DECEMBER 2020
Version 1

SCOTTISH CYBER CLUSTER ANALYSIS REPORT

Mapping of Scotland's cyber security cluster with insights from other cyber clusters

SCOTLANDIS

www.scotlandis.com | info@scotlandis.com | +44 1506 472200
ScotlandIS | Oracle Campus | Blackness Road | Linlithgow | EH49 7LR

EXECUTIVE SUMMARY

Scotland has a thriving and innovative cyber security community which is growing year on year. This report seeks to provide a 'snap-shot' of the cluster, providing an overview on the make-up and scale of the cyber security sector in Scotland as well as gaining insights from other UK cyber clusters and International clusters as well.

The aim is to both baseline the current status of the cyber security sector in Scotland so that in future we can track growth (or decline) across the cyber cluster and to get a better understanding of how other cyber clusters operate.

Cyber security is now integral to every business and sector across Scotland as we move towards a more digitally enabled society. Cyber skills are crucial if we are to grow Scotland's digital economy. Cyber-attacks and threats are growing across the globe and there is an increasing demand for specialist cyber security skills.

This report looks at the Scottish cyber security sector as a whole and the encompassing elements of the sector such as skills, innovation, areas of expertise, academia and more. It also covers learning and insights from other clusters around the UK and internationally.

Some key takeaways from the cyber cluster report are:

- The Scottish cyber cluster currently includes around 230 cyber security companies
- Approximately 48% are Scottish founded companies or company headquarter is in Scotland.
- In the past 5 years, around 10 new Scottish cyber companies are being set-up per year
- 70% of Scottish universities now offer courses in cyber security
- The cyber workforce in Scotland has seen steady growth with 4.3% of core cyber security job vacancies being placed in Scotland in the last three years.
- Scotland is competitive when it comes to cyber security salaries which helps Scotland to attract and retain key talent. Currently it ranks 4th place in UK ranking with a mean salary of £54,900.

TABLE OF CONTENTS

INTRODUCTION

The landscape of cyber security has changed rapidly over recent years and the importance of cyber security is being realised by all sectors across Scotland. The COVID-19 pandemic has highlighted the importance of cyber security for government, industry and individuals. Cyber security is now pivotal for any organisation to ensure it has sufficient capability to deal with potential attacks. Higher education establishments in Scotland have recognised this trend and we are continuing to see a growth in courses offered in data security, digital forensics, and ethical hacking.

This report is based largely on a Scottish cyber cluster survey which spanned all across Scotland and additionally includes stakeholder input from UK, European and Australian cluster management organisations. This paper will show the current landscape[1] of the cyber security sector across Scotland and will additionally seek insights from other cyber clusters. It is worth highlighting that this survey was conducted during the COVID-19 pandemic and in the years ahead it will be important to continue to chart developments in the cyber community to see if the period of growth continues or stagnates.

The cyber security sector as a whole can ensure that Scotland continues to be ripe for inward investment and create highly skilled and highly paid jobs across all regions in Scotland to create inclusive economic growth.

SCOTTISH CYBER CLUSTER

Scotland has seen significant growth in cyber security over the last few years and there are currently around 230 cyber security companies which have a presence in Scotland, of which approximately 48% are Scottish founded companies and/or the main company headquarter is in Scotland.

Figure 1 shows the increase in new Scottish cyber companies being set up in the last 5 years. If you include all new cyber start-ups (i.e. regardless of where they were founded), the number of new companies[2] which now have a presence in Scotland increases to 52 companies. This equates to approximately a 30% increase in the size of the cyber cluster from new companies alone.

[1] Snapshot taken in Q3 2020.

[2] New companies, in this context, are defined as being in existence for 5 year or less

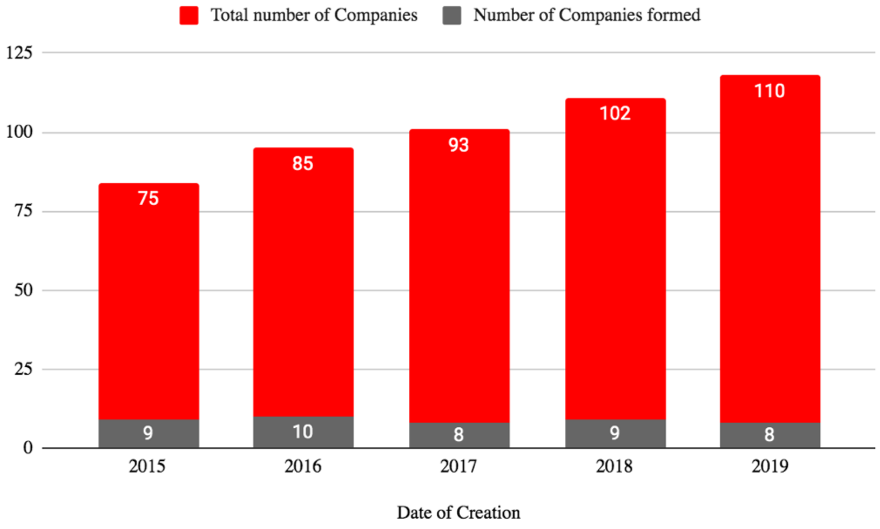


Figure 1. New Scottish cyber cluster companies over the last 5 years

On top of this more and more global cyber security companies are choosing to locate in Scotland, so the overall cluster will have increased beyond this figure. The year of when each company set up in Scotland is not currently available, however from the companies surveyed, 56% of the non-Scottish companies have moved into the region within the last 5 years[3].

Despite 2020 being a challenging year, the cluster has continued to grow, with a number of new companies being set up or being spun out of universities, such as Lupovis (spin out from Strathclyde), PRC (spin out from Glasgow university) and Memcrypt (spin out from Napier university), among others.

The cyber cluster is made up of a mix of companies offering cyber security products or services, consultancies, managed service providers and resellers. From data gathered it would appear that around 60% of Scottish cyber companies are developing products. Interestingly product development is not just being carried out by start-ups or dedicated product companies, there are also an increasing amount of existing cyber security services companies which are moving into product development – having identified a gap in the solutions currently on offer and also understanding the needs of their customers which are not being addressed.

From a survey carried out (see APPENDIX 1: RESEARCH APPROACH), approx. 48% of companies were dedicated cyber companies, with the remainder also offering non-cyber products as part of their wider portfolio.
As can be seen from the table below over 40% of the surveyed companies consider themselves as early stage start-ups, later stage start-ups or scale-ups, 36% are established SMEs with 19% being large enterprises demonstrating that there is a good

[3] This calculation excluded any new companies set up within last 5 years to avoid double counting

mix of company size and type in the cyber cluster which is key to a healthy ecosystem.

Type of company	Percentage
Early stage start-up	20.75%
Established SME	35.85%
Large enterprise	18.87%
Later stage/larger start-up	11.32%
Scale-up	11.32%
Social Enterprise	1.89%
Grand Total	100.00%

Table 1. Percentage split of company types

REVENUES

According to the DCMS UK Cyber sector report published by Ipsos MORI in January 2020, the total UK annual revenue within the sector has been estimated to reach £8.3bn. This reflects an increase of 46% since the 2017 baseline analysis (i.e. revenue has increased by £2.6bn from £5.7bn).[4]

However, gathering information on revenues specifically for the Scottish cyber cluster is difficult to capture due to a number of reasons:

- Many companies are not dedicated cyber companies and don't track revenues for different areas within the business
- Many companies are UK wide or global companies and don't break out the Scottish revenues separately.

