

UK Cyber Security Sectoral Analysis 2022

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

Sam Donaldson, Perspective Economics
David Crozier, Centre for Secure Information Technologies (CSIT)
Sergi Martorell and Iain McLaren, glass.ai
Jamie Douglas and Jayesh Navin Shah, Ipsos



Department for
Digital, Culture
Media & Sport



Contents

Foreword: Julia Lopez MP	1
Executive Summary	2
Introduction	2
Project Scope and Summary of Methodology	2
Key Findings	3
1 Introduction	4
1.1 Methodology and Sources	4
1.2 Consistency with the 2021 Cyber Security Sectoral Analysis	7
1.3 Interpretation of the Data	8
1.4 Acknowledgements	8
2 Profile of the UK Cyber Security Sector	9
2.1 Defining the UK Cyber Security Sector	9
2.2 Number of Cyber Security Firms Active in the UK	10
2.3 Products and Services Provided by the UK Cyber Security Sector	16
3 Location of Cyber Security Firms (UK)	20
3.1 Introduction	20
3.2 Location of UK Cyber Security Firms	20
3.3 UK Cyber Security Heatmap	22
3.4 Role of Cyber Security Clusters	23
3.5 International Activity	23
4 Economic Contribution of the UK Cyber Security Sector	25
4.1 Estimated Revenue	25
4.2 Estimated Employment	30
4.3 Estimated Gross Value Added (GVA)	33
4.4 Summary of Economic Contribution	34
5 Investment in the UK Cyber Security Sector	35
5.1 Introduction	35
5.2 Investment to Date	35
5.3 Investment by Location	37
5.4 Investment by Size	38
5.5 Investment by Company Type	39
5.6 Investors and Sources of Funding	40
5.7 Market Dynamics: Qualitative Feedback	41
6 Government Support for the Cyber Security Sector	45
6.1 Introduction	45
6.2 Recent Investments and Support Initiatives	45
6.3 Engagement with Cyber Sector Accelerator Schemes	47
6.4 Engagement with Other Regional Bodies and Organisations	50

6.5 Cyber Security Exports	53
6.6 Public Procurement.....	55
Regional Snapshots.....	57
Introduction.....	57
East Midlands.....	57
East of England.....	58
Greater London.....	59
North East	60
North West.....	61
South East.....	62
South West.....	63
West Midlands.....	64
Yorkshire and the Humber	65
Northern Ireland.....	66
Scotland	67
Wales	68
Appendices.....	69
A: Overview of Sources.....	69
B: Taxonomy and Definitions.....	70
C: Survey Methodology and Interpretation	71
D: Investment Definitions.....	71

Foreword: Julia Lopez MP



Over the last decade, we have established the UK as a cyber power, through building cutting-edge cyber security capabilities, and significant growth in our cyber security sector. In December 2021, the government published the National Cyber Strategy, which sets out how we will ensure that the UK in 2030 continues as a leading responsible and democratic cyber power, able to protect and promote our interests in and through cyberspace.

The strategy sets out our commitment to 'strengthening the UK cyber ecosystem, investing in our people and skills and deepening the partnership between government, academia and industry.' To achieve this, we must continue to foster the growth of a sustainable, innovative, and internationally competitive cyber security sector, delivering quality products and services, which meet the needs of government and the wider economy.

This Cyber Security Sectoral Analysis research has tracked the growth of the UK cyber security sector since 2018 and highlights the impressive performance of many of our firms, and their steadfast resilience in recent years.

Within this year's study, we are now tracking over 1,800 cyber security firms in the UK. In the last 12 months, the sector has demonstrated double-digit growth across a number of key measures. The sector's revenue has grown to more than £10 billion for the first time, and the

sector has added over 6,000 jobs. 2021 was also a record year for external investment into the sector – with over £1 billion raised by firms across the UK.

