Ipsos MORI
Social Research Institute

Perspective Economics

Queen's University Belfast | CSIT Centre for Secure Information Technologies

January 2020

UK Cyber Security Sectoral Analysis 2020

Research report for the Department for Digital, Culture, Media and Sport

Sam Donaldson, Perspective Economics
Jayesh Navin Shah and Daniel Pedley, Ipsos MORI
David Crozier, Centre for Secure Information Technologies
Professor Steven Furnell, University of Plymouth

Foreword

The UK is one of the world's leading digital nations, home to exceptional talent, cutting-edge innovation and rapid growth. In 2016, the Government published its National Cyber Security Strategy (2016-2021), where we set out our commitment to defend our systems and infrastructure, deter adversaries, and to develop a whole-society capability to protect our digital economy.

Since then, we have invested significantly - with £1.9bn allocated to the strategy - in supporting the development of the UK's cyber security ecosystem. The National Cyber Security Centre (NCSC), officially opened in February 2017, has provided world-class, user-friendly expertise for businesses and individuals and has also been at the forefront of protecting the UK from online threats, handling well over six hundred incidents in 2019[1] alone.

We know that Government cannot work alone in tackling the cyber threat, and that we must do all we can to support commercial innovation, academic know-how, and to promote clear routes to develop and harness a sustainable talent pipeline in cyber security.

When Government launched the National Cyber Security Strategy (NCSS), we set out the challenges often faced by the cyber security sector. We identified a need to help new innovative products and services reach the market, as well as to support early-stage companies secure investment for developing, testing and expanding their offer.

To help meet this challenge, we have invested in two world-leading innovation centres in London and Cheltenham, and have provided a range of support for entrepreneurs, start-ups and for the commercialisation of academic research to grow and strengthen the cyber security sector. We have also made the case to businesses and individuals to practice cyber hygiene, through initiatives such as Cyber Essentials.

As this research shows, there has never been greater demand, both at home and internationally, for the products, services and expertise offered by the UK cyber security sector. Over the last two years, there has clearly been significant progress within the sector, which has reported double-digit annual revenue and employment growth, as well as record investment in early-stage companies.

Much has been achieved through the National Cyber Security Strategy, and the strength and dedication of our commercial sector clearly underpins the UK's efforts to be one of the safest places to live and work.

Government will continue with its efforts to support the UK's world-leading cyber security sector to remain internationally competitive, to develop innovative and ground-breaking new products and services, to expand and access new markets, and to secure the best talent available to ensure sustainable growth.

The Rt Hon Matt Warman MP
Parliamentary Under Secretary of State
Minister for Digital and Broadband

[1] National Cyber Security Centre (2019) Annual Review: https://www.ncsc.gov.uk/news/annual-review-2019

Contents

List of figures

Executive Summary

Introduction

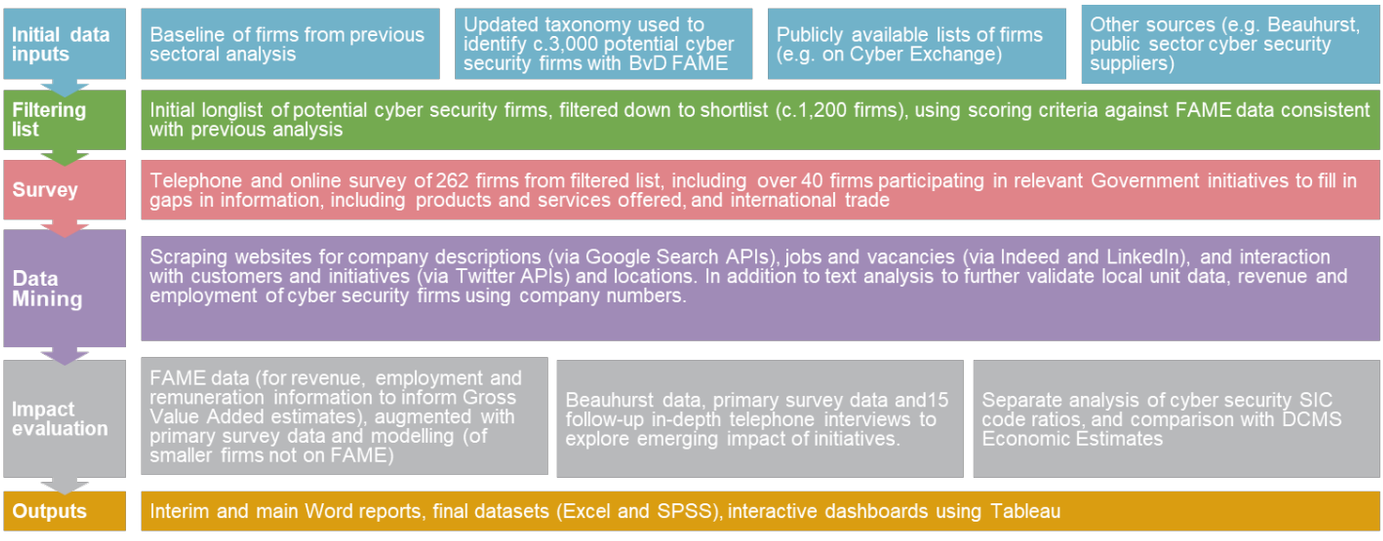
Ipsos MORI, in conjunction with Perspective Economics, the Centre for Secure Information Technologies (CSIT) at Queen's University Belfast, and Professor Steven Furnell (University of Plymouth) were commissioned by the Department for Digital, Culture, Media and Sport (DCMS) in January 2019 to undertake an updated analysis of the UK's cyber security sector.

This analysis builds upon the baseline UK Cyber Security Sectoral Analysis (published in October 2018[2]) that provided an estimate of the size and scale of the UK's cyber security industry. This provided a baseline (using 2015/16 financial data) for the number of UK cyber security companies; the cyber security sector's contribution to the UK economy (through revenue and GVA); the number of personnel employed in the cyber security sector; and an overview of the products and services offered by these firms.

As the UK's National Cyber Security Strategy[3] (NCSS) runs until 2021, this analysis effectively provides a mid-point review of the current size and scale of the UK's cyber security sector.

Project Scope & Summary of Methodology

The following diagram sets out a summary of the research methodology utilised.



Source: Ipsos MORI, Perspective Economics, and the Centre for Secure Information Technologies (2019)

[2] Donaldson, S, Hobson, J., Stow, C, and Crozier, D., (2018) 'UK Cyber Security Sectoral Analysis'. Available at: https://www.gov.uk/government/publications/uk-cyber-security-sectoral-analysis

[3] UK Government (2016) 'National Cyber Security Strategy – 2016-2021': Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

Key Findings

Number of Companies

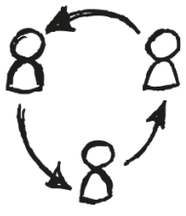
We estimate that there are 1,221 firms active within the UK providing cyber security products and services (2019).

- ↑ This reflects an increase of 44% since the baseline report (846 firms).

In the last two years, we have identified 118 new business registrations within the cyber security sector.

- ↑ In other words, a new cyber security business is registered every week within the UK.

90% of the sector consists of SMEs, with an associated estimated turnover of £2bn (24% of the sector's revenues).



Sectoral Employment

We estimate there are approximately 43,000 Full Time Equivalents (FTEs) working in a cyber security related role across the cyber security firms identified.

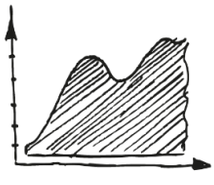
- ↑ This reflects an estimated increase of 37% in employee jobs over the last two years.

The majority (65%) of cyber security employment is based within large firms.

Sectoral Revenue

We estimate that total annual revenue within the sector has reached £8.3bn.

- ↑ This reflects an increase of 46% since the 2017 baseline analysis (i.e. revenue has increased by £2.6bn from £5.7bn).
- ↑ On average, we estimate that revenue per employee has reached £193,500 (an increase of 7% since baseline).



Gross Value Added

We estimate that total Gross Value Added (GVA) for the sector reached £3.77bn.

- ↑ This means total GVA has increased by 60% in the last two years, from £2.35bn).
- ↑ GVA per employee has reached £88,000 (an increase of 17%).

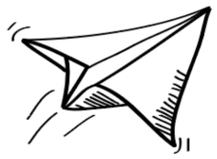
Products and Services

The most commonly provided cyber security products and services (see Section 2.3) by the sector include:

- Cyber Professional Services (provided by 71% of firms)
- Threat Intelligence, Monitoring, Detection and Analysis (46%)
- Endpoint Security (including Mobile Security (37%)

Emerging Sub-Sectors:

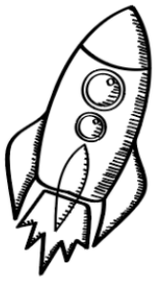
- ↑ IoT Security, SCADA and ICS, Post-Quantum Cryptography



Growth Drivers

The cyber security sector has grown through both increased domestic demand (particularly driven by the implementation of GDPR) and through increased exports.

Further, external investment and increased procurement of cyber security products and services has also helped to increase demand and growth within the sector (see Section 4.2).



Investment

Section 4 (Investment in the UK Cyber Security Sector) demonstrates that:

- ↑ 2019 was a record year for cyber security investment, with £348m in fundraising across eighty deals.

Indeed, over the last four years (2016-19), total external investment identified within the cyber security sector has exceeded £1.1bn, demonstrating how investment and confidence has grown in recent years.

Industry Support

The UK Government has invested in a range of initiatives to help cyber security start-ups, early-stage companies, and high growth companies develop market-leading products and secure external investment.

This research highlights that these initiatives have a key role to play in helping to:

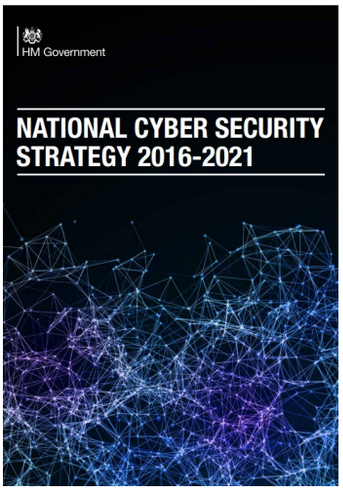
- ↑ develop new products and services (particularly innovative products that can tackle new cyber security challenges);
- ↑ connect high-potential, high-growth businesses with investors; and
- ↑ develop a more coherent ecosystem of cyber security providers, through promoting collaboration and mentoring.

1 Introduction

Ipsos MORI, in conjunction with Perspective Economics, the Centre for Secure Information Technologies (CSIT) at Queen's University Belfast, and Professor Steven Furnell (University of Plymouth) were commissioned by the Department for Digital, Culture, Media and Sport (DCMS) in January 2019 to undertake an updated analysis of the UK's cyber security sector.

This analysis builds upon the baseline UK Cyber Security Sectoral Analysis (published in October 2018[4]) that provided an estimate of the size and scale of the UK's cyber security industry. This provided a baseline (using 2015/16 financial data) for the number of UK cyber security companies; the cyber security sector's contribution to the UK economy (through revenue and GVA); the number of personnel employed in the cyber security sector; and an overview of the products and services offered by these firms.

As the UK's National Cyber Security Strategy[5] (NCSS) runs until 2021, this analysis effectively provides a mid-point review of the current size and scale of the UK's cyber security sector.



Setting the Scene: *"A burgeoning and innovative cyber security sector is a necessity for our modern, digital economy. UK cyber security firms provide world-leading technologies, training and advice to industry and government. But whilst the UK is a leading player, it faces fierce competition to stay ahead…"*

Objective: *The Government will support the creation of a growing, innovative and thriving cyber security sector in the UK in order to create an ecosystem where:*

- *security companies prosper, and get the investment they need to grow*
- *the best minds from government, academia and the private sector collaborate closely to spur innovation*
- *customers of the Government and industry are sufficiently confident and prepared to adopt cutting-edge services.*

Measuring Success: *The Government will measure its success in stimulating growth in the cyber security sector by assessing progress towards the following outcomes:*

- *greater than average global growth in the size of the UK cyber sector year on year*
- *a significant increase in investment in early stage companies*
- *adoption of more innovative and effective cyber security technologies in Government.*

With respect to measuring success, this report focuses upon understanding how the sector has grown year-on-year, and how early-stage companies have been able to secure investment and support.

[4] Donaldson, S, Hobson, J., Stow, C, and Crozier, D., (2018) 'UK Cyber Security Sectoral Analysis'. Available at: https://www.gov.uk/government/publications/uk-cyber-security-sectoral-analysis

[5] UK Government (2016) 'National Cyber Security Strategy 2016-21' Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

1.1 Methodology & Sources Used

The UK Cyber Security sector does not have a formal Standard Industrial Classification (SIC) code, and this study therefore closely aligns itself to that of the baseline analysis, in order to provide a time-series analysis of how the sector has progressed since baseline (2017).

The following methodology and research sources were used to provide an overarching shortlist of UK cyber security businesses, and to estimate their economic contribution related to the sale of cyber security products or services.

Stage 1: Desk Research

The research team conducted initial desk research to explore how the cyber security market had changed within the last two years. This included a review and identification of:

- UK cyber security regional networks and clusters (e.g. CyberExchange[6], Cyber Resilience Alliance[7], South Wales Cyber[8] etc.)
- published reports regarding the output or activities of the sector (e.g. UK Cyber Security Exports Strategy[9] and associated annual export statistics[10], the UK Cyber Security Skills Strategy[11], and the UK Cyber Security Breaches Survey[12])
- recent investments or initiatives in the cyber security sector (including review of investments and acquisitions, and identification of new industry initiatives e.g. Tech Nation Cyber[13])
- any emerging trends in the market (including supply-side and demand-side) e.g. enhanced demand attributable to GDPR compliance, or new product innovations requiring specific cyber security requirements (e.g. IoT security).

Stage 2: Taxonomy Review

Subsequently, a taxonomy review workshop was held in February 2019 with members of industry, Government, academia and representative bodies to test how the cyber security market should be defined and categorised (as of 2019). This provided an updated taxonomy and definitional terms to be used to identify a long-list of potential cyber security firms in the UK.

[6] Cyber Exchange: https://cyberexchange.uk.net/#/home

[7] Cyber Resilience Alliance (Gloucestershire, Worcestershire, The Marches, and Swindon & Wiltshire LEPs): https://www.cyberresiliencealliance.org/

[8] South Wales Cyber Security Cluster: https://southwalescyber.net/

[9] UK Government (2018) Cyber Security Export Strategy: Available at: https://www.gov.uk/government/publications/cyber-security-export-strategy

[10] Department for International Trade / Defence and Security Organisation (2019) 'UK Defence and Security Export Statistics for 2018' Available at: https://www.gov.uk/government/publications/uk-defence-and-security-exports-for-2018/uk-defence-and-security-export-statistics-for-2018

[11] Department for Digital, Culture, Media and Sport (2019)' Cyber Security Skills Strategy' Available at: https://www.gov.uk/government/publications/cyber-security-skills-strategy

[12] DCMS, Ipsos MORI, and University of Portsmouth (2019) 'UK Cyber Security Breaches Survey 2019' Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019

[13] Tech Nation (2019) Cyber Cohort: Available at: https://technation.io/programmes/cyber-security/

Stage 3: Initial Data Collection & Gap Analysis

The research team subsequently sought to identify potential active cyber security firms in the UK through:

- a review of the baseline firms (identifying the current status and determining inclusion in the updated set)
- a review of company participation within clusters, networks, and/or government supported initiatives
- a revised search strategy (using BvD FAME and wider search strategy).

A long-list was subsequently tested and refined to a final working list for the sectoral analysis. This list was then subject to extensive data gathering to identify metrics including (but not limited to):

- company name, registered number, company status, and date of incorporation
- registered and trading locations
- company website and contact details
- core description of company activities related to cyber security
- company size (large / medium / small / micro)
- participation within government supported initiatives (e.g. NCSC Cyber Accelerator) to support the cyber security sector was also flagged at this stage.

Stage 4: Cyber Security Sector Survey

Ipsos MORI carried out a representative survey of 262 cyber security firms from 1 May to 25 June 2019. The survey used the list of firms established in stage 3 of this study as a sample frame. The purpose of the survey was to collect data directly from the firms that could not be found in stage 3 of this study. It covered the following topics:

- the categories of products and services offered across firms
- the client sectors that cyber security firms work across
- revenue estimates (to supplement the other published data found in stage 3)
- international trade status
- perceived barriers to growth
- among the subgroup of firms that had participated in various Government-backed cyber growth schemes (HutZero, Cyber 101, Cyber Security Academic Startup Accelerator Programme (CyberASAP), NCSC Cyber Accelerator, and the London Office for Rapid Cybersecurity Advancement (LORCA)), the actions they had taken off the back of this scheme participation.

Appendix D provides the full technical details for the survey, including the data collection approaches and response rate.

A note on comparisons to the baseline Cyber Security Sectoral Analysis survey

As discussed in Section 1.2, this survey is very different to the one carried out in the baseline sectoral analysis (published in October 2018). The differences include:

- data collection mode and sampling approach – primarily telephone this time with a random-probability sampling approach, as opposed to the self-selecting online sample achieved in the previous analysis
- questionnaire – an entirely revamped questionnaire was used this time
- sample size – this year's survey achieved a much larger sample size (262, vs. c. 80 previously).

These major differences mean that none of the survey estimates from this year should be considered directly comparable to the ones in the baseline sectoral analysis.

Stage 5: Consultations

This research has also been supported by a series of extensive one-to-one consultations with policy and operational leads (for cyber security policy, and for a number of Government-supported initiatives to grow the cyber security sector), industry, and academics.

Stage 6: Data Blending

In August 2019, the results of the cyber security sector survey were utilised to inform gaps within the initial long-list of cyber security sector firms e.g. the extent to which a firm provided cyber security products or services and attributed revenues accordingly, or indeed, where a firm had received support from an initiative intended to help the sector – this includes their views on how support has helped them to grow.

This stage involved thorough data cleaning and joining to provide a final dataset of cyber security firms, and a granular (known and/estimated) profile of which firms are involved in cyber security, to what extent (to attribute employment, revenue, GVA etc), what firms offer to the market (within the taxonomy), and where firms have secured investment.

Stage 7: Data Analysis and Reporting

The final stage involved analysis of the final shortlist of firms to provide estimates of total number of firms, products and services offered, whether firms are 'dedicated or diversified' with respect to how much of their activity related to cyber security provision, revenue/GVA/employment estimates, locations (registered, trading and international presence), investment and survey feedback (anonymised at an individual level). The analysis within this report is consistent with the baseline.

Data Sources Used

The data sources used to underpin the sectoral analysis included:

- Bureau van Dijk FAME: This platform collates Companies House data and financial statements from all registered businesses within the UK.
- Beauhurst: Beauhurst is a leading investment analysis platform, that enables users to discover, track and understand some of the UK's high-growth companies e.g. identify investment, accelerator participation, and key information.
- Tussell: Tussell provides market insight into public sector procurement through identifying key contracts, spend, buyers and suppliers.
- Cyber Exchange: TechUK's Cyber Exchange directory enables cyber security providers to register an account and set out the products and services they provide to the market.
- web scraping: Our team has utilised web scraping[14] to extract and parse key company descriptions, locations and contact details from identified company websites.
- representative survey of cyber security firms: in Summer 2019, Ipsos MORI conducted a representative survey of cyber security firms. The feedback from 262 providers has been highly useful to understand the financial performance, growth drivers, and challenges for firms within the market.
- one-to-one consultations: Further, the team has also conducted c. 20 one-to-one consultations with key market providers, in addition to a taxonomy workshop, to ensure that the work can be best aligned to wider initiatives.

[14] Note: web scraping has observed 'robots.txt' – i.e. where access is permitted.

1.2 Consistency & Differences with the Baseline Cyber Security Sectoral Analysis

For transparency, this section sets out how our approach remains consistent with the baseline but has added robustness through the deployment of a new representative telephone survey of cyber security firms[15] and through the provision of revised and more granular metrics.

Consistency

As per the baseline study, this report also explores firms that:

- have a clear presence within the UK market, through a UK registered business that reports to Companies House on an annual basis
- demonstrate an active provision of commercial activity related to cyber security (e.g. through the presence of a website / social media)
- provide cyber security products or services to the market (i.e. sell or enable the selling of cyber solutions to other customers)
- have identifiable revenue or employment within the UK
- appear to be active at the time of writing (i.e. have not, or are not in the process of dissolution)
- are not charities, universities, networks and individual contractors (non-registered) – all excluded for analysis purposes.

It also draws upon consistent sources i.e. BvD FAME for company data, and Beauhurst for investment data. The financial analysis of firms is also consistent, as it utilises company information from the most recent financial year of accounts (analysis undertaken in July 2019, with FY17/18 as the modal year for published accounts) and the underpinning dataset sets out where employment, revenue, GVA and investment are either known or estimated (and the rationale underpinning this).

Methodological Variations

The Research Plan for this project identified that there were three key areas in which the research could be enhanced since the baseline, which have been incorporated into our analysis. These included:

- Representative Survey: This analysis uses a representative survey of firms via telephone. This approach has meant that where metrics have been estimated using the survey responses, these are much more robust than the initial baseline (which used an online survey of firms with c. 80 responses).

- Sector Segmentation: The baseline segmented firms against the taxonomy; however, several firms identified matched against more than one part of the taxonomy (e.g. offered both 'Cyber Professional Services' and 'Network Security'. Therefore, within this study, we have also sought to identify where firms mainly provide products or services (including managed services) to provide a segmentation that is easy-to-understand.

[15] Note: the baseline survey was not representative (c. 80 responses, administered via online survey) compared to this year's survey (representative sample contacted, with c. 240 responses via telephone) and therefore the two are not comparable.

- Data Gathering: The research team has also identified other data sources and approaches that are useful to gather more detailed information about firms active within the sector. Therefore, this research has drawn further upon web scraping of company websites, and new data sources (e.g. procurement data).

1.3 Interpretation of the data

Across this report, percentages from the quantitative data may not add to 100%. This is because:

- We have rounded percentage results to the nearest whole number.
- At certain questions, survey respondents could give multiple answers.

It is also important to note that the survey data are based on a sample of cyber sector firms rather than the entire population. Therefore, the are subject to sampling tolerances. The overall margin of error for the sample of 262 firms (within a population of 1,221 firms) is between c.3 and c.5 percentage points. The lower end of this range (3 percentage points) is used for survey estimates closer to 10% or 90%. The higher end (5 percentage points) is used for survey estimates around 50%. For example, for a survey result of 50%, the true value, if we had surveyed the whole population, is extremely likely to be in the range of 45% to 55%.[16]

1.4 Acknowledgements

The authors would like to thank Ben Shaps and Andy Penpraze from DCMS for their support across the study.

DCMS and the report authors would also like to thank those that participated within this research, including those that participated within the taxonomy workshops, the industry survey, consultations, and shared data, knowledge and feedback to help underpin this study.

Note: *As this research project utilises an experimental approach, we are happy to receive comments and feedback regarding the methodology.*

[16] This is based on 95% confidence intervals.

2 Profile of the UK Cyber Security Sector

2.1 Defining the UK Cyber Security Sector

Within the National Cyber Security Strategy (2016-21), cyber security is defined as:

The protection of internet connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.

Therefore, this sectoral analysis seeks to identify businesses active within the UK that provide products or services that enable the protection of internet connected systems and their users. In line with the baseline study, this analysis focuses upon organisations that:

- have a clear presence within the UK market, through a UK registered business that reports to Companies House on an annual basis
- demonstrate an active provision of commercial activity (e.g. through the presence of a website / social media)
- provide cyber security products or services to the market (i.e. sell or enable the selling of cyber solutions to other customers)
- have identifiable revenue or employment within the UK
- appear to be active at the time of writing (i.e. have not, or are not in the process of dissolution)
- are not charities, universities, networks and individual contractors (non-registered) – which are all excluded for analysis purposes.

The businesses included within this analysis are considered to provide one or more of the following products or services:

- Cyber professional services, i.e. providing trusted contractors or consultants to advise on, or implement, products, solutions or services for others
- Endpoint and mobile security, i.e. hardware or software that protects devices when accessing networks
- Identification, authentication and access controls, i.e. products or service that control user access, for example with passwords, biometrics, or multi-factor authentication
- Incident response and management, i.e. helping other organisations react, respond or recover from cyber attacks
- Information risk assessment and management, i.e. products or services that support other organisations to manage cyber risks, for example around security compliance or data leakage
- Internet of Things (IoT Security), i.e. products or services to embed or retrofit security for Internet of Things devices or networks
- Network security, i.e. hardware or software designed to protect the usability and integrity of a network
- SCADA and Information Control Systems, i.e. cyber security specifically for industrial control systems, critical national infrastructure and operational technologies

- Threat intelligence, monitoring, detection and analysis, i.e. monitoring or detection of varying forms of threats to networks and systems
- Awareness, training and education, i.e. products or services in relation to cyber awareness, training or education.

Section 2.3 sets out the type of cyber security products and services in further detail.

2.2 Number of Cyber Security Firms Active in the UK

Our analysis estimates that there are currently 1,221 firms active within the UK providing cyber security products and services. This reflects an increase of 44% since the baseline report (846 firms).

The following sections set out an overview of:

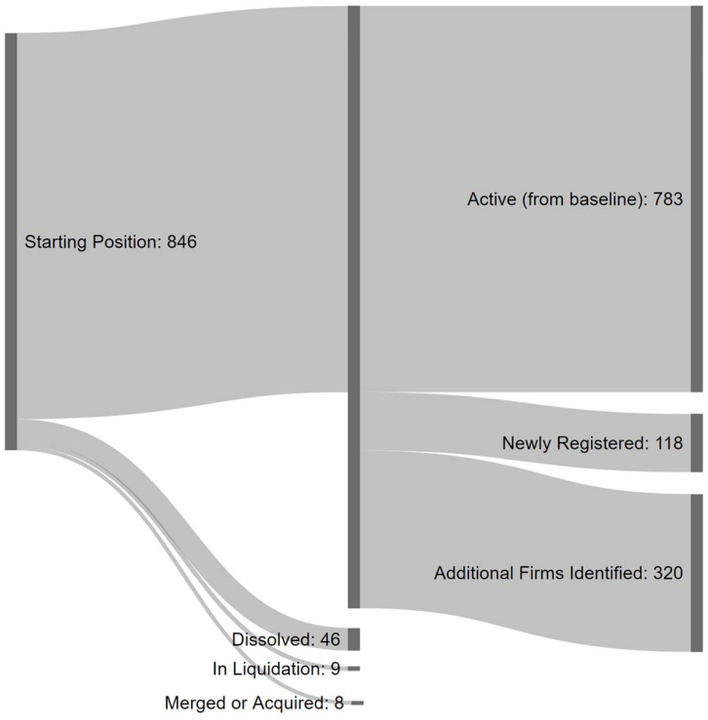
- the number of companies by date of incorporation (i.e. how many companies are new to the market?)
- the number of companies by region
- the breakdown between companies that appear dedicated or diversified
- the number of companies by Standard Industrial Classification (SIC) code
- the products and or services provided by each company.