The table below shows the responses from the surveyed companies regarding their approximate annual turnover relating to cyber security products and services. The largest section is 'less than £500k' which is reflective of the high percentage of start-ups, scale-ups and SMEs that make up the cluster. As the cluster and companies which make-up the cluster mature the expectation is that the revenues and size of the organisations will grow accordingly.

[4] UK Cyber Sector Analysis Report, Jan 2020 - https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2020

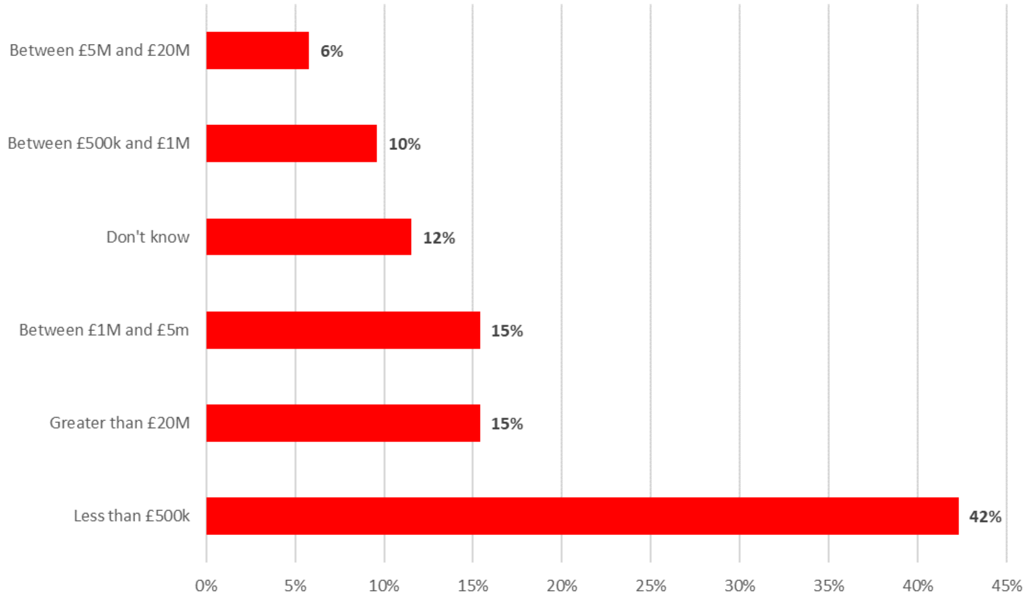


Figure 2. Percentage split of (approximate) cyber turnover in past financial year

ROUTE TO MARKET

The companies surveyed were asked to confirm the top 3 sectors they are currently doing business with which is shown in the diagram below.

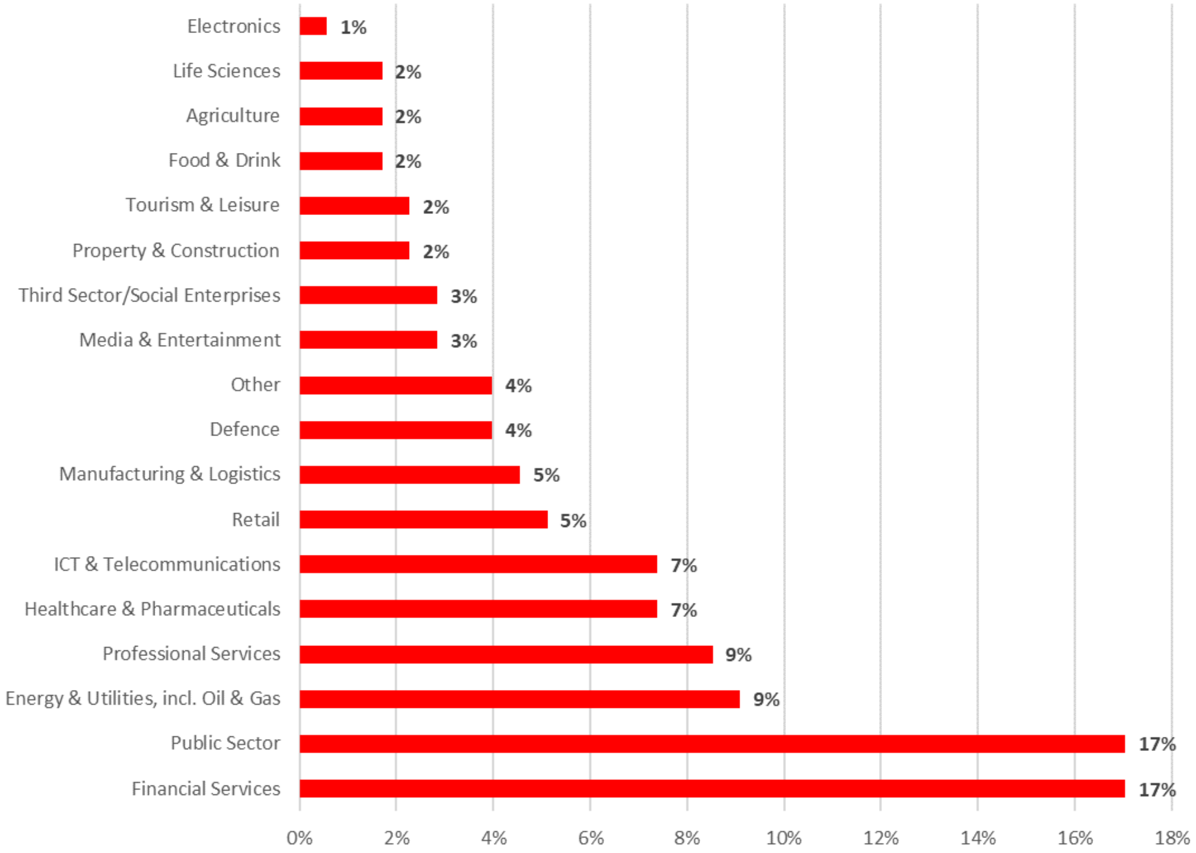


Figure 3. Key target sectors for cyber companies in Scotland

While public sector, ICT/telecommunications and professional services are understandably key sector targets for any cyber organisation, the significance of Energy, Financial and Healthcare in the market share can be both attributed to and supported by the fact these are three of Scotland's key industries of focus, with significant existing and prospective ecosystems incorporating industry, academia and government underpinning each.

However, it is important to note that while Scotland, and generally, the UK may be the core country of business, the survey responses support UK's intention of making cyber one of the key products of export, as more than 75% of companies surveyed serve customers on more than one continent. While there is no information on exact country breakdown, the following graph shows the continents on which the survey responders do business in.

