www.gov.scot/cyberresilience

Scottish Government
Riaghaltas na h-Alba
gov.scot

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

CYBER RESILIENCE – THE ECONOMIC OPPORTUNITY

KEY ACTIONS 2018-21

FOREWORDS

Digital technologies offer huge opportunities for Scotland as a modern, progressive and economically successful nation.

Our citizens, businesses, charities and public services are making increasing use of these technologies to innovate and play an active role in our society and economy.

New ways of connecting and communicating are helping to boost productivity and increase access to a global marketplace worth billions of pounds. Growth in digital trade offers exciting opportunities to increase Scotland's economic prosperity.

Scotland's digital strategy, Realising Scotland's full potential in a digital world, sets out how we will make sure that digital is at the heart of everything we do – how we deliver inclusive economic growth, reform our public service and prepare our children for the workplace of the future.

In short, digital is fast becoming one of the foundations upon which our modern society and economy are built.

We believe it is vital that those foundations are safe and secure.

As our citizens and organisations carry out more digital transactions and share more information online, so the risks to our data, intellectual property, finances and corporate reputations become greater.

By taking action to tackle these risks, and to ensure the fundamental safety and resilience of our digital activity against cyber threats, we can ensure a sound underpinning for our digital economy and society.

In 2015 we launched Scotland's cyber resilience strategy, Safe, Secure and Prosperous, which sets out a commitment to work towards making Scotland a world-leading nation in cyber resilience.

Since then, to help realise that ambition, we have published and begun to implement action plans in the key areas of learning and skills and public, private and third sector cyber resilience.

This economic opportunity action plan, the fifth in a series of five, has been developed in partnership with our enterprise agencies, the National Cyber Resilience Leaders' Board, the private sector and academia. It sets out the key practical steps we and our partners will take collectively to grow Scotland's cyber security industry, encourage the development of innovative cyber security research and deliver world-leading cyber security goods and services over the period to 2021.

Our collective aim is to put Scotland in a position to reap the economic benefits that the ever-growing global demand for cyber security goods and services will bring.

We believe that Scotland's global reputation for cyber resilience has the potential to be a determinant of future economic success. We look forward to working closely with the private sector, civil society and academia to make Scotland a prosperous and cyber resilient nation.

John Swinney

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

D Mackay

Derek Mackay, MSP
Cabinet Secretary for Finance, Economy and Fair Work

In a world where digital connectivity is ubiquitous and increasing, the importance of cyber resilience has never been greater. Demand for robust cyber security products and services is rising, with the global cyber security market expected to grow to over $144 billion over the next five years .

Scotland already has a head start in this area, with a rapidly evolving cluster of innovative cyber security companies, world class academic expertise and an agile ecosystem that allows us to capitalise on our complementary strengths across the digital space in areas such as Fintech and data. What is imperative now is that we do everything in our power to create the right conditions for this cyber cluster to grow and thrive, rapidly and sustainably.

What stands out for me about this plan is that it is intimately linked to the needs of industry, both in its development and ongoing delivery, and will require a truly collaborative effort if it is to succeed.
I value any opportunity where we can join up our efforts to deliver greater impact, and this plan is a fantastic starting point to allow that to happen. It is just a starting point though – now the real work begins, and I'm looking forward to seeing the contribution Scottish Enterprise can make within this partnership. Ultimately, if we succeed, the actions in this plan will not only support the growth of Scotland's cyber security cluster, but also have a direct contribution to that far broader aim of cementing Scotland's position as a secure place to live, work and do business.

Stephen Dunlop

Steve Dunlop
Chief Executive, Scottish Enterprise

CONTENTS

EXECUTIVE SUMMARY

1

1 EXECUTIVE SUMMARY

1.1 It has never been more important to be cyber resilient. Digital technologies bring enormous opportunities for Scotland – but also new threats and vulnerabilities. The global cyber attack on 12 May 2017, which affected more than 150 countries worldwide and impacted negatively on the NHS in Scotland and England, underlined the seriousness of the cyber threat. The increasing focus on privacy and ethics, including legislative changes such as the new General Data Protection Regulation and the NIS Directive[1], reinforces the importance of ensuring cyber security for digital services that handle citizens' personal data, and the protection of our essential services and national infrastructure.

1.2 The National Cyber Resilience Leaders' Board (NCRLB) and the Scottish Government believe that Scotland can become a world-leading nation in cyber resilience. Scotland has the capability to develop and supply world-leading research, goods and services at a time where domestic and global demand for cyber resilience is increasing.

1.3 This plan refers to this growing capability as "a cyber cluster" – the emergence of a new cluster of economic activity that creates a critical mass of competitive success, based on our technological, business and academic capabilities in this field. In the past, the term "cluster" often referred to highly concentrated or collocated groups of businesses, researchers and supporting institutions-all focused on a single market opportunity. This plan applies a broader, more up-to-date, interpretation of the cluster concept, to recognise the fact that Scotland has the characteristics of a geographically concentrated space, even when activities are spread across the whole of Scotland.

1.4 The focus of this plan is on creating the right conditions for Scotland's cyber security supply-side cluster to grow and thrive. It sets out actions that the Scottish Government and key partners will take during 2018-21 to ensure Scotland takes full advantage of these economic growth opportunities. It has been produced by the NCRLB and its economic opportunity sub-group, working in partnership with the Scottish Government, Scottish Enterprise, and Highlands and Islands Enterprise, and with input from other partners including academia and the private sector.

1.5 The aims of this action plan are to develop:

- the **right market conditions** to encourage and support the continued emergence of the cyber security business community in Scotland;
- the **right academic research capability and capacity** to support and grow cyber security business innovation in Scotland;
- the **right cluster management arrangements** to ensure the approach is coordinated and has impact;
- the **right supporting institutions** to stimulate innovation and renewal within the cluster; and
- the **right brand** to help promote Scotland's cyber security cluster in the UK and internationally, grow cluster exports and reflect Scotland's emerging position as the place to be for researching, developing and supplying cyber security goods and services.

[1] https://www.ncsc.gov.uk/guidance/introduction-nis-directive

This plan:

- Describes the **actions** that are required to achieve these aims;
- Assigns **ownership** of the actions to lead partners; and
- Sets out high-level **monitoring and evaluation proposals** that will allow us to determine progress towards realising our ambition.

1.6 The cluster is complex and consists of many parts. As well as core supply-side companies and their supply chains, it includes academia, researchers and research groups, and various supporting institutions. It is subject to environmental factors such as skills availability, legislation and government support. To ensure it functions coherently, a coordinated approach is essential. Overall coordination of this action plan will be led by the Scottish Government, working in close partnership with its enterprise and skills agencies, the NCRLB, Scottish Development International, Scottish industry and academia, and other Scottish stakeholders. It will also require strong links both within the UK (including the National Cyber Security Centre (NCSC), the National Crime Agency (NCA) and the UK Government's Department for International Trade (DIT), and internationally.

1.7 This plan is focused on creating the right conditions to support supply-side cluster growth. As the cluster evolves, so the actions required to support growth may change. Therefore, we will regularly review the actions and their impact through a process of monitoring and evaluation.

1.8 This plan contributes to the broader ambition set out in our national strategy for Scotland to become fundamentally cyber resilient. The Scottish Government and the NCRLB have developed other, linked, action plans for the public, private and third sectors, and for learning and skills, to achieve this. The outcomes of these action plans together will be complementary and reinforcing.