It also provides an overview of the number of firms that have exited the sector since the baseline study.

Entrants and Exits

This sectoral analysis has sought to identify new entrants to the cyber security sector, which includes both newly registered businesses as well as businesses that have decided to establish a cyber security practice within their existing commercial structure. Further, it has extensively reviewed market intelligence sources to mitigate any gaps where cyber security practices may not have been identified within the baseline report. Finally, it has also removed businesses that are no longer active or trading in the UK (either due to acquisition, a change in trading circumstances, or closure). The Sankey diagram below sets out the composition of the updated long-list of cyber security firms in the UK.

Figure 2.1: Sankey Diagram: Cyber Security Entrants and Exits since Baseline



Key Findings:

This process has yielded a total of 1,221 active firms (as of August 2019).

- 93% of cyber security firms from the baseline (2017) are still active.
- 46 (5%) have dissolved, 9 (1%) are in liquidation, and 8 (1%) appear to have merged with another firm or been acquired.
- A further 118 firms identified are newly registered (since 1st August 2017).
- 320 additional firms have been identified (existed to some extent at the baseline e.g. may have been pre-revenue or establishing their cyber offer - but have now been identified as involved in cyber security provision).

Entrants

Overall, we have identified 118 firms that are newly registered (since the August 2017 baseline), and a further 320 firms have been identified (existed to some extent at the baseline e.g. may have been pre-revenue or establishing their cyber offer - but have now been identified as involved in cyber security provision).

This means that, on average, there is one new cyber security business registered every week in the UK.

Further, the identification of 320 additional firms identified suggests that the last two years have been particularly active for companies seeking to expand their provision to include cyber security products and services e.g. consultancies including GDPR and risk governance within their client offering. It will be of interest to note how this trend develops in the coming years.

Exits

It is notable that 93% of cyber security sector baseline cohort has remained active two years following the baseline study. Within the UK, business death as a percentage of UK businesses was 12.2% (2017)[17] – in other words, approximately one in every eight businesses cease trading within the UK every year. This highlights the relative resilience and growth underpinning the baseline cohort.

An exit is not necessarily a negative outcome (explored further in Section 4.3). It can reflect acquisition of one company by another, which is not uncommon within the cyber security sector. It could also reflect the cessation of a company's trading activities for commercial or personal reasons.

[17] ONS (2017) Business Births, Deaths and Survival Rates: Available at: https://www.ons.gov.uk/businessindustryandtrade/changestobusiness/businessbirthsdeathsandsurvivalrates

Number of Firms by Region

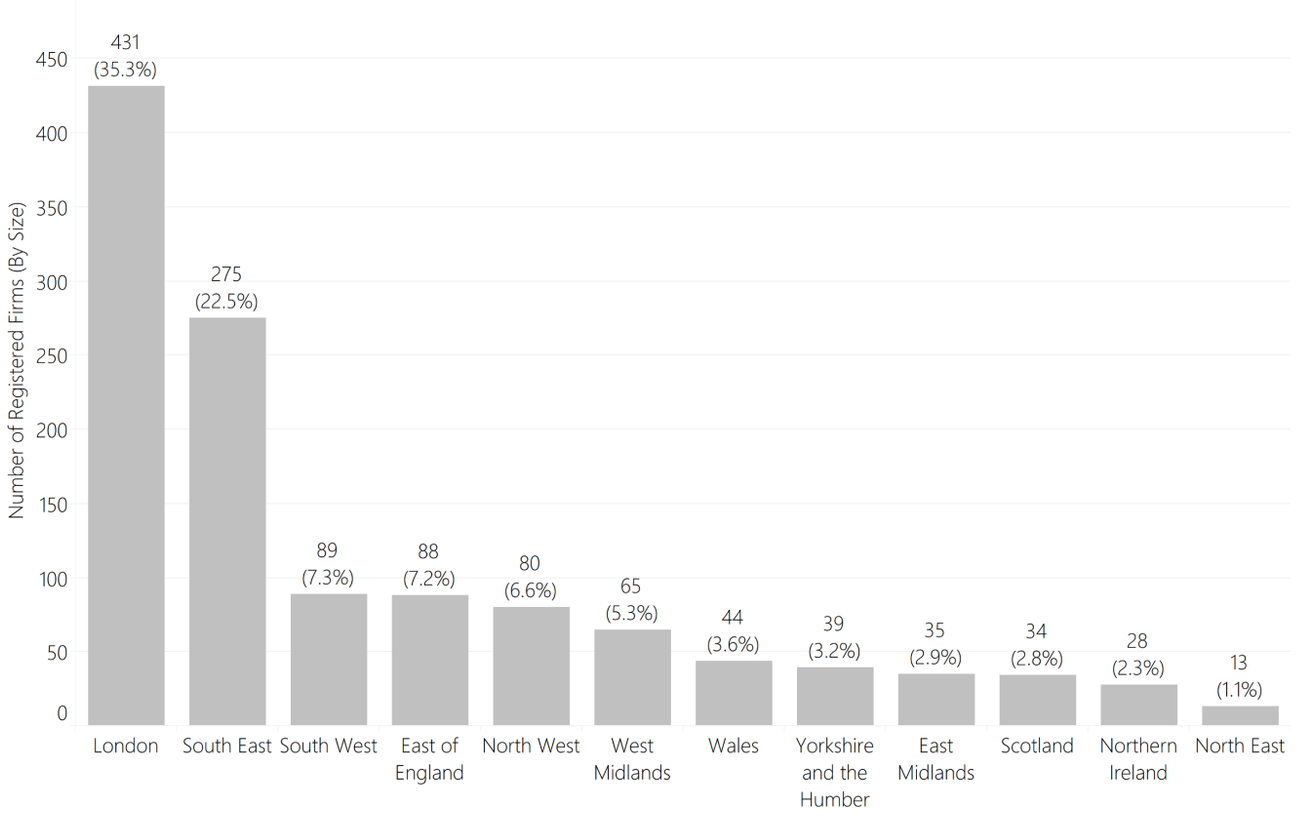
The figure below sets out the number of registered firms[18] providing cyber security products and services across the twelve UK regions.

The regional distribution of firms has remained consistent against the baseline report, with London (35%) and the South East (23%) remaining key locations with respect to the absolute number of registered firms. However, there has been notable growth within the North West of England (where firm count has more than doubled from 39 registered firms to 80 registered firms).

It is worth noting that the registered location of cyber security firms does not fully reflect the performance of regions with respect to cyber security activity, and this report has sought to identify trading locations across the UK to better inform the regional estimated for cyber security activity. This is further detailed in Section 2.4.

For example, regions such as Northern Ireland have a higher number of companies active in cyber security within their regional ecosystem, but these firms tend to be registered in other parts of the UK – whilst holding R&D offices in Northern Ireland etc.

Figure 2.2: Number of Registered Firms by Region



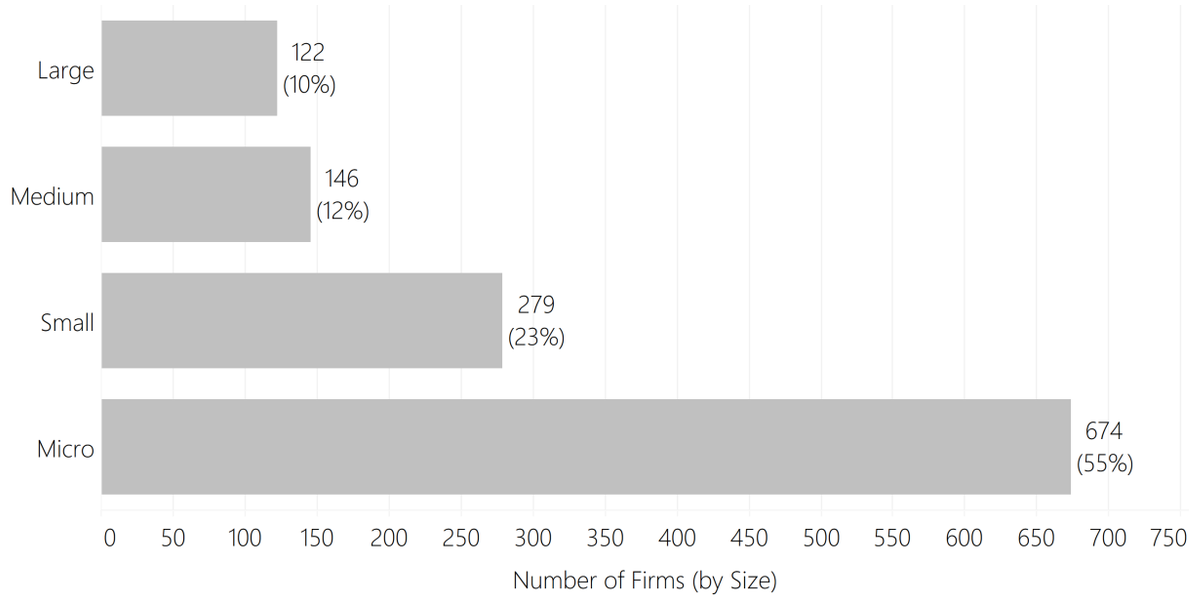
Source: Perspective Economics, BvD FAME (n=1,221)

[18] As of August 2019.

Number of Firms by Size

Within the baseline report, approximately 50% of firms identified were micro businesses. Since the baseline, this has increased to 55%, reflecting that there have been over 250 additional micro firms (420 to 674) identified within this analysis.

Figure 2.3: Number of Firms by Size



Source: Perspective Economics, BvD FAME

Table 2.1: Breakdown of Firms by Size

Category	Definition	Number of Firms	Percentage
Large Company	Employees >=250 And Turnover > €50m or Balance sheet total > €43m	122	10%
Medium Company	Employees >50 and < 250 And Turnover <= €50m or Balance sheet total <= €43m	146	12%
Small Company	Employees >10 and < 50 And Turnover <= €10m or Balance sheet total <= €43m	279	23%
Micro Company	Employees < 10 And Turnover <= €2m or Balance sheet total <= €2m	674	55%
	Total:	**1,221**	**100%**

Source: Perspective Economics, BvD FAME

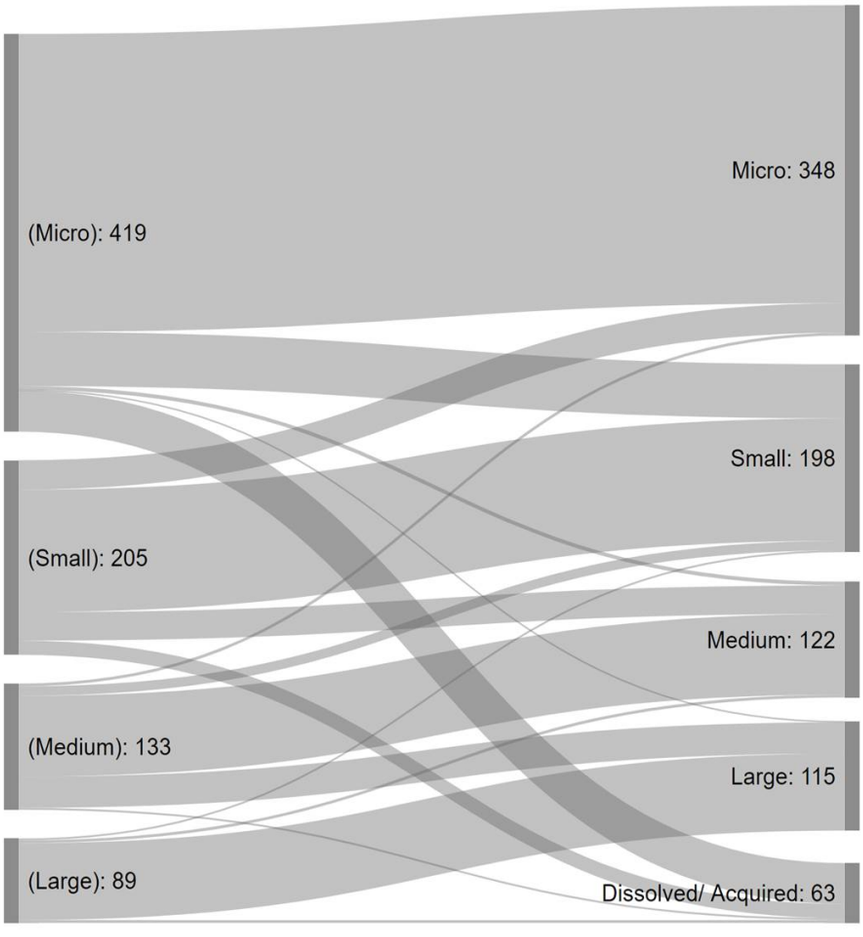
Change in Size of Firms (Since Baseline)

For the 846 cyber security firms included within the baseline study, the diagram below sets out how each of these have changed in size since 2017.

Typically, most firms (72%, n = 609) have not changed in estimated size bracket since the baseline i.e. have remained micro, small, medium or large respectively. However, 15% (n = 125) have increased in size by at least one bracket (e.g. micro to small, small to medium etc) within the last two years. A small number also appear to have decreased in size bracket (6%, n = 49), or are no longer active (7%, n=63) in their baseline form (dissolved or acquired).

It is worth noting, however, that tracking estimated size brackets provided an overview of trajectory, but granular changes can provide further detail. For example, a firm with one employee at baseline that grows to nine employees in this time period would remain a 'micro firm' whereas a firm that grows from eight employees (micro) to ten employees would become a 'small firm', despite having a lower proportional growth rate.

Figure 2.4: Change in Size (Since Baseline)



Micro – Micro: 75%
Micro – Small: 14%
Micro – Medium: 1%
Micro – Large: 0.2%
Micro – Dissolved/Acquired: 10%

Small – Micro: 15%
Small – Small: 63%
Small – Medium: 15%
Small – Large: 0%
Small – Dissolved/Acquired: 7%

Medium – Micro: 2%
Medium – Small: 8%
Medium – Medium: 64%
Medium – Large: 25%
Medium – Dissolved/Acquired: 2%

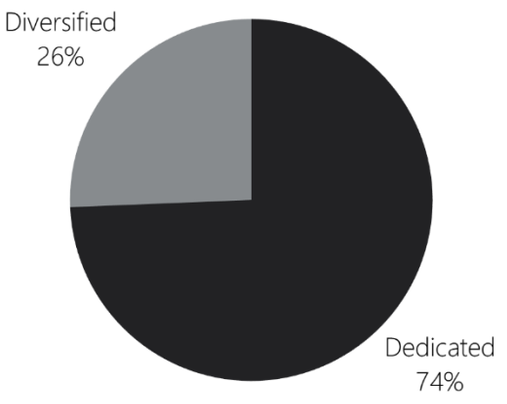
Large – Micro: 0%
Large – Small: 2%
Large – Medium: 3%
Large – Large: 91%
Large – Dissolved/Acquired: 3%

Source: Perspective Economics, BvD FAME (n = 846)

Dedicated and Diversified Providers of Cyber Security Products and Services

Figure 2.5: Percentage of Dedicated and Diversified Cyber Firms

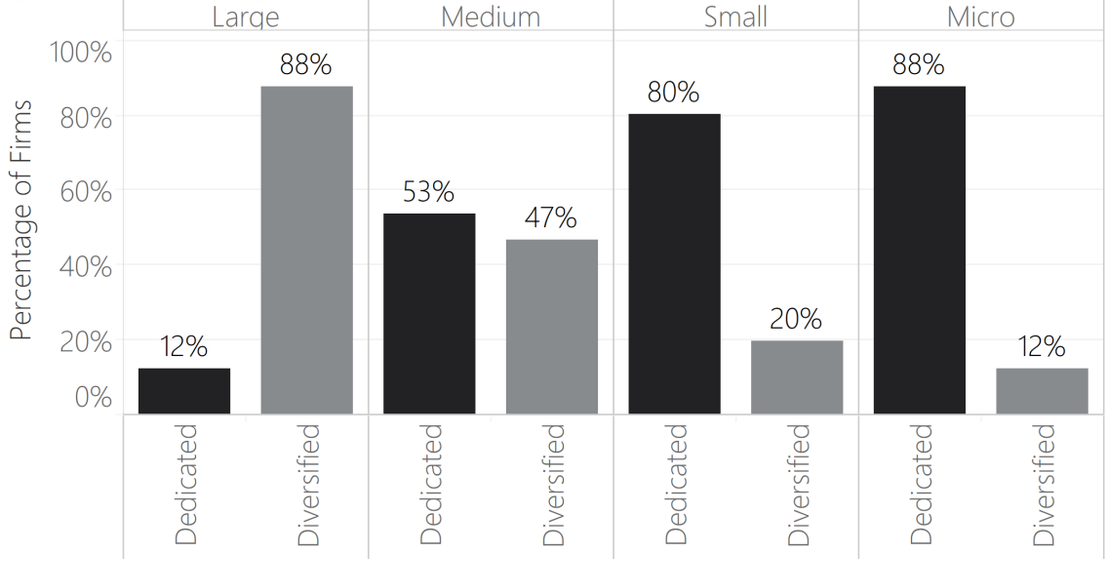
Within this sectoral analysis, it is considered important to provide an estimate of where firms are either:



- Dedicated[19] i.e. most (>75%) of the business' revenue or employment can be attributed to the provision of cyber security products or services; or
- Diversified i.e. less than 75% of the business' revenue or employment can be attributed to the provision of cyber security products or services.

The rationale underpinning the need to provide this distinction is attributable to seeking to understand how firms either set up to solely provide cyber security, or firms that provide cyber security as one product or service among others vary with respect to size, scale, growth and market activity. Within the current dataset, approximately three-quarters (74%) of firms are dedicated providers of cyber security products and services. Disaggregating of these firms by size (as below) also highlights that micro and small firms within this analysis are much more likely to be dedicated (88% and 80% respectively), whereas there are relatively few large dedicated cyber security firms (12%). In other words, this reflects the decision of several large and medium sized companies in the UK to establish cyber security practices to complement existing provision e.g. management consultancies, managed service providers, or telecoms firms developing a cyber security division that sells to the market.

Figure 2.6: Percentage of Dedicated and Diversified Firms (by Size)



Source: Perspective Economics

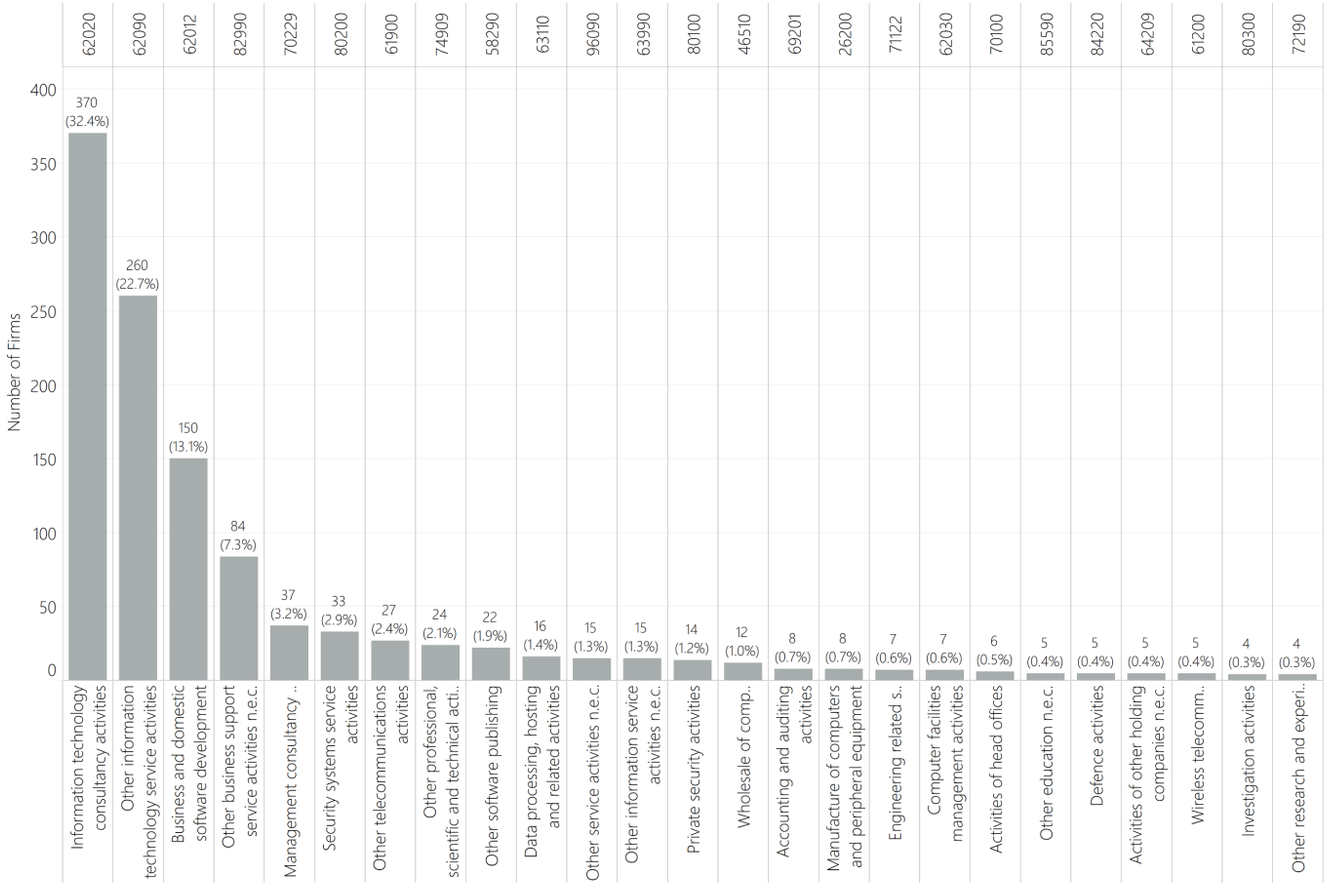
[19] Note: The baseline study had a category called 'Mostly Dedicated' to account for firms with between 75-99% relating to cyber security. This category reflected less than 2% of all firms, and therefore this study is now using two variables for ease of reference i.e. Dedicated >75% and Dedicated <75% of activity.

Number of Firms by SIC code

Analysis of the sector firms by Standard Industrial Classification (SIC) code (2007) does demonstrate that most firms (69%) are aligned to SIC code 62 (Information Technology firms).

However, as stated within the project methodology, SIC codes are intended to reflect broad sectoral definitions, and their limitations are well recognised for seeking to capture the extent and contribution of IT or Digital sub-sectors, such as cyber security.

Figure 2.7: Percentage of Firms by SIC Code



Source: Perspective Economics, Companies House API

2.3 Products and Services Provided by the Cyber Security Sector

Within the baseline study, the cyber security sector was segmented into nine key categories[20]. In Spring 2019, the research team held a Taxonomy Workshop to discuss how the cyber security sector had developed within the last few years, and to agree if and how a taxonomy should be updated. Following this workshop, the following taxonomy was agreed, which incorporates small changes to best reflect the current offering of the wider sector.

Table 2.2: Taxonomy Overview

Taxonomy Category	Agreed Definition (Short)	Definition Change Since Baseline
Cyber professional services	Providing trusted contractors or consultants to advise on, or implement, cyber security products, solutions or services for others.	No Change
Endpoint and mobile security	Hardware or software that protects devices when accessing networks.	Changed from 'End-User Device Security' and added Mobile Security as a growth area.
Identification, authentication and access controls	Products or service that control user access, for example with passwords, biometrics, or multi-factor authentication.	No Change
Incident response and management	Helping other organisations react, respond or recover from cyber-attacks.	No Change
Information risk assessment and management	Products or services that support other organisations to manage cyber risks, for example around security compliance or data leakage	No Change
Internet of Things	Products or services to embed or retrofit security for Internet of Things devices or networks	New Category: UK Growth Area / Specialism.
Network security	Hardware or software designed to protect the usability and integrity of a network.	No Change
SCADA and Information Control Systems	Cyber security specifically for industrial control systems, critical national infrastructure and operational technologies	No Change
Threat intelligence, monitoring, detection and analysis	Monitoring or detection of varying forms of threats to networks and systems.	Added 'Threat Intelligence' to 'Monitoring, Detection and Analysis'
Awareness, training and education	Products or services in relation to cyber awareness, training or education.	No Change.

Source: Ipsos MORI, Perspective Economics and Centre for Secure Information Technologies

[20] These included: Network Security | Information Risk Assessment & Management | Cyber Professional Services | End-User Device Security | Monitoring, Detection and Analysis | Training, Awareness & Education | Identification, Authentication and Access Control | Incident Response & Management | SCADA and Industrial Control Systems

Further, within the taxonomy workshop, it was also agreed that it would be useful to explore how the sector could be segmented into companies that provide (as their main cyber security offering):

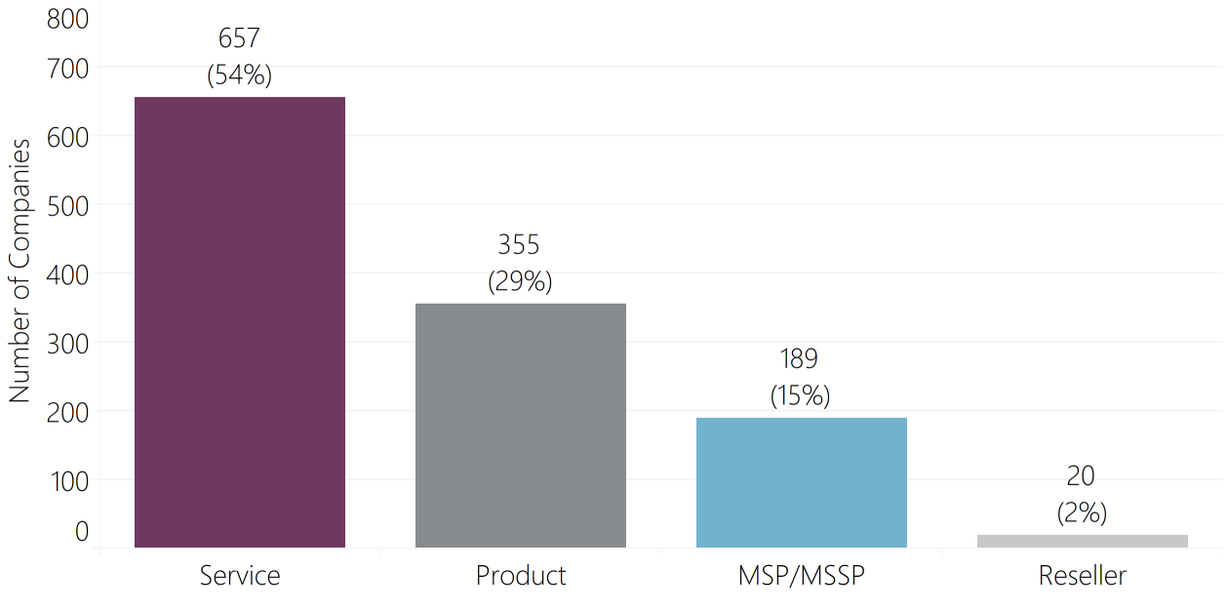
- Cyber security **product(s)** i.e. the business has developed and sells a bespoke product (hardware or software solution) to the market
- Cyber security **service(s)** i.e. the business sells a service to the market e.g. cyber security advisory services, penetration testing etc.
- Provide **Managed (Security) Services**: i.e. the business offers other organisations some degree of cyber security support e.g. establishes security protocols, monitoring, management, threat detection etc – typically for a monthly or annual fee
- **Reseller**[21] i.e. the business packages and resells cyber security solutions (usually through licencing agreements).