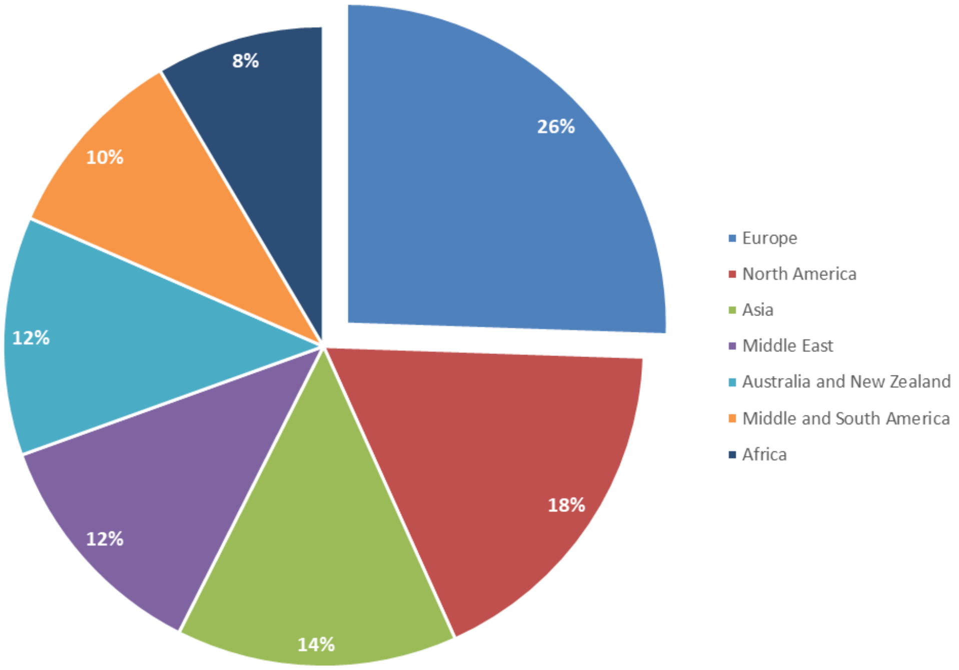


Figure 4. Percentage split of cyber companies' customer locations

The figure shows that predictably Europe is the predominant place of business, with significant customer bases being in North America and Asia. It is also important to mention that that the remainder of responding companies that do not fall in the aforementioned 75%, likely do business in multiple European countries as well, even if it is marked as a single continent in the survey. This is a good indicator that Scotland is an important player on the global cybersecurity market, utilising its innovative organisations and high-quality workforce available.

SCALING AND INNOVATION

In the 2020 UK Cyber Sector Analysis[5] report the following graphs were published relating to the number of investments and value of investments made between end of 2017 and end 2019.

The total investment made during this period was £968million, which was invested through 290 investments. According to this report Scotland won £6million of this with a total of 14 investments being made. This equates to 6.2% of the investment amount and 4.8% of the number of investments. Considering that Scotland has 8% of the British population it would appear that Scotland is not doing as well as it should be when it comes to both volume and amount of investments. If we compare Scotland to Northern Ireland (NI), which is significantly smaller than Scotland population wise[6], and yet received over 3 times the amount of investment in this same period. Interestingly the number of investments was the same, demonstrating that Northern Irish companies were receiving sizably larger investment amounts per investment.

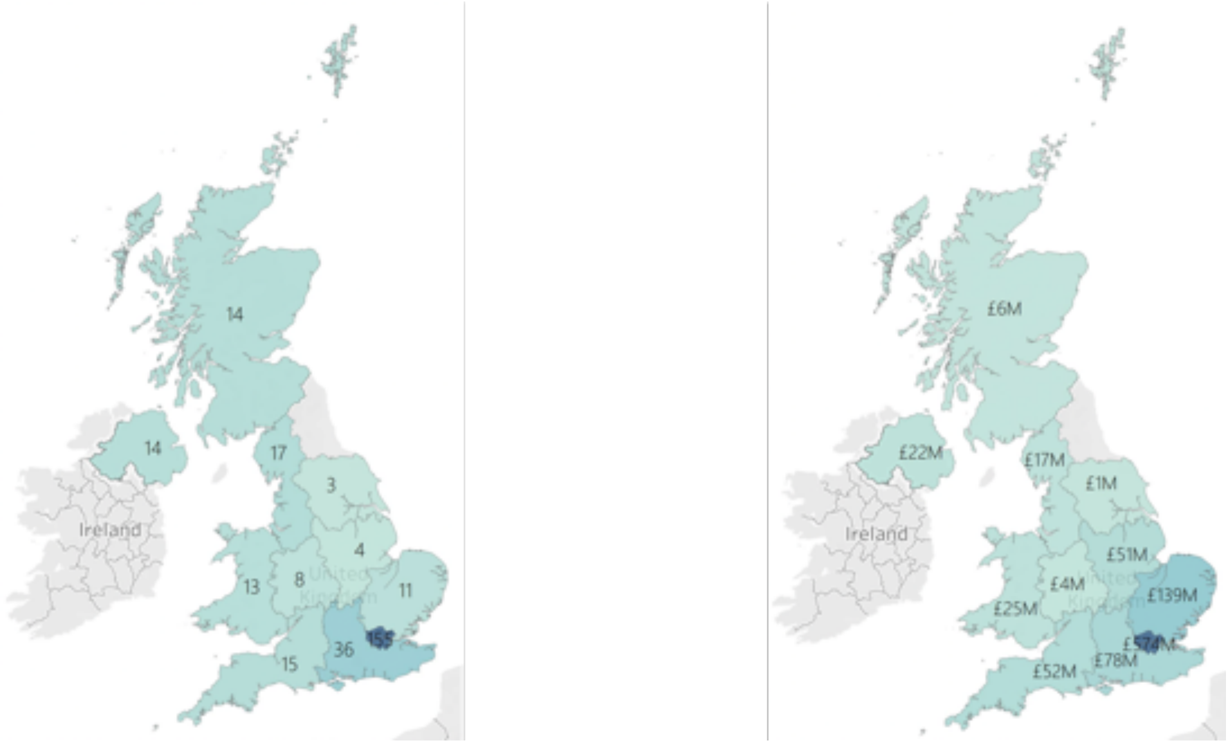


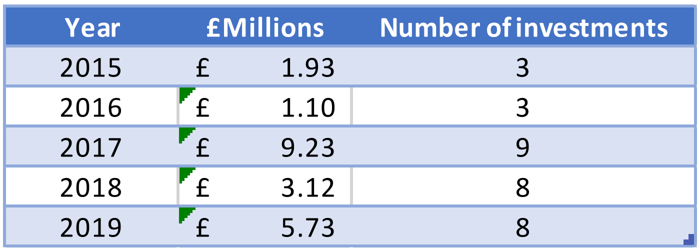
Figure 5. Number and amount of investments throughout the UK from end of 2017 to end 2019

Collating data from various sources[7] on specific investments provides the following information:

[5] UK Cyber Sector Analysis report, Jan 2020, https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2020

[6] Scotland has a population of circa 5.5million, NI circa 1.9 million and Britain has circa 67.9million

[7] Perspective Economics data (extracted from Beauhurst) and Dealroom.co



Year	£Millions	Number of investments
2015	£ 1.93	3
2016	£ 1.10	3
2017	£ 9.23	9
2018	£ 3.12	8
2019	£ 5.73	8

Table 2. Investment per year in Scottish cyber companies

This table shows higher numbers that the UK Cyber Sector report due to the definition of cyber security being narrower in that report. For example, investment in Boundary Technologies Ltd was not included in the UK Cyber Sector Analysis, as this study did not include smart home security devices within scope.

Of the companies surveyed only 27% sought investment during the last 24 months and all of these were successful in their applications.

Therefore, from information gathered it would appear that funding is available to those seeking it and yet the number of investments and the amount of investment are less than they should be considering the size of Scotland. This may be due to the low volume of high growth businesses (majority of businesses seeking organic and steady growth) and also the dependency on Scottish investment organisations. Based on information available[8] it would appear that approximately 80% of the number of investments came from Scottish investment companies with the remaining 20% coming from UK investment companies.

Despite the challenges of 2020 with COVID-19 waylaying many a business plan, there have still been a few success stories with Quorum Cyber (£2.7M) and Boundary Technologies (£1.7M) both successfully winning large sums of investment and Symphonic Software were acquired by Ping Identity with Par Equity selling its share in the company for $31 million US dollars (achieving a blended 8.3x return)[9].

Of the companies surveyed 43% were considering seeking investment of some sort over the next 12 months with the split of investment type being shown below – a number of companies selected multiple options as can be expected.

