

Finance and Resources Committee

10.00am, Thursday 27 August 2015

Scottish Government Consultation on the draft Cyber Resilience Strategy for Scotland - Response

Item number	7.12
Report number	
Executive/routine	
Wards	ALL

Executive summary

This report provides a response to the Scottish Government's consultation on the draft Cyber Resilience Strategy for Scotland.

This consultation takes forward their commitment to building cyber resilience amongst Scotland's communities, businesses and public services. It seeks views from individuals and organisations, across sectors, on how Scotland can become even more resilient from cyber attacks and crime when using online technologies.

The draft Strategy has been produced by the Scottish Government, with input from a wide range of partners across the public and private sectors.

Links

Coalition pledges	P30, P33
Council outcomes	CO23, CO24, CO25, CO26
Single Outcome Agreement	

Scottish Government Consultation on the draft Cyber Resilience Strategy for Scotland - Response

Recommendations

- 1.1 It is recommended that the Finance and Resources Committee:
 - 1.1.1 agree the consultation responses, as set out in appendix one, be submitted to the Scottish Government.

Background

- 2.1 On the 5 June 2015 the Council received an invitation to respond to a consultation being undertaken by Scottish Government on the draft Cyber Resilience Strategy for Scotland.
- 2.2 The Strategy has been developed in partnership with a wide range of stakeholders, the draft strategy sets out the direction on how Scotland and its people can become more resilient online; how Scotland can be more alert to online risk and know how to quickly recover from any cyber-attack.
- 2.3 The consultation runs from 5 June to the 28 August 2015.

Main report

- 3.1 The draft Cyber Resilience Strategy for Scotland, see appendix 2, has been developed by the Scottish Government to address a key issue emerging from the commitment to delivering digital connectivity across the whole of Scotland by 2020: The Digital Future Strategy.
- 3.2 With this increasing use and dependence on cyberspace new types of risk have emerged. The strategy's focus is helping individuals and organisations to protect themselves from criminals and other malicious users of cyberspace, building on the "[UK Cyber Security Strategy: Protecting and Promoting the UK in a digital world](#)¹".

¹ See: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cybersecurity-strategy-final.pdf

3.3 It is not intended to be a technical document. Rather it is targeted at raising awareness and knowledge across the full range of users of internet services and through increased awareness

3.4 The consultation seeks views on 12 questions:

- Q1: Are the guiding principles right for this strategy? Are there any other principles that should be considered when continuing to develop the strategy?
- Q2: Do you agree with the vision?
- Q3: Do you agree with the three strategic outcomes? Are there additional outcomes that should be considered?
- Q4: Do you think we are focusing on the right objectives? Are there additional key objectives that should be considered?
- Q5: Do you agree with the main areas of focus for effective leadership and promoting collaboration? Are there other areas that should be considered?
- Q6: Do you agree with the main areas of focus for raising awareness and ensuring effective communication? Are there other areas that should be considered?
- Q7: Do you agree with the main areas of focus for developing education and skills in cyber resilience? Are there other areas that should be considered?
- Q8: Do you agree with the main areas of focus for strengthening research and innovation? Are there other areas that should be considered?
- Q9: Are there additional actions that will help us achieve making Scotland and its people more cyber resilient?
- Q10: Do you think the monitoring and evaluation arrangements are sufficient?
- Q11: Have you ever experienced cyber crime (see examples diagram on page 9?) If so, did you report it? Please provide details.
- Q12: Would you be willing to share your experiences with us?

3.5 The responses proposed to these specific questions are set out in Appendix 1. In addition the Council has identified a number of related issues that it proposed to provide as part of the response and these are included at the end of Appendix 1.

3.6 In summary, it is recommended that the Council welcomes the development of a national strategy, but highlights the need for this to be rooted in an Action Plan which is clear about the actions that will be undertaken at UK National, Scottish

National, and Local Authority levels.

Measure of success

- 4.1 The strategy indicates the expectation that stakeholders will share their action plans and keep track of milestones and progress on an annual basis. As part of the new ICT Contract the Council will be, both, assuring security of our own services, and through social benefit be seeking to undertake digital enablement works for residents. These will be reported on as part of the ongoing management of the new contract.

Financial impact

- 5.1 There is no direct financial impact from this consultation.

Risk, policy, compliance and governance impact

- 6.1 In terms of this consultation exercise there are no direct implications in relation to risk, compliance or governance.
- 6.2 Engagement with the Strategy and national actions plans would support risk management of potential threats to Council services as well as supporting the residents and businesses in Edinburgh to be cyber aware.

Equalities impact

- 7.1 There are no equalities impacts associated with this report.

Sustainability impact

- 8.1 The impacts of this report in relation to the three elements of the Climate Change (Scotland) Act 2009 Public Bodies Duties have been considered. In summary, the proposals in this report would have no material impact on sustainability.

Consultation and engagement

- 9.1 Consultation has taken place with the Resilience Unit of the Council.

Background reading / external references

[Countering the Cyber Threat to Business](#)

Alastair Maclean
Chief Operating Officer
Deputy Chief Executive

Contact: Ritchie Somerville, Chief Information Officer (Interim), Customer Services

E-mail: ritchie.somerville@edinburgh.gov.uk | Tel: 0131 529 3409

Links

Council outcomes	CO25 - The Council has efficient and effective services that deliver on objectives CO26 - The Council engages with stakeholders and works in partnership to improve services and deliver on agreed objectives
Appendices	Appendix 1 – Responses to the consultation on proposal for a Cyber Resilience Strategy for Scotland Appendix 2 – Consultation on proposal for a Cyber Resilience Strategy for Scotland: Consultation Document

Responses to the consultation on proposal for a Cyber Resilience Strategy for Scotland

Q1: Are the guiding principles right for this strategy? Are there any other principles that should be considered when continuing to develop the strategy?

Response:

The focus of this strategy is one which appears to be best described as cyber awareness. In this context the principles cover the main issues. However, the balance of focus is slightly confusing. There are many users of the Internet, all with different roles, and this strategy seeks to bridge the position between:

- *ensuring a safe and secure operation and*
- *the parallel need for economic development*

This is a complex balancing act, and the strategy could benefit from separating these two aspects more distinctly to ensure its purpose and direction are as clear as they can be for all the audiences it intends to target.

The internet is a global resource and all responses to it need to be considered in that context. It is important that the principles reflect the key themes of security that exist at a global, European and UK level, with differentiations being about how these will apply in a Scottish context. This is particularly relevant for the “UK Cabinet Office Cyber Security Strategy”, given the joint responsibility in this area.