The following sub-sections set out a breakdown of the cyber security sector by product and service provision, and by taxonomy category.

Product and Service Provision

Further to the taxonomy categorisation, it is also useful to segment the sector into those that provide (at a broader level) products, services, or other solutions to the market. It is worth noting that there will be some overlap where firms provide both products and services. However, analysis of company trading descriptions suggests that approximately two-thirds (69%) of firms are mainly involved in service provision (including managed services), and just under a third (29%) are mainly involved in cyber security product development.

Figure 2.8: Categorisation by Product, Service or Other



Source: Perspective Economics

[21] Note only a small number of resellers are included – whereby they also appear to offer other services aligned to the agreed cyber security taxonomy e.g. advisory support with implementation of cyber security products or services.

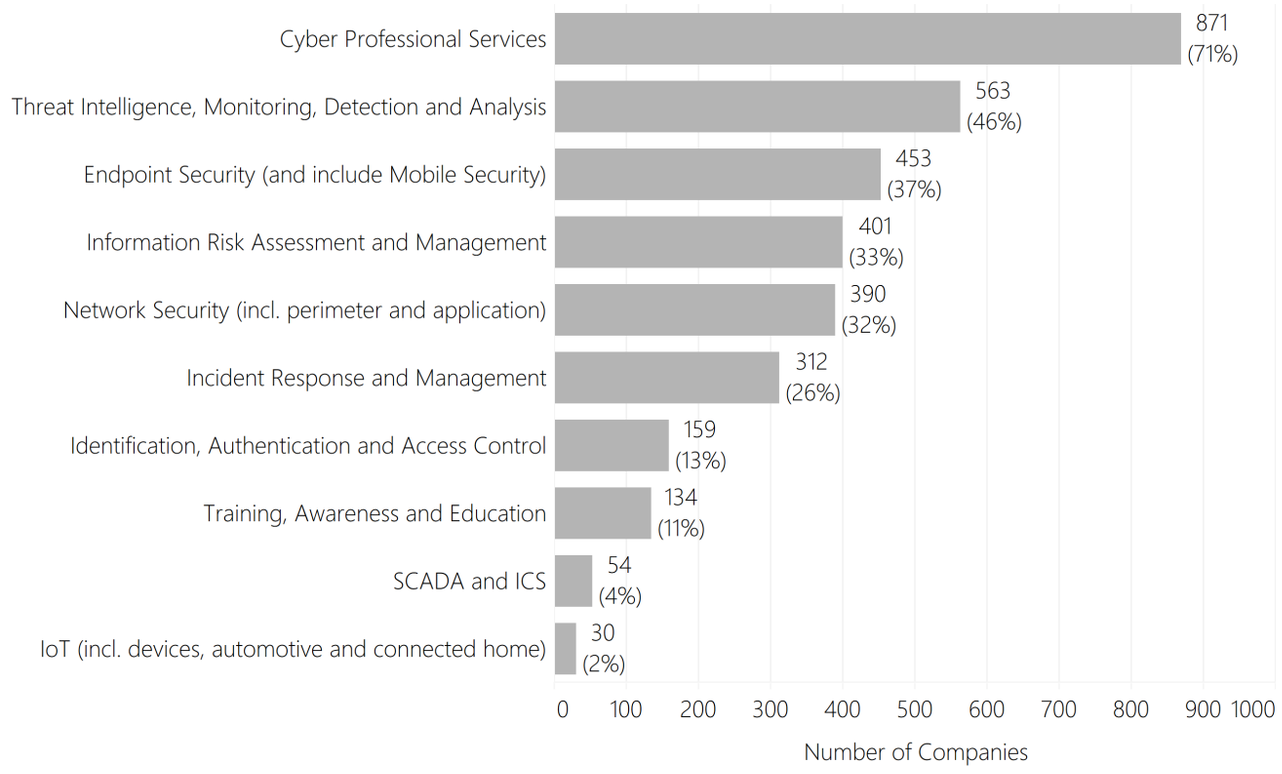
Taxonomy Segmentation

Within this study, we have matched company descriptions with the key terms within each taxonomy category, followed by a manual check to assign companies to one (or more) taxonomy categories with respect to their product and service provision. We also asked firms about what products and services they offered within the survey; however, the responses indicated that firms appeared to offer many of these and did not sufficiently indicate specialisms. On this basis, the graph below is based upon our analysis of trading descriptions.

The graph below demonstrates that 'Cyber Professional Services' is the most commonly provided taxonomy category (71% of businesses), which reflects both the breadth of the taxonomy category as well as the often lower barriers to entry in establishing an advisory business compared to creating and bringing a cyber security product to market.

At the lower end, there is emerging evidence that SCADA and ICS, as well as IoT focused cyber security companies are meeting bespoke market requirements, and this may be likely to increase in future as firms align their offering to embed 'Secure by Default' standards or meet regulatory requirements for their clients.

Figure 2.9: Percentage of Firms Providing a Product or Service aligned to Taxonomy



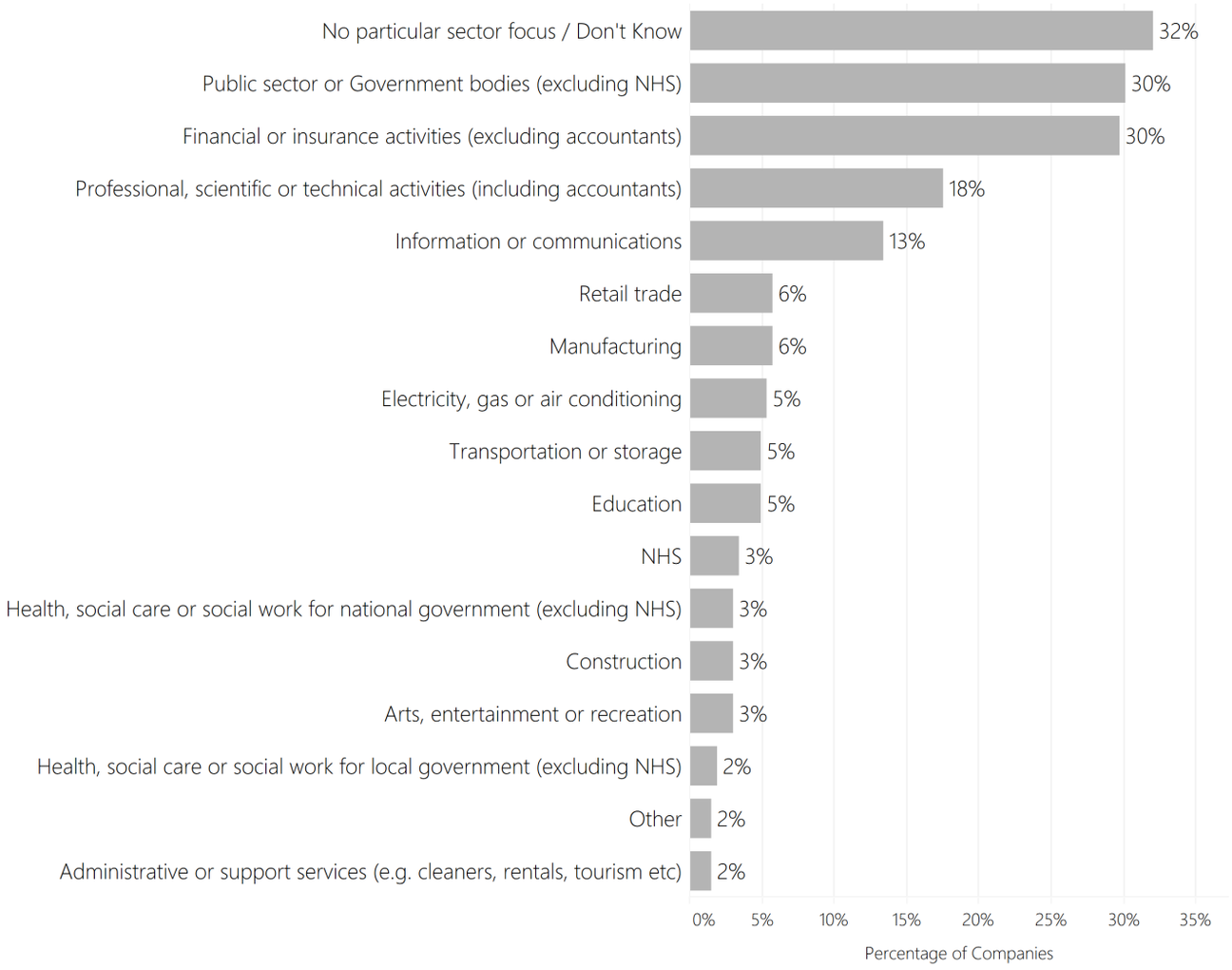
Source: Perspective Economics

Clients and Customers

Within the survey of cyber security companies, businesses were asked whether the products and services they offered were provided to any particular sectors ("*Do your main customers for cyber security come from any particular industry sectors? You can name up to three industry sectors")*

Just under a third (32%) of respondents noted that they did not have (or were not aware of) a sector focus. For those businesses which could segment their main customers by sector, the largest customer segments were the Public Sector (30%) and 'Financial or Insurance Activities' (30% of businesses) followed by broader Professional, Scientific or Technical Activities providers (18%), as well as other IT or Communication firms (13%).

Figure 2.10: Percentage of Businesses with a Sector Focus (Customers) – Survey Estimates



Source: Ipsos MORI (Survey of Cyber Security Firms, n= 262)

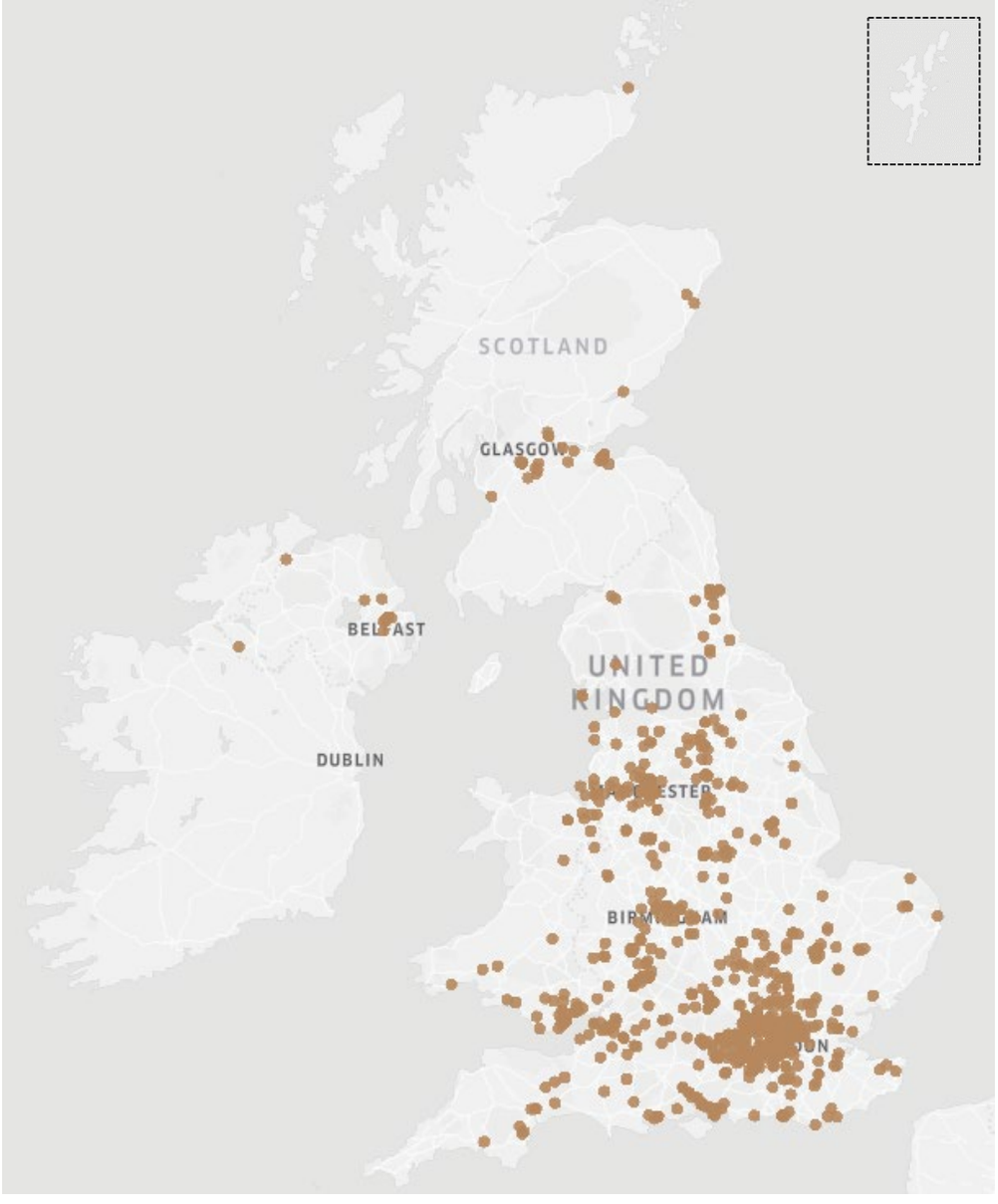
2.4 Geographic Location of the Cyber Security Firms in the UK

Understanding the registered and trading addresses of cyber security firms in the UK enables regional analysis, and for the identification of notable clusters or hotspots of activity. However, at this stage, this reflects registered and trading locations only – and it is often the case that UK businesses may register in one location (e.g. London) but operate within other regions. In this event, revenues and or employment attributable to the business may not fully reflect performance across the regions (i.e. some regions may be over or under-estimated as a result of registered locations). However, this provides a useful indication of where cyber security firms are located across the United Kingdom.

Registered Locations in the UK

The map below sets out the location of all identified registered cyber security businesses in the UK, signalling density within London and along the North West, West Midlands and South West corridor.

Figure 2.11: Registered Location of Cyber Security Firms



Source: Perspective Economics, Mapped with Mapbox

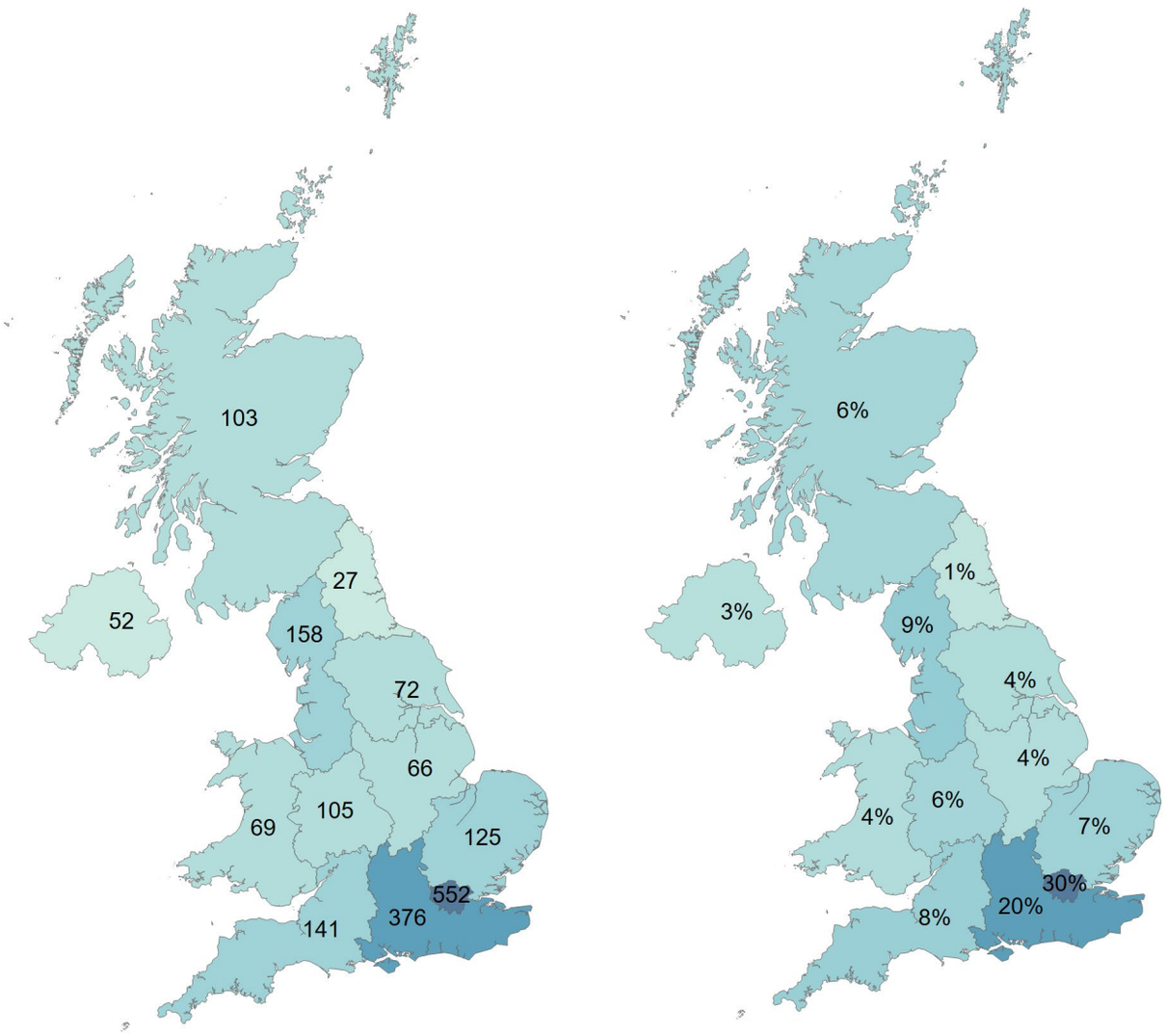
Registered and Trading Locations in the UK

As noted previously, many of the firms within the sector may have more than one office across the UK e.g. a registered headquarters in London, and an R&D office in Wales etc.

Through analysis of company websites, we have identified 1,846 offices across the 1,221 firms (whereby 77% of companies have one known and registered office, and 23% have more than one office location).

The maps below demonstrate that once trading locations are reflected within the data, the percentage of firms in London and the South East falls from 57% to 50%, and that other regions all show a marked increase which would be expected in line with their respective economic geographies.

Figure 2.12: Number and Percentage of Registered and Trading Locations (Offices)



Source: Perspective Economics (n=1,846)

International Presence

This section sets out i) where UK registered firms are active in other countries (reflected by an office location) (Fig 2.13), and ii) cyber security companies active in the UK by their initial national headquarters (Fig 2.14). Within the UK's cyber security sector, there are 192 UK companies (21% of UK headquartered firms) that appear to have an international presence. Further, 31 (16%) of the businesses identified were active in more than ten identifiable countries. The European Union is a key market for UK firms, as 103 UK companies have a European office in place. Indeed, UK firms are actively trading in Ireland, France and Germany. The United States is also a key region, with 91 (47%) companies that have a physical US office in place. Further countries of significance for UK firms with an international presence include Australia, UAE, South Africa, India, Singapore and the Netherlands.

Figure 2.13: UK Headquartered Businesses with an International Presence (i.e. Office Location)

Source: Perspective Economics (n=192 companies headquartered in the UK)

The map below sets out the initial national presence of companies identified within the dataset. Over the last few years, the UK has been a clear international destination for firms and foreign direct investment from the United States (139 firms, i.e. 11% of the overall UK sector), as well as Israel (9), Germany (9), France (7) and Canada (7).

Figure 2.14: Country of Origin (Number of Companies established outside of the UK, but have a current UK presence)

Source: Perspective Economics (n=208 companies headquartered outside of the UK, but active within the UK market

3 Economic Contribution of the UK Cyber Security Sector

3.1 Estimated Revenue

In the most recent financial year, annual cyber security revenue within the sector is estimated at £8,293,244,945 (£8.3bn). This figure is estimated using:

- revenue figures available for dedicated (100%) cyber security firms that publish annual accounts
- revenue figures available for diversified cyber security firms (multiplied by the estimate of the proportion of the firm's activity related to cyber security)
- reported cyber security revenue estimated (for the most recent financial year) through the cyber sector survey held in Summer 2019
- where gaps exist, employment has been sourced or estimated, with revenue estimated using 'revenue per employee' (estimated by size using known data) multiplied by 'number of employees' to provide an estimated revenue figure on a firm-by-firm basis.

This revenue estimate relates to revenue attributable to cyber security activity only. The following subsections set out revenue by size, revenue by size and dedicated/diversified categorisation, and revenue by key company offer.

Revenue by Size

Over three-quarters (£6.3bn, 76%) of all UK cyber security revenue is earned by large firms (which demonstrates the earning power of these firms given that they reflect 10% of all market providers). This includes several very large providers of telecommunications, aerospace, defence and security, and consultancies for which the size and scale of their respective cyber security product and service divisions reflect a considerable proportion of the wider market.

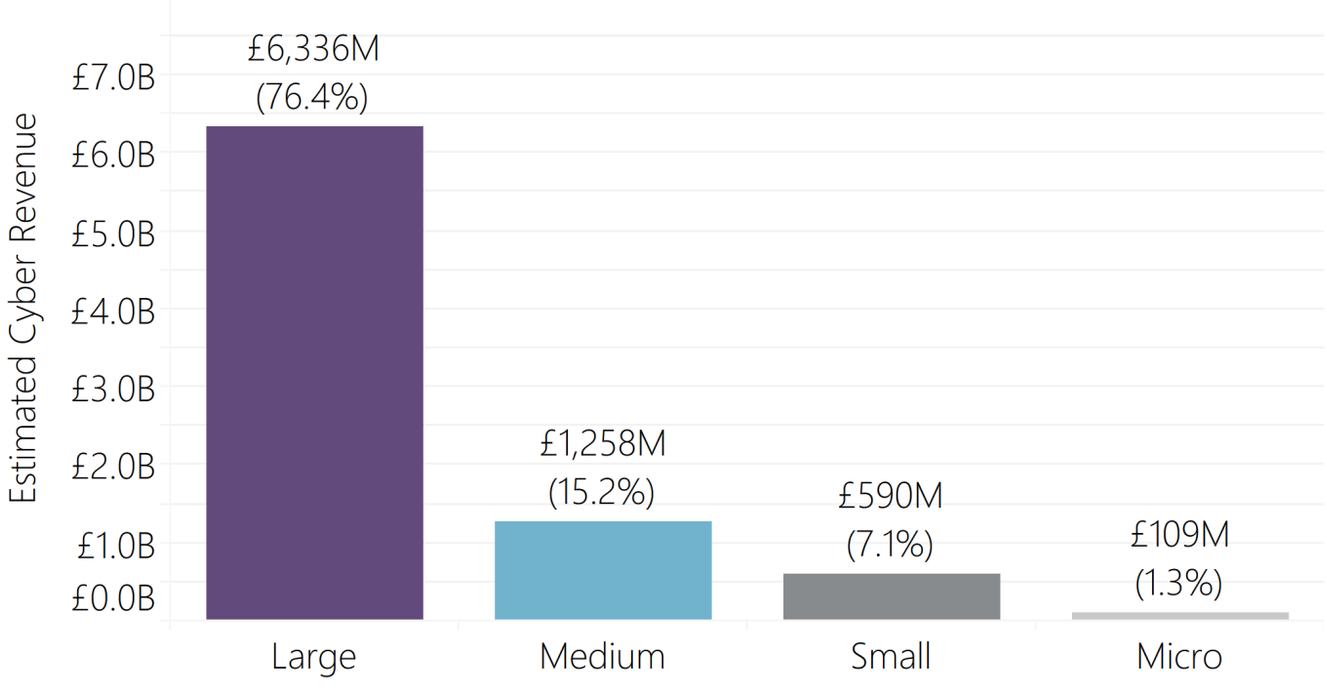
Within the baseline study, there were 89 large providers of cyber security products and services, which has now risen to 122 providers (an increase of 37%). However, in the same time period, large firm cyber revenues have increased from £4.2bn to £6.3bn (increase of 50%). This suggests that cyber security is a significant growth area for several large diversified firms, who have been keen to expand to meet rapid demand for cyber security products and services (either directly or as part of the end-product).

For small and medium firms (excl. micro), the baseline study had 337 firms which has now risen to 425 firms (an increase of 26%). In the same time period, their revenues have increased from £1.4bn to £1.85bn (increase of 32%). This suggests that whilst total revenues have increased, that this tier is a competitive marketplace, with several hundred small and medium firms vying for business within a growth landscape.

For micro firms, the baseline study had 420 firms which has now risen to 674 firms (an increase of 60%). In this same time period, estimated revenues have increased from £89m to £109m (an increase of 22%). Whilst it is worth stressing that several of these firms are pre-revenue, and that the aggregate figure is reliant upon estimation (given that micro firms typically do not provide full accounts) – this suggests that the last two years

has resulted in a proliferation of micro firms and start-ups – of which, these will take time to fully establish their presence in the market. It will be highly interesting to track the performance of these firms in the coming years, as well as understanding their growth ambitions.