However, we know that work must continue to ensure the UK remains resilient and prosperous, and that this is shared across all parts of the country as part of the Levelling Up agenda. We have therefore continued to support investment, skills, and collaboration across the cyber security ecosystem.

This includes supporting innovators to grow and scale through the NCSC (National Cyber Security Centre) for Startups, LORCA (London Office for Rapid Cybersecurity Advancement), and Cyber Runway programmes. We are working to narrow the skills shortfall in cyber security, through the Cyber Explorers youth programme, the CyberFirst bursary scheme, new apprenticeship standards, skills bootcamps, and professionalising the cyber security workforce, with work being led by the new UK Cyber Security Council.

Ensuring collaboration across the regions is also critical to the success of the UK's cyber security ecosystem, and the UK Cyber Cluster Collaboration (UKC3) is building new partnerships between industry, schools and colleges right across the country.

The growth of the cyber security sector continues to be one of the UK's tech success stories. I would like to thank everyone working in cyber security for their contribution over the past year, and we will continue to do all we can to help make the UK the safest place to live and work online.

A handwritten signature in black ink that reads "Julia Lopez MP".

Julia Lopez MP

Minister of State for Media, Data, and Digital Infrastructure

Executive Summary

Introduction

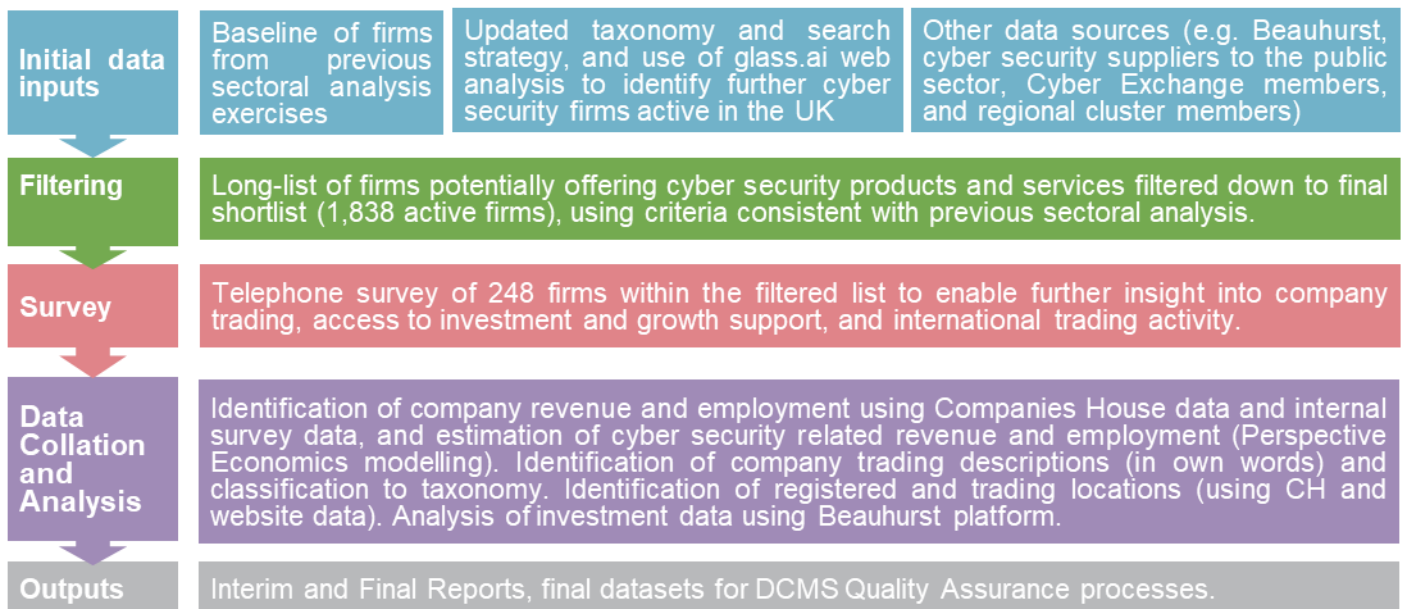
Ipsos, Perspective Economics, glass.ai and the Centre for Secure Information Technologies (CSIT) at Queen’s University Belfast were jointly commissioned by the Department for Digital, Culture, Media and Sport (DCMS) in February 2021 to undertake an updated analysis of the UK’s cyber security sector.