In terms of other principles, It is essential to recognise that the Internet is not a national resource; nations, multi-national organisations, business great and small, as well as possibly a greater proportion of individuals from all walks of life, all work and play here. In this context it is important that we, in Scotland, recognise that much of the resource and service in cyber space are provided without a great deal of reference to national boundaries. Making them safer or more secure cannot be a single nation’s remit, and a principle regarding collaboration to support safety and security could be helpful.

Q2: Do you agree with the vision?

Response:

The vision statement, in isolation, does not explain itself clearly nor express the role of Government, at all its levels, in this vision. .

Whilst clearly we would all want to ensure that people and businesses in Scotland can use the Internet in ways that are safe and secure and deliver prosperity, there is

a need to anchor this in relation to the actions that government will take. For example:

“Our vision is to support safe and secure participation in cyberspace and enable Scotland to prosper through engagement with new digital marketplaces and communities.”

Q3: Do you agree with the three strategic outcomes? Are there additional outcomes that should be considered?

Response:

While the nation can improve awareness of the risks and confidence in using online technologies, it cannot provide safety other than through making people aware of those risks.

Of the three stated outcomes, outcome three is least well expressed:

“We all have confidence in the resilience of our digital public services.”

The focus here is on Confidence, a personal belief, and to seek to measure this could lead to a level of complexity that exceeds the underlying theme: ensuring that digital public services are resilient.

The focus should rather be on ensuring that security and resilience are an integral part of the provision of such services rather than a ‘wrapper’ added later. The change in emphasis should therefore be:

“Our digital public services operate with a level of resilience we can all have confidence in.”

No obvious additional outcomes are apparent at this time.

Q4: Do you think we are focusing on the right objectives? Are there additional key objectives that should be considered?

Response:

The objectives do appear to have an appropriate focus. There are two comments we would add, to strengthen this section7.

This section would benefit from greater clarity on whom is included in the “we all” referred to.

If this is, as it appears, a general call to arms then it needs to be seen in the context that the CESG and Institute of Directors report referenced in the strategy, “Countering the cyber threat to business” identified that “basic information risk management can stop up to 80% of the cyber attacks seen today.” This statement was made in the context of “the responsibility to manage your organisation’s cyber risks starts and stops at board level.” In this context it is important that the objectives work both for individual organisations and for the collective.

There may be some benefit in making the distinction within the objectives about what “I can do”, what “we will do”.

Q5: Do you agree with the main areas of focus for effective leadership and promoting collaboration? Are there other areas that should be considered?

Response:

Yes, the main areas of focus make sense. However the strategy is confusing in relation to the statement “aspects of protecting Scotland’s critical national infrastructure are reserved to the UK Government”. Given that the audience for this strategy will not be limited to those with a professional understanding of this subject area, there would be benefit in tabulating the differences between UK Government and Scottish Government cyber security responsibilities.

It is important to also recognise the existing body of good practice that already exists in Scotland, such as the GSi code of connection. There should be advantages possible for all from the stipulation of further funded common standards.

Q6: Do you agree with the main areas of focus for raising awareness and ensuring effective communication? Are there other areas that should be considered?

Response:

The industry and government has a wide number of useful security and alert feeds already. The Scottish local authorities have a very well established and long standing security community that has shared much and contributed towards many Scottish initiatives and is well regarded by SOCITM, SOLACE, as well as the Cabinet Office and CESG.

Security industry professionals are already developing and promoting best practice, and have ever since computers were invented. Promoting or supporting initiatives like GetSafeOnline is helpful in raising education and awareness for citizens and consumers.

There may be some benefit from referencing the role of SOCITM, SOLACE and other professional bodies, and the contribution they can make, in this strategy.

Q7: Do you agree with the main areas of focus for developing education and skills in cyber resilience? Are there other areas that should be considered?

Response:

Yes. However, it is important to recognise the educational initiatives that already exist, in many different forms.

Again, given the wide audience for this strategy, it is important to differentiate between cyber awareness in the community, that can be taught at school for example, and information security, that is a well established profession, albeit one that Scotland may wish to seek to excel in.

Q8: Do you agree with the main areas of focus for strengthening research and innovation? Are there other areas that should be considered?

Response:

Yes. This is a fast moving and dynamic area, and one where observed learning (watching what people are doing, particularly the hacking community) is critical.

Q9: Are there additional actions that will help us achieve making Scotland and its people more cyber resilient?

Response:

The development of an action plan and timetable outlining the activities, milestones and outcome, to support the delivery of the Cyber Resilience Strategy would ensure clarity of understanding, and how best to contribute.

Other more specific actions that could contribute include:

- Electronic one time password tokens possibly aligned to MyGovScot so that everyone can improve identity security*
- Education, support and free tools for parents to help them protect their children from themselves.*

Q10: Do you think the monitoring and evaluation arrangements are sufficient?

Response:

The strategy suggests “The Scottish Government will be asking stakeholders to share their action plans and keep track of milestones and progress on an annual basis” As it is not clear at this point who the exact stakeholders are to this strategy it is difficult to understand what action plans may look like or include. In this regard measuring anything would seem aspiration rather than achievable in any meaningful way.

This relates to the response to Q9 above. The Strategy needs to have a dedicated action plan which can then be monitored and evaluated for impact.

Q11: Have you ever experienced cyber crime (see examples diagram on page 9?) If so, did you report it? Please provide details.

Response:

Yes. In line with legislative requirements and good practice the incident was reported to GovCertUK and the Information Commissioner Office.

Q12: Would you be willing to share your experiences with us?

Response:

Yes.

Additional Comments:

- 1.1 There is a need to ensure that links and interdependencies with the forthcoming Scottish Government Resilience Strategy are clear and well explained.
- 1.2 The position of the Strategy in relation to NHS Scotland and its Boards, needs to be clarified, along with other Emergency Services and Utilities. There may be benefit from their inclusion, given the experience in resilience planning.
- 1.3 More detail is required on the expectation around the cascaded development of action plans by stakeholders to the Strategy, and the measurement and communication of these plans, as referenced on page 11 of the consultation document.
- 1.4 Again on page 11, reference is made to many aspects of the Scotland's CNI being reserved to the UK Government, as referenced in the formal responses above. Going forward, stakeholders will need to have a fuller understanding of which parts of this are reserved and what measures UK Government is taking to preserve continuity of these services to Scotland. Given the interdependencies inherent in these, a failure in any part of the system can impact on other aspects e.g. Electricity/Water/Communications/Fuel/Finance.
- 1.5 There would be benefit for stakeholders if the strategy was able to better explain how the Scottish Strategy integrates with the UK Strategy, perhaps through a strategy map.
- 1.6 Further detail on governance, the definition of key strategic policies and resource allocation would enhance the Strategy or a resultant action plan and increase stakeholder buy-in.