Figure 3.1: Total Cyber Security Revenue by Size of Firm



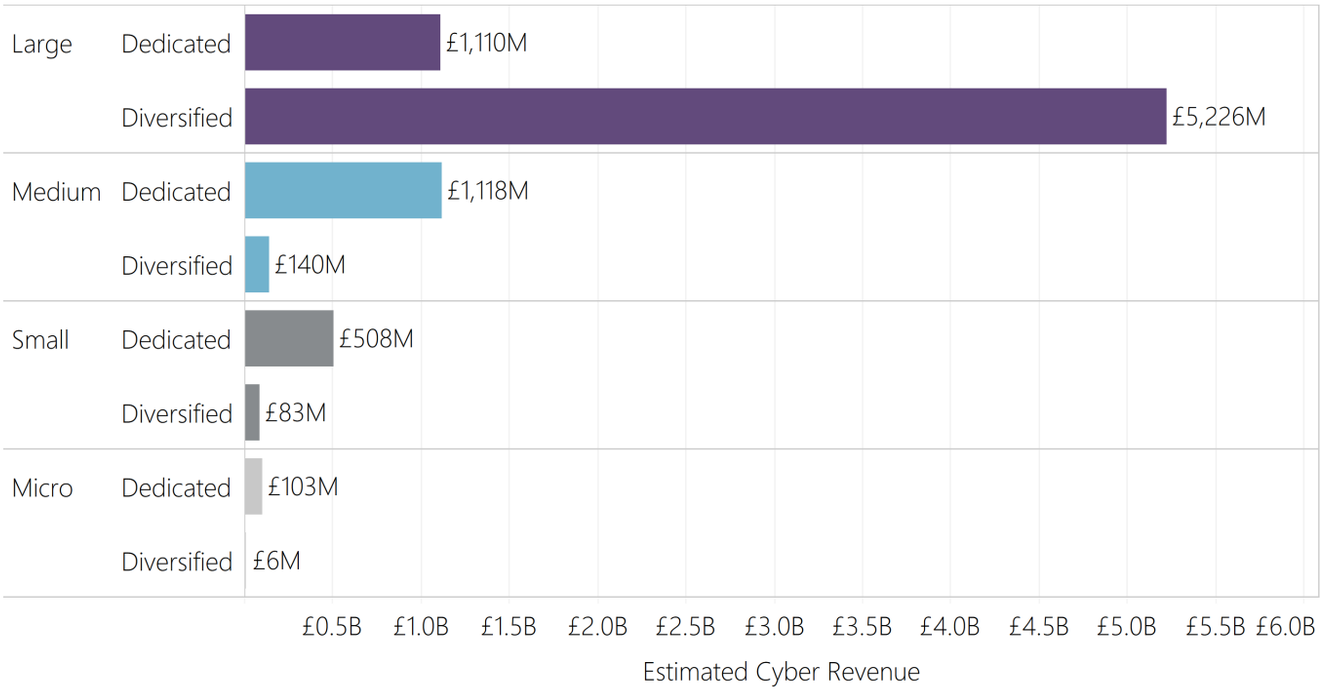
Source: Perspective Economics, BvD FAME, Ipsos MORI[22]

Segmentation of revenue by both size and by whether the firm is understood to be 'dedicated' or 'diversified' also provides an interesting overview of which firms are driving the revenue within the sector. Of the larger firms, 'diversified' firms are generating significant revenues through their cyber security offer (83% of total large firm cyber security revenues). However, the reverse holds for SMEs – whereby dedicated firms generate the greatest proportional revenue (e.g. 89% of revenues for medium firms, 86% for small, and 94% for micro firms). This suggests that the UK market is home to:

- Approximately twenty 'anchor' large and diversified firms, which are estimated to generate over £50m each in cyber security revenues. This can often be a very small proportion of the firm's revenues (often in billions) but reflects a significant proportion of the UK's cyber sector.
- A significant 'dedicated' and growing middle market: There are sixty-five firms that we have identified as dedicated providers of cyber security with over £10m in annual revenues.
- Rapid growth in the presence of new to market (micro) firms, with an increase in the number of micro firms within this analysis increasing by 60%.

[22] Analysis of BvD FAME data supplemented by extrapolated survey estimates (Ipsos MORI).

Figure 3.2: Total Cyber Security Revenue by Size and by Dedicated / Diversified status



Source: Perspective Economics, BvD FAME, Ipsos MORI[23]

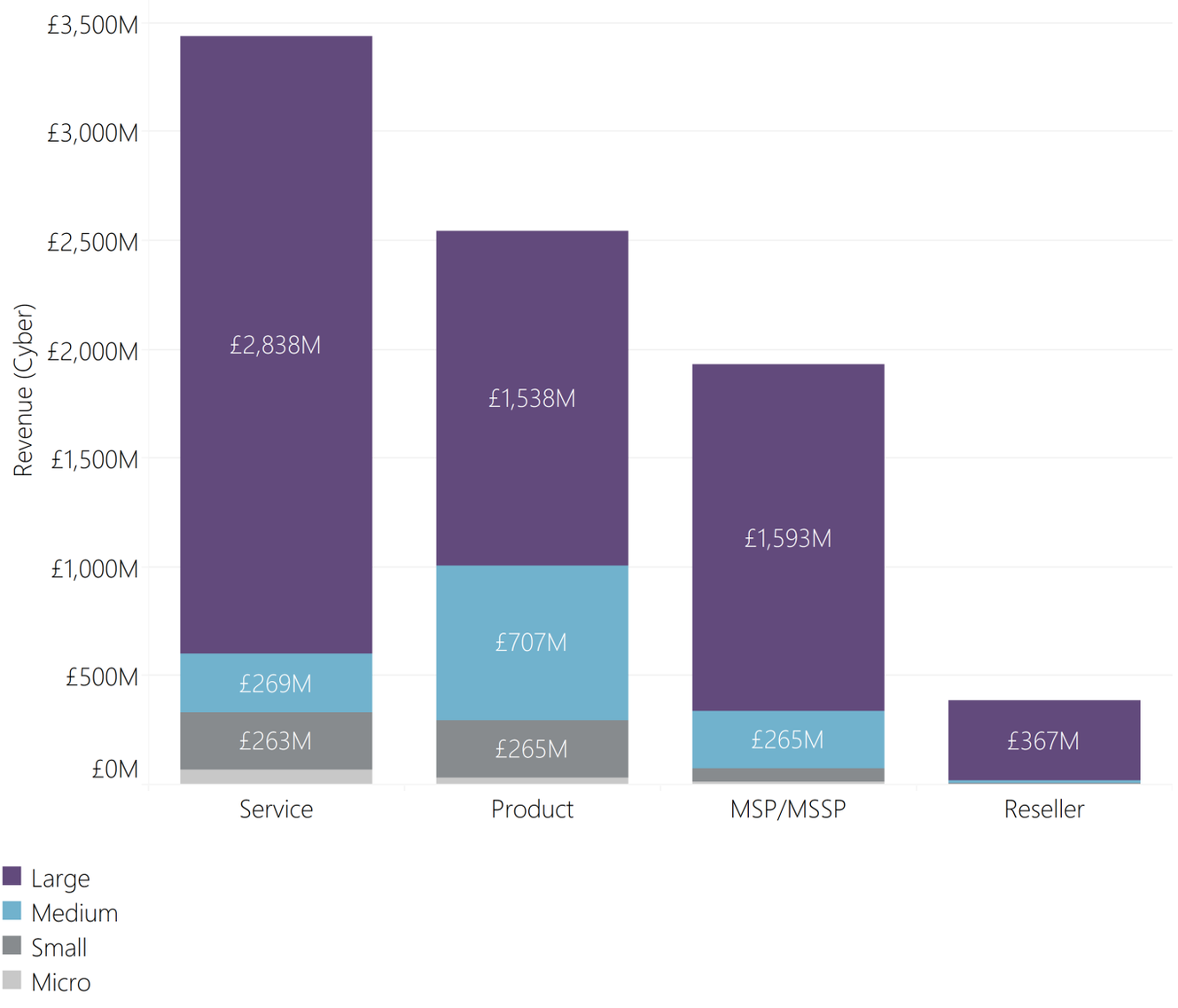
Finally, segmentation of revenues by size and by those companies that either provide (as a core role) cyber security products, services, managed services, or resell (set out in Fig 3.3) also provides some useful insight.

Whilst large firms dominate most of the categories with respect to revenue, the graph below highlights that total revenue within the sector is mostly generated by cyber professional services and managed security services (consisting of an estimated £4.6bn in revenues). As the revenue in scope was generated in the year where GDPR compliance was a significant demand factor, this may explain much of the resultant growth.

However, revenues for firms that typically provide cyber security products (e.g. hardware or solution solutions created in-house) demonstrates that most of the medium sized firm revenue comes from the sale of products (£707m, 56% of total medium size revenues). This may be worth exploring further with respect to export and growth potential.

[23] Analysis of BvD FAME data supplemented by extrapolated survey estimates (Ipsos MORI).

Figure 3.3: Total Cyber Security Revenue by Product / Service Offer



Source: Perspective Economics, BvD FAME, Ipsos MORI[24]

[24] Analysis of BvD FAME data supplemented by extrapolated survey estimates (Ipsos MORI).

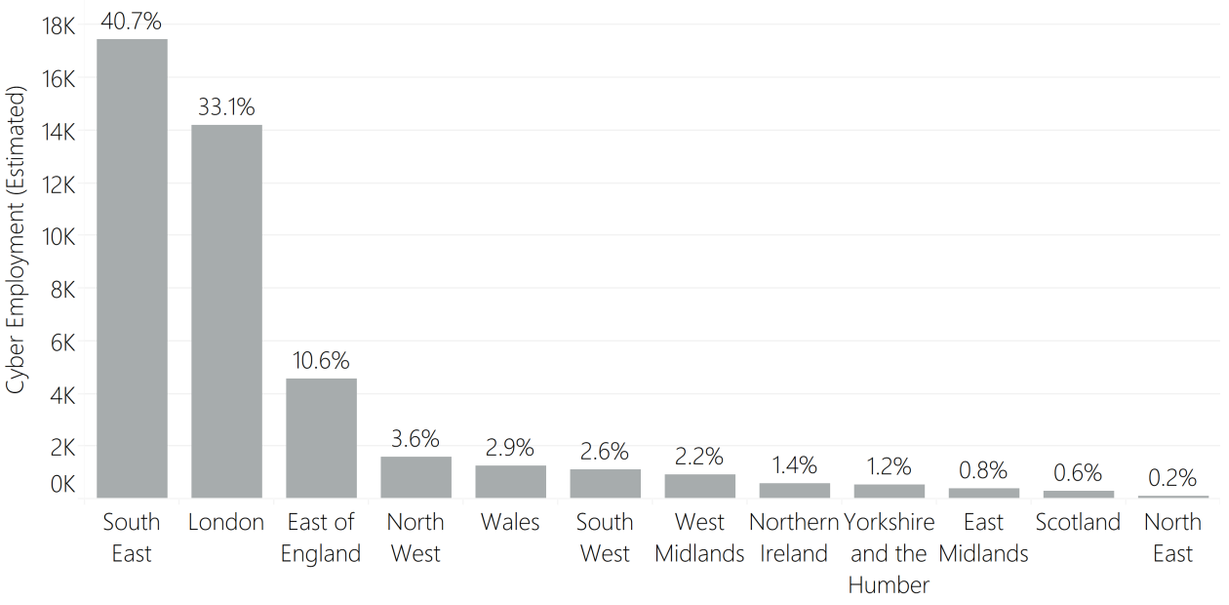
3.2 Estimated Employment

We estimate that there are 42,855 Full Time Equivalents (FTEs) working in a cyber security related role across the 1,221 cyber security firms identified. This reflects an increase of 37% in employee jobs over the last two years (baseline = 31,339 jobs).

As with the baseline analysis, our analysis uses company accounts (where employment figures are provided) where possible, and where gaps exist, we have drawn upon the sector survey, consultations, desk review and LinkedIn to estimate employment. It is worth noting that this estimated figure of c. 43,000 cyber security professionals relates only to those working for these companies. A wider figure for the number of cyber security professionals is likely to be significantly higher given those working in cyber security roles in non-cyber security companies (e.g. finance or insurance companies) or the public sector. Indeed, the Tech Partnership estimated that the cyber security workforce had reached approximately 58,000 in 2017[25] - this figure is now likely to be closer to c. 100,000 based upon suggested growth trends.

Aggregating each company level estimate for cyber security related employment to the regional level highlights that cyber security employment appears to be relatively concentrated within London, the South East, and the East of England (85% combined). However, this reflects employment at a *registered* level, and therefore employment is understated for the other regions. For example, firms registered in Northern Ireland hire an estimated 400 people within cyber security, but the region is home to c. 1,700 cyber security professionals[26] – which demonstrates the importance of cyber security firms being able to draw in talent from across the regions through different offices across the UK.

Figure 3.4: Percentage of Cyber Security Employment by Region (Registered Location)



Source: Perspective Economics, BvD FAME, Ipsos MORI[27]

[25] Computer Weekly (2017) 'UK cyber security workforce up 163% in five years' Available at: https://www.computerweekly.com/news/450412399/UK-cyber-security-workforce-up-163-in-five-years

[26] CyNation (2019) 'Growth Ambitions for Northern Ireland cyber security industry'. Available at: https://cynation.com/growth-ambitions-for-northern-ireland-cyber-security-industry/

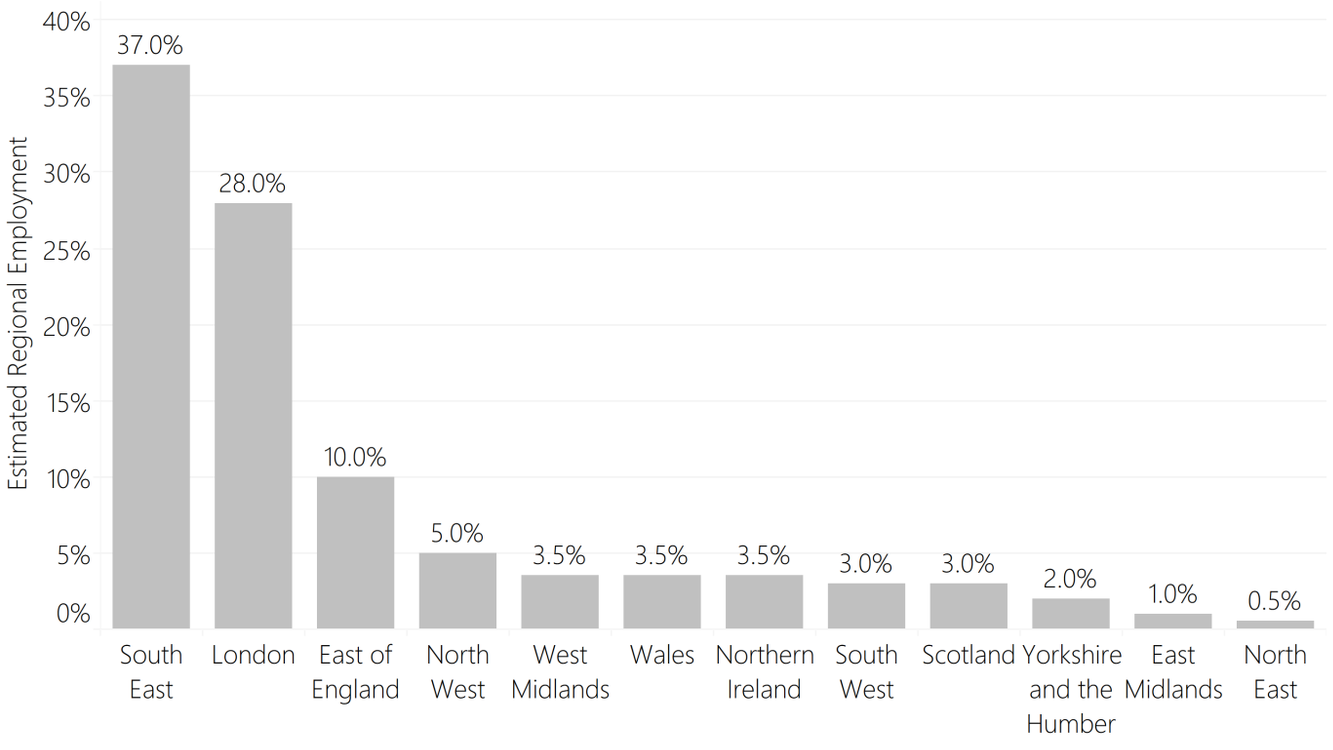
[27] Analysis of BvD FAME data supplemented by extrapolated survey estimates (Ipsos MORI).

As noted previously, it is important to understand how cyber security employment might be reflected across the regions (with respect to trading locations, rather than registered offices).

We therefore provide an estimate of cyber security employment by region in Figure 3.5 below (based upon analysis of trading location hotspots and other existing market intelligence e.g. Science and Innovation Audits and local reviews).

This provides a notable, and more realistic uplift in estimated cyber security employment across most of the regions (other than London, South East, and East of England).

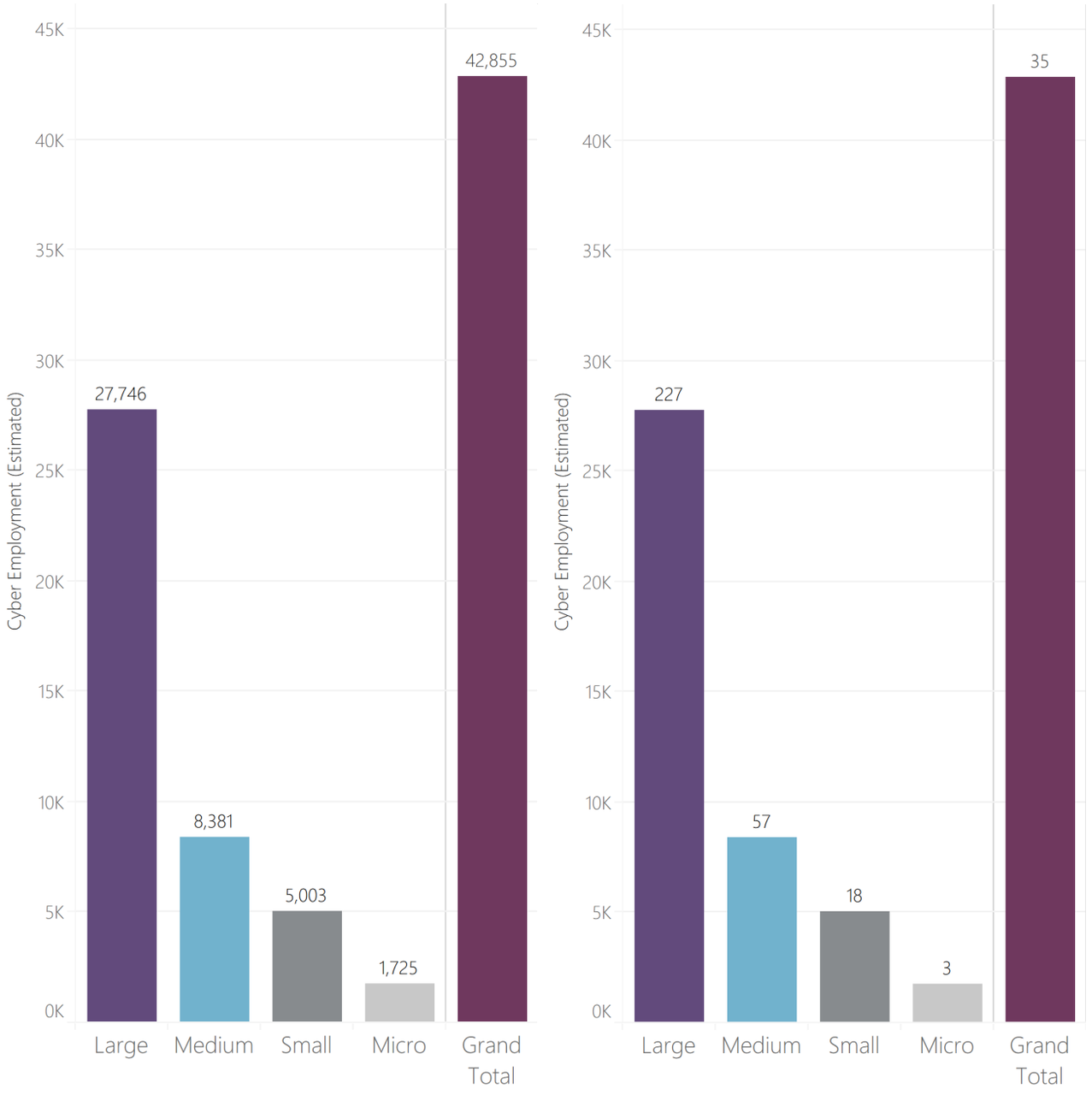
Figure 3.5: Percentage of Cyber Security Employment by Region (Estimated)



Source: Perspective Economics

Analysis of estimated cyber security employment by company size demonstrates that, in line with the baseline findings, most of the cyber security employment is based within large firms (65%). The average size of a cyber security team for the larger employers is 227 (an increase of 4% from 219). The average size of a cyber security team within medium sized firms has also increased from 51 to 57 (an increase of 12%). Average employment within small and micro firms has remained relatively constant since the baseline (18 and 3 staff respectively).

Figure 3.6: Total and Average Number of Employees by Firm Size

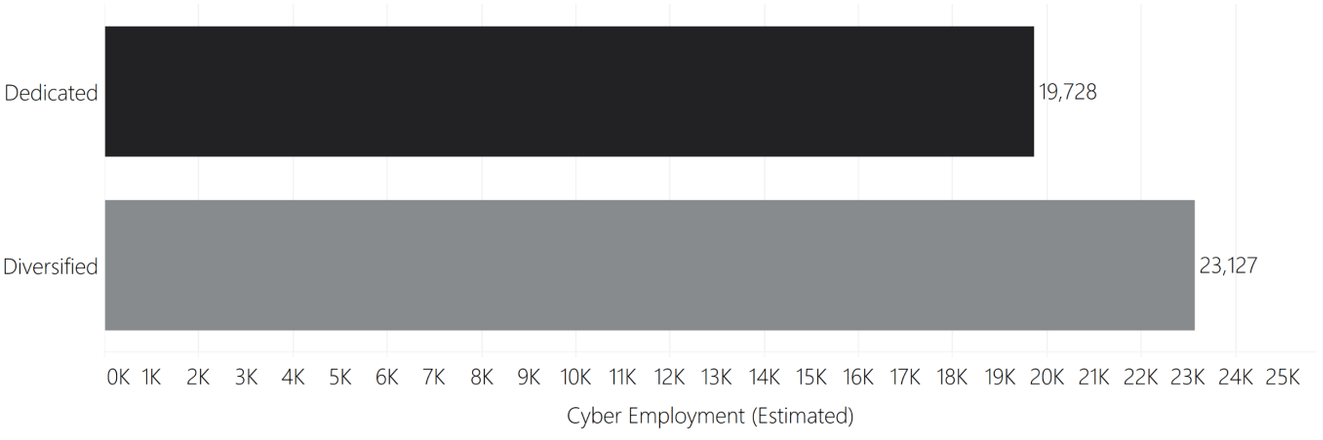


Source: Perspective Economics, BvD FAME, Ipsos MORI[28]

[28] Analysis of BvD FAME data supplemented by extrapolated survey estimates (Ipsos MORI).

The figure below sets out employment segmented by 'Dedicated' and 'Diversified' firms, whereby employment is, in line with the baseline, relatively evenly split (46% and 54% respectively). As there are approximately three times as many 'dedicated' as 'diversified' firms, this suggests that dedicated employers on average have a smaller cyber workforce (22 staff) than diversified firms (average of 74 staff) – which can often include teams of several hundred people (e.g. large consultancy practices etc).

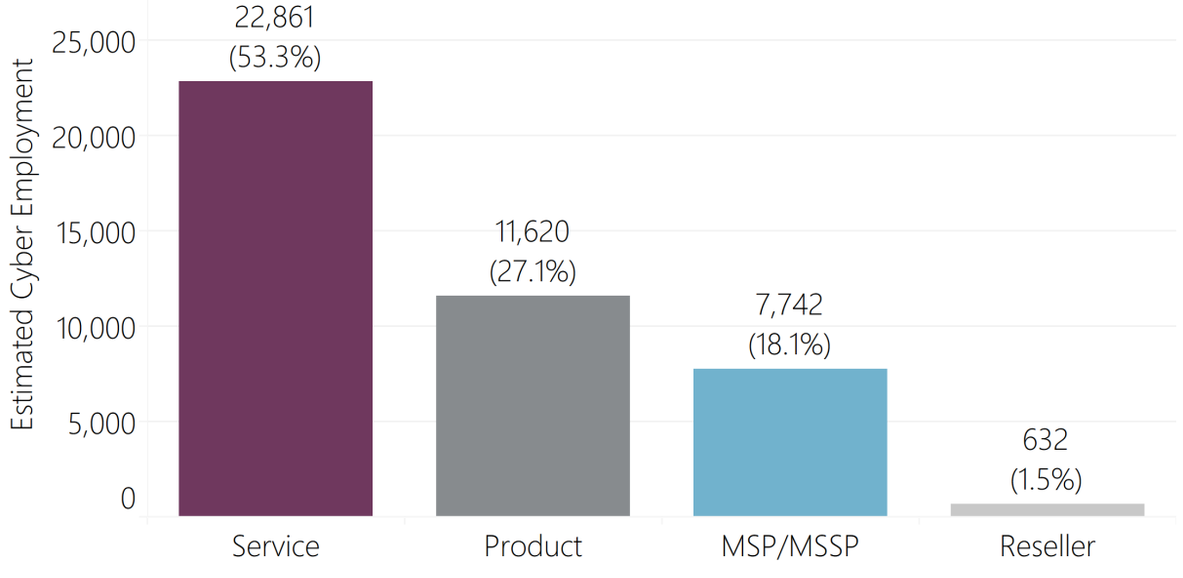
Figure 3.7: Total Number of Employees by Dedicated / Diversified Status



Source: Perspective Economics

Finally, the figure below sets out employment segmented by company core offering. Interestingly, 71% of employees work within a company that primarily offers cyber security services or managed services, compared to 27% that work primarily within a product environment. This may be worth exploring in future detail regarding skills implications and any variance in expected skillsets and qualifications e.g. implementing secure networks, software engineering and programming skills etc.

Figure 3.8: Percentage of Cyber Security Employment by Product / Service Offer



Source: Perspective Economics

3.3 Estimated Gross Value Added (GVA)

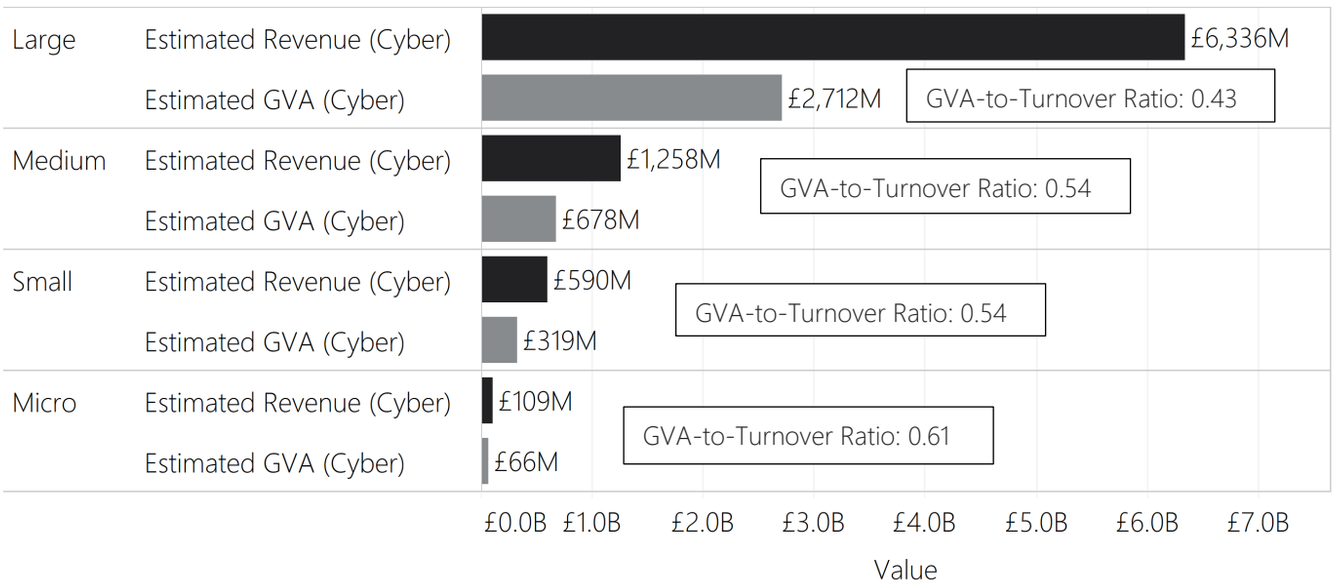
Gross Value Added (GVA) is used as a measure of productivity (at a firm level, or above). It captures the sum of a firm's Gross Profit, Employee Remuneration, Amortisation and Depreciation. In this respect, any increase in GVA can highlight an improvement in the performance of a firm or a sector, as evidenced through higher profitability or enhanced earnings.