1.9 This plan contributes to progressing the priorities set out in Scotland's Economic Strategy[2], including:

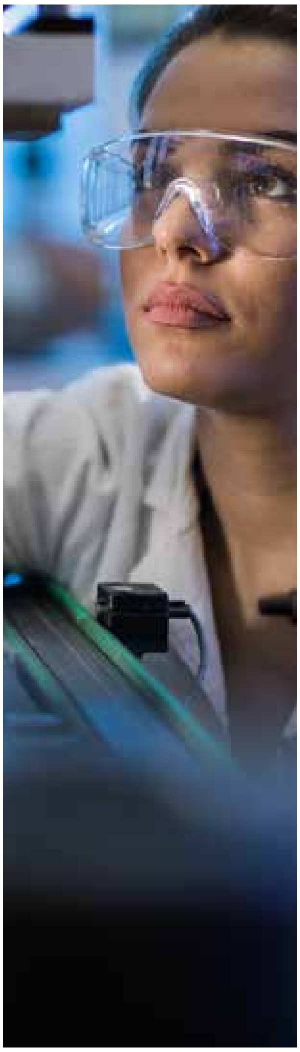
– promoting inclusive growth;

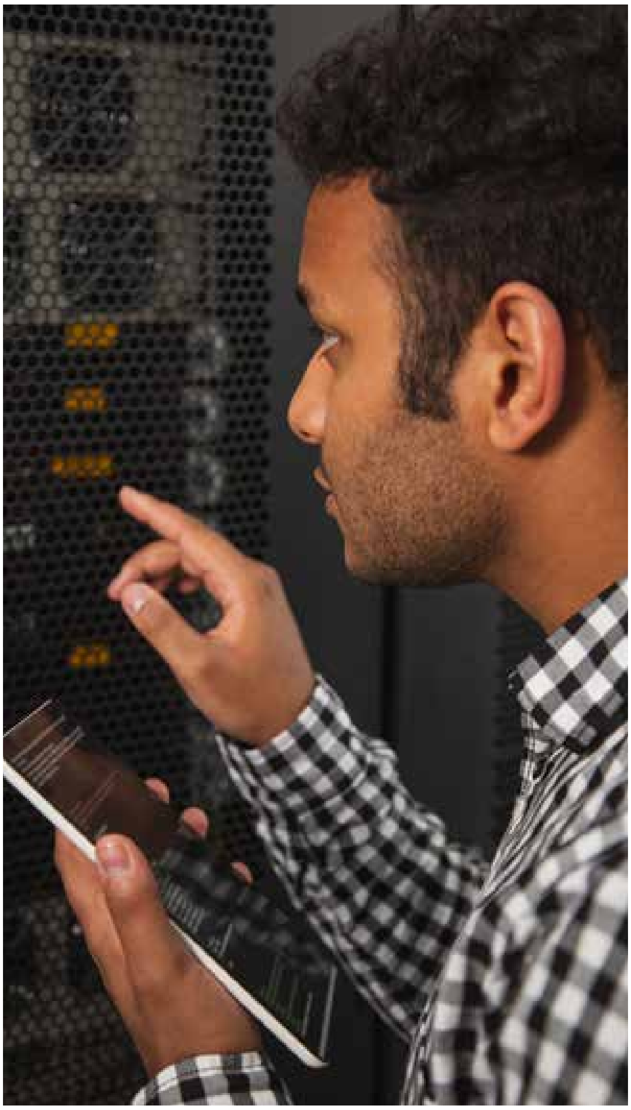
– fostering a culture of innovation and investment; and

– promoting Scotland on the international stage to boost trade and investment, influence and networks.

[2] https://beta.gov.scot/publications/scotlands-economic-strategy/

KEY ACTIONS





2

2 KEY ACTIONS

These are the key actions that the Scottish Government and its partners will take in support of the plan's objectives, through to 2021:

Action A1:

The Scottish Government, through an ongoing commitment to all five cyber action plans[3], will continue to clearly state and demonstrate its ambition to make Scotland a world-leading nation in cyber resilience, sending strong long-term demand signals to the supply side that they can be confident in their own expansion. The Scottish Government will play a key role in proactively engaging in, and influencing policy development at Scottish, UK and EU levels to ensure there is an effective voice representing Scottish cyber security companies and interests. This includes engaging with the UK Government as it develops a royal charter body to support professionalisation and collaboration across the UK. This activity will be ongoing.

Action A2:

The Scottish Government will work in partnership with Scottish Enterprise, Highlands and Islands Enterprise and other key partners to encourage the ongoing development of innovative solutions to public and private sector challenges relating to cyber resilience. This will include launching calls to industry through mechanisms such Civtech, CAN DO, or Open Innovation Challenges. The first challenge will be launched in 2018.

Action A3:

The Scottish Government will work in partnership with Scotland's academic institutions to encourage growth in world-leading research, innovation and skills to stimulate market needs and create economic impact. This activity will be ongoing.

Action A4:

On an ongoing basis, the Scottish Government will support opportunities for industry and academic experts to contribute to future cyber resilience policy development and thought-leadership at the Scottish, UK and EU levels. In the immediate term, the Scottish Government will commission the collaboration of universities who make up the Scottish Informatics and Computer Science Alliance (SICSA) Cyber Nexus to work with industry and other partners to produce a research piece into the concept of digital communications infrastructure in Scotland as a "fifth utility". This will consider the current and expected future "state of the art", and the extent to which Scotland could achieve a competitive advantage by driving forward change in this area using existing or new powers. The findings of this research, to be delivered by summer 2019, will help inform wider policy development in respect of "secure by design". This activity will be ongoing.

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

Action B1:

Scotland has a growing capability and global visibility in cyber security research, innovation and skills benefiting the sector. The Scottish Government and the collaborative of universities who make up the SICSA will build on the current government-funded SICSA programme of work to support academic institutions to expand this research. This work will aim to be of sufficient scale to attract and retain at least one globally renowned academic, provide for long-term facilities, and nurture junior research talent. It will also explore new ways of working that could better support the integration of academic ideas and expertise with the medium–to-long-term needs of industry. This action will be ongoing.

Action B2:

The Scottish Government will continue to work with the Scottish Funding Council to strengthen the requirements for cyber security research to be included within our university and college outcome agreements. This action will be ongoing.

Action B3:

The Scottish Government and its enterprise and skills agencies will continue to clearly state their support for the creation of a cyber-focused Centre for Doctoral Training in Scotland, and will work with SICSA, universities and industry to explore practical routes that all sectors could use to engage with, or support such a programme – for example through the provision of data. This action will be ongoing.

Action C1:

Scottish Enterprise will work with the Scottish Government and other key partners to establish a cluster management function for cyber within an accredited Cluster Management Organisation (CMO), with enough resource, capacity and capability to match the ambition of developing a globally relevant cyber security cyber security cluster. This will include steps to help the CMO achieve EU accreditation standards to agreed levels within a realistic timeframe. The CMO will be expected to participate in appropriate national advisory forums, work closely with partners to determine how best Scotland can benefit from UK wide industry initiatives emanating from the UK Government and NCSC, and encourage the development of networks, coherence and partnership working, particularly with other aligned clusters such as Fintech. The CMO will initially be established by autumn 2018.