[8] Perspective Economics data (extracted from Beauhurst) and Dealroom.co

[9] https://scottishfinancialnews.com/article/par-equity-sells-stake-in-symphonic-software-for-31-million

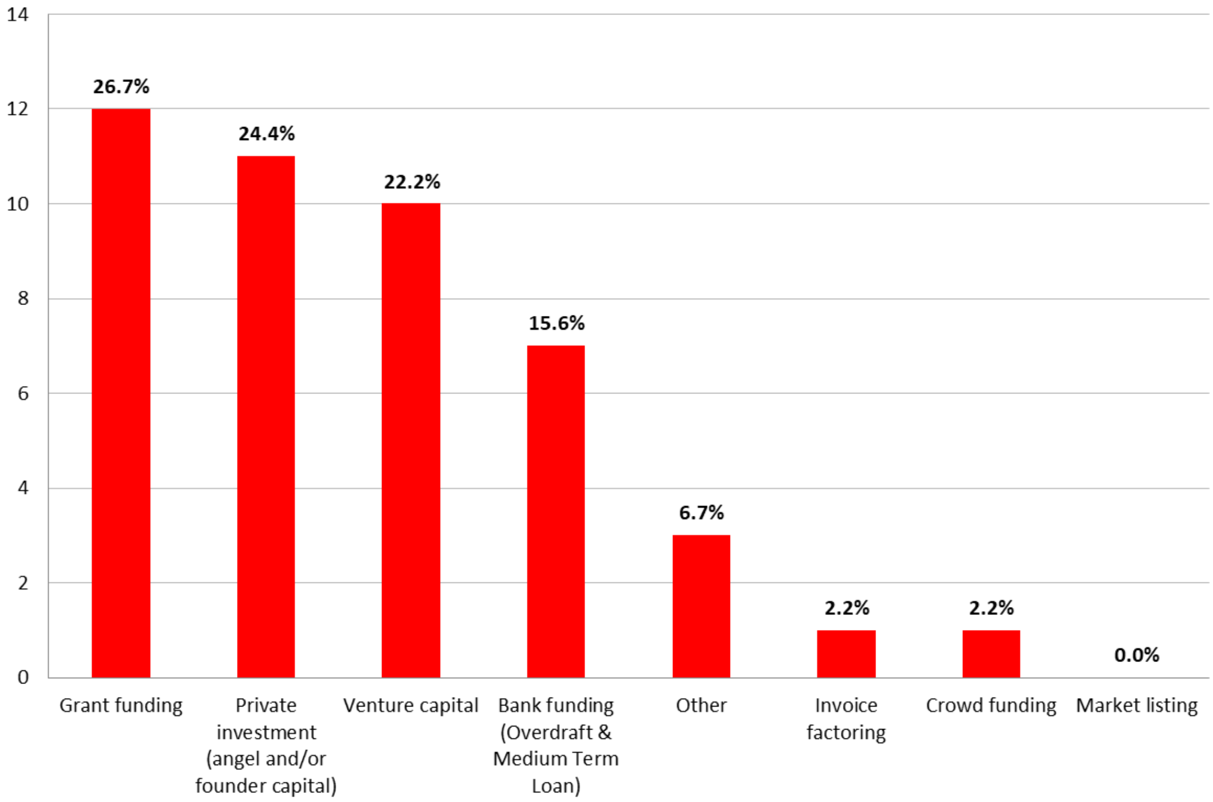


Figure 6. Sources of funding being sought over the next 12 months

AREAS OF SPECIALISM

From the survey, the areas of expertise which generated the largest proportion of companies' turnover is presented below – with cyber professional services being the most common (44.9% of businesses), followed by network security (10.2% of businesses) and threat intelligence, monitoring and detection (10.2% of businesses).

The Scottish cyber cluster has a high volume of cyber security service companies which offer a range of services for companies such as penetration testing, vulnerability scanning, security testing services and many more. Hence the high proportion of business with services as the main area of turnover is not too surprising.

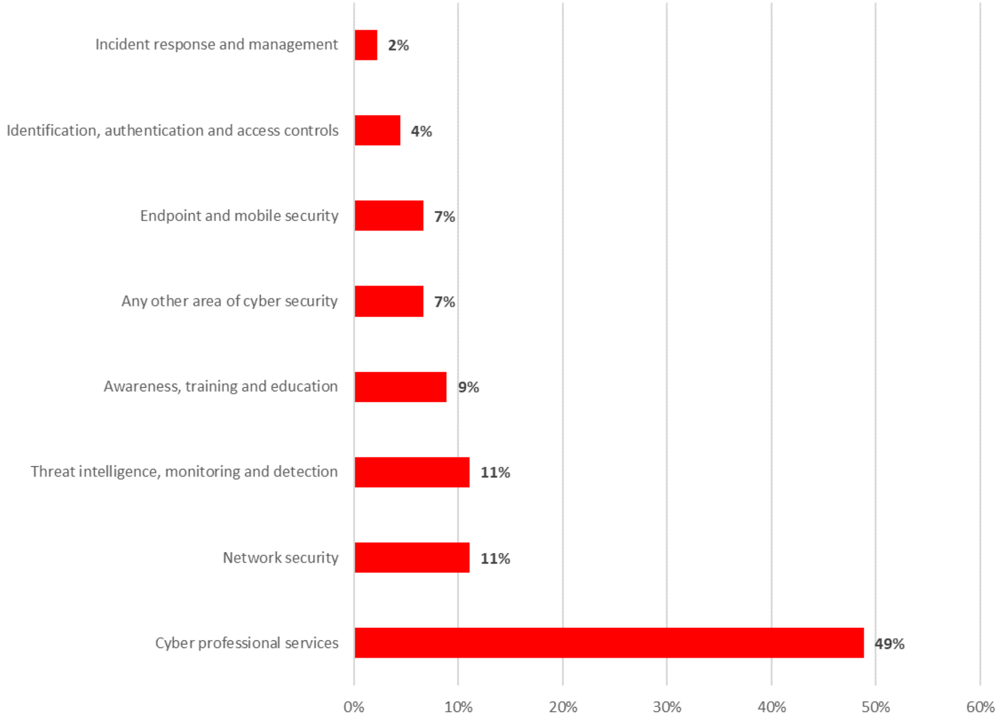


Figure 7. Areas of specialism across the cyber companies based on turnover

ACADEMIC EXCELLENCE

Scotland's higher education system has been well acclaimed over the years for its approach to innovation and research. Cyber security is still a relatively new sector, but the creation of academic courses has grown significantly in the last 5-10 years.

The University of Glasgow was the first University in Scotland to offer specific cyber related courses as they offered a Security and Cryptography module by 1999. By 2002, Scotland's strengths in cyber security education were beginning to emerge strongly within computer science degree teaching. At this time, it was already possible to take specialist modules in Forensic Computing (University of Abertay), Networking Security and Security of Information Systems (both Edinburgh Napier University), and Security and Cryptography (University of Glasgow). In addition, the University of Edinburgh had just started a Computer Security module covering a very wide range of topics, from cryptography and protocols to how to program securely. Specialist applied undergraduate degrees emerged shortly afterwards. The University of Abertay launched its BSc (Hons) in Ethical Hacking in 2006, with Edinburgh Napier University beginning to offer BSc (Hons) Computer Security and Forensics at around the same time.

Scotland's reputation in cyber security and computing science has been growing over the years. Scotland has 8% of the UK's population but has been attracting 15-18%

of the UK's computer science research grant and contract income.[10] It is worth noting that Scottish universities place a greater emphasis on recruiting internationally for their students more than universities in the rest of the UK. Whilst this may help funding in the short term, there remains a risk that all of the ideas, innovation and research leaves Scotland upon the completion of studies.