Within the most recent financial year (2017/18), we estimate that cyber security related GVA within the sector (1,221 firms) was £3.77bn. Within the baseline analysis, the sector's estimated GVA was £2.35bn, which means total GVA has increased by £1.42bn (+60%) in the last two years.

The majority of GVA within the sector can be attributed to large firms (£2.7bn, 72% of GVA), which is expected given the significant proportion of associated revenues and employment. The GVA-to-Turnover ratio across all firms is 0.46 i.e. for every £1 that the cyber security sector generates in revenue, 46p in direct GVA is generated.

This is higher than the baseline figure of 0.41, suggesting an improvement in gross profitability and/or remuneration over the last two years for cyber security firms. Further, within the baseline analysis, GVA per employee was estimated to be £74,965. This has now increased to £88,069 per employee (i.e. an increase of 17%), which is higher than the DCMS Digital GVA per employee estimates (2018) of £87,000[29].

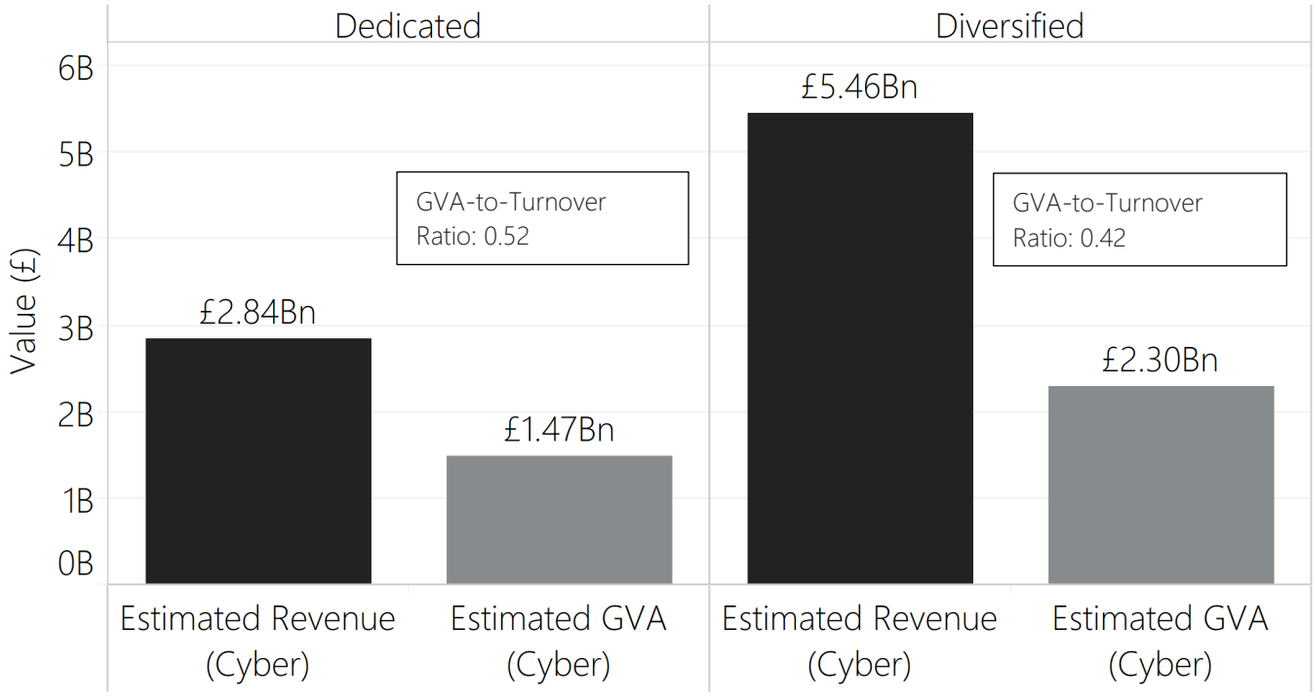
Figure 3.9: Estimated Gross Value Added by Size of Firm



Source: Perspective Economics, BvD FAME

[29] *Calculation used: Digital GVA (£130.5bn) / Employment (1,500,000) = £87,000 per employee*
Sourced from: DCMS (2018) 'DCMS Sectors Economic Estimates Provisional GVA' Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759707/DCMS_Sectors_Economic_Estimates_2017__provisional__GVA.pdf And DCMS Sectors Economic Estimates - Employment' Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/726136/DCMS_Sectors_Economic_Estimates_2017_Employment_FINAL.pdf

Figure 3.10: Estimated Gross Value Added by Dedicated / Diversified Status



Source: Perspective Economics, BvD FAME

3.4 Summary of Economic Contribution

The table below sets out the key findings regarding the economic contribution of the UK's cyber security sector.

Summary of Economic Contribution (2019)

	Number of Firms	Estimated Revenue (Cyber)	Estimated GVA (Cyber)	Estimated Cyber Security Employment	Estimated Revenue Per Employee	Estimated GVA per Employee
Large	122	£6,335,639,203	£2,712,150,886	27,746	£228,344	£97,749
Medium	146	£1,257,992,412	£677,596,844	8,381	£150,101	£80,849
Small	279	£590,394,344	£318,722,570	5,003	£118,008	£63,706
Micro	674	£109,218,985	£65,717,448	1,725	£63,315	£38,097
Grand Total	1,221	£8,293,244,945	£3,774,187,748	42,855	£193,519	£88,069
Change since baseline:	*44%*	*46%*	*61%*	*37%*	*7%*	*17%*

Source: Perspective Economics

4 Investment in the UK Cyber Security Sector

4.1 Introduction

This section draws upon the Beauhurst platform (www.beauhurst.com) which tracks announced and unannounced investments in high-growth companies from across the UK. The baseline report identified 201 investments within 84 firms that were included within the baseline analysis (with investments made since 2007, up to and including August 2017).

Our team has matched Company Registration Numbers and Company Names identified within this current analysis with the platform to identify 531 investments in 180 companies (since 2006).

In order to provide a meaningful analysis of how investment in cyber security companies has performed since the baseline, our core analysis is undertaken from between 1st January 2017 (to provide a full 2017 overview) to 31st December 2019. However, the introductory charts provide a full-time series analysis for all investment data to demonstrate how the last three years compares with the previous timeframe.

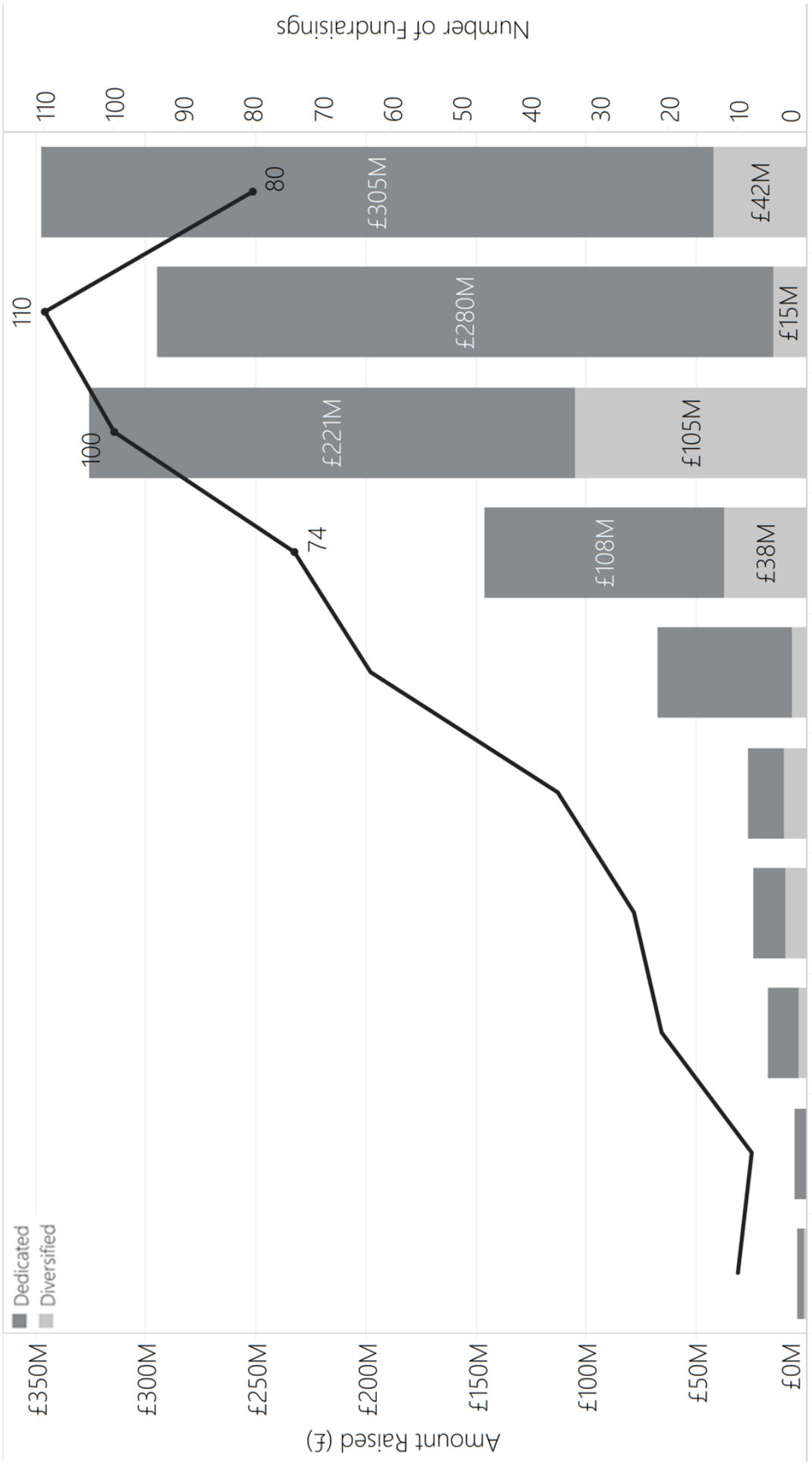
Investment to Date

The investment timeline below (Figure 4.1) demonstrates that 2019 was a record year for cyber security investment, with £348m in fundraising across eighty deals.

Whilst the number of investments decreased by 27% (from 110 to 80 between 2018 and 2019), the total value increased from £295m to £348m, demonstrating larger investments being made within the sector within the last year.

Indeed, over the last four years (2016-19), total investment identified within the cyber security sector has exceeded £1.1bn, demonstrating how investment and confidence has grown in recent years.

Figure 4.1: Overview of Investment Timeline



Source: Beauhurst

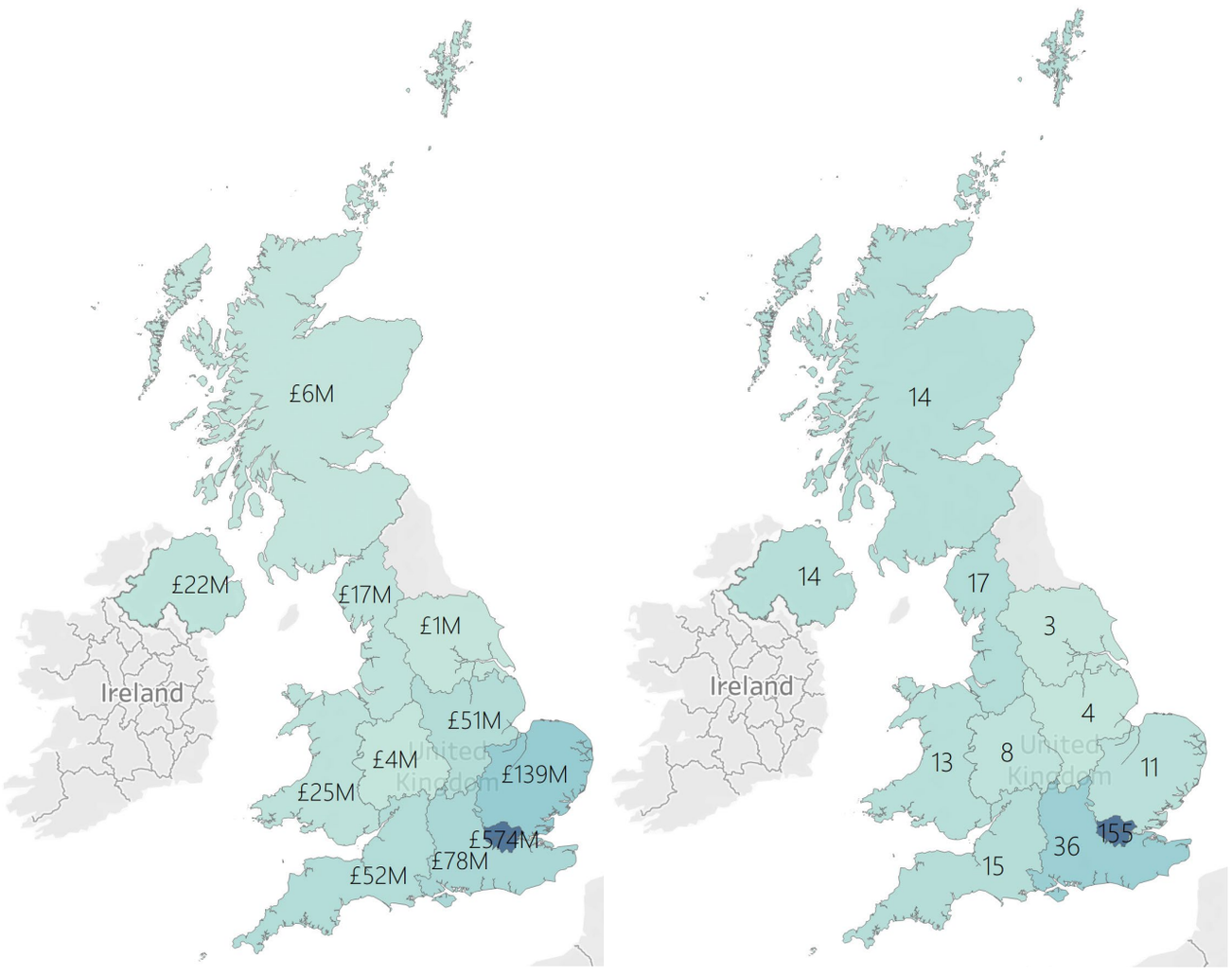
Investment by Location (2017 to 2019)

The maps below set out an overview of investment performance within cyber security by UK region (left = total amount of investment, right = the number of investments identified) since 2017.

Greater London is the top performing region with 155 investments totalling £574m. In other words, the region receives more than half of the UK's investment in cyber security. There is also considerable investment across the South East and East of England (£78m, 36 deals and £139m, 11 deals respectively).

Across the other nine regions of the UK, although cyber security investment is lower, there is evidence that the regions are becoming more engaged with the investment community; Northern Ireland, Scotland and Wales have all performed well with respect to investment since the baseline.

Figure 4.2: Total Investment (Volume and Number) by Region (since 2017)



Source: Beauhurst Total: n = 290 & Total = £968m

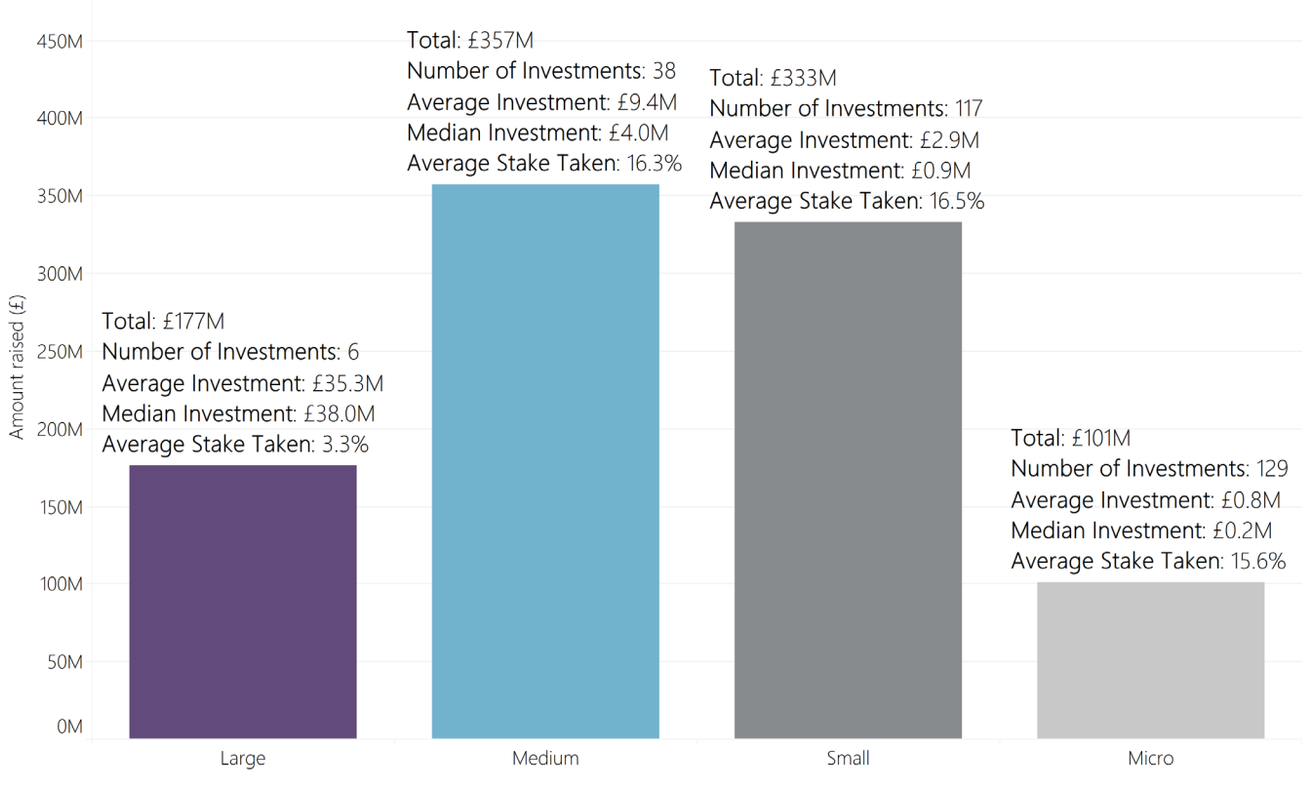
Investment by Company Size

The chart below sets out the volume of investment by (current) company size within the cyber security sector since January 2017.

Of the 290 investments since January 2017, 246 (85%) have been raised by small and micro sized firms, with an average stake taken of 16% – potentially suggesting an appetite within the investment community to invest in emerging cyber security firms within the UK market.

Further, large firms and medium firms have raised £177m (6 deals), and £357m (38 deals) respectively – demonstrating that firms of all sizes across the market have been engaged in raising investment.

Figure 4.3: Investment by Company Size (since 2017)



Source: Beauhurst

Investment by Company Offer

The figures below highlight how, since January 2017, there has been a clear investment preference for companies that primarily offer cyber security products, reflecting 76% (219) of the volume of investments, and 85% (£821m) of the respective investment value.

Figure 4.4: Investment by Product / Service Offer (since 2017)

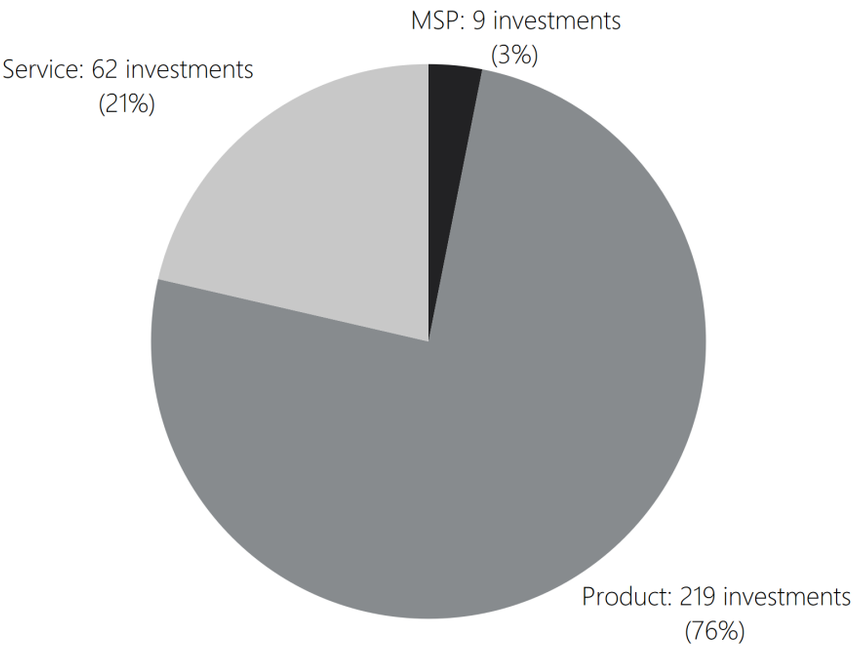
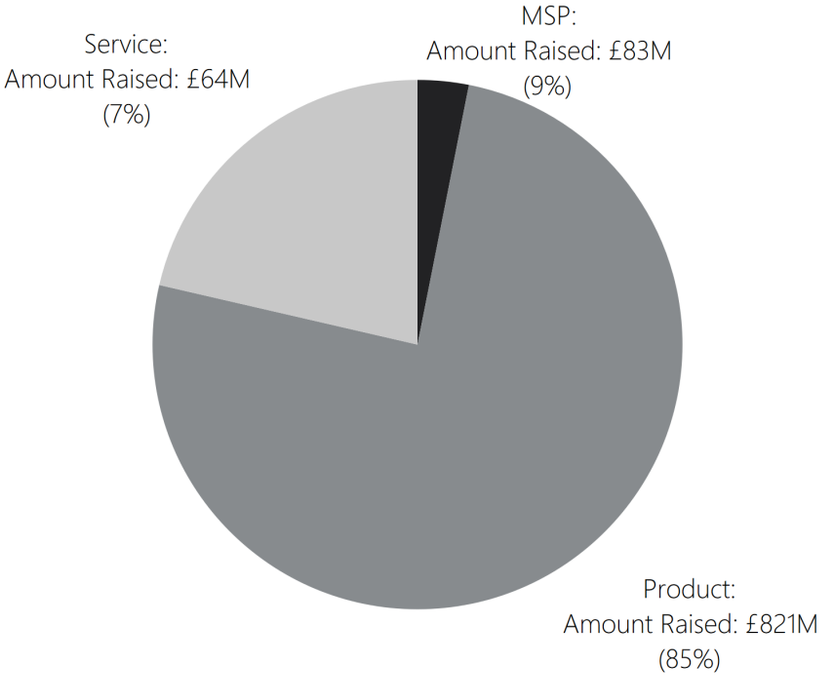


Figure 4.5: Value of Investment by Product / Service Offer (since 2017)



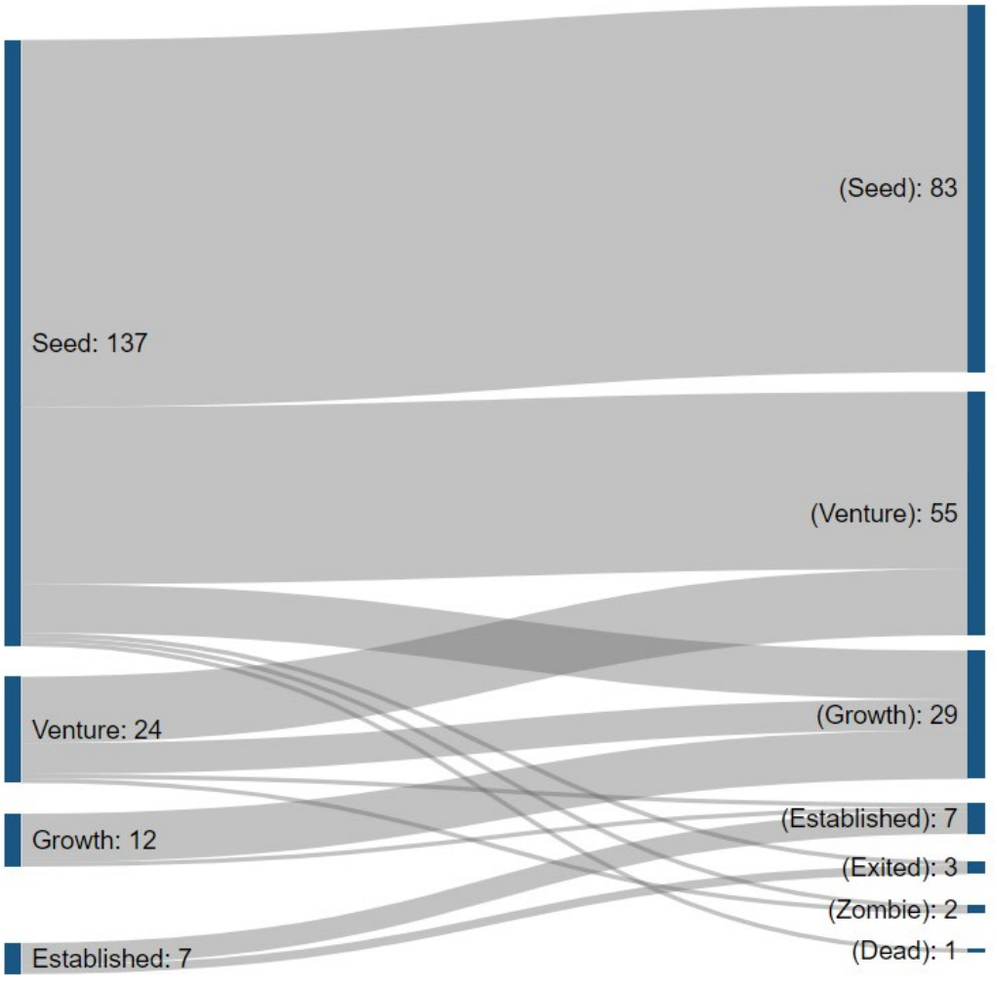
Source: Beauhurst, Perspective Economics (n= 290, and Total = £968m)

4.2 Company Evolution and Company Exits

This section explores the number of firms that have received some form of investment and compares their stage of evolution when they were at seed, venture, or growth stage[30] at the point of the deal, and how this has changed (as of December 2019). It also sets out an overview company exits e.g. due to acquisitions, mergers or IPOs.

