Establish a central gateway for trusted advice and guidance
5. Assure the public around the use of digital public services
6. Encourage sharing of information relating to cyber incidents, threats and vulnerabilities
7. Develop methods on how to measure impact

and be a nation that can claim, by 2020, to have

■ We have a growing and renowned cyber resilience research community

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

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

EDUCATION, SKILLS & PROFESSIONAL DEVELOPMENT

1. Map existing cyber resilience skills across learning settings to identify gaps
2. Explore opportunities to embed cyber resilience into curricula
3. Introduce cyber resilience into workplace learning and development
4. Explore ways to embed cyber resilience into teacher training
5. Grow the number of apprenticeships in cyber security and resilience
6. Explore ways to develop and retain cyber expertise in Scotland

RESEARCH & INNOVATION

1. Establish a sustainable and coherent approach to research
2. Establish a baseline to identify the economic, societal and individual impacts of cyber crime
3. Share research to develop our knowledge and understanding
4. Establish a baseline for current levels of trust and confidence in digital public services
5. Develop new and innovative ways to help businesses and organisations become cyber resilient
6. Learn from other nations and information to combat cyber crime

ANNEX B

The Strategic Working Group worked together to co-develop this strategy from February – October 2015.

There were representatives from:

- Education Scotland
- KPMG
- Microsoft
- Police Scotland
- Scottish Business Resilience Centre
- Scottish Enterprise
- Scottish Government
- Scottish Informatics and Computer Science Alliance
- SELEX ES
- SKAILL Cyber Defence
- Skills Development Scotland

ANNEX C

Every person and business in Scotland will benefit from:

| | |
|--|--|
| Strong passwords | Using three random words is one way to creating a strong password e.g. SeeCatEek |
| Downloading software updates | Software updates contain vital security upgrades which help protect your device from viruses and hackers. You will be asked to install them – always click yes! |
| Installing software security | Anti-virus software removes viruses, quarantines and repairs infected files, and can help prevent future viruses. Remember to use anti-virus on your mobile devices too. |
| Be aware of suspicious emails | Delete suspicious emails as they may contain fraudulent requests for information or links to viruses. If you are being pressured to make a quick decision or to give any personal or financial information DELETE THE EMAIL immediately. |
| Protect and secure mobile devices | Secure your portable devices and the information they contain. Establish a password and enable screen lock or auto lock on all devices and install an antivirus app. |
| Secure wireless networks | Secure your home or office wireless networks and think carefully before sharing private details on public wifi. |
| Firewall | Firewalls act as protective barriers between computers and the internet. Check your security settings for a built-in personal firewall. If you have one, turn it on |

Businesses in Scotland will further benefit from:

| | |
|-----------------------|---|
| Staff training | Most data breaches are due to human error. Make your staff aware of cyber security threats and how to deal with them. |
| Access | Ensure that only those who should have access to systems have access and at the appropriate level e.g. remove 'admin access' from those that don't need it. Don't forget to remove access rights from staff who have left the organisation. |

Information on how to get the basics right:

[Cyber Streetwise](#)
[Get Safe Online](#)

Guidance and tools on cyber security for business:

[Cyber Essentials Scheme](#)
[10 Steps to Cyber Security](#)
[Small Businesses: What you need to know about cyber security](#)



The Scottish
Government
Riaghaltas na h-Alba

© Crown copyright 2015

OGL

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

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

First published by The Scottish Government, November 2015
ISBN: 978-1-78544-765-5 (web only)

Published by The Scottish Government, November 2015

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS58656 (11/15)