70% of Scottish universities now offer courses in cyber security, across bachelor's degrees, masters and PhDs. Scotland universities have a number of cyber security firsts such as Abertay University in Dundee had the first Ethical Hacking degree course in the world. Within the UK, currently the only fully certified NCSC Bachelor's degree is in Scotland at Edinburgh's Napier University. Scotland also has a number of NCSC certified masters[11]. Scotland is also home to an Academic Centre of Excellence in Cyber Security Research (ACEs-CSR) with Edinburgh University having received this accolade, one of 19 across the UK.[12]

Supporting the cyber security community in Scotland is Scottish Informatics and Computer Science Alliance (SICSA)[13] which is a "research pool" funded by the Scottish Funding Council. SICSA, which has a specific cyber theme as part of its remit, promotes international excellence in University-led research, education and knowledge exchange. SICSA Cyber Nexus aims to ensure that Scottish higher education institutions are working collaboratively to help make Scotland more cyber resilient and creating a vibrant innovation community. The diagram captures a rough mapping of areas of expertise across universities and regions within Scotland for example Dundee region is particularly well known for ethical hacking and gaming while Edinburgh region is known for its focus on AI and Big Data.

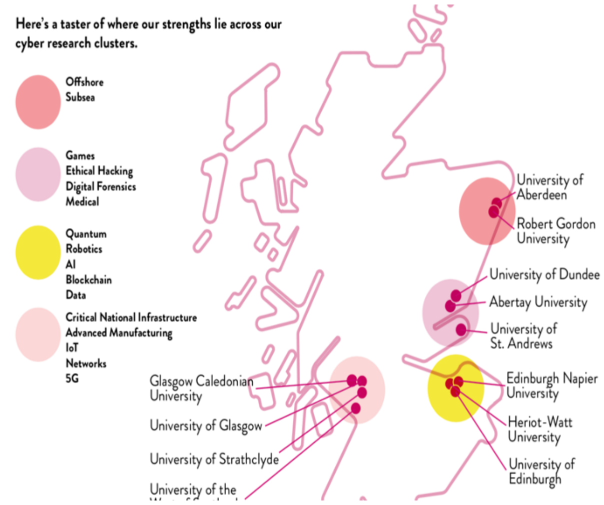


Figure 8. Diagram of cyber research strengths by region (@SICSA)

[10] HESA, Higher Education Staff Statistics: UK, 2018/19 (DT025), Table 11. https://www.hesa.ac.uk/data-and-analysis/staff/table-11.

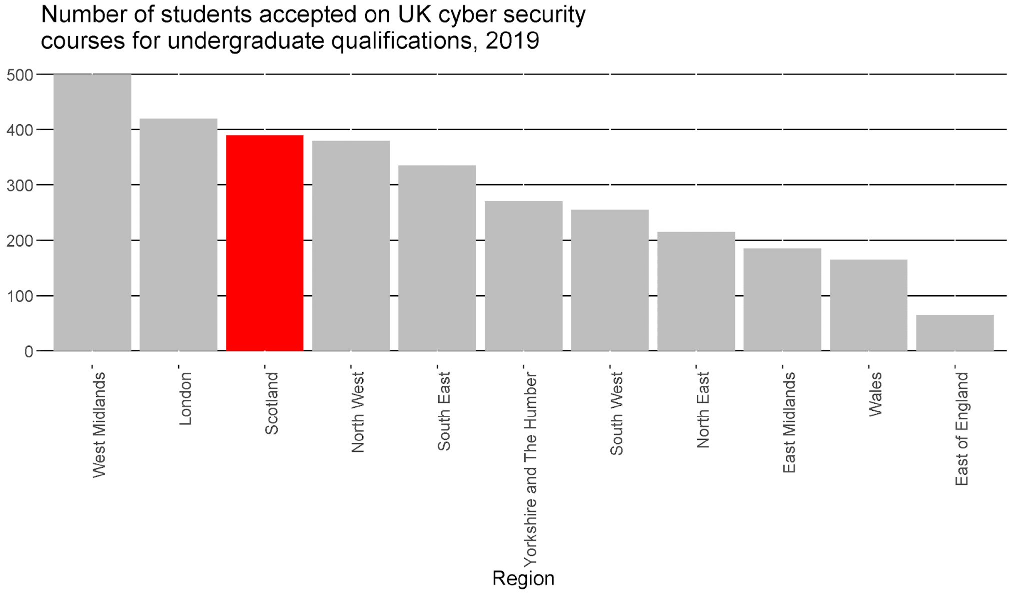
[11] NCSC certified masters available in Scotland are: MSc Ethical Hacking and Cyber Security at Abertay University and MSc in Advanced Security and Digital Forensics at Edinburgh Napier University

[12] NCSC list of ACE-CSRs https://www.ncsc.gov.uk/information/academic-centres-excellence-cyber-security-research

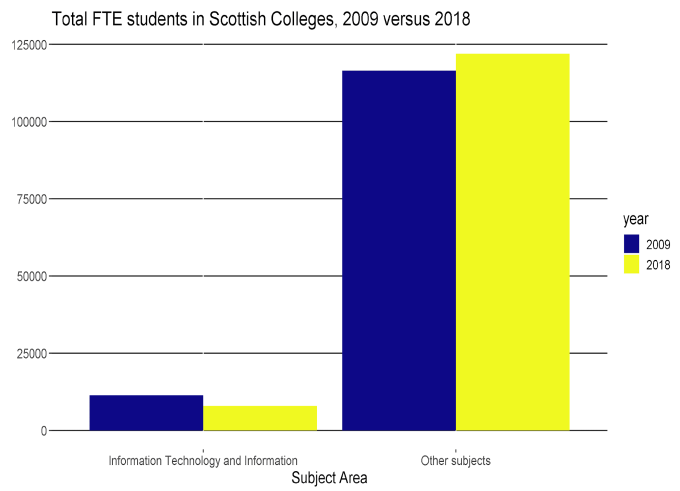
[13] https://www.sicsa.ac.uk/research/sicsa-cyber-nexus/

To support the growth of the industry, it is essential to provide a sufficient amount of high quality and accessible workforce. Therefore, it is important that Scotland provides an increasing number of new cyber security professionals, trained locally and to an excellent calibre. While the previous sections have described the ecosystem being suitable to supply high-grade graduates, the challenge is to keep up with the demand by increasing the number of students recruited and retained at Scottish cyber degrees.

The number of students studying cyber security has doubled since 2015 with numbers going from just under 200 undergraduates in 2014 increasing to just below 400 undergraduates in 2019. Scotland has the 3rd highest number of students studying cyber courses when compared to other parts of the UK as the table below demonstrates.



Source: Data purchased from UCAS



Source: Scottish Funding Council's College Statistics 2018-19, Background tables

The uptake in cyber and information technology courses in Scottish colleges has declined slightly as shown in the graph. In the 10 years between 2009 and 2018 there was an approximately 30% drop in interest for the technology subjects, which does not correlate to the overall increase in admissions for all other subjects. The reason for this is unknown, but this needs to be tackled with a cross-ecosystem approach, by strengthening the pipeline from secondary education through to routes into industry offered via these courses.

Scotland is continually expanding the available courses in cyber with a cyber security HNC introduced in 2018 and HND being added in 2019 with the uptake increasing since their introduction. The expectation is that numbers studying these courses and technology subjects generally will increase over the next few years as the numbers of colleges offering these course ramp up.

CYBER SKILLS IN SCOTLAND

The digital skills gap has long been an issue in Scotland as per the rest of the UK and beyond, and the COVID-19 pandemic has accelerated such gaps.