Action D1:

The CMO, Scotland's enterprise agencies, and the Scottish Government will work together to develop a comprehensive shared understanding of Scotland's cyber security landscape. This will include identifying our strengths (in both a UK and global context), mapping out the current picture in terms of the various hubs and centres of expertise that exist across Scotland, and understanding the effectiveness of existing models and mechanisms for innovation, support and coordination of activity. This first phase of activity will be completed by summer 2019.

We expect this action to raise to the surface any need for additional support mechanisms that could help to rapidly accelerate growth in the cluster, and further specific actions may flow from this as a result.

Action D2:

The Scottish Government and Scotland's enterprise agencies will work with supporting institutions and innovation centres (such as CivTech, CENSIS and The Data Lab) to ensure cyber security is embedded into any centrally-funded technology innovation activity. This includes ensuring that the outputs of publicly-funded innovation projects are developed with adequate, proportionate levels of cyber security in mind, and that innovation centres are equipped to advise or signpost on such issues. This will be in place by autumn 2019.

Action E1:

The CMO will work with industry, universities and other key partners such as the Scottish National Investment Bank to maximise the impact of existing investment platforms, to support Scottish cyber security entrepreneurs in getting exposure to potential investors, and to support potential investors to make more informed decisions. This action will be ongoing.

Action E2:

The CMO will work closely with Scotland's enterprise agencies, in particular Scottish Development International, to attract direct foreign investment and increase exports in the area of cyber security. This will include developing a strong international proposition. To ensure maximum impact, the CMO and enterprise agencies will work with the UK Government's Department of International Trade to identify collaborative opportunities. This action will be ongoing, with the first phase – developing a proposition – completed by summer 2019.

Action E3:

The CMO, the Scottish Government and Scotland's enterprise agencies will work together with other key partners to maximise engagement, increase impact, and amplify messages across our international networks (such as trade ambassadors, global scots, and other in-market actors and connections). This activity will be ongoing.

INTRODUCTION

3

3 INTRODUCTION

3.1 There is a real opportunity for Scotland to be a world-leading nation in cyber resilience. *Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland*[4], was published in 2015. It set out Scotland's vision for a cyber resilient Scotland where:

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

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

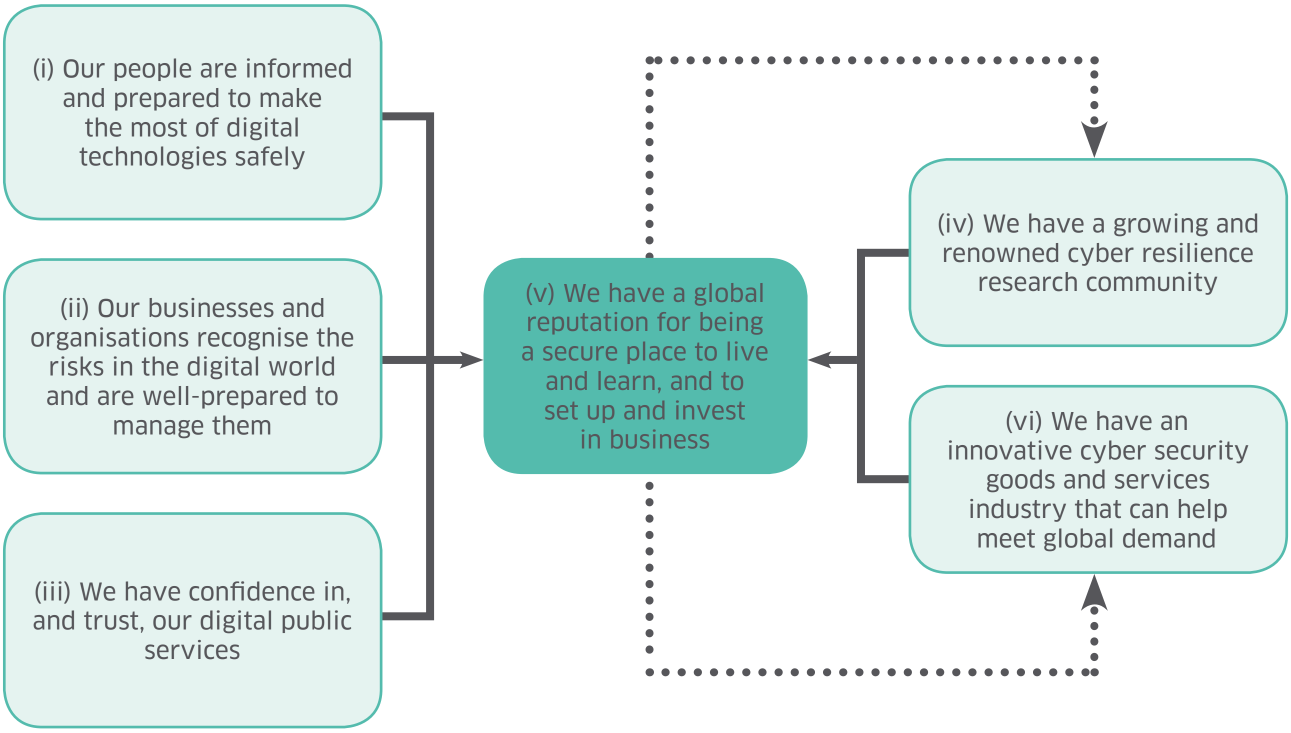
(iii) We have confidence in, and trust, our digital public services

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

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

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

These outcomes are mutually reinforcing, and progress towards one can help support progress towards another:


(i) Our people are informed and prepared to make the most of digital technologies safely
(ii) Our businesses and organisations recognise the risks in the digital world and are well-prepared to manage them
(iii) We have confidence in, and trust, our digital public services
(v) We have a global reputation for being a secure place to live and learn, and to set up and invest in business
(iv) We have a growing and renowned cyber resilience research community
(vi) We have an innovative cyber security goods and services industry that can help meet global demand

(Figure 1)

[4] https://beta.gov.scot/publications/safe-secure-prosperous-cyber-resilience-strategy-scotland/

4 FOCUS OF THIS PLAN

4.1 This action plan has at its core the concept of a Scottish cyber security cluster, which means the emergence of a new cluster of economic activity that creates a critical mass of competitive success, based on our technological, business and academic capabilities in this field.

4.2 As well as core supply-side companies, clusters encompass a whole ecosystem that includes suppliers, customers, related-industries, government, universities, supporting institutions and agencies – which, working well together, allow the cluster to flourish.

4.3 This plan is about creating the right conditions that will help our emerging cyber security cluster to develop and thrive. It focuses mainly on outcomes iv, v and vi (see figure 1 above). It aligns with the other plans described in section 5.

5 STRATEGIC FIT

5.1 This plan is one of a suite of five action plans that the Scottish Government committed to develop in the Programme for Government 2017-18. The others are:

- **Learning and skills** (published in March 2018), focused on ensuring (i) our citizens have the appropriate understanding, knowledge and behaviours to live and work safely and securely in the digital world; and (ii) our cyber security workforce have the appropriate specialist skills. The success of this action plan will be vital to embedding a culture of cyber resilience in Scotland.

- **Public sector** (published in November 2017), **private sector** and **third sector** (published in June 2018), focused on driving up fundamental levels of cyber resilience across the three sectors.