Consultation on proposal for a Cyber Resilience Strategy for Scotland

June 2015

CONTENTS

	Page Number
Purpose of this consultation	3
Responding to this consultation paper	3
Consultation questions	5
1 A message from the Deputy First Minister	6
2. Why do we need a cyber resilience strategy?	7
3. What are the aims of the strategy?	10
4. How can you help?	11
5. What principles is the strategy built on?	12
6. What is our vision?	13
7. What can we all do to become cyber resilient?	14
8. How will we use this strategy to achieve real change?	22
9. How will we know we are succeeding?	23
Annex	
A. Glossary	24
B Respondent Information Form	25

1. Purpose of this consultation

This consultation takes forward our commitment to building cyber resilience amongst our communities, our businesses and our public services. It seeks views from individuals and organisations, across sectors, on how Scotland can become even more resilient from cyber attacks and crime when using online technologies. It has been produced by the Scottish Government, with input from a wide range of partners across the public and private sectors.

2. Responding to this consultation paper

Responses should reach us by **28 August 2015**. Earlier responses would be welcome.

Please complete your response using the online system at Consult.scotland.gov.uk/cyberconsultation or send your response with the completed [Respondent Information Form](#) (See “Handling your Response” below) to:

Cyberresilience@scotland.gsi.gov.uk

Or:

Cyber Resilience Policy Team
Scottish Government
4th Floor
5 Atlantic Quay
150 Broomielaw
Glasgow
G2 8LU

If you have any queries contact the Cyber Policy Team on 0300 244 6832.

This consultation, and all other Scottish Government consultation exercises, can be viewed online on the consultation web pages of the Scottish Government website at <http://www.scotland.gov.uk/consultations>.

The Scottish Government has an email alert system for consultations <http://register.scotland.gov.uk>. This system allows stakeholders, individuals and organisations to register and receive a weekly email containing details of all new consultations (including web links). It complements, but in no way replaces, SG distribution lists, and is designed to allow stakeholders to keep up to date with all SG consultation activity, and therefore be alerted at the earliest opportunity to those of most interest.

Handling your response

We need to know how you wish your response to be handled and, in particular, whether you are happy for your response to be made public. Please complete the consultation online at Consult.scotland.gov.uk/cyberconsultation or complete and return the [Respondent Information Form](#) as this will ensure that we treat your

response appropriately. If you ask for your response not to be published we will regard it as confidential, and we will treat it accordingly.

All respondents should be aware that the Scottish Government are subject to the provisions of the Freedom of Information (Scotland) Act 2002 and would therefore have to consider any request made to it under the Act for information relating to responses made to this consultation exercise.

Next steps in the process

Where respondents have given permission for their response to be made public and after we have checked that they contain no potentially defamatory material, responses will be made available to the public in the Scottish Government Library. These will be made available to the public in the Scottish Government Library by and on the Scottish Government consultation web pages by 18 September 2015. You can make arrangements to view responses by contacting the SG Library on 0131 244 4552. Responses can be copied and sent to you, but a charge may be made for this service.

What happens next?

Following the closing date, all responses will be analysed and considered along with any other available evidence to help us reach a decision on the questions contained in the consultation. We will analyse responses to support the further development of the strategy, which we aim to be publish in November 2015.

Impact Assessments

This consultation will allow us to gather information and evidence to inform the development and subsequent publication of the Business Regulatory Impact Assessment, Equality Impact Assessment, Privacy Impact Assessment and Children's Rights and Wellbeing Impact Assessment.

Comments and complaints

If you have any comments about how this consultation exercise had been conducted, please send them to the contact details above.

3. Consultation Questions

Specific questions on which the Scottish Government is seeking views are listed below and are summarised on the [Respondent Information Form](#) at the end of this document. To aid our analysis it would be helpful if responses could be structured around these questions. However, we welcome contributions on any aspect of the draft strategy and consultees are free to provide additional comments, suggestions and information which they feel are not covered by this format.

Q1: Are the guiding principles right for this strategy? Are there any other principles that should be considered when continuing to develop the strategy?

Q2: Do you agree with the vision?

Q3: Do you agree with the three strategic outcomes? Are there additional outcomes that should be considered?

Q4: Do you think we are focusing on the right objectives? Are there additional key objectives that should be considered?

Q5: Do you agree with the main areas of focus for effective leadership and promoting collaboration? Are there other areas that should be considered?

Q6: Do you agree with the main areas of focus for raising awareness and ensuring effective communication? Are there other areas that should be considered?

Q7: Do you agree with the main areas of focus for developing education and skills in cyber resilience? Are there other areas that should be considered?

Q8: Do you agree with the main areas of focus for strengthening research and innovation? Are there other areas that should be considered?

Q9: Are there additional actions that will help us achieve making Scotland and its people more cyber resilient?

Q10: Do you think the monitoring and evaluation arrangements are sufficient?

Q11: Have you ever experienced cyber crime (see examples diagram on page 9?) If so, did you report it? Please provide details.

Q12: Would you be willing to share your experiences with us?

A message from the Deputy First Minister

We all want to see a Scotland where people feel confident online and can safely use the internet, where businesses can prosper, where our children are not exploited and where online public services are resilient as well as simple to use.

There can be little doubt that the internet and mobile technologies have transformed the way we all go about our business. The opportunities provided in this digital world are clear for all to see and experience.

However, our increasing reliance on online technologies makes us potentially more vulnerable to the criminals who seek to exploit these technological advancements for malicious purposes, whether that is online bullying, child sexual exploitation, the theft of intellectual property or the damage to critical infrastructure. The internet therefore brings great opportunities but with risks that we all increasingly need to be alive to. I want us all to minimise these risks and maximise the opportunities so that Scotland is seen as one of the best places to be on-line.

The 2014 *Programme for Government* signalled our intention to develop and bring forward a cyber resilience strategy that will take a positive approach to developing cyber resilience in Scotland, for the benefit of our people and our economy.

We are here to listen to what you have to say and this is your opportunity to give us your views. This is why we are launching this consultation. *A Cyber Resilience Strategy for Scotland: Safe, Secure and Prosperous Online* sets out a compelling vision to ensure that Scotland has the ability to resist and rapidly recover from cyber incidents to benefit from the economic and personal opportunities and advantages that online technologies provide. The focus is to position cyberspace as an enabler for individuals, industry, and the public sector.