The figure below sets out how companies have changed since receiving their first investment. This covers 180 companies. For example, for the seed companies, 61% of companies that received investment at the seed stage have remained as 'seed', whilst over a quarter (29%) have now reached 'venture' status. It can be challenging progress through the stages of company evolution, but investment is an important factor in driving this development across the sector. Interestingly, of those seven companies that were 'established', three of these have since exited, potentially demonstrating the ambition of many cyber security firms to grow and subsequently exit through a takeover etc.

Figure 4.6: Stage of Evolution at First Deal Date vs Current Stage of Evolution



Source: Beauhurst (n=180)

[30] See Definitions for Seed, Venture, Growth and Established, Exited, Dead and Zombie (as defined by Beauhurst) in Appendix F

4.3 Company Exits

With respect to the investment data, Beauhurst indicates that 26 companies included within the baseline have since been acquired with notable acquisitions including:

- Simulty Labs by Arm; acquired for £11.7m in July 2017;
- MWR InfoSecurity by F-Secure; acquired in June 2018 for $106m (+); and
- Zonefox by Fortinet, acquired in October 2018 (spinout from Edinburgh Napier University in 2009, sold for an undisclosed sum).

4.4 Valuation

Of the 180 companies identified within the Beauhurst investment data, the total (most recent) post-money valuation (following an investment made) is estimated at £4bn.

The most significantly valued company is one of the UK's rare 'unicorns' (i.e. valuation over £1bn) – Darktrace, which was most recently valued at £1.2bn.

Further exploration of the data also shows that, of the 94 companies incorporated since 2014 (i.e. within the last five years) that have received some form of investment, the majority (78%) of these are valued at over £1m (at the most recent investment), and almost a third (31%) are valued at more than £5m.

Further, the total post-money valuation for firms involved with a government initiative[31] and that have been incorporated since 2014 is £401m (across 31 firms, average of £12.9m).

4.5 Forms of Investment and Sources of Funding

Overall, looking at the investments secured by the identified cyber security companies, Beauhurst data indicates that:

- There were 195 funds involved, of which 90% are still active. This is an increase from the baseline (whereby 68 funds were identified).

- Further, within the baseline, there were only 10 funds that could provide more than £25m (based upon typical investment activity or known sector / investment restrictions. This has since increased to 18 funds – reflecting that the UK investment community may have matured in recent years (with respect to the cyber security sector).

[31] See Section 6 (involved in one or more of the following: HutZero, Cyber101, CyberASAP, NCSC Cyber Accelerator or LORCA)

5 Understanding Market Growth

5.1 Overview of Growth Since Baseline (2017)

As highlighted below, the sector has grown significantly within the last two years with respect to number of companies active, in addition to revenue, GVA and employment. This includes double-digit growth with respect to the number of companies, associated revenue, GVA and employment within this two year period.

A full overview of the change in number of companies, revenue, GVA, and employment (by company size) between the baseline study and this analysis is set out within Appendix G.

Table 5.1: Summary of Growth since Baseline (2017 – 2019)

Metric	2017 (Baseline)	2019	Absolute Change	Percentage Change
All Companies				
Number of Companies	846	1,221	375	+44%
Estimated Revenue	£5,681,730,723 (£5.7bn)	£8,293,244,945 (£8.3bn)	£2,611,514,222 (+ £2.6bn)	+46%
Estimated GVA	£2,349,347,289 (£2.35bn)	£3,774,187,748 (£3.77bn)	£1,424,840,459 (+ £1.42bn)	+61%
Estimated Employment (Cyber Security)	31,339	42,855	11,516	+37%
Estimated Revenue per employee	£181,298	£193,519	£12,221	+7%
Estimated GVA per employee	£74,965	£88,069	£13,104	+17%

Source: Perspective Economics

5.2 Reasons for Market Growth

The UK cyber security market has clearly grown significantly since the baseline report with respect to the number of companies involved in the sector and the increase in market revenues associated with the provision of cyber security products and services.

There are several reasons for this growth, as detailed below.

Increasing Market Demand

Over the last few years, the domestic demand for cyber security products and services has been driven by several demand factors, including but not limited to:

Regulation:

The Government's Cyber Security Regulation and Incentives Review (2016) set out clearly that the Government had a key role in the implementation of additional regulation to improve cyber risk management across all strands of the economy, not just within Critical National Infrastructure. Whilst not seeking to overburden businesses, ensuring businesses adhere to basic guidance can help protect all parties involved from cyber risk and associated damages.

Indeed, there is a recognition of information asymmetry i.e. that many organisations are unaware or feel unable to deal with the management of cyber risk, and therefore government can help to simplify or stimulate activities that organisations should take to improve compliance.

The key piece of regulation introduced since the baseline sectoral analysis has been the implementation of the General Data Protection Regulation (GDPR) in May 2018. This requires businesses to report cyber security breaches, and failure to do so – or demonstration of poor cyber risk management – can result in fines of up to 20 million euros, or 4% of turnover.

Analysis of the current sectoral data does demonstrate that there has been a considerable increase in the number of companies involved within cyber professional services and cyber security advisory and implementation support, and this may explain much of the market growth between 2017 and 2019.

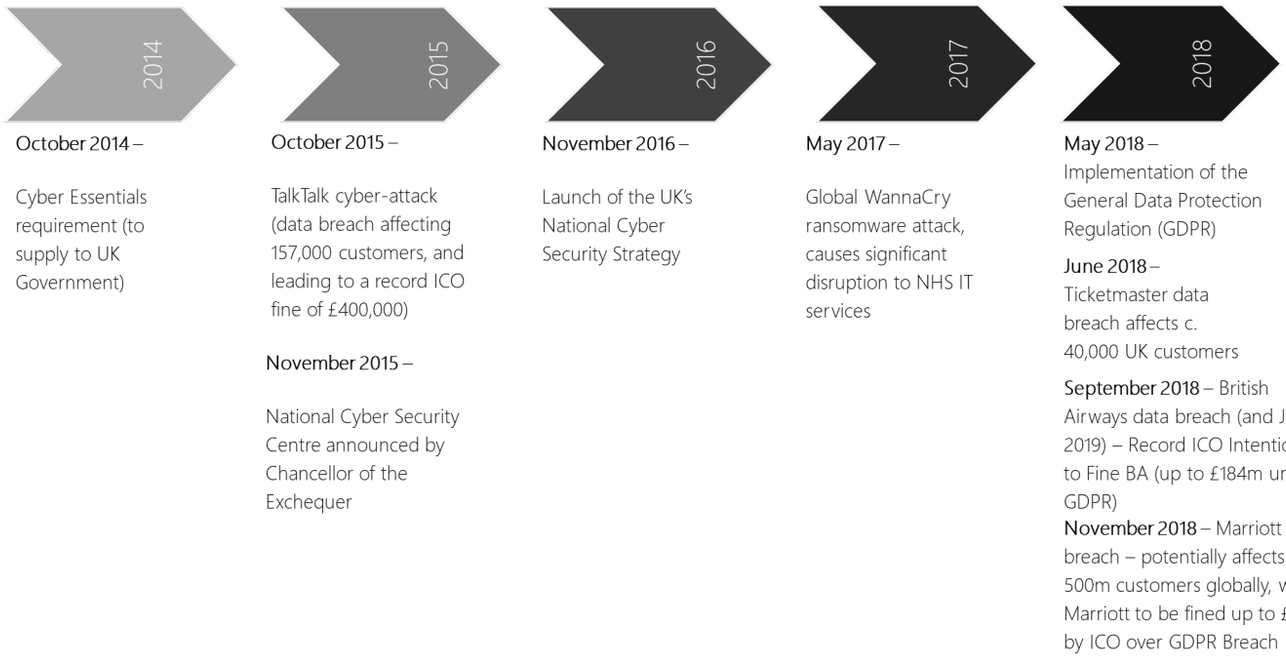
Further, a recent Ipsos MORI survey of firms (*Understanding the Cyber Security Skills Labour Market 2020, undertaken for DCMS*) demonstrates that the number of firms that outsource their cyber security provision has increased from 30% to 42% of businesses within the last nine to twelve months.

It will be important to track whether the increase in demand attributable to GDPR implementation will remain sustainable, i.e. will cyber security budgets within firms remain in place or grow in the coming years. Indeed, there has been some debate whether the ICO would show its teeth following the implementation of GDPR – however, the recent intentions to fine British Airways (£183m) and Marriott (£99m) for data breaches may arguably result in cyber security budgets within larger firms being ring-fenced or bolstered.

Greater Knowledge and Exposure to Cyber Risk:

Further to regulation, there has also undoubtedly been a greater exposure and awareness to cyber risk and the potential implications of breaches and cyber-attacks in recent years.

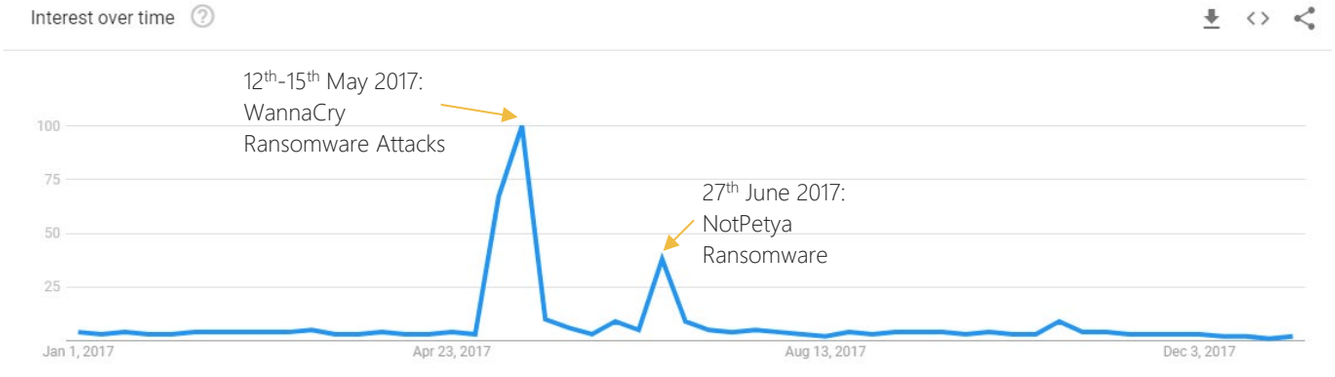
Figure 5.1: Timeline of Notable Cyber Security Incidents and Events in the UK



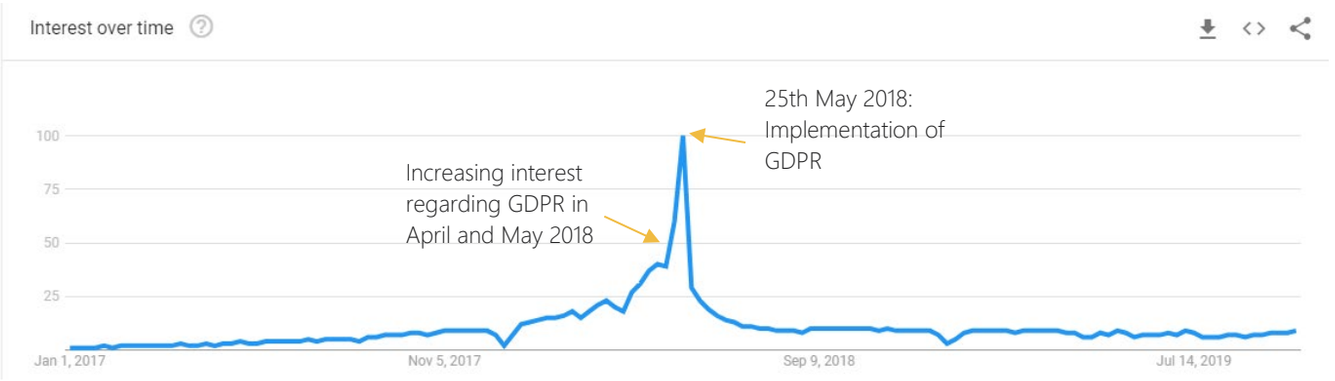
Source: Perspective Economics

Indeed, this behaviour is reflected by Google Trends data (i.e. volume of searches for 'ransomware' and 'GDPR'. The significant challenge is making sure that approaches to cyber security are not solely ad-hoc or reactive but become embedded within 'business as usual' with expenditure on cyber security products and solutions as common as accountancy or legal services.

"Ransomware" (2017)



"GDPR" (2017-19)



Source: Google Trends

Proliferation of Internet-Connected Devices:

Finally, the proliferation of internet-connected devices has also been a driver of demand. For example, Ericsson[32] predicts that there will be approximately 29 billion connected devices by 2022, of which IoT will be related to 18 billion.

This significant growth has led to increased interest within IoT security, as well as Government initiatives to embed 'Secure by Design' principles into IoT devices. Indeed, this is likely to be a major area of demand for the coming years. As F-Secure's Chief Research Officer recently commented, the 'proliferation of 'stupid' IoT devices (e.g. with default usernames and passwords) can be likened to the 'asbestos of the future'[33] if not tackled.

[32] Ericsson (2019) 'Internet of Things Forecast' Available at: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

[33] TechRadar (2019) 'IoT devices could be the asbestos of the future' Available at: https://www.techradar.com/uk/news/iot-devices-could-be-asbestos-of-the-future

The Role of Investment and Acquisitions

"There is a clear upward trend in the amount of capital raised by the UK's ambitious digital security companies over the last eight years. This differs when looking at the funds raised by all our tracked companies across all sectors, with the total number of fundraisings and value raised declining since 2017.

"The increasing fundraising for digital security companies means that these companies can spend more on R&D and innovation, which will aid their efforts in growth. The rising trend also indicates that digital security is a growing industry, with these companies continuing to capture investor attention."

Source: Beauhurst (2019) 'Top Digital Security Startups'[34]

As set out within Section 4 (Investment) and within the Beauhurst summary above, the UK's cyber security sector has been of clear interest to investors within recent years, and has shown a clear upward trend.

For several firms at an early stage that receive investment, this can be the difference in being able to secure talent and move from an idea to a Minimal Viable Product (MVP) to a commercially viable product or service. However, there are some factors that may shape investment and acquisition within the UK sector, as set out below:

- The recent increase in the number of registered firms may now be followed by a move towards consolidation: There is an emerging market view[35] that the increase in investment and acquisition reflects a path towards consolidation, where larger providers can buy up emergent technologies and integrate these into existing technology stacks. For example, in recent years, there have been several significant investments and acquisitions within the sector by established firms, e.g. Blackberry's acquisition of Cylance, and Orange's acquisition of SecureData. This may also be shaped by customer demand – for example, if a commercial client is able to move towards a unified offering rather than engage with different providers for different services (threat detection, end-point security, data loss prevention etc), this may be compelling.

- Currency Valuation: The UK market may also be shaped by the position of sterling. For example, the recent purchase of Sophos by Thoma Bravo for $3.8bn follows a series of other significant buy-outs in the UK by US funds – who may take currency valuation into account when undertaking investments.

- Market Sentiment: Further, whilst cyber security is still viewed as very much a growth industry, there are signs that market sentiment and investor confidence globally is waning somewhat given market and political uncertainties. This may shape the cyber security market in the coming years, particularly if investors feel that they are able to acquire businesses seeking an exit for competitive valuations, or if the perceived rate of return is stronger than other investments.

However, it is worth noting that within an industry such as cyber security that must provide new solutions to new problems, it is likely there will remain sustained opportunities for start-ups and new entrants to the market.

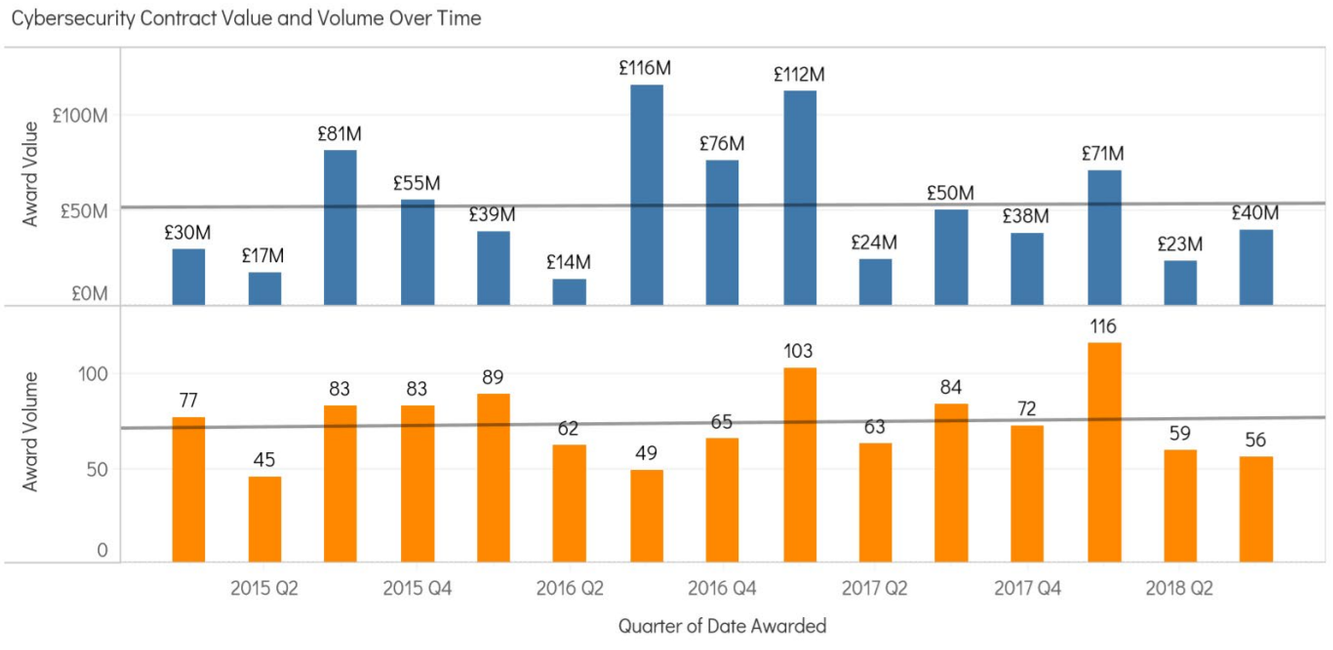
[34] Available at: https://about.beauhurst.com/blog/top-digital-security-startups/

[35] For example: https://www.cyberscoop.com/cybersecurity-consolidation-cylance-blackberry-thoma-bravo/

The Role of Public Procurement & Government

The National Cyber Security Strategy (2016-21) sets out the role of government procurement in growing the sector and making it easier for smaller cyber security businesses to do business. Tussell data suggests that on average, that public bodies in the UK award approximately £50m each quarter in cyber security contracts – and have awarded (through public and competitive procurement) £785m in contracts between Q1 2015 – Q3 2019 (19 quarters).

Figure 5.2: Cyber Security Contracts (Value and Volume)



Source: Tussell (www.tussell.com)

Tussell data estimates that since 2015, 37% (411) of contracts have been awarded to SMEs with a combined value of £158m (20% of the overall award value). This is below the Government's procurement aspiration that £1 in every £3 of government procurement (by 2022) should be spent with SMEs.[36]

This means that larger providers have been awarded 63% of contracts, with 80% of the overall award value. Some of the largest providers include 'strategic suppliers to Government' e.g. large MSPs and telecommunications providers.

[36] UK Government (2018) 'The SME spend target must go on' Available at: https://www.gov.uk/government/news/the-sme-spend-target-must-go-on

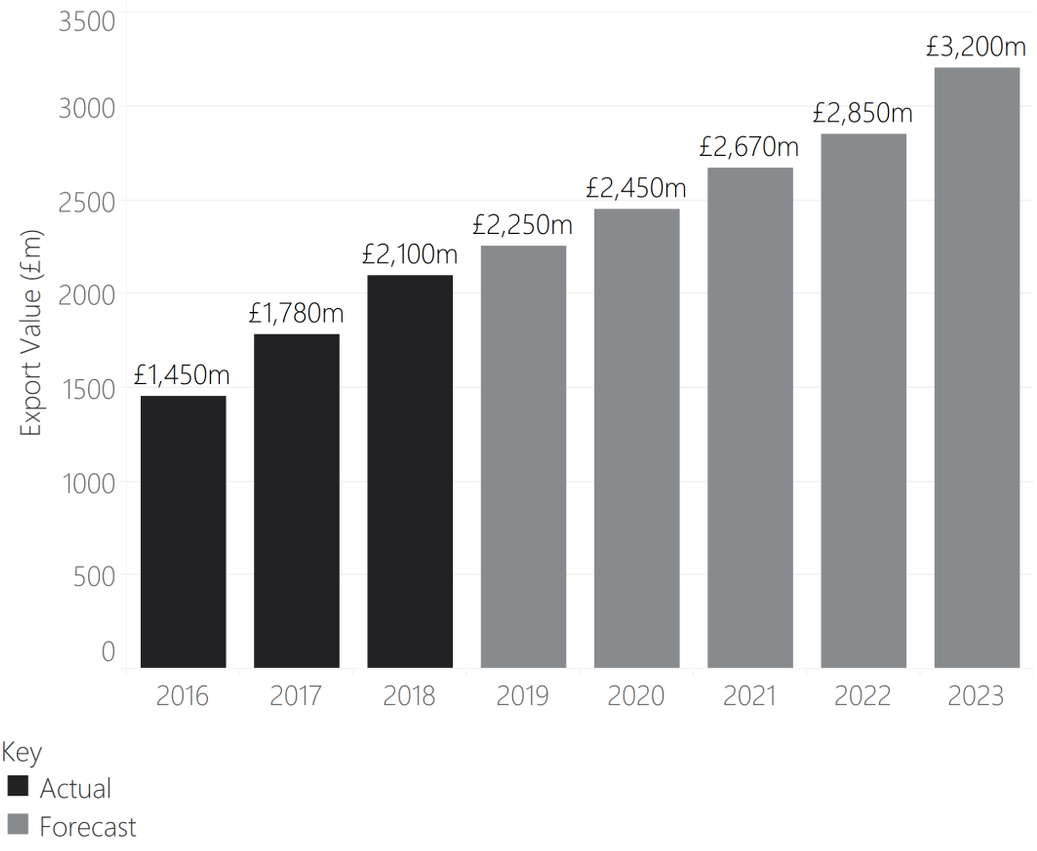
Exports

A key determinant of revenue growth for the cyber security sector in recent years has been that of export growth. As set out within the UK Defence and Security Export Statistics, UK cyber exports were in excess of £2bn in 2018, meaning that approximately one in every £4 of revenue earned by the sector comes from exports.

"Cyber security remains the largest UK HMG Security sub-sector and has grown by 13% from 2017 due to the ongoing demand for reliable and market leading cyber security solutions. UK cyber exports are forecast to grow at a minimum of 9% which is broadly in line with global market growth. There is opportunity for UK industry to outperform this forecast.

"An assessment of the export regions shows Europe with almost 50% of exports and is over double the next largest region. Europe will remain very important for cyber security exports in the future."

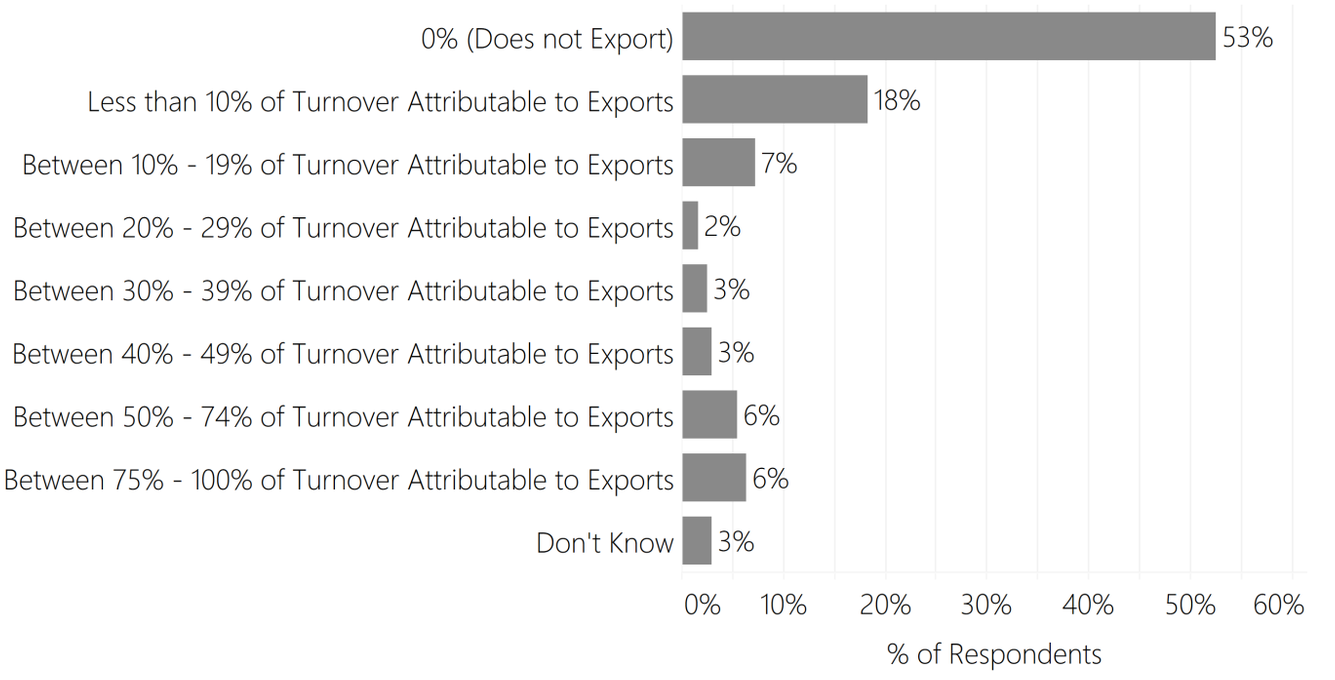
Figure 5.3: UK Cyber Security Exports (2016-18) and Forecast to 2023



Source: UK Defence and Security Export Statistics (2018)

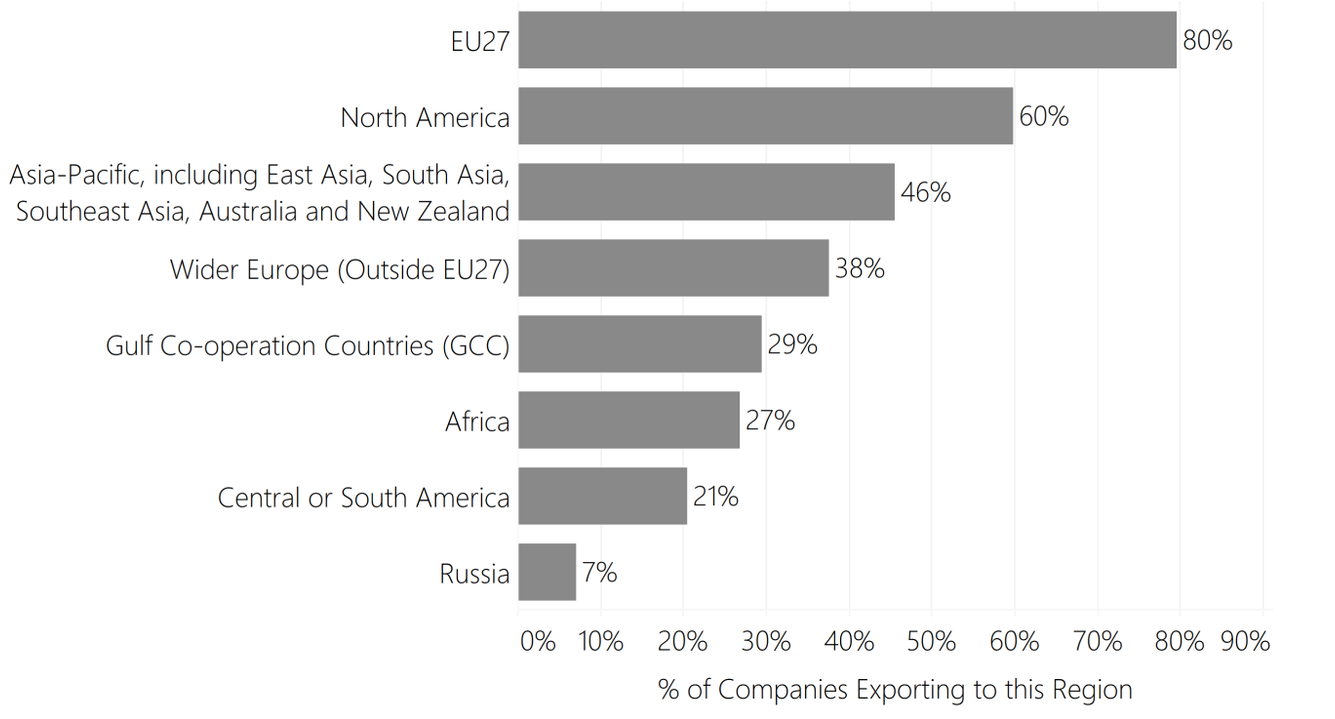
Within the survey of cyber security businesses in Summer 2019, businesses were asked whether they exported, to what extent, and to which regions. Just under half (47%) of businesses exported (Fig 5.4) to the following regions (Fig 5.5).