5.2 The cyber resilience action plans are intended to complement each other and be mutually reinforcing.

5.3 This action plan also feeds into Scotland's broader Economic[5] and Digital[6] Strategies. It complements and supports the aims of these strategies and specifically contributes to:

- Several key aims of Scotland's *Economic Strategy*, including: fostering a culture of innovation; supporting the development of highly innovative businesses and supporting high impact research in Scottish universities; creating underlying conditions which will make Scotland a major destination for investment; and promoting Scotland on the international stage to boost our trade and investment, influence and networks.

- Two key aims of Scotland's *Digital Strategy* which are: to work with industry to create the conditions in which our digital technologies industry can thrive; and to ensure that our critical national infrastructure is secure and resilient against cyber attack.

5.4 As this plan is rolled out, the Scottish Government will continue to engage across its internal policy directorates to ensure that cyber resilience continues to be understood in that broader strategic economic context.

[5] https://beta.gov.scot/publications/scotlands-economic-strategy/

[6] https://www.gov.scot/Publications/2017/03/7843

6 ECONOMIC BENEFIT

6.1 A thriving cyber security cluster has the potential to contribute significantly to Scotland's economic prosperity in many ways, including:

Innovation benefits – The development of new goods and services will increase spending on research and development (R&D) – both for higher education (HERD) and business (BERD).

Investment benefits – The creation of new companies and the expansion of existing companies will require additional funding capital and will provide high quality opportunities for new financial investment in Scotland.

Inclusive growth benefits – A new and expanding supply of cyber-related research, goods and services will create additional employment (one of the principal ways citizens share in economic opportunities). Additional employment means there will be a need for continued investment in skills, training and education (including for under-represented groups) to support this.

Internationalisation benefits – A growing, high-quality offering of research, goods and services will result in more competitive and increased exports, as well as attracting more foreign companies and talent to locate in Scotland.

6.2 We also anticipate broader benefits from the impact of this economic opportunity action plan, combined with the outputs of the other four action plans. Together, they will support the goal of building a fundamentally resilient digital economy, well equipped to protect itself from cyber attacks. It is difficult to put a definitive value on that, although a range of figures have been placed on the costs of cyber attacks to the UK economy. It is clear such solid resilience will be essential to realising wider opportunity in the global digital economy and placing Scotland as a leader on the world stage in terms of cyber resilience.

7 ACTIONS

7.1 This plan sets out the actions that the Scottish Government and its key partners will take in support of the plan's objectives through to 2021. Where there are strong links with, or dependencies on, other action plans this is made clear in the text.

7.2 This plan is focused on creating the right conditions to support supply-side cluster growth. As the cluster (and its surrounding ecosystem) evolves, so the actions required to support growth may change. Therefore, we will regularly review the actions through a process of monitoring and evaluation.

7.3 In developing this action plan, the Scottish Government and NCRLB have sought the views of various stakeholders, including Scotland's enterprise and skills agencies, academia, and Scottish industry. These partners will play a vital role in implementation and delivery of the action plan, and the Scottish Government and the NCRLB will ensure that arrangements are put in place for appropriate ownership, collaboration and delivery of activity.

7.4 The Scottish Government is clear that while it can work with partners to create the right conditions to help our Scottish cyber security cluster to thrive, achieving growth in this area will ultimately require leadership, commitment, ownership and resource from the Scottish cluster itself.

7.5 The actions are grouped under the five key objectives, A – E.
Objective A: Develop the right market conditions to encourage and support the continued emergence of the cyber security business community in Scotland.

Action A1:

The Scottish Government, through an ongoing commitment to all five cyber action plans, will continue to clearly state and demonstrate its ambition to make Scotland a world-leading nation in cyber resilience, sending strong long-term demand signals to the supply-side that they can be confident in their own expansion. The Scottish Government will play a key role in proactively engaging in, and influencing policy development at Scottish, UK and EU levels to ensure there is an effective voice representing Scottish cyber security companies and interests. This includes engaging with the UK Government as it develops a royal charter body to support professionalisation and collaboration across the UK. This activity will be ongoing.

Scottish Ministers have signalled their desire to make Scotland a world-leading nation in cyber resilience (demonstrated by the formation of the Scottish Government's Cyber Resilience Unit, the NCRLB and the publication of the five cyber action plans). The Scottish Government believes that being a world-leading nation means more than adopting high standards and best practice: it also involves encouraging and supporting supply-side businesses to grow in number, scale and turnover, and to help create the right conditions for a cyber resilient Scotland. The NCRLB believes it is essential to Scotland's cyber cluster that these signals continue to be communicated over the long-term to create and ingrain a stable and informed landscape for supply-side investment decisions.

It is expected that the cyber action plans for the public, private and third sectors will have the effect of building demand for cyber goods and services in Scotland. The public sector action plan anticipates the introduction of appropriate, proportionate standards of cyber resilience for those bidding for support or contracts with the public sector. It also creates a cadre of public sector organisations ('cyber catalysts') who will work together to identify opportunities for the adoption of innovative approaches to cyber resilience, potentially adding to new local demand for cyber-related goods and services.

Action A2:

The Scottish Government will work in partnership with Scottish Enterprise, Highlands and Islands Enterprise and other key partners to encourage the ongoing development of innovative solutions to public and private sector challenges relating to cyber resilience. This will include launching calls to industry through mechanisms such Civtech, CAN DO, or Open Innovation Challenges. The first challenge will be launched in 2018.

Where an emerging market is reliant on the early pull of the public sector, it is vital that supply-side companies (both actual and potential) can see evidence of demand for innovation. This is often facilitated through procurement contracts (and this should continue where appropriate) but it is more successful in acting as a stimulant where 'funded innovation call' mechanisms are used. CivTech[7] is an example of an initiative available for the public sector, and newer, larger-scale mechanisms such as the "CAN DO"[8] initiative could also be considered in this context. Where innovative elements can be readily separated from incumbent IT contracts, such funded innovation calls will be used by the Scottish public sector.

Action A3:

The Scottish Government will work in partnership with Scotland's academic institutions to encourage growth in world-leading research, innovation and skills to stimulate market needs and create economic impact. This activity will be ongoing.

As an integral part of the cyber cluster, it is vital that academia is encouraged to innovate through collaboration with partner organisations, investors and industry. This will ensure our educational institutions create, harness and add value to economic opportunities arising from research, technology and know-how.

Through their research and innovation, universities will promote and champion Scotland's expertise to national and international audiences through joint research programmes, academic exchanges, conferences and publications. This will help develop international relationships and partnerships to 'sell' Scotland's "cyber brand", which will be essential to growing global business. It will also underpin inward investment opportunities for businesses attracted to Scotland from abroad who want to gain access to our markets and expertise.

[7] https://civtech.atlassian.net/

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

Action A4:

On an ongoing basis, the Scottish Government will support opportunities for industry and academic experts to contribute to future cyber resilience policy development and thought leadership at the Scottish, UK and EU levels. In the immediate term, the Scottish Government will commission the collaboration of universities who make up the SICSA Cyber Nexus to work with industry and other partners to produce a research piece into the concept of digital communications infrastructure in Scotland as a "fifth utility". This will consider the current and expected future "state of the art", and the extent to which Scotland could achieve a competitive advantage by driving forward change in this area using existing or new powers. The findings of this research, to be delivered by summer 2019, will help inform wider policy development in respect of "secure by design".