This is something that government cannot do alone – we all have a stake in it. By working together, I strongly believe that we can make Scotland one of the safest places in the world to live and do business, ensuring our economy and our people reap the rewards of expanding digital opportunities.



A handwritten signature in black ink, which appears to read "John Swinney". The signature is written in a cursive style and is positioned below the portrait.

John Swinney
Deputy First Minister

2. Why do we need a cyber resilience strategy?

The digital age is transforming Scotland

The growth of the internet and online technologies offers speed, agility, efficiency and access that have transformed the way we do business, the way we spend our leisure time, the way our public services run and the way our national infrastructures operate.

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

Our businesses rely more and more on online connectivity and reap the benefits, thanks to widening trade partners, more innovation and greater competition. This in turn helps grow our economy.

Also, there is a huge potential for Scotland to meet the ever-growing global demand for cyber resilience and security professionals, goods and services. If Scotland does not seize these opportunities, we will be left behind.

Our public services are increasingly being provided online with the aim of improving access for all, reducing costs while improving operational performance. For example the future *mygov.scot* will be the online place for people in Scotland to access public services.

In our national infrastructure, Scotland relies more and more on online technologies to run the systems that heat our houses, provide fuel for our vehicles and ensure that our water is safe to drink. Linking our national infrastructures such as energy, telecommunications, and transport systems to the internet brings considerable benefits in terms of efficiency and innovative practice.

These important transformations will only continue as we enter the age of the “internet of things”.

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.

The Scottish Government has committed to delivering digital connectivity across the whole of Scotland by 2020. The *Digital Future Strategy* outlines the steps required to ensure Scotland is well placed to take full advantage of all the economic, social and environmental opportunities offered by the digital age.

- The estimate of Scotland's total sales conducted over computer networks in 2012 was £38bn¹
- In 2014, a third of the businesses expect internet sales to make up at least 20% or more of their total sales over the next 2-3 years²
- 92% of businesses in Scotland have broadband³
- The Scottish Household Survey 2012 shows that almost 80% of adults use the internet for personal use
- 65% of Scots are happy to shop online⁴

With these opportunities come new risks

Our increasing dependence on and use of cyberspace has brought new risks.

At the highest level of risk, cyberspace is now widely considered to be as strategically important for national security as defending attacks from land, sea and air. The UK's National Security Strategy⁵ places cyber attacks as a Tier 1 threat.

The malign use of cyberspace ranges across a spectrum: from script-kiddies⁶ testing skills against the security of systems, to criminals committing traditional crimes facilitated online, through to politically-motivated hacking and commercial and government espionage.

Consequences of cyber attacks	
Personal	Online crime has a clear impact on the lives of families in Scotland. As our use of online technology increases we are at more risk of becoming victims of criminal or unscrupulous behaviour. This can lead to a number of serious consequences including fraud or extortion, accidental disclosure of personal information, or being subject to forms of abuse including stalking, bullying and exploitation.
Organisational	Organisations of all sizes have information assets, such as databases of client details - crucial to their function and of value to cyber criminals. Cyber criminals often operate through stealth with businesses often failing to notice cyber attacks until some time after the initial compromise. Businesses may be reluctant to share news or information about their attack. Criminals focus on the easiest targets and we know that small and medium enterprises (SMEs) are particularly vulnerable.
Economic	The UK Government previously estimated the cost of cybercrime to the UK to be in excess of £27bn per annum, and the main loser – at a total estimated cost of £21bn – is UK business. In January 2015 GCHQ stated that 8 in every ten of the biggest British companies have suffered a serious cyber attack, costing the UK economy tens of millions of pounds annually.
National	There is the potential to damage Scotland's reputation as a safe place to live, work and trade, if, for instance, its infrastructure is attacked, is subject to hostile reconnaissance or its intellectual property is stolen.

¹ This is an estimate only and is intended to provide an indication of the scale of activity. It is based on UK-level data - adjusted for Scotland's share of UK employees in each sector

² <http://www.gov.scot/Resource/0047/00473602.pdf>

³ <http://www.gov.scot/Resource/0047/00472573.pdf>

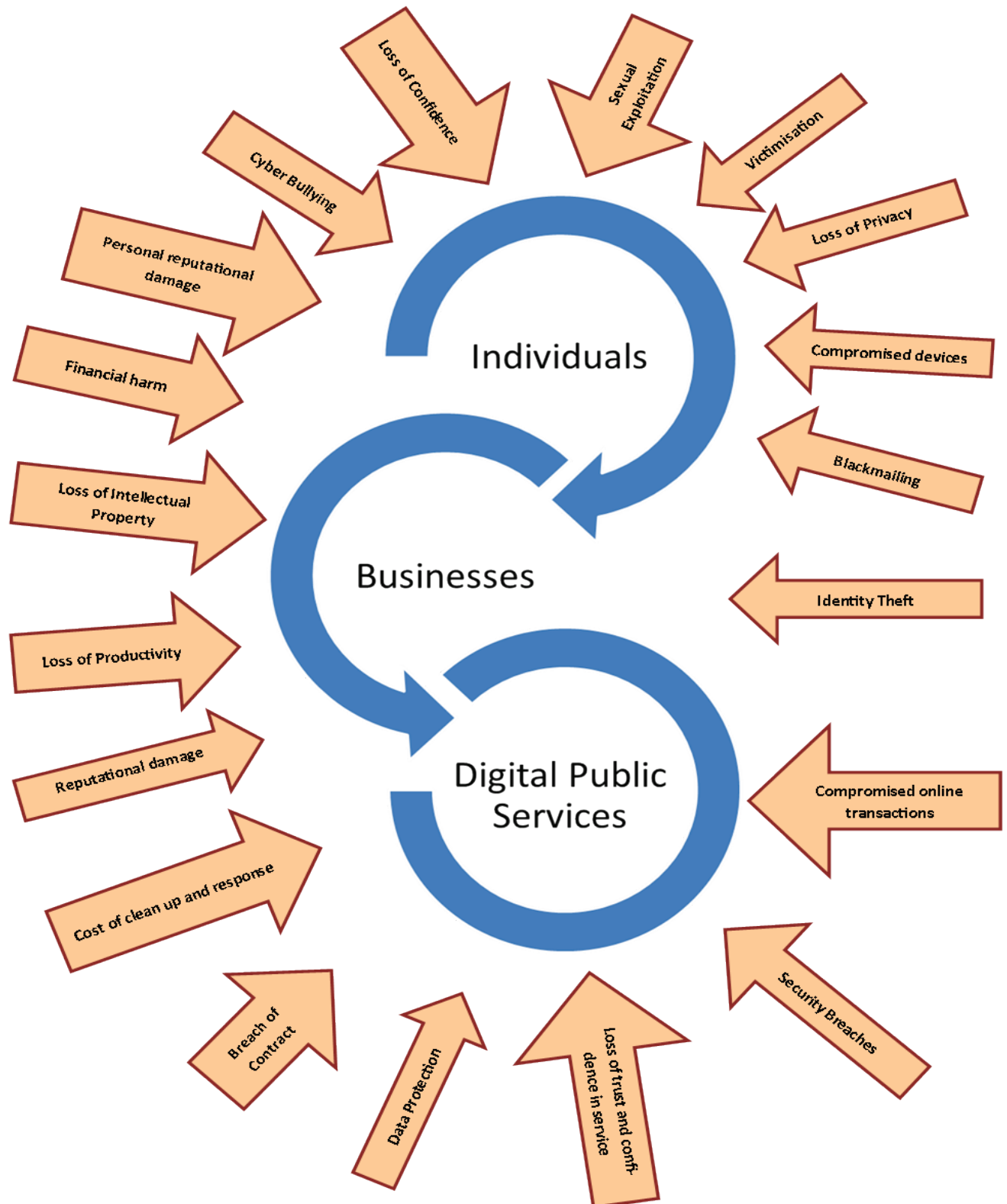
⁴ <http://www.scotlandsdigitalfuture.org/digital-participation>