According to the DCMS UK Cyber Skills report[14], in the last 3 years 4.3% of core cyber security job vacancies were placed in Scotland (i.e. approx. 4,500 vacancies in the last three years)[15]. London has had significantly more than other regions (35.5%) with numbers varying strongly among other parts of the UK with the lowest being North East England (1.2%), Northern Ireland (1.5%) and Wales (1.4%).

Taking an aggregated estimate of registered firms in Scotland, with non-registered but active employers in Scotland's cyber sector, as well as other private and public roles (e.g., within CISO functions, finance and insurance, and law enforcement), it has been estimated that Scottish cyber security employment is likely to consist of approximately 4,000 FTEs in total which comes from

- Circa 1,500 - 2,000 'sector-facing' private roles and another

[14] Cyber Security Skills in the UK Labour Market 2020 report: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020

[15] Timescale used was September 2016 to August 2019

- Circa 1,000 roles (e.g. in CISO functions within banks / insurers)
- 1,000 public sector / law enforcement roles.

It should be noted that this these figures are projections by Perspective Economics based upon UK and other regional estimates. They note that this is a conservative estimate and requires further detail regarding some of the largest employers within the region (e.g. large cyber security teams within financial services institutions for example).

The survey responses showed that 45% of the cyber security companies surveyed have 5 or less cyber employees in Scotland. Of these companies, the majority were SMEs with 5 or less employees in their entire business.

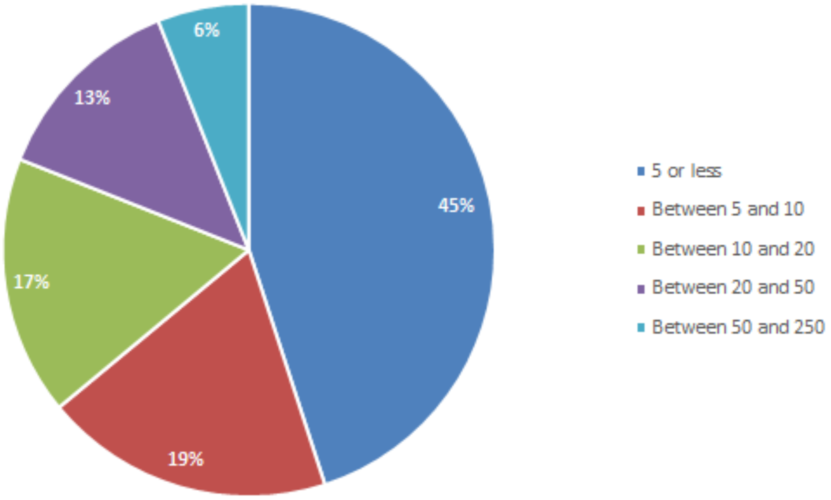


Figure 9. Number of Scotland based cyber employees in cyber companies

If these numbers were extrapolated across the entire cluster this would indicate that there is an average of around 4000 people working in cyber security companies in Scotland[16].

According to the report by ISC2 the global cyber security workforce skills gap has now exceeded 4 million. The majority of this gap exists in Asia (2.9million) with 295,000 being in Europe.[17]

A report by the Federation of Small Businesses on skills and training has identified that over a fifth of small businesses are failing to take advantage of the digital world partly because their staff lack digital skills (22%) but also because of concerns about cyber

[16] The calculated minimum is around 2000 and maximum is just over 6500.

[17] ISC2 report - https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

security (21%).[18] The COVID-19 pandemic acutely demonstrated this and also highlighted the scale of the challenge facing a number of Scotland's key sectors to truly embrace digital.

Scotland's capital city has become synonymous with our success in the cyber security sector. Edinburgh is very much a "cyber hotspot" in the UK, alongside some other key regions such as London and the West Midlands. Edinburgh is number 4 in the UK for absolute number of cyber jobs postings and Glasgow is ranked at number 10. According to Bright Tech Future, Edinburgh and Glasgow are two of nine cities, outside the capital, which now have more than a fifth of the workforce employed in tech. Edinburgh, in particular, ranks in the top 3 for desirable locations for cyber security roles.[19]

Scotland as a whole, is very competitive when it comes to cyber security salaries, currently it ranks 4th place in UK ranking with a mean salary of £54,900, which helps Scotland to attract and retain cyber talent. This marks an ongoing shift towards a growing cyber community in Scotland that is competitive with the wider UK.

WIDER SCOTTISH CYBER CLUSTER

There are many organisations outside the actual cyber security companies which play a key role in the cyber cluster and the wider cyber security ecosystem. They break down largely as:

- academia and research institutions (see academia section for info),
- accelerators and innovation centres such as CENSIS,
- end users across the public, private and third sectors,
- supporting bodies and key public sector stakeholders (for example SBRC, SDS, SCVO).
- And Scottish Government and Scottish Enterprise who play a key role in supporting and funding numerous cyber focussed projects and initiatives

The cyber cluster is part of the wider Scottish cyber and digital ecosystem who work collaboratively to deliver the Scottish Government's mission[20] for Scotland to be a secure place to live, work and do business.

GOVERNANCE AND FRAMEWORK OF THE SCOTTISH CYBER CLUSTER

The Scottish Cyber cluster operates out of the ScotlandIS Cluster Management organisation (CMO) which is now ESCA silver accredited in cluster management

[18] http://www.fsb.org.uk/docs/default-source/fsb-org-uk/skills-and-training-report.pdf?sfvrsn

[19] Cyber Security Skills in the UK Labour Market 2020 report: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020

[20] https://www.gov.scot/publications/safe-secure-prosperous-cyber-resilience-strategy-scotland/pages/5/

excellence[21]. It is currently the only silver accredited CMO in the UK and is home to a number of tech clusters. The cluster is currently publicly funded however it is expected to be self-funded at some point.

There is an advisory group, which meets every 2-3 months, made up of largely industry and some representatives from academia. This group (of 10 advisors) is a volunteer group, which helps to provide guidance and support to the cluster, as well as getting directly engaged in cluster activities.

The cluster manager reports to the CEO of ScotlandIS, who provides support and guidance for the cluster manager, as well as the CMO providing some marketing and event support. There is also a strong partnership with Scottish Enterprise, who are key stakeholders for the cluster.

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

UK CYBER CLUSTERS

The UK have over 20 cyber clusters many of which have been operating for some time. The concept of providing regional cyber security clusters was laid out by the UK Government's Cyber Security Strategy in late 2014. The cyber clusters act independently, although there is regular engagement with DCMS in particular.

The way the cyber clusters operate, what they focus on and how they fund themselves varies a lot across the clusters. This section looks to highlight a number of the more active clusters and to provide some insights into how they operate.

Overall the clusters across the UK tend to focus on these main areas:

- Cyber security sector innovation and growth.
- Cyber skills pipeline working across schools, colleges, universities and industry, to ensure there is a right mix of future talent to support the cyber security needs of businesses.
- Cyber resilience – ensuring businesses and individuals have sufficient knowledge and access to training on cyber security through working with local resilience centres (where they exist) and local police forces.

The level of focus on these areas may vary between clusters, i.e. with some predominantly focussed on innovation and growth, and others more actively involved in the cyber resilience side. The emergence of the business resilience centres[22] in some locations may also change the focus of the clusters over the next few years to focus less on cyber resilience, and more on innovation and skills.

YORKSHIRE CYBER SECURITY CLUSTER (YCSC)

The Yorkshire cyber security cluster (YCSC) was founded in 2015 and has 22 cyber companies in their cluster region with 14 of these companies being headquartered in this region. They have a larger and active wider ecosystem with around 175 companies being involved in the wider cluster activities. They do not use a formal membership registration approach, instead companies or individuals who attend at least 3 events are considered part of the cluster.