Much of the work on cyber resilience in Scotland and the rest of the UK to date has focused on the measures that end users can take to protect themselves from existing cyber threats (for example, taking action to change default router passwords, or to make judgements themselves around the types of antivirus software they need or don't need). Some key private sector partners have argued that in the longer term, a more "provider-focused" approach to cyber security is required, treating digital services in a similar way to traditional utilities where service providers have a responsibility to ensure adequate levels of resilience and security within their service provision. Providers of such services would be required to take action to ensure consumers receive "clean" digital communications services, similar to what we have come to expect from other utility providers (for example, consumers of water are not generally required to fit filters in their own homes to feel confident that their supply is uncontaminated).

How or if this might work in practice is not fully understood. To improve our understanding of any potential economic opportunities in this area, the collaborative of universities who make up the SICSA Cyber Nexus will be commissioned to work with industry and other partners to produce a research piece into the concept of digital communications infrastructure in Scotland as a "fifth utility".

Related to this, the UK Government has begun to formally explore the topic of "secure by design[9]", and the Scottish Government will continue to engage proactively with the UK Government and industry and academic experts as this thinking is developed.

[9] https://www.gov.uk/government/publications/secure-by-design

6.5 Objective B: Develop the right academic research capability and capacity to support and grow business innovation in Scotland

Action B1:

Scotland has a growing capability and global visibility in cyber security research, innovation and skills benefiting the sector. The Scottish Government and the SICSA will build on the current government-funded SICSA programme of work to support academic institutions to expand this research. This work will aim to be of sufficient scale to attract and retain at least one globally renowned academic, provide for long-term facilities, and nurture junior research talent. It will also explore new ways of working that could better support the integration of academic ideas and expertise with the medium – to-long-term needs of industry. This action will be ongoing.

Successful clusters need access to the skills and resources that support innovative thinking and problem solving. The Scottish Government has provided funding under the UK National Cyber Security Funding Programme for an academically-focused Network Integrator and associated projects. These are helping to encourage and coordinate activity in the academic cyber security and resilience areas, and are supporting companies to find their way around the resources which currently exist there.

The NCRLB believes that the drivers for academics to work with companies in Scotland could and should be strengthened. There are various relevant initiatives (such as innovation centres), but areas of focus can sometimes be activity-based rather than strategic (involving long-term relationships and mutual planning). Cyber is an emerging and fast-moving topic, and as such there is a need to execute and deliver activities quickly to maintain a competitive advantage. However, it is important that this is tempered with longer-term planning to ensure activities are well placed to maximise return on investment, add value, fill gaps and align with long-term strategic objectives. As an emerging technical topic, cyber resilience has the inherent potential to be an area in which new ideas can be trialled. This creates a good opportunity to consider how, in trialling those new ideas, greater emphasis can be placed on the development of strong strategic relationships between academia and industry.

Action B2:

The Scottish Government will continue to work with the Scottish Funding Council to strengthen the requirements for cyber security research to be included within our university and college outcome agreements. This action will be ongoing.

As the national, strategic body for the funding of further and higher education in Scotland, the Scottish Funding Council's (SFC) role is to support colleges and universities in Scotland to deliver high-quality learning and teaching, world-leading research and greater innovation in the economy. Their investment enables our higher education institutions to carry out world-leading research.

The Scottish Government will continue to work with SFC to encourage our further and higher education institutions to build research capabilities in cyber security, in turn contributing to Scotland's economic growth.

Action B3:

The Scottish Government and its enterprise and skills agencies will continue to clearly state their support for the creation of a cyber-focused Centre for Doctoral Training in Scotland, and will work with SICSA, universities and industry to explore practical routes that all sectors could use to engage with, or support such a programme – for example through the provision of data. This action will be ongoing.

Ensuring there is sufficient cyber-related PhD research capacity in Scotland will have an impact on both supply-side academic capacity and industrial collaboration capacity. The establishment of a Centre for Doctoral Training (CDT) would be a core mechanism to ensure that PhD places could be made available, in volume, in Scotland. The Learning and Skills action plan[10] also includes a commitment from the SICSA to work with the Scottish Government to consider the establishment of a CDT or other forum to bring industry together with researchers. The establishment of a CDT relies on having appropriately accredited academic departments, numbers of which are growing in Scotland. At the time of writing, Scotland-based CDT applications to the UK authorities are already in progress. If successful, that may address the challenge of growing Scotland's PhD capacity. However, if not successful, there will be a requirement to consider alternative means for addressing this challenge.

6.6 Objective C: Develop the right cluster management arrangements to ensure the approach is coordinated and has impact

Action C1:

Scottish Enterprise will work with the Scottish Government and other key partners to establish a cluster management function for cyber within an accredited CMO, with enough resource, capacity and capability to match the ambition of developing a globally relevant cluster. This will include steps to help the CMO achieve EU accreditation standards to agreed levels within a realistic timeframe. The CMO will be expected to participate in appropriate national advisory forums, work closely with partners to determine how best Scotland can benefit from UK wide industry initiatives emanating from UK Government and NCSC, and encourage the development of networks, coherence and partnership working, particularly with other aligned clusters such as Fintech. The CMO will initially be established by autumn 2018.

Most successful clusters in Europe are underpinned by a professional CMO. Even in mature clusters, these CMOs usually have a degree of public co-funding as much of the benefit they add goes to the wider economy as well as their member companies.

As the cyber security cluster develops, it will be important for organisations to have the opportunity to network and collaborate, promote effective cyber security practices, share learning and knowledge, capitalise on opportunities, and to have a voice that can influence national decision making, skills development, and technological development.

[10] https://www.gov.scot/Publications/2018/03/2748

The cyber security community in Scotland has not yet matured enough to substantially resource a CMO that can provide coordination and highlight challenges and source opportunities for that community. However, there is a well-understood path from today's phase, (of largely government provision of network integrators), developing through a risk-sharing phase between private and public sector, to a mature, steady state phase, involving a fully-fledged CMO. The CMO would be expected to demonstrate a clear commitment to develop such a road map, with significant engagement and buy in from industry.

One early task for the CMO would be to use targeted resources to improve the information available around Scotland's export capabilities in cyber-related goods and services to international markets, and ensure a balanced approach to supply-side campaigns aimed domestically and internationally.

There is clear overlap between the cyber security opportunity in Scotland and the emerging opportunity known as Fintech. Making secure, robust, efficient private financial transactions is at the core of much of the rising demand for disruptive technology in the financial services sector. A cyber CMO will need to liaise with its sister organisations in Scotland to develop understanding of when to collaborate over common topics and when to differentiate.

The UK Government is making significant investment in supporting and growing cyber security companies. This includes the Cyber Growth Partnership[11], which aims to boost the UK's global market position in cyber security products and services, and other activities being undertaken by the NCSC such as:

- Cyber Accelerator, which gives innovative startups access to cyber expertise[12]
- Industry 100, which enables industry reps to work alongside the NCSC[13]
- NCSC-funded cyber work placements, which aim to build relationships with talented young people and potentially offer future employment[14]
- Cyberinvest, which aims to encourage industry investment in cyber research[15]

The CMO will need to work closely with the Scottish Government and its partners to ensure that Scotland benefits from these and other relevant initiatives.