⁵ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

⁶ An unskilled individual who uses scripts or programs developed by others to attack computer systems and networks, and deface websites

We need to be alert to the risks so that we can make the most of the opportunities. Cyber risks are constantly evolving and are here to stay, but as with other kinds of (non-cyber) risks, we need to acknowledge and address them.

Diagram: Types of cyber risks and cybercrime



3. What are the aims of the strategy?

Often other nations' cyber security strategies have primarily focused on systems and control measures for defence and security purposes. While this is extremely important, the most common risks are changing as our society becomes increasingly dependent on networked technologies and much of the risk comes from the individual.

This strategy: *A Cyber Resilience Strategy for Scotland: Safe, Secure and Prosperous Online* builds on the *UK Cyber Security Strategy: Protecting and Promoting the UK in a digital world*⁷. Our focus is on helping individuals and organisations to protect themselves from criminals and other malicious users of cyberspace. It recognises the particular requirements of Scotland, our institutions and our business community, for instance the enormous and distinct part small to medium sized businesses play in Scotland's economy⁸. We know that many small companies work from home and do not always have access to the latest skills and knowledge.

This strategy provides a current picture of the importance of cyber resilience for Scotland's citizens, businesses and public services. It outlines a vision and strategic outcomes, and sets the key areas for the Scottish Government and its partners to focus on.

Cyberspace is the complex environment that results from the interaction of people, software and services on the internet by means of the technological devices and networks connected to it. This environment does not exist in any physical form.

Cyber resilience is all about being confident in your own knowledge and how to keep your information and that of others safe. It is the actions or steps taken to mitigate and respond to threats from cyberspace (sometimes referred to as "cybercrime" or "cyber attacks"). It means being able to prepare for, adapt to, withstand and rapidly recover and learn from disruptions caused by cybercrime.

Cyber security is the protection of systems, networks, infrastructure and data in cyberspace

⁷ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

⁸ Small and Medium sized businesses account for 99.3% of the Scottish business landscape.

4. How can you help?

The strategy is for policy makers - at local and national level: it highlights the importance of cyber resilience across all relevant policy areas. It is dependent on and, in turn, supports many other strategies and programmes, such as Scotland's Economic Strategy⁹, Digital Future Strategy¹⁰, Digital Justice Strategy¹¹, Curriculum for Excellence¹², e-Health Strategy¹³, Equally Safe¹⁴ and the forthcoming Serious & Organised Crime Strategy and the Resilience Strategy. It is a strategic document that all policy makers can refer to when developing and implementing policies/strategies/initiatives - no matter what the policy area, as cyber is present in every aspect of society.

It is for stakeholders and delivery partners who engage with individuals and families in a range of settings including Police Scotland, Education Scotland, Skills Development Scotland, schools, local authorities, Scottish Enterprise, the Scottish Business Resilience Centre, Skills Development Scotland, colleges and universities and Highlands and Islands Enterprise.

It is for the private sector, for businesses, industry and enterprises. It provides direction for organisations, employers and employees to face the cyber challenge to become stronger and more successful online.

It is for the third sector. Third sector organisations are well placed to support families and communities to become more cyber resilient.

Once we have heard back from all those interested, a detailed action plan will follow this strategy to help everyone involved to develop their own action plans which will, in turn, contribute to making Scotland and its people more cyber resilient.

⁹ <http://www.gov.scot/Publications/2015/03/5984>

¹⁰ <http://www.gov.scot/resource/doc/981/0114237.pdf>

¹¹ <http://www.gov.scot/Resource/0045/00458026.pdf>

¹² <http://www.educationscotland.gov.uk/learningandteaching/thecurriculum/>

¹³ <http://www.gov.scot/Publications/2012/11/7663>

¹⁴ <http://www.gov.scot/Resource/0045/00454152.pdf>

5. What principles is this strategy built on?

National leadership: The scale and complexity of the cyber resilience challenge requires strong and committed national leadership. Central to delivering this strategy is the adoption of an approach which involves collaborative leadership and a focus on the delivery of better outcomes.

Shared responsibilities: We are all users of technology. Therefore we all have a role to play in taking steps to protect ourselves and our organisations.

Working together: All parties have a role in helping to create a safer online environment, being open to sharing knowledge, skills and effective practice.

Protecting Scotland's values: By pursuing this cyber resilience strategy to enhance safe, secure and prosperous use of online technologies, we will protect Scots' values including preserving our right to privacy and protecting the most vulnerable in our society.

1) CONSULTATION QUESTION

Are these the right guiding principles for this strategy?

Are there any other principles that should be considered when continuing to develop this strategy?

6. What is our vision?

In the first half of 2015, the Scottish Government brought together a Strategic Working Group to agree a vision and strategic outcomes for a more cyber resilient Scotland.

Our vision is for a cyber resilient Scotland that is safe, secure and prosperous.

2) CONSULTATION QUESTION

Do you agree with the vision?

We will turn this vision into reality by achieving the following **three strategic outcomes**:

- 1. Our citizens are informed, empowered, safe and confident in using online technologies.**
- 2. Our businesses are resilient and can trade and prosper securely online.**
- 3. We all have confidence in the resilience of our digital public services.**

By achieving these outcomes we will contribute positively to many of the National Outcomes in the National Performance Framework¹⁵, and 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

This strategy also plays its part in achieving the ambitions of *Scotland's Economic Strategy* by helping Scottish businesses succeed at a global level, increasing competitiveness, and tackling inequality through helping all people to use the internet safely and securely.