Figure 5.4: Proportion of Turnover Attributable to Exports for UK Cyber Security Firms (that export products or services outside of the UK) – Survey Estimates[37]



Source: Ipsos MORI (Survey), n = 236

Figure 5.5: Percentage of Companies that Export to the Following Regions (Among the 47% that Export) – Survey Estimates



Source: Ipsos MORI (Survey), n=112

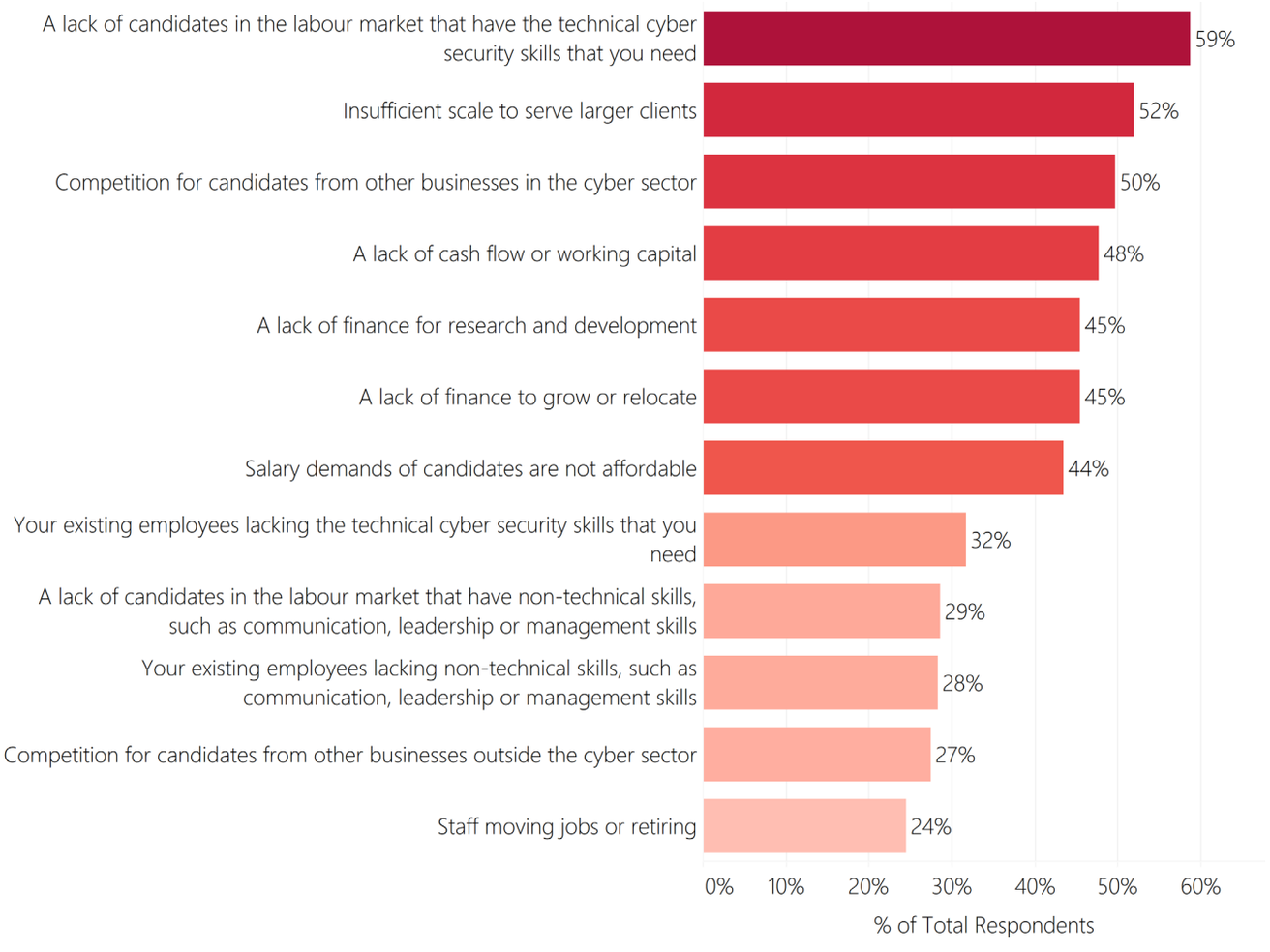
[37] Approximately what percentage of your turnover is attributable to exports? By exports, we mean where products or services are purchased and used overseas by non-UK customers or clients.

5.3 Barriers to Growth

Within the survey of cyber security businesses, we asked firms to what extent they perceived the following conditions as barriers to growth for their businesses (defined as 'affecting their ability to meet your business goals'). The total percentages below reflect those who responded, 'To a great extent' or 'To some extent'.

Overall, the most significant challenge (59% of responses) serving as a barrier to growth for cyber security firms is 'a lack of candidates in the labour market that have the technical cyber security skills needed'.

Figure 5.6: Perceived Barriers to Growth for Cyber Security Firms – Survey Estimates



Source: Ipsos MORI (Survey), n=262

6 Government Support for the Cyber Security Sector

6.1 Overview of Sectoral Support

The National Cyber Security Strategy sets out that Government will help to facilitate an ecosystem which, at its heart, will include a '*programme of initiatives to give start-ups the support they need to get their first customers and attract further investment*'.

There are a wide range of initiatives, incubators and accelerators targeted towards cyber security firms in the UK, which are backed by a mix of government, industry and academic support. These include initiatives to support early-stage ideas and individuals start and grow their own cyber security companies (e.g. HutZero, Cyber 101, CyberASAP), as well as those intended to support and scale-up high-potential high-growth companies (e.g. the NCSC Cyber Accelerator, the London Office for Rapid Cybersecurity Advancement (LORCA)). There are also a range of well-established initiatives and communities such as CyLon, Level39, SetSquared, and Tech Nation Cyber.

This section sets out some of the common metrics, complementarity, and emerging impacts of some of these funded initiatives (HutZero, Cyber 101, CyberASAP, NCSC Cyber Accelerator, and LORCA) – which have collectively supported more than two hundred individuals and businesses in the last three years.

Supporting Cyber Security Ideas, Innovations, and Start-Ups

As the National Cyber Security Strategy sets out:

"The most ground-breaking products and services, that offer the potential to keep us ahead of the [cyber] threat, struggle to find customers who are willing to act as early adopters."

It is therefore important to support businesses involved in cyber security that may have ideas that could materialise into world-leading products but need time to enter and convince the market to adopt and implement.

In order to support early-stage ideas and start-ups, DCMS has funded three key initiatives, namely:

- HutZero: HutZero is a collaboration between Cylon and Centre for Secure Information Technologies (Queen's University Belfast), It offers a three-month programme designed to help entrepreneurs at the start of their journey. The programme starts with a five-day bootcamp to develop team working skills as well as business and technical knowledge. HutZero staff are then available to participants for advice and support for the remainder of the programme. Over the last three years, HutZero has supported almost one hundred individuals, and helped to create ten new registered companies within the cyber security ecosystem.

- Cyber 101: Delivered in a partnership between the Digital Catapult, The Accelerator Network, Centre for Secure Information Technologies (Queen's University Belfast) and Inogesis. Cyber 101 offers a three-stage series of face-to-face events known as Bootcamps, Deep Dives and Demo-days. They provide expert

advice and industry representatives to support the development of critical business skills, contacts and commercial opportunities. It has supported over 160 businesses within the last three years and works across various regions.

- Cyber Security Academic Start-Up Accelerator Programme (CyberASAP): Innovate UK & Knowledge Transfer Network collaborate to help academics in UK universities commercialise their cyber security ideas. They offer a year-long programme divided into three phases: the first focused on developing a value proposition, the second on market validation of the proposition and the third on development of a Minimum Viable Product (MVP) to be presented to funders and industry representatives.

Accelerating High-Growth Companies

Further, DCMS has also supported initiatives that are tailored towards companies that are demonstrating high potential or high-growth and could feasibly be supported to receive further investment and to grow their customer base. These include:

- National Cyber Security Centre (NCSC) Cyber Accelerator: The National Cyber Security Centre, GCHQ and Wayra have partnered to deliver a 9-month programme of support for start-up cyber security businesses who aim to bring 'better, faster and cheaper' security products to market. The programme comprises of a financial grant of £25,000 per participant alongside technical and business support.

- The London Office for Rapid Cybersecurity Advancement (LORCA) is a collaboration between Plexal, Centre for Secure Information Technologies (Queen's University Belfast) and Deloitte. They offer a bespoke, 12-month package of support for successful cohort applicants to scale and grow solutions. Support includes dedicated office space, access to technical and entrepreneurial expertise as well as events to support connections with finance and industry contacts. DCMS has provided £13.5m in funding for LORCA, which is used to provide serviced workspace with workshop facilities, engineering expertise, testing facilities, access to international networks, legal / commercial / marketing / recruitment expertise, and access to potential funders.

  LORCA's ambition is to stimulate the growth of at least 72 high-potential companies, grow up to 2,000 jobs, secure £40 million in investment, and ultimately "Maximise the commercial opportunity", "Minimise barriers to scale" and "Get solutions to market more quickly".

6.2 What has the support provided meant for the cyber security sector?

This section sets out some of the self-reported impacts and data relating to some of the businesses involved in one or many of the initiatives set out within Section 5.1. It is not a full impact assessment which requires further analysis of the counterfactual (i.e. how these businesses may have performed in absence of the support), but it does set out the views of some beneficiaries, as well as a comparison of how businesses supported are estimated have grown in comparison to other businesses within the sector (revenue, GVA and employment).

Views of Survey Respondents & Consultees

Within the cyber sector survey conducted in Summer 2019, 44 respondents involved within initiatives reported that, since participating:

- 80% had started or developed a new product or service
- 77% had improved or innovated within existing products or services
- 68% had improved commercial performance (sales or profitability)
- 68% had entered a new domestic market or expanded their customer base in the UK
- 48% reported they had improved their ability to secure external investment
- 34% entered a new overseas market or expanded international customer base
- 30% located to new office space
- 23% started their own business (via Cyber 101 / HutZero).

Whilst this does not necessarily mean all the positive impacts are fully attributable to the schemes, it does indicate that the companies participating in these various growth initiatives have overwhelmingly moved in a positive direction since the start of their participation.[38] The following subsections explore these in detail (attained through the survey feedback, consultations, and review of performance data).

Coherency and Shared Leadership

Consultations with key initiative leads and businesses supported indicated a broadly shared view that the initiatives to date have helped to enable a sense of market coherency, and that there has been a shared sense of leadership rather than duplication of efforts.

"If you are a cyber security company, it wasn't always clear where to go for support. Things have improved, and between all the providers, I think we do a good job in supporting the sector"
Initiative Lead

[38] The survey also asked about companies' own perceptions of the impact of the schemes and what would have happened without them. We have not reported these data here, for two reasons. Firstly, these are self-reported impacts and therefore not a true impact assessment. Secondly, the results, based on a very small sample size (44), are very skewed towards Cyber 101 scheme participants. This is a relatively low-intensity scheme where companies may not fully recognise the direct and indirect impacts it has had on them. Therefore, we judged the data from these questions to be misleading as to the true impact of the wider range of Government-backed schemes that exists.

Overall, consultees indicated that the benefits of support provided to the cyber security sector included:

- Enhanced knowledge of where to receive support / signposting: One consultee stated they felt finding support was relatively coherent and provided an example of where one team had applied to a commercial initiative for support but was unsuccessful. They were subsequently signposted to a different early-stage support initiative where they were able to develop their business proposition more fully.

  Indeed, one initiative lead commented that they felt they were now well-known within the cyber security community and were reaching out to potential new cyber entrepreneurs by advertising on platforms such as Reddit, which had led to a competitive application process given the volume of applications.

- Participants can benefit from the sense of a clear growth trajectory, with a clear logic for moving along accelerators: Several of the participants within early-stage initiatives (e.g. Cyber 101) have gone on to take part within the NCSC Cyber Accelerator and LORCA. For many consultees, this progression made sense – and demonstrated a clear flow for companies to move along as they grow alongside the support.

Networks and Collaboration

Another benefit identified by stakeholders was that of enhanced networking and collaboration, which has led to examples of team-working, collaboration, sharing of best practice, and investment. Some of the benefits stated included:

- Recognition and Certification: For many of the businesses supported, participating in a government-backed initiative can be viewed as a 'stamp of recognition', and DCMS also backs awards for innovative start-ups across the sector. Several consultees noted that this support often helped to provide investors with confidence that the business was likely to continue growing, and to back it accordingly.

  Indeed, in reviewing company websites and social media profiles as part of this cyber sectoral analysis, several early-stage companies often include logos of the initiatives they have participated within – showing a recognition that often being enrolled in such initiatives can demonstrate that the company is moving in a positive direction, and has begun to establish itself within the marketplace.

- Regular Communication: A common benefit invoked by many consultees was that these initiatives enabled cyber security businesses to not have to work within a siloed approach – and that they could work collaboratively and complement each other's efforts:

  "For each of our cohorts, they would create a WhatsApp group, and still keep each other updated, promote each other's job specifications and recommend software engineers and testers"

- Access to Expertise: Participating within a government-backed initiative can often provide participants with both technical and non-technical expertise. There are several examples of where businesses have been able to change their business strategy, or access technical skills that would not have been available otherwise.

"The Cyber 101 mentors[39] put our business on the right path and to a better understanding around business processes that we didn't have. Digital Catapult exposed us to the right people, companies and experts to help take the company to the next level." (Cyber SME – from Cyber 101 case studies)

- Alumni: It was also recognised that having a 'cohort' approach works well across the initiatives, as attendees keep in touch with one another, and share referrals.

Development of New Companies & Clusters

"We should be careful in equating success and economic growth – there are some really innovative companies that might grow less [with respect to revenue] but offer much more to the UK ecosystem."
Initiative Lead

Aligned to the National Cyber Security Strategy, increasing the number and survival rate of early-stage companies is crucial to securing and embedding innovation within the UK's wider cyber security ecosystem. Within consultations, some of the key benefits of supporting the development of new companies and clusters through the provision of growth initiatives included:

- Establishment of New Companies and Clusters (that may not have happened otherwise): For the initiatives targeted at early-stage provision (e.g. CyberASAP and HutZero), one of the key metrics is that of the number of new companies registered (that subsequently trade). Since starting, there have been ten new companies registered as a result of HutZero and eight (registered or intending to) through CyberASAP.

- *"One of our participants took a week's annual leave to test his idea. He subsequently applied for a commercial initiative and had set up [a now successful business] within weeks."*

- Clearer Route to Convert Academic Ideas into Commercial Products: Consultations with CyberASAP have indicated that the provision of an accelerator focused upon commercialising academic ideas into commercial propositions has been successful to date. Indeed, the team involved have been able to support projects from a wide range of universities (including non-research intensive universities). Some of the key successes to date are set out below:

GraphicsFuzz	Awen Collective	KETS Quantum Security
Originating at Imperial College, provides security and reliability testing for Graphics Processors (GPUs) which are shipped in every desktop, laptop, smartphone, and	Another Alumnus from the first year, Awen Collective Ltd – spun out of the University of South Wales – is an award-winning software company, which reduces	A start-up from the University of Bristol KETS Quantum Security provides future-proof communications security for devices and networks, powered by

[39] 80 mentors from over 50 organisations engaged in the Cyber 101 programme to date, including experts from BAE Systems, PwC, UKBAA, Digital Shadows, Mercia Technologies, DIT, NCSC, Titania, TechUK and others.

will be a critical component in self-driving cars. ▪ Acquired by Google in August 2018 on the basis of the MVP (Minimum Viable Product) developed as part of CyberASAP. ▪ The skills and capabilities have remained in the UK (the founders continue to work on the project as part of Google's London-based development team). ▪ The software itself has also now been released as open source.	the cost of cyber-threats to critical national infrastructure and advanced manufacturing through digital forensics and incident response software. ▪ Crowned Cyber Den Champions in 2018 at NCSC's CyberUK conference & exhibition. ▪ Received £50K funding from IoT Accelerator Wales in April 2018 to develop their industrial digital forensics solutions. ▪ Recently joined Tech Nation Cyber to scale-up their business. ▪ Received SEIS Seed investment from StartupFundingClub in April 2019. ▪ Number of Employees: 5 and recruiting for 1 more.	quantum security on chip. The company now employs 9 people, and is currently recruiting a further 3 staff. ▪ Named the "UK's most innovative small cyber security company 2018" at Information Security Europe 2018. ▪ Raised £2 million investment (publicly funded projects and a seed equity round) to further develop technologies for quantum-secured communications which will improve the secure transmission of information such as banking details and medical records. ▪ In 2017 was one of three start-ups to join Facebook & BT's TIP Ecosystem Acceleration Centre (TEAC) in the UK.

Source: CyberASAP, KTN, Innovate UK

- Regional Cluster Development: Further, a number of consultees spoke of how the initiatives were doing well in promoting regional events and investor days outside of London and the South East (with Belfast, Edinburgh, South West, and Newport all mentioned). This meant that the initiatives were ultimately sharing and showcasing quite diverse products, and opening up exposure to some of the other resources available to UK cyber firms e.g. Digital Catapult, AI clusters etc.

- Reduce Failure Rates: Additionally, consultees noted that participants within the initiatives could be supported to an appropriate level. For example, if an entrepreneur had a potential idea for a cyber security product or business, they could test this relatively early on – without exposing themselves to significant risk or failure later on in the process. This has, in the view of consultees, had the effect of substantially reducing failure rates among the cohorts. For example, for Cyber 101:

  "Cyber 101 was set up to improve the survival rate of cyber security start-ups in the UK. We track this across the cohort, especially with companies between the age of 1-5 years as the survival rate can decrease from over 90% to 40% as the start-ups enter into their 5th year. The current survival rate of Cyber 101 companies is 97% across all ages."

- Supporting Products for a Competitive Marketplace and Affordability: Finally, where products are at the market stage, it is also key that solutions are, as NCSC states within its Cyber Accelerator, "*better and more affordable than existing products. They must also help with [the Government's] underlying mission: To make the UK the safest place to live and work online.*"

  There is evidence that several of the firms supported within the later stages are not offering more of the same, but rather are providing innovative and efficient products to market – which have exhibited revenue and investment growth accordingly.

Economic Growth & Investment

For several of the DCMS backed initiatives to grow the cyber security sector, the anticipated impacts include increased revenue, employment and profitability for firms supported. Whilst it is expected that DCMS will undertake evaluation of each of the growth initiatives it has funded, this section sets out an initial view of how firms that have participated within a government initiative have performed with respect to revenue, GVA and employment in comparison with those that have not. It subsequently also sets out investment raised by firms supported.

It is worth noting that the revenue, GVA and employment comparison is based upon:

- Cyber security firms that were identified at baseline (2017) and current research (2019) stages and remain active; and
- Cyber security firms that have been incorporated between 2014 and 2017 (this comparison explores early-stage companies);
- Cyber security firms that were identified as 'micro' within the baseline study;
- Revenues for these firms are estimated at both baseline and current stage, and therefore changes in revenue are estimates only.

Further, comparison of metrics between firms that have participated within a government-funded initiative may invoke potential for selection bias (i.e. those firms that have performed well following incorporation may be more likely to demonstrate signs of high-growth and therefore be more likely to be selected by an accelerator scheme etc.)

However, the figures below set out an interesting overview of how micro firms (at baseline) registered since 2014 have performed where involved and not involved in initiatives.

The charts below reflect the estimated combined financial performance of:

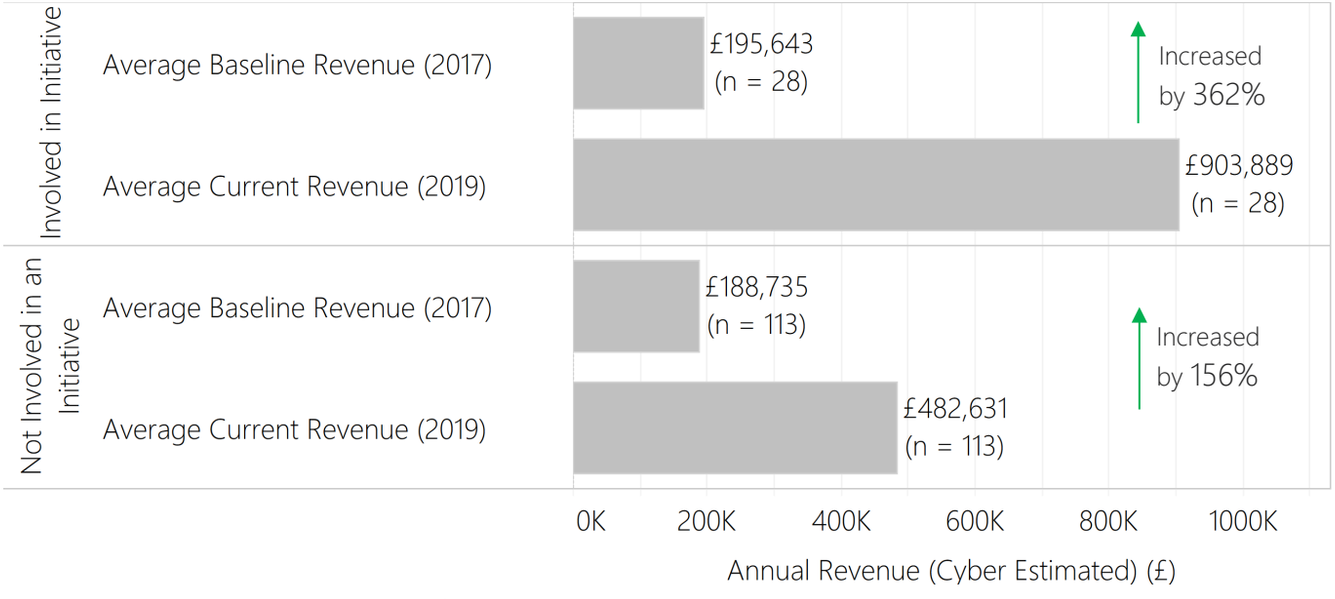
- 28 firms that were micro size within the baseline study, and that have taken part within one or more cyber security growth initiative
- 114 firms were micro size within the baseline study, and that have not taken part within any cyber security growth initiative.

It is worth emphasising that the change in each of the performance metrics reflects the percentage change with two sets of estimated figures (based upon the cyber security sectoral analysis methodology). Further, where growth is higher within firms that have participated within an initiative – this does not ultimately mean that the growth is fully attributable to the initiative and may also reflect that high-growth or high-potential firms may be more likely to participate within a growth initiative.

However, it does show the change in financial performance for these sets of firms within the last two years, and provides an indication that firms participating within cyber security growth initiatives have exceeded the wider growth rates within the broader sector. We estimate that the companies that have participated within a growth initiative have, on average, grown their revenues from £195,643 to £903,889). This reflects a substantial growth rate of 362%. For those firms that have not participated in an initiative, these have increased their revenues, on average, from £188,735 to £482,631). This reflects a growth rate of 156%.

In other words, both cohorts began with similar revenue estimates at the point of baseline, but the firms supported by one or more initiatives are now, on average, almost twice the size of their counterparts – reaching revenues of just under £1m, as shown in Figure 6.1 below.