[11] https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security#appendix-6-promoting-economic-growth-in-the-cyber-security-sector

[12] https://www.ncsc.gov.uk/information/cyber-accelerator

[13] https://www.ncsc.gov.uk/information/industry-100

[14] https://www.ncsc.gov.uk/new-talent

[15] https://www.ncsc.gov.uk/articles/cyberinvest-securing-our-future-through-research

6.7 Objective D: Develop the right supporting institutions to stimulate innovation and renewal within the cluster

Action D1:

The CMO, Scotland's enterprise agencies, and the Scottish Government will work together to develop a comprehensive shared understanding of Scotland's cyber security landscape. This will include identifying our strengths (in both a UK and global context), mapping out the current picture in terms of the various hubs and centres of expertise that exist across Scotland, and understanding the effectiveness of existing models and mechanisms for innovation, support and coordination of activity. This first phase of activity will be completed by summer 2019.

We expect this action to raise to the surface any need for additional support mechanisms that could help to rapidly accelerate growth in the cluster, and further specific actions may flow from this as a result.

Cyber resilience has many dimensions. There are currently various facilities and centres of expertise in Scotland (and potentially more will be created, for example through City Deal or other new/scale up activities). Ensuring these are well-coordinated and do not duplicate effort would reduce the need for one all-encompassing cyber centre in Scotland.

Action D2:

The Scottish Government and Scotland's enterprise agencies will work with supporting institutions and innovation centres (such as CivTech, CENSIS and The Data Lab) to ensure cyber security is embedded into any centrally-funded technology innovation activity. This includes ensuring that the outputs of publicly-funded innovation projects are developed with adequate, proportionate levels of cyber security in mind, and that innovation centres are equipped to advise or signpost on such issues. This will be in place by autumn 2019.

Accelerators are a particular type of institution that support new or scaling businesses. There are various views on the current situation and the precise solution in Scotland. Scotland may benefit from a globally-accredited technology accelerator (either with cyber security as a cross-cutting theme or as a dedicated focus), and if deemed appropriate this could be realised through encouraging and inviting globally trusted accelerators to open here, or through growing our own indigenous service providers to global standards. Consideration should also be given to how best to link with and build on NCSC's existing cyber accelerator approach. If a dedicated accelerator is not appropriate, it is vital that any technology accelerator in Scotland which receives public funds embeds cyber-security support as part of their offering to clients.

Scotland is most likely to develop a reputation as a world-leading nation in cyber resilience where the development of digital solutions is secure by design[16], with cyber resilience "baked-in" from the start. This quality proposition could be a strong differentiator for Scotland compared to the production of goods quickly, cheaply and without consideration being given to cyber resilience as a fundamental part of product/

[16] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

service development. If the Scottish brand is to be regarded as robust and trusted, then it would be illogical for our institutions to support the development of low quality technology. The public sector must be vigilant in what it funds, and impose the necessary diligence to ensure it does not support technology-based initiatives that work against any such national brand or messaging. This extends across all government initiatives and partners and includes any hubs or centres that are centrally funded.

6.8 Objective E: Develop the right brand to help promote Scotland's cyber security cluster across the UK and internationally, grow cluster exports, and reflect Scotland's emerging position as the place to be for researching, developing and supplying cyber goods and services

Action E1:

The CMO will work with industry, universities and other key partners such as the Scottish National Investment Bank to maximise the impact of existing investment platforms, to support Scottish cyber security entrepreneurs in getting exposure to potential investors, and to support potential investors to make more informed decisions. This action will be ongoing.

The private equity investment scene for the cyber security cluster in Scotland is not unique – it has the usual characteristics found across all digital markets in Scotland. The main requirement is to ensure that potential investors are well informed about cyber and the growth opportunities that could be generated, helping to stop cyber specific investment opportunities being lost in the general digital background. Focussed work would allow campaigns to be developed, aimed at increasing investor sophistication regarding this niche cluster.

Action E2:

The CMO will work closely with Scotland's enterprise agencies, in particular Scottish Development International, to attract direct foreign investment and increase exports in the area of cyber security. This will include developing a strong international proposition. To ensure maximum impact, the CMO and enterprise agencies will work with the UK Government's Department of International Trade to identify collaborative opportunities. This action will be ongoing, with the first phase – developing a proposition – completed by summer 2019.

Scotland's own fundamental cyber resilience position is significant in providing the proof-point for any international proposition it can make for its cyber goods and services offering. The action plans on public, private and third sector resilience, along with the learning and skills action plan, set out how progress towards this fundamental cyber resilience is to be achieved.

With market demand for cyber-related goods and services being so diverse, any international proposition needs to be able to be tailored to suit the particular target at any time. There should be a universal brand with core messages and proof-points which can be adapted with specific case studies for each sector, geography or application area. This is a resource-intensive activity.

This plan clearly states that Scotland's cyber offering will be based around quality rather than a sector focus. In creating a differentiated story for Scotland, the approach should be consistent with that overarching aim, with a focus on quality first and foremost (with the balance of focus across sectors being driven by market demand, rather than creating top down artificial silos for particular sectors). Consideration will be given to how the national digital infrastructure story (which is a key element of positioning Scotland as a world-leading nation in cyber resilience) could, over time, be made into a significant international differentiator by design, implementation and operation.

Action E3:

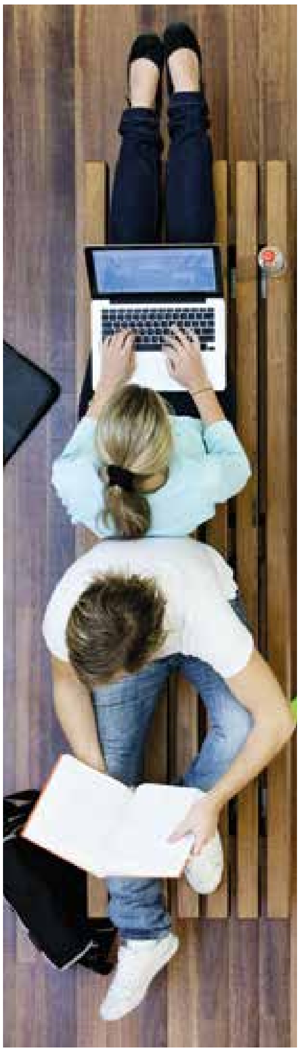
The CMO, the Scottish Government and Scotland's enterprise agencies will work together with other key partners to maximise engagement, increase impact, and amplify messages across our international networks (such as trade ambassadors, global-scots, and other in-market actors and connections). This activity will be ongoing.

In developing a Scottish brand, we will ensure awareness of any broader activities or initiatives (for example, the UK Cyber Export Strategy[17]), and consider if and how it might be appropriate to share activity, resource or messaging to amplify our reach and impact.

Although no single individual represents Scotland as a "cyber resilience ambassador" at present, Scotland has wide-reaching international networks. There is an opportunity to better utilise these networks in a coherent fashion in order to promote Scotland's cyber security offering. The impact and usefulness of these networks must be fully understood before considering what other additional resources might be required – including a specific ambassadorial role for cyber security.