3) CONSULTATION QUESTION

Do you agree with the three strategic outcomes?

Are there additional outcomes that should be considered? If yes, what are they and why?

¹⁵ <http://www.gov.scot/About/Performance/scotPerforms>

7. What can we all do to become more cyber resilient?

We are living in a digital world where activities happen at great speed and we all require to develop a culture of cyber resilience as the norm.

The first thing to do is accept the potential risk and become more cyber aware. The reality is that around 80% of cybercrime can be prevented by simply getting the basics right¹⁶. It is not all about high level controls, understanding the technology and buying in expensive cyber security software or professional advice. We all have a stake in becoming more resilient. In doing so, we will enjoy the benefits that online technologies present.

Becoming more cyber resilient requires a sustained, collective effort. We will focus on four key objectives:

- 1. Provide effective leadership and promote collaboration**
- 2. Raise awareness and ensure effective communication**
- 3. Develop education and skills in cyber resilience**
- 4. Strengthen research and innovation**

None of these objectives is more important than another. In fact, they are mutually dependent to ensure success of this strategy.

4) CONSULTATION QUESTION

Do you think these are the right objectives to focus on?

Are there additional objectives that should be considered?

¹⁶ GCHQ, Countering the cyber threat to business, Spring 2013

Objective 1: Provide effective leadership and promote collaboration

The Scottish Government has a strong track record in successfully leading work on national resilience through a collaborative approach. We will take this same approach to cyber resilience. At present, we do not propose legislation or regulation. Instead, successful implementation of this strategy will be through involving partners and stakeholders at every stage of planning and development.

While many aspects of protecting Scotland's critical national infrastructure are reserved to the UK Government, the Scottish Government will, where it has powers to do so, coordinate a collaborative approach to manage and ensure that critical services remain available despite cyber attacks.

No one individual or organisation can meet this challenge by itself. A collaborative, multi-stakeholder approach must be taken within and across sectors including government, industry, commerce and academia. Even industry competitors must become partners to help promote the safe use of the internet and digital technologies and to share current information.

Public Bodies becoming more cyber resilient

The Scottish Government has worked closely with a number of public bodies in Scotland including all local authorities to implement a common set of technical, physical and procedural security measures to provide a level of mutual trust for the communication and processing of public sector data. Initiatives such as the UK 'Cyber Essentials' scheme and the '10 Steps to Cyber Security' are being adopted and are helping the public sector in Scotland align itself with best practice whilst equipping organisations with the knowledge they need to defend against common cyber-attacks.

In recognition of the rise in cyber-attacks, the annual Holyrood Connect awards celebrating public sector excellence in ICT in Scotland, now in its 3rd year, have introduced the 'Connect Security' award.



It is important the Scottish Government models best practice in cyber resilience for the rest of the public sector – other government agencies, local authorities etc. We will therefore, continue to enhance cyber resilience within our online services. While we do not anticipate legislating, we will hold to account, other public public bodies for the resilience of their online services. Main areas of focus:

- The Scottish Government to set up and lead a national strategic implementation group to implement, monitor and evaluate the impact of this strategy
- The Scottish Government to be at the forefront of providing safe and secure services, and sharing their knowledge with other organisations
- Collaborating with partners, the Scottish Government will lead and coordinate efforts to develop national cyber resilience
- Ministers and their officials continue to raise the profile of the importance of cyber resilience across a range of policy areas
- Ministers report on the Government’s progress in building a culture of cyber resilience and good practice across the Scottish Government and its agencies
- The standards of cyber resilience adopted by the Scottish Government’s online services – and those of other public agencies - will be available to service users.

5) CONSULTATION QUESTION

Do you agree with the main areas of focus for effective leadership and promoting collaboration?

Are there any other areas that should be considered?

Objective 2: Raise awareness and ensure effective communication

Criminals make use of the internet either through weaknesses in system coding or more commonly by exploiting human behaviour. Human beings are therefore the primary cyber risk, often due to lack of understanding and sometimes naïve online behaviour. It is vital individuals and businesses build resilience and that we all foster a culture of cyber awareness and preparedness.

Trusted networking between businesses and government will ensure the usefulness of sharing sensitive information on cyber threats, vulnerabilities and their potential consequences.



Online Code of Conduct: 10 tips for staying safe online



www.getsafeonline.org

PUT A PIN ON IT

Whether it's a phone, website or a social media account, your first line of defence is a **PIN** or **Password**. Never use the same password, make sure it is hard to guess (don't use your pet's name, your birthday or your favourite football team) and never share your passwords with anyone.



BE SOFTWARE SAVVY

Protect all your devices with anti-virus software and make sure you regularly install updates to any programs or apps, as they often include improved security settings.



LOOK FOR THE PADLOCK

When shopping or banking online always check there is a padlock symbol in the web browser window when you have logged in or registered, and that the web address begins with **'https://'**. The 's' stands for 'secure'.



POST IN HASTE, REPENT AT LEISURE

What goes online stays online so never say anything that could hurt, anger or endanger yourself or someone else.



SECURE THE WIFI

Make sure your home WiFi is protected with a strong password that only you and your family know. When out and about never use a hotspot that may be unsecured, especially when what you're doing is personal or private.



KEEP IT PRIVATE

Check the privacy settings on all of your social media accounts so that only the people you want to share your information with can see it.



LOG-OUT/LOG-OFF

Always make sure you log out of your accounts when you've finished with them and log off a computer when you've finished using it.



BID SMARTLY

When using an auction site, make sure you never transfer any money directly to a bank account or hand over any personal details. If you're thinking of making a big purchase like a car, or finding somewhere to live, always make sure it exists and is genuine.



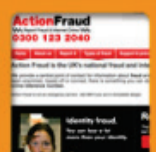
MANAGE YOUR MESSAGES

Never open or forward a suspicious looking email, or respond to a social media message from someone you don't know.



REPORT IT

If you are a victim of online fraud, report it to www.actionfraud.police.uk, this way we can all help to make the internet a safer place.



Main areas of focus:

- The Scottish Government alongside its partners to co-ordinate general awareness raising activity to promote a culture of cyber resilience among all Scottish citizens, including promoting the national online safety websites Get Safe Online¹⁷ and E-crime Scotland¹⁸ across Scotland
- Stakeholders and partners to implement audience-specific awareness raising activity, targeted at employees, educators, leaders and board members
- Working alongside the UK Government, the Scottish Government and partners from across the business world to form a network to share information about online threats and vulnerabilities.
- Industry professionals to develop and promote best practice in cyber resilience

6) CONSULTATION QUESTION

Do you agree with the main areas of focus for raising awareness and ensuring effective communication?