Yorkshire is home to Sheffield Hallam University, which recently has had its MSc in Cyber Security certified by NCSC. A number of their companies have been through LORCA, the GCHQ Cyber Accelerator. The chair of the Cluster, Melanie Oldham also represents the clusters on the Cyber Growth Partnership[23] programme as well.

[22] https://www.brimcentre.com/

[23] https://www.techuk.org/cyber-growth-partnership

The YCSC is entirely volunteer run with no paid resources currently involved. Cluster members give their time to support the cluster activities. They have a steering committee (6 members plus the cluster manager) who run the cluster. They also have an advisory group which supports the governance and direction of the cluster. YCSC run a monthly cluster event as well as further ad hoc events through the year, such as schools' cyber skills events.

YCSC have stated that their strength lies in their focus on cyber skills agenda covering schools, colleges and universities, the diversity of the cluster and the collaboration among the cluster members. They also seek to provide a platform to connect heads of academia, public sector, cyber products and services to collaborate, share best practice, support growth and innovation. YCSC has plans to continue to grow and to strengthen the cluster and are looking at ways of doing this with a focus on securing funding to help achieve this. One of the challenges this cluster faces is the time constraints of its management team due to it being managed entirely by volunteers.

CHELTENHAM CYBER SECURITY CLUSTER (CYNAM)

The Cheltenham Cyber Security Cluster (CyNam) has the prestige of being in close proximity to GCHQ and being part of a rapidly growing region of cyber security and tech innovation through Hub8 and the planned Cyber Central. It has been operating as a cluster for just under 4 years (late 2016). It covers primarily the Cheltenham area but has expanded to cover Gloucestershire too.

The cluster has 123 cyber companies operating in that region with around 12% of these companies developing new cyber products. According to Cynam, 89 of the companies are headquartered in the area however only 49% of those are registered in that area – which is a trend we have also identified in Scotland.

The CyNam cluster has a wide membership with around 2400 individual members at the time of writing – this is predominantly from the Cheltenham area but does include individuals from across the UK and outside the UK as well. They are home to an ACE through the University of Bristol and also have a NCSC certified BSc/MSc at the University of West England.

The CyNam cluster has identified their key strengths as the GCHQ proximity which provides a number of advantages, such as the high quality software engineering and data scientist skills available in the area, the volume of start-ups which have spun out of GCHQ and the concentration of former military and defence personnel in the region, which strengthen the cyber skills and expertise.

CyNam runs a number of large events throughout the year (typically 3 events per year). They are free to attend and are funded through sponsorship. They also run further networking events and focussed workshops throughout the year. The cluster works closely with Hub8 which is a co-working space focussed at the cyber security sector. CyNam is self-funded and operational costs are funded through annual sponsorship from industry partners, with events funded by event sponsors.

The cluster management team is the board, made up of 7 directors of local cyber businesses which provide professional services including legal, finance, HR and with an additional director working in an i100/ Cyberfirst role. Execution of activities is supported by the dedicated CyNam Operations Manager which is a funded role for 3 days a week through the industry partner sponsorship. The board of directors is voluntary.

The cluster collaborates closely with its neighbouring clusters of Bristol, Bath and South Wales. The Cheltenham cyber security sector is expected to significantly grow over the next few years with a large investment being made by the Cheltenham Borough Council to develop Cyber Central.

NORTH EAST ENGLAND CYBER SECURITY CLUSTER (CYBER NORTH)

The North East England Cyber Security Cluster (Cyber North, population around 3.5million) covers from Northumberland to Teesside (across 12 local authorities) and is the neighbouring cluster to the Scottish cluster. It has been operating as a cluster for 3 years. There are 68 cyber companies operating in the region with 55 of them being headquartered in that area. The wider cluster would include over 100 companies (with professional services etc.) however information is still being collated on the wider ecosystem at this time. There are currently a small number of start-ups operating in that area.

Both Newcastle and Northumbria Universities are recognised ACEs. The main focus of the cluster is regional jobs growth, with the mission being to make the North East England the place for cyber security through being a region of high cyber awareness and infrastructural resilience, a centre of excellence in the delivery of Cyber related services, a centre of excellence in the development of high quality students and employees and noted for research and development in cyber.

The cluster is governed by a steering group which currently has 8 members. The cluster manager is funded for 1 day per week. The funding has come from an industry partner and the local council. The cluster is part of Dynamo North East, a business led organization working to grow the North East tech sector. The steering group meets monthly.

CyberNorth is intending to grow the cluster through greater engagement with cybersecurity companies, with other clusters and with DCMS, and is aiming to become self-financing at some point in the future too. Funding of the cluster is currently identified as a challenge. The cluster is also creating a business case for a North East Cyber innovation centre (ORCANE).

GLOBAL CLUSTERS

In addition to there being many UK cyber clusters, there are naturally cyber clusters around the globe. The term 'cluster' may not necessarily be prevalent in all countries but nonetheless similar activities in terms of promoting innovation, providing guidance and training on cyber resilience and cyber security best practice and seeking to grow the sector are happening in many countries around the world.

It is important that Scotland looks at cyber clusters beyond the UK to gain learning and insights from other countries, and work will continue to gather these insights and build relationships with these clusters. It is however worth adding that the model is very different across countries, and as Scotland is part of the UK, the responsibility and accountability of various aspects sit across a number of UK-wide and Scottish organisations, while other countries can have that much tighter coupling of having all elements under the one body or organisation.

ESTONIA CYBER CLUSTER (EISA)

Estonia (population 1.3m) has a strong reputation in providing secure digital solutions, including a country-wide digital identity used by all citizens. The Estonian Information Security Association (EISA) was set up in early 2018. This is considered to be the cyber cluster organisation in Estonia (or closest equivalent). It has 2 universities and 6 cyber security companies (4 of which are headquartered in Estonia) as formal members, with a wider cluster of around 35 companies. This extends to approximately 45 when you include wider ecosystem partners as well.

In terms of skills and cyber pipeline, Estonia has reported the following numbers:

- Total volume of undergraduate students: 790
- Total volume of graduated cyber students: 180
- Volume of PhDs ongoing: 21

When asked about their strengths the Estonian cluster provided the following responses:

- **Strong ecosystem and collaboration** – EISA has been created to formalise the ties between the private sector, public sector and academia in the ecosystem, but the collaboration and public-private partnership has always been very strong. A few collaboration examples are the handling of 2007 cyber-attacks against Estonia and 2017 ROCA vulnerability case.
- **Fundamental eGovernment technologies -** This is what the Estonian ecosystem is known for; the successful eGovernment is built on public-private partnerships. These technologies include for example secure digital identity, distributed data exchange platform usage, KSI blockchain timestamping in registries, etc.

- **Cyber range and exercises** – Estonia has quite a few companies working successfully in this field.

The EISA has stated that their main focus is formalising the existing ties between the cybersecurity partners in Estonia boost collaborative participation, as well as influence the European and international policies on cybersecurity. Their mission is the advancement of cooperation in Estonia between the private sector, academia and the government in the field of information and cyber security.

EISA is managed by the Board of Directors (currently 3 members). The association acquires its resources from yearly membership fees. One project manager works for EISA part-time. There are 8 members – 6 companies and 2 universities with the membership structure being based on stature.

The events are mainly organised in conjunction with the government - Information System Authority and the Ministries of Economics, Foreign Affairs, Interior and Defence, such as the cyber ecosystem meetings, the creation of the cybersecurity strategy, etc.