[17] https://www.gov.uk/government/publications/cyber-security-export-strategy

APPENDICES



APPENDIX ONE: High-level Monitoring and Evaluation Framework

Key Action	Action Required Of	Requirements	Deadline
A1	SG, CMO	Engage with cyber community to seek input as and when policy conversations arise	Ongoing
A2	SE, SG	Launch funded innovation call	Winter 2018
A2	SE, SG, HIE, NCRLB, CMO	Explore potential pipeline of future innovation calls	Ongoing
A3	SG, academic institutions	Encourage growth in world-leading research, innovation and skills to stimulate market needs and create economic impact.	Ongoing
A4	SICSA, SG	Engage with partners including industry to deliver expert research piece into the concept of digital communications infrastructure in Scotland as a “fifth utility”.	Summer 2019
A4	SG	Support opportunities for industry and academic experts to contribute to future policy development, thought leadership and innovative thinking in respect of “secure by design” at the Scottish, UK and EU levels.	Ongoing
B1	SICSA	Demonstrate growth of cyber-focused research activity versus 2018 baseline	Autumn 2021
B2	SFC	Build in cyber activity to college and university outcome agreements	Ongoing
B3	SICSA	Establish a cyber CDT in Scotland	Timings dependent on application process
C1	SE	Establish a Scottish CMO	Autumn 2018
D1	CMO, SE	Complete comprehensive benchmarking/mapping activity and provide recommendations on future action	Summer 2019
D2	SG, SE, Innovation Centres	All Scottish innovation centres to include cyber considerations within their offering to clients	Autumn 2019
E1	CMO	Engage with partners and the investment community to generate an investment focused activity plan.	Summer 2019

Key Action	Action Required Of	Requirements	Deadline
E2	CMO, SDI, SE	Develop suite of proposition materials to support us in describing Scotland’s cyber capabilities	Summer 2019
E2	SDI, SE	Demonstrate any increased levels of trade and investment for cyber activity in Scotland	Autumn 2021
E3	CMO, SE, SDI, SG	Develop an international stakeholder engagement plan	Spring 2019

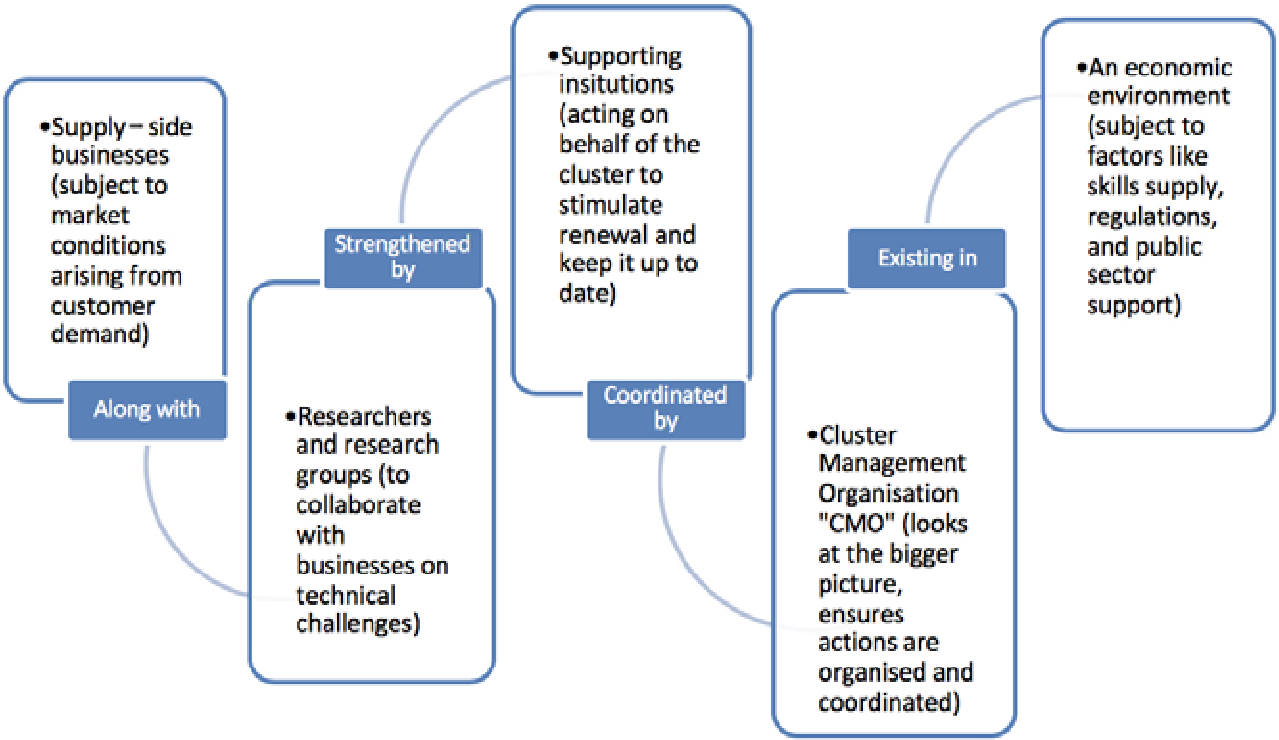
APPENDIX TWO: Clusters and Cluster-Building

What Is a Cluster?

Clusters, essentially, are a “critical mass” of economic activity and success, based on technological, academic and business capabilities in a particular field.

The term cluster traditionally referred to geographically concentrated (or even co-located) supply-chains of businesses, researchers and associated institutions all focussing on a single market opportunity[18]. It is becoming evident that location, or co-location, is not necessarily the critical factor in cluster success. Compared to other factors, tight geographic boundaries are becoming an increasingly poor predictor of a cluster’s community structure[19], and with today’s ubiquitous mobility and connectivity, companies are increasingly seeking to make connections beyond those geographical boundaries.[20]

Scotland has recognised that it has the characteristics of a geographically concentrated space even when referring to activities spread across the whole of Scotland. This is enabled by our high degree of national policy coordination and aided by ever-increasing ways of communicating effectively across greater distances. A cluster could be considered an ecosystem which consists of:


•Supply – side businesses (subject to market conditions arising from customer demand)
Along with
•Researchers and research groups (to collaborate with businesses on technical challenges)
Strengthened by
•Supporting insitutions (acting on behalf of the cluster to stimulate renewal and keep it up to date)
Coordinated by
•Cluster Management Organisation "CMO" (looks at the bigger picture, ensures actions are organised and coordinated)
Existing in
•An economic environment (subject to factors like skills supply, regulations, and public sector support)

[18] See e.g. http://www.clusterobservatory.eu/index.html

[19] Turkina and Van Asche, 2016

[20] Structure and Evolution of Global Cluster Networks, Oxford Academic Journal Geography Research, 2016

The development of each of these areas – **market conditions, research capability** and **capacity, cluster management, upgrading institutions and economic environment** (including an international proposition) – is required in order for the cluster to mature and thrive.

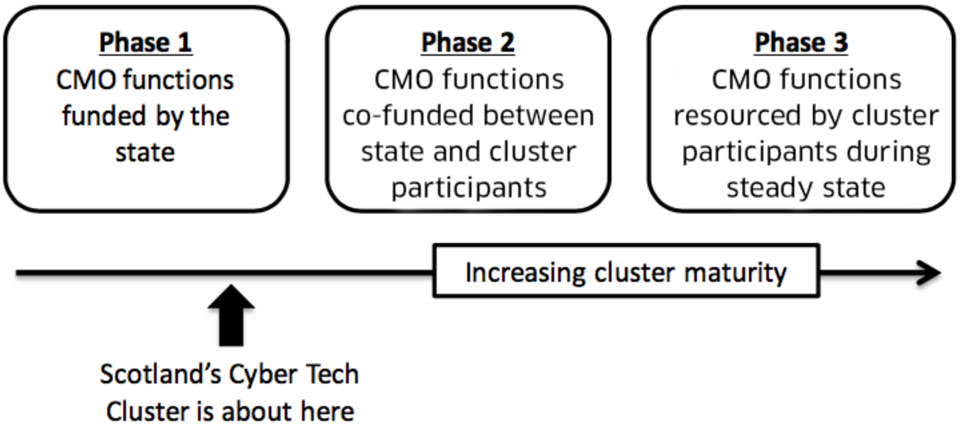
The Cluster Development Journey

New economic opportunities are initially characterised by the appearance of businesses and researchers touching on the subject area. At first, they may not be fully occupied by the topic or may not have realised that the topic has been formalised. Government has a partial role in creating an environment under which the business and research community can emerge and coalesce. This role is most certainly secondary to the entrepreneurial drive required from businesses themselves, but is nonetheless important.