Are there any other areas that should be considered?

¹⁷<https://www.getsafeonline.org/>

¹⁸<https://www.ecrimescotland.org.uk/>

Objective 3: Develop education and skills in cyber resilience

We all should be able to exploit digital opportunities for our personal fulfilment and professional development, whilst knowing how to protect ourselves from risks. Education and skills are an important part of the cyber resilience agenda.

Cyber resilience skills for every citizen

Every child, young person and adult must have cyber skills for learning, life and work.

In addition to public awareness raising campaigns, the curriculum needs to develop skills which will allow learners to become more cyber resilient, and learning materials and guidance needs to be available for all educators, including those in non-formal learning contexts, such as youth work and the voluntary sector.

Core cyber competence for all professions

Many jobs already feature or have some connection to digital technology and this will only intensify. Whether it's a healthcare worker entering or accessing patient data, a maintenance professional managing a WiFi-enabled heating control system, or a farmer using satellite technology to plot optimum crop yields – any technology in cyber space may be vulnerable to malicious or accidental damage. Therefore, training in all vocational areas, not just digital occupations, need to include specific learning outcomes relating to cyber resilience.

Schools and Police Scotland working together for a safe online experience



First year pupils at Kyle Academy in Ayr take part in a 12-week course on Cyber Security.

The course, 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

POLICE
SCOTLAND

Building an effective workforce of cyber security professionals in Scotland

It is crucial that we have technical expertise in cyber security, and that we support the growth of a world-leading professional sector in cyber security work. For Scotland's continued economic growth we must ensure professional learning opportunities are available to support the development of this rapidly growing economic sector.

Main areas of focus:

- The Scottish Government and its partners promote the development and delivery of cyber resilience education in early learning and childcare settings, schools, colleges, universities and other learning settings
- Business partners build cyber resilience capabilities within workforces
- Scottish Enterprise and other business partners help develop the cyber security and resilience goods and services industry in Scotland

7) CONSULTATION QUESTION

Do you agree with the main areas of focus for developing education and skills in cyber resilience?

Are there any other areas that should be considered?

Objective 4: Strengthen research and innovation

Cyberspace is continuously evolving and it is important that we keep up with this change.

The true size and scale of cyber related criminality, and the cost to people and organisations, is challenging to measure for a number of reasons, including lack of clarity on when, what, where, who and how to report such issues. It is important that the recording of cybercrimes is developed in such a way that can help create a baseline for measurement and help decide our priorities.

Scottish researchers should be at the forefront of building knowledge and intelligence. Universities and colleges should work together with industry user groups and the Scottish Government. Scottish participation in international forums should be encouraged. The Scottish Government with the help of Police Scotland should be able to articulate the cost to our economy as a result of cybercrime and limited cyber resilience among our citizens and businesses.

Scottish businesses, especially those in high technology sectors need to protect their intellectual property. Scottish business organisations, including the enterprise companies, should be at the leading edge of collaborative measures to enhance the cyber resilience of key sectors and enterprises.

The UK Government has set a national target of exporting £2 billion of cyber security goods and services annually¹⁹. Scotland's world beating university research combined with our entrepreneurial expertise should create a steady stream of start-up companies in this sector creating a long term economic benefits.

Main areas of focus:

- The Scottish Government, Police Scotland and other partners progress with research to baseline the cost of cybercrime to Scotland
- Partners undertake and share research on understanding “what works” in preventing cybercrime, using knowledge from local, national and international angles
- Partners work together to target funding for cyber resilience research
- Enterprise funding is targeted at innovative methods to support the cyber resilience of individual or groups of enterprises.

8) CONSULTATION QUESTION

Do you agree with the main areas of focus for strengthening research and innovation?

Are there any other areas that should be considered?

¹⁹ <http://www.contracts.mod.uk/features/uk-cyber-security-strategy-the-next-big-export/>

8. How will we use this strategy to achieve real change?

Implementation

This high level strategy for cyber resilience in Scotland is the overarching driver for change.

For each of the outcomes, the Scottish Government and its partners are developing a detailed action plan setting out the short, medium and long term activities. These specific measures will be published in early 2016. Within this action plan there will be practical activities, projects and improvements to support individuals and organisations to become more cyber resilient, as well as steps to build up the cyber security goods and services sector in Scotland.

Please help us to address this task together. It is essential that stakeholders commit to successfully implementing the strategy and associated action plan. Successful implementation of this strategy will require the input and the action from every part of Scottish society – communities, small businesses, large organisations, local authorities, third sector organisations, academia, law enforcement and central government and, of course, citizens themselves.

9) CONSULTATION QUESTION

Are there actions that will help us achieve making Scotland and its people more cyber resilient?

9. How will we know if we are succeeding?

The Scottish Government will be asking stakeholders to share their action plans and keep track of milestones and progress on an annual basis. This will help to provide regular updates to the national strategic implementation group (see Objective 1).

Given the rapid technological changes and local, national and international developments in this area, it is vital to capture learning and share effective practice.

We will know we are succeeding if we are able to see a step-change in the cyber resilience of citizens, businesses, organisations and government. Scotland will:

- ✓ be a place where individuals and families can make the most of the internet safely
- ✓ be a place where businesses can operate and trade with minimal risk
- ✓ have an excellent global reputation for being a secure place to set up businesses and to trade with
- ✓ have trusted and effective online public services
- ✓ ensure that critical emergency, infrastructure and key services such as financial services can continue to work effectively in the face of a cyber attack
- ✓ capitalise on, and grow, a cyber security goods and services industry to meet the demand of the rest of the world

10) CONSULTATION QUESTION

Do you think these monitoring and evaluating arrangements are sufficient? If not, what arrangements would you like to see?

11) CONSULTATION QUESTION

Have you ever experienced cyber crime (see diagram on page 11)? If so, did you report it? Please provide details.

12) CONSULTATION QUESTION

Would you be willing to share your experiences with us?

Annex A

Glossary

Cybercrime: an umbrella term used to describe two distinct, but closely related criminal activities: cyber-dependent and cyber-enabled crimes. Cyber-dependent crimes are offences that can only be committed by using a computer, computer networks, or other forms of ICT e.g. malicious software, hacking. Cyber-enabled crimes are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT e.g. fraud, theft.