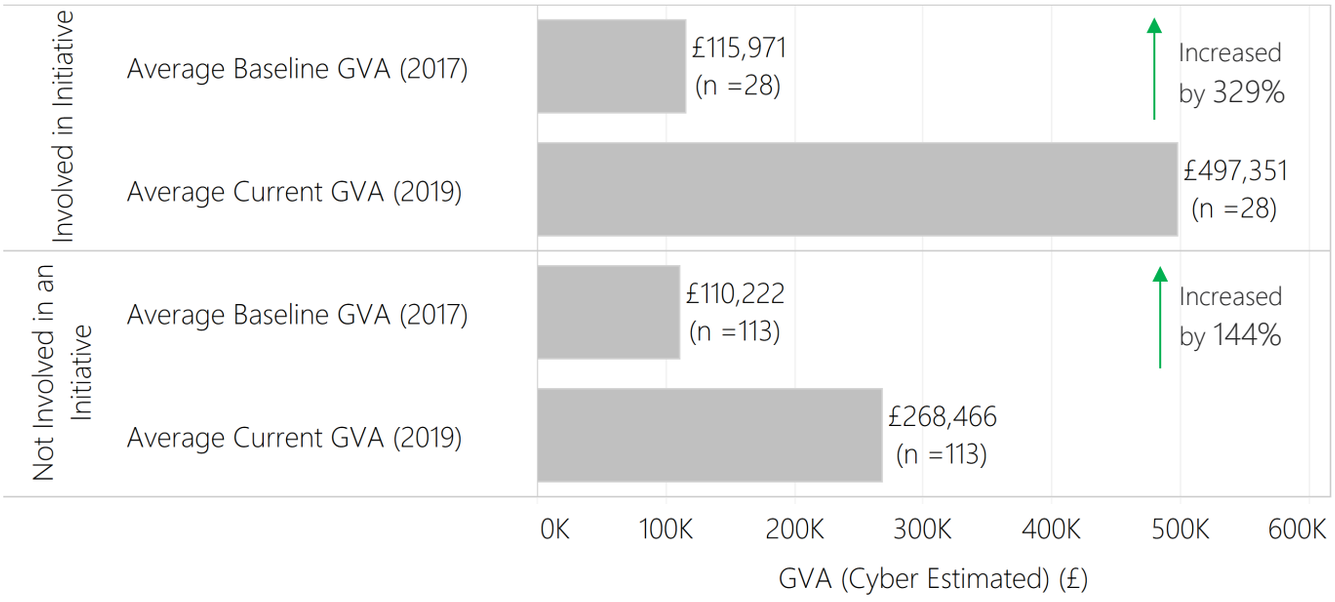
Figure 6.1: Comparison in Average Firm Level Revenue (Baseline and Current)



Source: Perspective Economics (n=28 and n=114)

Analysis of the estimated change in GVA (Figure 6.2) between the two cohorts suggests a similar performance to revenue growth, with average GVA increasing by 329% and 144% respectively.

Figure 6.2: Comparison in Gross Value Added (GVA) (Baseline and Current)



Source: Perspective Economics (n=28 and n=114)

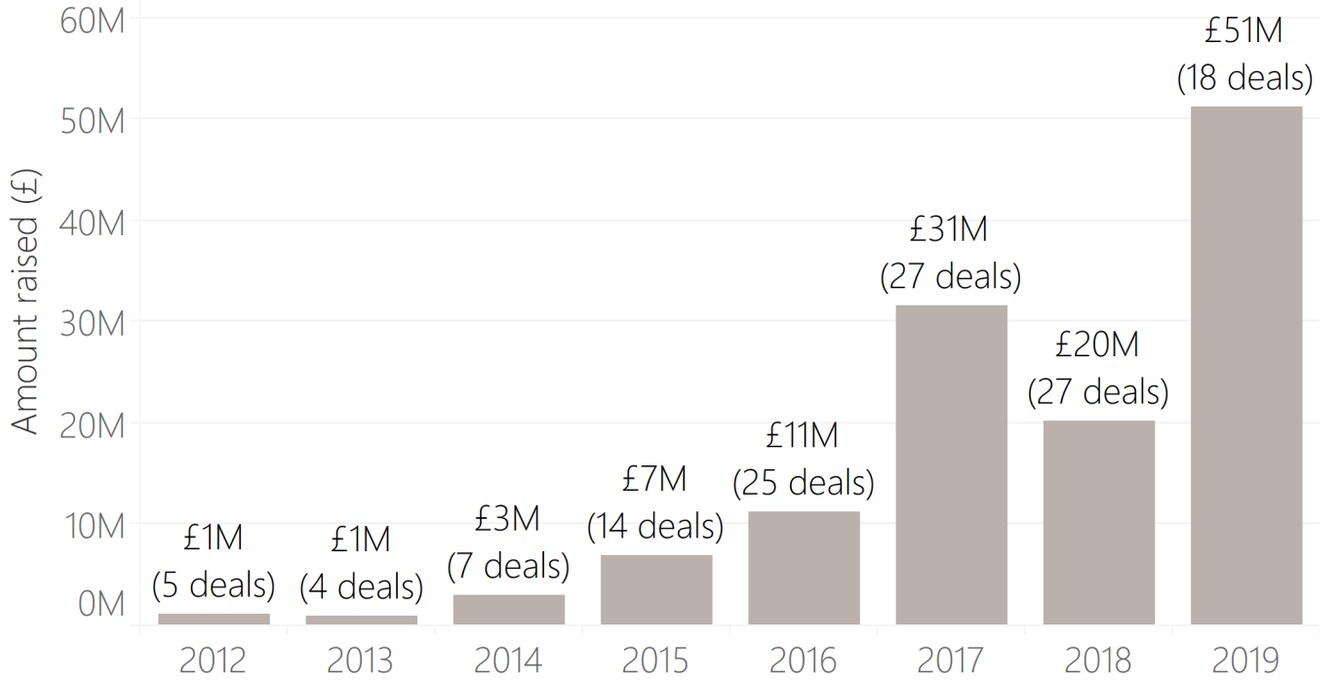
Further, analysis of the estimated change in employment (Figure 6.3) also demonstrates that, whilst starting from a smaller baseline, employment growth reached 197% for supported firms, compared to 90% for those not receiving support from an initiative.

Figure 6.3: Comparison in Cyber Security Employment (Baseline and Current)

Source: Perspective Economics (n=28 and n=114)

Finally, Figure 6.4 sets out an overview of the investment secured by companies supported by government backed initiatives in recent years. This highlights a positive trend in investment for these cohorts, particularly since 2017.

Figure 6.4: Investment Received by Companies involved in a Government Initiative



Source: Beauhurst, (Total = £126m covering 127 investments with 48 companies supported)

7 Conclusions

7.1 Overview of the Size and Scale of the UK Cyber Security Market

Number of Companies

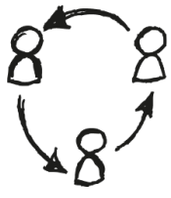
We estimate that there are 1,221 firms active within the UK providing cyber security products and services (2019).

- ↑ This reflects an increase of 44% since the baseline report (846 firms).

In the last two years, we have identified 118 new business registrations within the cyber security sector.

- ↑ In other words, a new cyber security business is registered every week within the UK.

90% of the sector consists of SMEs, with an associated estimated turnover of £2bn (24% of the sector's revenues).



Sectoral Employment

We estimate there are approximately 43,000 Full Time Equivalents (FTEs) working in a cyber security related role across the cyber security firms identified.

- ↑ This reflects an increase of 37% in employee jobs over the last two years.

The majority (65%) of cyber security employment is based within large firms.

Sectoral Revenue

We estimate that total annual revenue within the sector has reached £8.3bn.

- ↑ This reflects an increase of 46% since the 2017 baseline analysis (i.e. revenue has increased by £2.6bn from £5.7bn).
- ↑ On average, we estimate that revenue per employee has reached £193,500 (an increase of 7% since baseline).

Gross Value Added

We estimate that total Gross Value Added (GVA) for the sector reached £3.77bn.

- ↑ This means total GVA has increased by 60% in the last two years, from £2.35bn).
- ↑ GVA per employee has reached £88,000 (an increase of 17%).

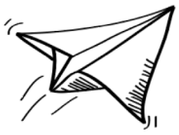
Products and Services

The most commonly provided cyber security products and services include:

- Cyber Professional Services (provided by 71% of firms)
- Threat Intelligence, Monitoring, Detection and Analysis (46%)
- Endpoint Security (including Mobile Security (37%)

Emerging Sub-Sectors:

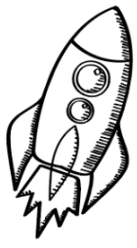
- ↑ IoT Security, SCADA and ICS, Post-Quantum Cryptography



Growth Drivers

The cyber security sector has grown through both increased domestic demand (particularly driven by the implementation of GDPR) and through increased exports.

Further, external investment and increased procurement of cyber security products and services has also helped to increase demand and growth within the sector (see Section 4.2).



Investment

Section 4 (Investment in the UK Cyber Security Sector) demonstrates that:

- ↑ 2019 was a record year for cyber security investment, with £348m in fundraising across eighty deals.

Indeed, over the last four years (2016-19), total external investment identified within the cyber security sector has exceeded £1.1bn, demonstrating how investment and confidence has grown in recent years.

Industry Support

The UK Government has invested in a range of initiatives to help cyber security start-ups, early-stage companies, and high growth companies develop market-leading products and secure external investment.

This research highlights that these initiatives have a key role to play in helping to:

- ↑ develop new products and services (particularly innovative products that can tackle new cyber security challenges);
- ↑ connect high-potential, high-growth businesses with investors; and
- ↑ develop a more coherent ecosystem of cyber security providers, through promoting collaboration and mentoring.

7.2 Opportunities and Challenges for the Cyber Security Sector

Overall, this report has demonstrated the significant growth in recent years within the UK's cyber security sector, with respect to number of companies actively providing products and services, and associated revenue, GVA and employment.

There are clearly opportunities for the UK market, including:

- Promoting investment, research and development in the next generation of cyber security products and services. There is recognition that the UK cyber security market should not solely be measured with respect to financial metrics, but that success should also highlight the UK strengths in research and in developing cyber security solutions that meet new challenges and help to secure emerging technologies. This is particularly important given the UK Industrial Strategy's focus upon supporting the development and embedding of technologies such as 5G, autonomous vehicles, and quantum computing across a range of sectors.

- Growing exports and international activity. As shown by this research and the annual DIT/DSO Cyber Security Export Statistics, the UK cyber security sector's revenues are increasingly being driven through export activity and international engagement. Indeed, the DIT/DSO figures predict annual export sales to grow by at least 9% per annum over the next four years. Further, there are also growing opportunities for UK firms to secure Critical National Infrastructure, both domestically and internationally in the coming years.

- Responding to positive regulations and initiatives designed to keep users and businesses safe online. Growth within the cyber security sector has been arguably driven considerably within the last two years by the introduction of the General Data Protection Regulations (GDPR) and enhanced business understanding of the risks and potential consequences of failing to store data securely. Further, initiatives such as the Cyber Essentials scheme (with the requirement to hold this or equivalent when supplying to government) has increased demand for cyber security advisory support across the UK economy. It will be crucial to understand in the coming years how demand changes, and if these regulations lead to ensuring that corporate and individual spending on cyber security provision is maintained or grows and is recognised as an essential part of doing business.

  Further, when the UK leaves the European Union, this may have implications with respect to how UK firms may store and access personal data (of UK, EU, and international citizens). In the event of regulatory divergence, this may increase complexity and as a result, increase demand for governance, risk and compliance (GRC) services.

- Promoting affordability and accessibility. The UK cyber security sector has become clearer and more coherent to external parties. For example, the Cyber Exchange platform provides users with a breakdown of more than 600 companies by area and offer, which should help to enable users to make informed choices about cyber security provision, improve market competitiveness, and ultimately – help to promote affordability and accessibility for those companies that need to invest in cyber security solutions that meet their needs.

However, there are also challenges, which the cyber security sector will require support and monitoring within the coming years:

- Access to talent. As reflected with the survey findings, three out of every five cyber security businesses are reporting that there is a lack of candidates within the labour market with the cyber security skills that they need. Whilst high remuneration has reflected the challenge in securing staff, there is a risk that without sufficient throughput of new talent into the cyber security sector, further growth may be significantly challenging. Against the backdrop of high demand for cyber security talent, the sector may experience opportunity costs (e.g. inability to service contracts or grow beyond a certain scale) if the skills gap is not tackled in the coming years.

  However, it is worth noting that several of those companies identified within the sectoral analysis have also been active in schemes such as CyberFirst (helping to encourage and nurture new cyber talent), which highlights the potential of government, industry and academia working together to help both increase the number of potential cyber security staff, but to also best align their skills to the needs of industry and research.

  Commercialisation. UK universities have arguably improved in recent years in the commercialisation of academic research[40], and initiatives such as the Innovate UK / Knowledge Transfer Network (KTN) Cyber Security Academic Startup Accelerator Programme (CyberASAP) have also helped to develop cyber security start-ups from academic ideas. It is essential that such practical support is maintained to help establish new cyber security start-ups, and to bring ideas through to commercialisation that might not have otherwise made their way into the UK or international market.

- Ensuring sustainable growth and demand. Whilst demand for cyber security products and services has increased within the last few years, it is important that this demand is sustainable. For example, where businesses have invested in improving their cyber security (which benefits their customers and ensures compliance with regulatory and legal requirements) in recent years, this investment should ideally become part of the business' procedures and governance on a long-term basis, rather than a one-off investment – to help prevent risk and longer-term costs associated with increased cyber risk.

- Market consolidation. The number of companies involved in providing cyber security products and services has increased substantially within the last few years. However, given recent increases in investments and acquisitions – it will be interesting to monitor how and if market consolidation occurs, and how this might shape the market in coming years (e.g. firm-level mergers, creation of joint product offers, implications for pricing structures and market competition etc.)

[40] FT (2019) 'UK Universities intensity efforts to develop start-ups' Available at: https://www.ft.com/content/8e74ad10-e0be-11e9-b8e0-026e07cbe5b4

Appendices

A: Report References

Beauhurst (2019) 'The UK's Top Digital Security Start-Ups' Available at: https://about.beauhurst.com/blog/top-digital-security-startups/

Computer Weekly (2017) 'UK cyber security workforce up 163% in five years' Available at: https://www.computerweekly.com/news/450412399/UK-cyber-security-workforce-up-163-in-five-years

Cyber Exchange: https://cyberexchange.uk.net/#/home

Cyber Resilience Alliance (Gloucestershire, Worcestershire, The Marches, and Swindon & Wiltshire LEPs): https://www.cyberresiliencealliance.org/

CyNation (2019) 'Growth Ambitions for Northern Ireland cyber security industry'. Available at: https://cynation.com/growth-ambitions-for-northern-ireland-cyber-security-industry/

Department for Digital, Culture, Media and Sport (2018) 'DCMS Sectors Economic Estimates Provisional GVA' Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759707/DCMS_Sectors_Economic_Estimates_2017__provisional__GVA.pdf

Department for Digital, Culture, Media and Sport (2018) DCMS Sectors Economic Estimates - Employment' Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/726136/DCMS_Sectors_Economic_Estimates_2017_Employment_FINAL.pdf

Department for Digital, Culture, Media and Sport, Ipsos MORI, and University of Portsmouth (2019) 'UK Cyber Security Breaches Survey 2019' Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019

Department for Digital, Culture, Media and Sport (2019)' Cyber Security Skills Strategy' Available at: https://www.gov.uk/government/publications/cyber-security-skills-strategy

Department for International Trade / Defence and Security Organisation (2019) 'UK Defence and Security Export Statistics for 2018' Available at: https://www.gov.uk/government/publications/uk-defence-and-security-exports-for-2018/uk-defence-and-security-export-statistics-for-2018

Donaldson, S, Hobson, J., Stow, C, and Crozier, D., (2018) 'UK Cyber Security Sectoral Analysis'. Available at: https://www.gov.uk/government/publications/uk-cyber-security-sectoral-analysis

Ericsson (2019) 'Internet of Things Forecast' Available at: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

FINSMES (2019) 'Crypto Quantique Raised $8m in Seed Funding' Available at: http://www.finsmes.com/2019/09/crypto-quantique-raises-8m-in-seed-funding.html

FT (2019) : US private equity group to buy Sophos for $3.9bn: Available at: https://www.ft.com/content/8a82836a-ee49-11e9-bfa4-b25f11f42901

National Cyber Security Centre (2018) Annual Review. Available at: https://www.ncsc.gov.uk/news/annual-review-2018

ONS (2017) Business Births, Deaths and Survival Rates: Available at: https://www.ons.gov.uk/businessindustryandtrade/changestobusiness/businessbirthsdeathsandsurvivalrates

South Wales Cyber Security Cluster: https://southwalescyber.net/

Tech Nation (2019) Cyber Cohort: Available at: https://technation.io/programmes/cyber-security/

TechRadar (2019) 'IoT devices could be the asbestos of the future' Available at: https://www.techradar.com/uk/news/iot-devices-could-be-asbestos-of-the-future

UK Government (2016) 'National Cyber Security Strategy – 2016-2021': Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

UK Government (2018) 'The SME spend target must go on' Available at: https://www.gov.uk/government/news/the-sme-spend-target-must-go-on

UK Government (2018) Cyber Security Export Strategy: Available at: https://www.gov.uk/government/publications/cyber-security-export-strategy

B: Overview of Sources

Data Sources Used

The data sources used to underpin the sectoral analysis included:

- Bureau van Dijk FAME: This platform collates Companies House data and financial statements from all registered businesses within the UK
- Beauhurst: Beauhurst is a leading investment analysis platform, that enables users to discover, track and understand some of the UK's high-growth companies e.g. identify investment, accelerator participation, and key information
- Tussell: Tussell provides market insight into public sector procurement through identifying key contracts, spend, buyers and suppliers
- Cyber Exchange: TechUK's Cyber Exchange directory enables cyber security providers to register an account and set out the products and services they provide to the market
- web scraping: our team has utilised web scraping[41] to extract and parse key company descriptions, locations and contact details from identified company websites
- a representative survey of cyber security firms: in summer 2019, Ipsos MORI conducted a representative survey of cyber security firms. The feedback from 262 providers has been highly useful to understand the financial performance, growth drivers, and challenges for firms within the market.

[41] Note: web scraping has observed 'robots.txt' – i.e. where access is permitted.

- one-to-one consultations: further, the team has also conducted c. 20 one-to-one consultations with key market providers, in addition to a taxonomy workshop, to ensure that the work can be best aligned to wider initiatives.

C: Taxonomy and Definitions

Taxonomy Category	Agreed Definition (Short)	Definition Change Since Baseline:
Cyber professional services	Providing trusted contractors or consultants to advise on, or implement, cyber security products, solutions or services for others.	No Change
Endpoint and mobile security	Hardware or software that protects devices when accessing networks.	Changed from 'End-User Device Security' and added Mobile Security as a growth area.
Identification, authentication and access controls	Products or service that control user access, for example with passwords, biometrics, or multi-factor authentication.	No Change
Incident response and management	Helping other organisations react, respond or recover from cyber-attacks.	No Change
Information risk assessment and management	Products or services that support other organisations to manage cyber risks, for example around security compliance or data leakage	No Change
Internet of Things	Products or services to embed or retrofit security for Internet of Things devices or networks	New Category: UK Growth Area / Specialism.
Network security	Hardware or software designed to protect the usability and integrity of a network.	No Change
SCADA and Information Control Systems	Cyber security specifically for industrial control systems, critical national infrastructure and operational technologies	No Change
Threat intelligence, monitoring, detection and analysis	Monitoring or detection of varying forms of threats to networks and systems.	Added 'Threat Intelligence' to 'Monitoring, Detection and Analysis'
Awareness, training and education	Products or services in relation to cyber awareness, training or education.	No Change.

D: Survey Methodology and Interpretation

Survey data collection

Ipsos MORI carried out the survey fieldwork from 1 May to 25 June 2019.

The primary data collection was by telephone. This followed a random-probability approach, with interviewers making a minimum of 10 calls to each lead (unless the respondent took part in an interview before then). This is a gold-standard surveying approach and is considered the most robust way of undertaking business surveys.

We used the list of firms identified as being part of the cyber sector as the overall sample frame. Perspective Economics and Ipsos MORI made several efforts to improve the quality of this sample before and during the survey, including finding named contacts and alternative contacts online, both on company websites and on databases such as Beauhurst.

From the original list of 1,221 firms, we found telephone numbers for 1,108. All these leads were included in the survey, effectively making this a census of the available sample frame. As such, the 262 achieved interviews are a simple random sample without any stratification (i.e. boosting of certain subgroups).

In order to reduce gaps in the data, we also offered respondents who had said "don't know" at various key questions in the survey a chance to revise this response in a follow-up online survey. Overall, 16 respondents supplemented their original telephone answers through the online survey.

Achieved sample composition and comparison to non-survey estimates

The following table shows the composition of the 262 interviewed firms by size (from questionnaire data), compared to the population profile from the BvD FAME database (shown in Chapter 2). Three firms in the survey were unable to say how many staff they had.

	Survey achieved proportion	BvD FAME estimate
Micro (1 to 9 employees)	61% (n=159)	55%
Small (10 to 49)	29% (75)	23%
Medium (50 to 249)	4% (11)	12%
Large (250+)	5% (14)	10%

These figures are not *directly* comparable because the BvD FAME size definitions also incorporate turnover. The comparison suggests that there is no major size skew in the sample. Nevertheless, it is likely that the survey slightly underrepresents medium and large firms in the sector. This is a common occurrence in random-probability business surveys, as larger businesses typically have a lower propensity to take part.

While one solution would be to weight the survey data to match the BvD FAME profile, **we have opted not to weight the data** for the following reasons:

- Part of the purpose of the survey was to understand the overall population profile – the survey estimates themselves are likely to be more reliable and up-to-date than the BvD FAME data.
- The random-probability sampling approach ensures that the survey is still representative.

- Applying weights to a very small overall sample of 262 interviews is not common, as weighting reduces the statistical power of the survey estimates.

Response rate

The unadjusted response rate for the survey is 24% (262/1,108). However, this does not account for the fact that a proportion of the 1,108 telephone numbers sampled were unusable (e.g. wrong numbers, disconnected etc.). Over the course of the survey, Ipsos MORI attempted wherever possible to find alternative numbers. We also discovered that a small number of firms had been taken over by other firms within the sector, so were no longer separate companies.

Taking into account these issues, the total *usable* sample can be adjusted down to 946. Therefore, the adjusted response rate is 28%.

E: Inclusion / Exclusion Criteria for Defining Cyber Security List

Where firms identified were active and included within the baseline study and were still active and providing cyber security products and services, these were retained within the cyber sectoral analysis dataset.

Where firms were newly identified to the study (i.e. were not previously included within the baseline), the scoring criteria is consistent with the baseline report[42].

This means the team utilised the following scoring approach, but also – utilised web scraping to identify more thorough company descriptions, which were tested against the taxonomy categories to determine fit. This consisted of both an automated (fuzzy match) check of key words in descriptions against the taxonomy definitions (and word list), as well as a manual check where appropriate.

[42] See Appendix C of the Baseline Report.

F: Stage of Evolution Definitions

The definitions below are sourced from Beauhurst's (www.beauhurst.com) Glossary of Terms.

Seed

As a rough guideline: a youngish company with a small team, low valuation and funding received (low for its sector), uncertain product-market fit or just getting started with the process of getting regulatory approval. Funding likely to come from grant-awarding bodies, equity crowdfunding and business angels.

Venture

As a rough guideline: a company that has been around for a few years, has either got significant traction, technology or regulatory approval progression and funding received and valuation both in the millions. Funding likely to come from venture capital firms.

Growth

As a rough guideline: a company that has been around for 5+ years, has multiple offices or branches (often across the world), has either got substantial revenues, some profit, highly valuable technology or secured regulatory approval significant traction, technology or regulatory approval progression, funding received and valuation both in the millions. Funding likely to come from venture capital firms, corporates, asset management firms, mezzanine lenders.

Established

As a rough guideline: a company that has been around for 15+ years, or 5-15 years with a 3 year consecutive profit of £5m+ or turnover of £20m+. It is likely to have multiple (often worldwide) offices, be a household name, and have a lot of traction. Funding received, if any, is likely to come from corporates, private equity, banks, specialist debt funds and major international funds.

Exited

The company has completed an IPO or been acquired.

Zombie

The company's website and/or social media presence show prolonged neglect and/or its Companies House status is somehow troubled – Administration, Liquidation, Dissolution First Gazette, etc. (Merely doing a down-round is not by itself a reason for us to class a company as 'Zombie'. And a company may not be trading, because it is just a holding company, but that doesn't mean we'd classify it as 'Zombie': its subsidiaries may be doing their thing normally.)

Dead

The company has met one or more of these conditions: It has declared it has definitively ceased all activity; its top parent company has been dissolved; and or it has been at Zombie stage for a prolonged period of time.

G: Key Metrics: Change since Baseline (2017)

Metric	2017 (Baseline)	2019	Absolute Change	Percentage Change
All Companies				
Number of Companies	846	1,221	375	**44%**
Estimated Revenue	£5,681,730,723	£8,293,244,945	£2,611,514,222	**46%**
Estimated GVA	£2,349,347,289	£3,774,187,748	£1,424,840,459	**61%**
Estimated Cyber Employment	31,339	42,855	11,516	**37%**
Estimated Revenue per employee	£181,298	£193,519	£12,221	**7%**
Estimated GVA per employee	£74,965	£88,069	£13,104	**17%**
Large				
Number of Companies	89	122	33	**37%**
Estimated Revenue	£4,197,673,387	£6,335,639,203	£2,137,965,816	**51%**
Estimated GVA	£1,714,963,109	£2,712,150,886	£997,187,777	**58%**
Estimated Cyber Employment	19,486	27,746	8260	**42%**
Estimated Revenue per employee	£215,420	£228,344	£12,924	**6%**
Estimated GVA per employee	£88,010	£97,749	£9,739	**11%**
Medium				
Number of Companies	132	146	14	**11%**
Estimated Revenue	£1,066,625,313	£1,257,992,412	£191,367,099	**18%**
Estimated GVA	£435,470,039	£677,596,844	£242,126,805	**56%**
Estimated Cyber Employment	6,776	8,381	1,605	**24%**
Estimated Revenue per employee	£157,412	£150,101	-£7,311.72	**-5%**
Estimated GVA per employee	£64,267	£80,849	£16,582.63	**26%**
Small				
Number of Companies	205	279	74	**36%**
Estimated Revenue	£328,448,253	£590,394,344	£261,946,091	**80%**
Estimated GVA	£152,842,742	£318,722,570	£165,879,828	**109%**
Estimated Cyber Employment	3,814	5,003	1,189	**31%**
Estimated Revenue per employee	£86,116	£118,008	£31,892	**37%**
Estimated GVA per employee	£40,074	£63,706	£23,632	**59%**
Micro				
Number of Companies	420	674	254	**60%**
Estimated Revenue	£88,983,771	£109,218,985	£20,235,214	**23%**
Estimated GVA	£46,071,399	£65,717,448	£19,646,049	**43%**
Estimated Cyber Employment	1,263	1,725	462	**37%**
Estimated Revenue per employee	£70,454	£63,315	-£7,139	**-10%**
Estimated GVA per employee	£36,478	£38,097	£1,619	**4%**

[This page is intentionally blank]

For more information

Ipsos MORI
3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

www.ipsos-mori.com
http://twitter.com/IpsosMORI

Perspective Economics
48-60 High Street
Belfast
BT1 2BE
www.perspectiveeconomics.com

Centre for Secure Information Technologies
Queen's University Belfast
ECIT Building, Queen's Road,
Belfast
BT3 9DT
www.qub.ac.uk/ecit/CSIT/