There are generally three phases to building a new cluster: (1) *emergence*, where the early participants cannot provide coherence within their own resources and the state usually has to fully-fund the CMO role, (2) *adolescence*, where the participants start to see the value of coherence and begin to find ways to contribute to CMO resourcing, and (3) *maturity*, whereby the participants can provide cluster coherence through a steady-state CMO supported by substantial levels of private resource.

There is a respected accreditation scheme for CMO activity in Europe[21]. The scheme is straightforward to enter and provides support as a CMO develops its capability and capacity from bronze 'label' to gold.

The emerging community of cyber security businesses and researchers in Scotland is small but is showing positive signs of healthy growth. To support emergence thus far, the Scottish government has enabled the CMO role through the provision of fully-funded Network Integrators. Recently the basis of this has changed to involve contribution in kind from the cluster itself, confirming the general view that cluster-building is coming towards the end of phase 1. The cluster has the potential as a future vehicle for the genuinely transformative collaboration that will be required to make Scotland world-class in cyber-resilience.


Phase 1
CMO functions funded by the state
Phase 2
CMO functions co-funded between state and cluster participants
Phase 3
CMO functions resourced by cluster participants during steady state
Increasing cluster maturity
Scotland's Cyber Tech Cluster is about here

[21] https://www.cluster-analysis.org/

APPENDIX THREE:

Supporting Institutions

"Supporting institutions" is a term used to loosely describe the various organisations, centres of excellence or mechanisms that aim to help improve capability, build capacity, and encourage growth, vigour and renewal.

Innovation centres are a specific type of supporting institution designed to increase the pace of business innovation by encouraging collaboration between business and academia, helping draw on research and expertise to solve problems posed by industry, and providing space for collaborative work and shared access to equipment.

Accelerators are organisations that offer focussed support and funding to start ups, often including access to mentorship, networking, office space and other resources.

The term "hub" generally refers to a specific location, building or group of buildings that brings together expertise in a particular subject area.

Possible areas of focus for cyber supporting institutions are varied, with functions that include:

- Hosting of penetration testing services
- Industrial collaboration, outreach and awareness raising
- A place for SMEs to turn to during cyber security crises
- A centre of excellence for academic research into cyber resilience
- A centre of learning and cyber experience for apprentices
- A co-location opportunity for agencies involved in cyber crime prevention, detection and prosecution
- A Scottish node for UK cyber authorities.

Across Scotland, there are already numerous supporting institutions that either focus on, or relate closely to cyber, including for example:

- SICSA's Cyber Nexus
- Scottish Business Resilience Centre
- The Cyber Academy
- Edinburgh Napier University's SOC Lab
- The University of Edinburgh's Centre of Excellence for Cyber Security Research
- Scotland IS
- CENSIS

This is not an exhaustive list and we expect more to develop. To operate to maximum effect, it will be important that Scottish supporting institutions respond to four key challenges:

1. Coordination – where each institution fulfils a clear value-added role, and duplication of effort is avoided

2. Strategic alignment – where each institution supports the overall strategic vision for cyber in Scotland and the UK

3. Best practice – where our supporting institutions exemplify our national brand values of quality, integrity and trust

4. Collaboration – where our supporting institutions capitalise as much as possible on Scotland's broader digital capabilities, such as data and Fintech.

We anticipate that the actions in this plan that focus on coordinating and coalescing the cyber landscape will help address these challenges.

APPENDIX FOUR:

The cyber security landscape (snapshot as at September 2018)

The NCA reported that 2017 was "punctuated by cyber attacks on a scale and boldness not seen before"[22]. The cost of cyber attacks to UK businesses in 2016 was in the region of £29.1 billion, with around 3 million organisations affected[23].

Recent high profile attacks that have had an impact include:

- The global Wannacry attack in May 2017 which affected more than 150 countries worldwide, seriously impacted the NHS in Scotland and England, and caused Nissan to shut down production in their Newcastle factory for two days.
- The largest ever recorded cyber heist on the Bangladesh bank (reportedly to the tune of $100m).
- The Equifax attack where it was reported that over 145 million US customers had sensitive data breached.
- A reported $500m theft of cryptocurrency from a Japanese exchange in January 2018.

Alongside this threat, the ubiquitous use of data (and a need to manage it appropriately) has sparked an increased focus on privacy and ethics, which is evident in recent legislative changes such as the new General Data Protection Regulation (GDPR), the NIS Directive (which aims to raise security and resilience of network and information systems across the EU), and the UK Government's current work on developing security standards for Internet of Things (IoT)[24].

All of these factors contribute to an increasing demand for robust cyber security products and services, with the cyber security market expected to grow globally to over $144 billion by 2023.[25]

Scotland's cyber security company base has grown considerably in response to Scottish, UK and International demand, from a baseline of around 50 companies in 2017, to just over 90 companies, with a roughly even split between products and services. These companies span several areas including risk and assurance, digital forensics, serious gaming, payment engines and block-chain.

In addition, there are cyber security departments and services embedded within other businesses (for example, financial and business services organisations). Six Security Operations Centres (SOC's) operate in Scotland, and the number is increasing. An increasing number of financial institutions have chosen to carry out their cyber security operations in Scotland.

[22] The Cyber Threat to UK Business 2016-17, NCA

[23] Beaming business research report, 2017

[24] Secure by Design Report, DCMS, 2018

[25] Global Cyber Security Market Report 2013-23, VisionGain

As well as a growing company base, Scotland has world class research and academic capability in the field of cyber security. SICSA supports a specific cyber security research theme[26], and at least six Scottish Universities now offer relevant cyber qualifications. Edinburgh Napier University was the first University in the UK to have their cyber security masters course recognised by GCHQ, Abertay was one of the first universities in the world to offer an ethical hacking degree, and the University of Edinburgh's School of Informatics is formally recognised as an Academic Centre of Excellence for Cyber Security Research (in a context where cyber skills are becoming increasingly valuable, with an anticipated global shortage of 1.8 million cyber professionals by 2020).[27]

Coupled with an ecosystem that includes numerous supporting institutions and aligned public sector support, when compared with previous emerging markets and technologies, the Scottish cyber supply-side appears to have the necessary ingredients, show the right characteristics and demonstrate enough early scale to make a claim to be considered a credible, potential high-impact cluster worthy of support at this time.

[26] SICSA cyber security research theme overview

[27] The Life and Times of Cyber Security Professionals, Enterprise and Strategy Group, 2017

Scottish Government
Riaghaltas na h-Alba
gov.scot

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

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

ISBN: 978-1-78781-177-5

Published by The Scottish Government, September 2018

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS452506 (09/18)