In terms of future growth and vision, EISA envisages growing slowly but steady, which means inviting other established cybersecurity companies as members. EISA will also continue working with the government to deliver common projects. EISA sees lack of resources as a challenge and would seek to receive funding from the government to support the expansion of EISA activities and to allow participation in more EU consortium projects.

IRELAND CYBER CLUSTER (CYBER IRELAND)

Cyber Ireland, the national cyber security cluster organisation, was launched in May of 2019 with a cluster strategy and board, after 6 months of stakeholder engagement and development. Cyber Ireland brings together industry, academia and government to represent the needs of the cyber security ecosystem in Ireland, and aims to enhance the innovation, growth and competitiveness of Ireland's cyber security ecosystem. Cyber Ireland has a number of objectives, including:

1. Talent & Skills - Sustainable generation of a critical mass of talented information security professionals.
2. Innovation - Enhanced cyber security research and innovation between industry and with academia.
3. Promotion & Networking - Stronger national industry sector branding, and bringing the cyber security cluster together through events to facilitate networking, sharing of experiences and collaboration.

4. Internationalisation - Increased international competitiveness to support SMEs and attract FDI.

Cyber Ireland has almost 200 member organisations, 165 of which are from industry, including 30 start-ups. There are 20 knowledge providers, encompassing universities, research centres and training groups.
It is estimated that around 7000 people are employed in the cyber security sector in Ireland, with there being circa 30,000 individuals with security certifications across the country.

The cyber cluster received government funding for the initial 2 years, and has recently launched a new membership model in July 2020, due to that funding period nearing its end. Cyber Ireland is run out of Cork Institute of Technology, however it does cover all of Ireland (which excludes Northern Ireland). The cluster is run by a cluster manager and a marketing manager, both of whom are funded staff. There is also additional support from staff at Cork Institute of Technology where the cluster is based. It is governed by a board made up of eight representatives from industry, three from academia and three from government, including the National Cyber Security Centre, and has a regional representation from across the country, as well as ensuring a minimum of 30% female board members. It also reports to government funders on a bi-annual basis.

Cyber Ireland works with other cyber clusters from across the world, but in particular with Denmark, Wales, Northern Ireland, Israel and Canada. They are part of Global EPIC[24] and use this platform to collaborate with these clusters. They also collaborate with other clusters in Ireland, such as Technology Ireland, among others.

Cyber Ireland has stated that their main challenges are in providing value to their members in a changing environment with COVID-19, transitioning to a paid membership model and ensuring ongoing funding and sustainability. The cluster is also keen to stay focussed on being an innovation cluster and not digressing into being an industry association or networking organisation.

AUSTRALIA (AUSTCYBER)

The AustCyber website states that it “supports the development of a vibrant and globally competitive cyber security sector”. AustCyber was established in

[24] https://globalepic.org/HomePage

2017 as an independent, not-for-profit organisation, which is funded by federal government grants. It ties in to 2 main programmes in Australia – Australia's Cyber Security Strategy and the Industry Growth Centres Initiative. AustCyber has 17 staff members listed with an additional 4 board members.

Its strategic objectives are:

- Grow an Australian cyber security ecosystem
- Export Australia's cyber security capabilities to the world
- Make Australia the leading centre for cyber education

In terms of growing the cyber ecosystem they focus on:

- Helping start-ups to find first customers
- Making access to capital and VC easier
- Improving research focus and accelerate to commercialisation
- Simplifying procurement
- Providing measurement

Australia businesses (including public sector) spend about £2.26bn (A$4bn) with an additional £0.73bn GBP (A$1.3bn) over next 10 years. The cyber security sector in Australia employs around 20,500 people. AustCyber carried out a recent survey which indicated that around 90% of the cyber companies in Australia are SMEs, with an average firm age of approximately 7 years. 53% of the firms were less than 5 years old.

AustCyber has confirmed that the focus of the cyber companies are predominantly on software & platform security, attacks & defence, human services (human, organisation and regulatory aspects), system security and infrastructure security. The highest spend on cyber comes from the financial services, federal government and telecommunications sectors.

CONCLUSION

This report has documented a 'snap-shot' of the Scottish cyber cluster providing that baseline from which growth can be tracked in future. It has additionally provided an overview of some UK and internationally based clusters, in order to get a better understand of the focus and operations of other clusters.

As highlighted in the report, the Scottish cyber cluster has many positives that it can take encouragement from, such as; a large cyber community with a good mix of company types and sizes at all stages of their journeys from start-ups, scale-ups, SMEs to large global enterprises. These organisations are being set-up throughout Scotland with companies being established across all the major cities and beyond. Additionally, there is a strong and well recognised academic and research capability in Scotland which is continuing to grow, and an ongoing focus on cyber skills at all levels. Collectively these combine for a strong cyber security job market in Scotland both in terms of volume of jobs being posted and also quality and associated salary. On the whole there is much to celebrate when it comes to Scotland's cyber security cluster.

It is only correct as part of this analysis to also include where improvements do need to be made and this is certainly in the area of investment, which is below par in comparison to other parts of the UK. This will be an area of focus that will be taken forward to understand the cause and to also find a solution.

Building on the learning and insights from other UK and global clusters, and bearing in mind that the clusters varied in focus and structure, we can still take the following messages away:

- Clusters need to be funded (whether through government or members) in order to be sustainable and impactful
- Clusters help through being a focal point for the community and providing connections to other sectors, other cyber clusters, local government and the wider innovation and academic ecosystem.
- The clusters that really benefit their community are the ones with a global outlook and focusses on building relationships beyond their geographical reach.
- Clusters can and should play a key role in supporting innovation within their clusters

It is hoped that this report is considered to be informative and that it documents an accurate view of the Scottish cyber cluster at the time of writing (September 2020). Further work to refine the insights and understanding of the cluster is being planned, such as the identification of areas of specialisms and emerging sub-clusters. This will lead to an even better understanding of what makes the Scottish cyber cluster unique, and additionally help to form the strategy on how to continue to grow and develop the Scottish cyber cluster.

APPENDICES

APPENDIX 1: RESEARCH APPROACH

The following approach was used to carry out research and data gathering for this report.

- **Scope agreement**
  The scope was circulated to Scottish Enterprise and the Economic Opportunity Action Plan working group for review and further discussion.

- **Desk research**:
  The initial gathering of information was done as desk-based research using a number of different sources, many of which have been highlighted through the document. Additionally, a number of bodies or organisations were contacted such as SICSA, SDS, Scotland Colleges, Ipsos MORI, Perspective Economics and more.

- **Surveying**

A number of surveys were sent out:

- Survey to individual Scottish cyber cluster companies. The survey responses were based on the 56 responses received. [Note: this number has factored in some companies which sent 2 survey responses in from different individuals, which were then merged to 1 response per company]. 56 was the usable volume of survey responses.
- Questionnaires were sent to a number of UK cyber clusters (6 in total), of which the 3 responses received were included in the report.
- Questionnaires were also sent to some international clusters. They normally involved a phone call prior to the survey being sent out, to establish the relationship and explain the context.

- **Additional note on data comparison**

It is worth noting that the data in the UK cyber sector report, which has been referenced a number of times throughout this report, will differ from the Scottish cyber cluster report for 2 main reasons:

- The cyber cluster includes all cyber companies operating in Scotland, while the UK sector report focuses upon the economic contribution of (dedicated)[25] cyber security firms registered as UK headquartered in Scotland.
- The definition of cyber security is narrower in the UK cyber sector than it is in the Scottish cyber cluster - for example this report included Online Safety Technology companies while the UK cyber sector focuses solely upon the DCMS cyber security taxonomy.

[25] Dedicated, in this context, means that the company only provides cyber security products and does not have a wider portfolio outside of cyber security.