Cyber resilience: being able to prepare for, adapt to, withstand and rapidly recover and learn from disruptions from cyber criminality/attacks. To do this, people need to develop the skills, knowledge and understanding of the risk, in whatever setting they find themselves in, and then take the necessary steps to prepare for and respond to such events.

Cyber security: the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets

Cyberspace: Cyberspace is the complex environment that results from the interaction of people, software and services on the Internet by means of the technology devices and networks connected to it, which does not exist in any physical form.

Hacking: breaking into computer systems

Annex B Cyber Resilience Strategy



RESPONDENT INFORMATION FORM

Please Note this form **must** be returned with your response to ensure that we handle your response appropriately

1. Name/Organisation

Organisation Name

Title Mr Ms Mrs Miss Dr *Please tick as appropriate*

Surname

Forename

2. Postal Address

<input type="text"/>		
<input type="text"/>		
<input type="text"/>		
<input type="text"/>		
Postcode	Phone	Email

3. Permissions - I am responding as...

Individual / **Group/Organisation**
Please tick as appropriate

(a) Do you agree to your response being made available to the public (in Scottish Government library and/or on the Scottish Government web site)?

Please tick as appropriate Yes No

(b) Where confidentiality is not requested, we will make your responses available to the public on the following basis

Please tick ONE of the following boxes

Yes, make my response, name and address all available

or

Yes, make my response available, but not my name and address

or

Yes, make my response and name available, but not my address

(c) The name and address of your organisation **will be** made available to the public (in the Scottish Government library and/or on the Scottish Government web site).

Are you content for your **response** to be made available?

Please tick as appropriate Yes No

(d) We will share your response internally with other Scottish Government policy teams who may be addressing the issues you discuss. They may wish to contact you again in the future, but we require your permission to do so. Are you content for Scottish Government to contact you again in relation to this consultation exercise?

Please tick as appropriate Yes No

CONSULTATION QUESTIONS

National leadership; Shared responsibilities; Working together; Protecting Scotland's values

Q1 Are the guiding principles right for this strategy?

Yes No

Are there any other principles that should be considered when continuing to develop the strategy?

Comments

Our vision is for a cyber resilient Scotland that is safe, secure and prosperous

Q2 Do you agree with the vision?

Yes No

Strategic Outcomes:

- 1. Our citizens are informed, empowered, safe and confident in using online technologies*
- 2. Our businesses are resilient and can trade and prosper securely online*
- 3. We all have confidence in the resilience of our digital public services*

Q3 Do you agree with the strategic outcomes?

Yes No

Are there additional outcomes that should be considered?

Comments

Key Objectives:

- 1. Provide effective leadership and promote collaboration*
- 2. Raise awareness and ensure effective communication*
- 3. Develop education and skills in cyber resilience*
- 4. Strengthen research and innovation*

Q4 Do you think these are the right objectives to focus on?

Yes No

Are there additional key objectives that should be considered?

Comments

Objective 1: Provide effective leadership and promote collaboration

Main areas of focus:

- *The Scottish Government to set up and lead a national strategic implementation group to implement, monitor and evaluate the impact of this strategy*
- *The Scottish Government to be at the forefront of providing safe and secure services, and sharing their knowledge with other organisations*
- *Collaborating with partners, the Scottish Government will lead and coordinate efforts to develop national cyber resilience*
- *Ministers and their officials continue to raise the profile of the importance of cyber resilience across a range of policy areas*
- *Ministers report on the Government's progress in building a culture of cyber resilience and good practice across the Scottish Government and its agencies*
- *The standards of cyber resilience adopted by the Scottish Government's on-line services – and those of other public agencies - will be available to service users.*

Q5 Do you agree with the main areas of focus for effective leadership and collaboration?

Yes No

Are there other areas that should be considered?

Comments

Objective 2: Raise awareness and ensure effective communication

Main areas of focus:

- *The Scottish Government alongside its partners to co-ordinate general awareness raising activity to promote a culture of cyber resilience among all Scottish citizens, including promoting the national online safety websites Get Safe Online and E-crime Scotland across Scotland*
- *Stakeholders and partners to implement audience-specific awareness raising activity - targeted at employees, educators, leaders and board members*
- *Working alongside the UK Government, the Scottish Government and partners from across the business world to form a network to share information about online threats and vulnerabilities*
- *Industry professionals develop and promote best practice in cyber resilience*

Q6 Do you agree with the main areas of focus for raising awareness and ensure effective communication?

Yes No

Are there other areas that should be considered?

Comments

Objective 3: Develop education and skills in cyber resilience

Main areas of focus:

- *The Scottish Government and its partners promote the development and delivery of cyber resilience education in early learning and childcare settings, schools, colleges, universities and other learning settings*
- *Business partners build cyber resilience capabilities within workforces*
- *Scottish Enterprise and other business partners help develop the cyber security and resilience goods and services industry in Scotland*

Q7 Do you agree with the main areas of focus for developing education and skills in cyber resilience?

Yes No

Are there other areas that should be considered?

Comments

Objective 4: Strengthen research and innovation

Main areas of focus:

- *The Scottish Government, Police Scotland and partners progress with research to baseline the cost of cybercrime to Scotland*
- *Partners undertake and share research on understanding “what works” in preventing cybercrime, using knowledge from local, national and international angles*
- *Partners work together to target funding for cyber resilience research*
- *Enterprise funding is targeted at innovative methods to support the cyber resilience of individual or groups of enterprises*

Q8 Do you agree with the main areas of focus for strengthening research and innovation?

Yes No

Are there other areas that should be considered?

Comments

How will we use the strategy to achieve real change?

For each of the outcomes, the Scottish Government and its partners are developing a detailed action plan setting out the short, medium and long term activities. These specific measures will be published in early 2016. Within this action plan there will be practical activities, projects and improvements to support individuals and organisations to become more cyber resilient, as well as steps to build up the cyber security goods and services sector in Scotland.

Q9 Are there additional actions that will help us achieve making Scotland and its people more cyber resilient?

Comments

How will we know if we are succeeding?

The Scottish Government will be asking stakeholders to share their action plans and keep track of milestones and progress on an annual basis. This will help to provide regular annual updates to the national strategic implementation group.

Q10 Do you think the monitoring and evaluation arrangements are sufficient?

Yes No

If not, what arrangements would you like to see?

Comments

Q11 Have you ever experienced cyber crime (see examples on page 16)?

Yes No

If so, did you report it? Please provide details.

Comments

Q12 Would you be willing to share your experiences with us?

Yes No



© 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

ISBN: 978-1-78544-391-6 (web only)

Published by The Scottish Government, June 2015

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS49679 (06/15)

W W W . G O V . S C O T