This analysis builds upon the previous [UK Cyber Security Sectoral Analysis](#) (published in February 2021) that provides a recent estimate of the size and scale of the UK’s cyber security industry. This provided an assessment of:

- The number of businesses in the UK supplying cyber security products or services
- The sector’s contribution to the UK economy (measured through revenue and Gross Value Added, or GVA)
- The number employed in the cyber security sector
- The products and services offered by these firms

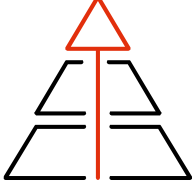
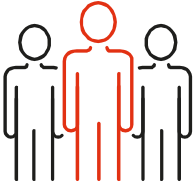
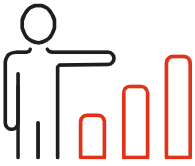
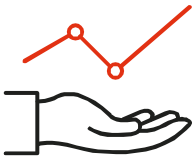

Project Scope and Summary of Methodology

The diagram below sets out a summary of the research methodology used. This is consistent with previous studies to support a time-series analysis of the sector’s performance to date.



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

Key Findings

	<p>Number of Companies</p> <ul style="list-style-type: none"> We estimate that there are 1,838 firms active within the UK providing cyber security products and services
	<p>Sectoral Employment</p> <ul style="list-style-type: none"> We estimate there are approximately 52,700 Full Time Equivalents (FTEs) working in a cyber security related role across the cyber security firms identified This reflects an estimated increase of 6,000 cyber security employee jobs within the last 12 months (an increase of 13%)
	<p>Sectoral Revenue</p> <ul style="list-style-type: none"> We estimate that total annual revenue within the sector has reached £10.1 billion within the most recent financial year This reflects an increase of 14% since last year's study (and is twice the growth rate experienced in the previous year's study, suggesting that 2021 was a positive year for the industry)
	<p>Gross Value Added</p> <ul style="list-style-type: none"> We estimate that total GVA for the sector has reached c. £5.3 billion This means total GVA has increased by a third in the past year (the largest increase to date seen within the sectoral analysis project series) We estimate that GVA per employee has increased from £85,700 to £101,000 within the last year (an increase of 17%), suggesting improved productivity reflected through company profitability and staff remuneration. This is now higher than the current estimated GVA per employee for the DCMS Digital Sector (DCMS Economic Estimates) of £95,000 per employee
	<p>Investment</p> <ul style="list-style-type: none"> 2021 was a record year for cyber security investment raised in the UK. We have identified over £1 billion raised by dedicated cyber security firms in the last 12 months, across 84 deals

1 Introduction

This analysis builds upon the previous [UK Cyber Security Sectoral Analysis](#) (published in February 2021) that provides a recent estimate of the size and scale of the UK's cyber security industry.

This provided an assessment of the number of businesses in the UK supplying cyber security products or services; the sector's contribution to the UK economy (measured through revenue and Gross Value Added, or GVA); the number employed in the cyber security sector; and an overview of the products and services offered by these firms.

The Cyber Security Sectoral Analysis project has helped to track the growth and performance of the UK's cyber security sector since 2018. In December 2021, the Government published the [National Cyber Strategy 2022](#), which commits to **strengthening the structures, partnerships, and networks necessary to support a whole-of-society approach to cyber**, and **fostering the growth of a sustainable, innovative, and internationally competitive cyber and information security sector, delivering quality products and services**. This analysis therefore provides an evidence base to track the health of the cyber security industry on an annual basis.

1.1 Methodology and Sources

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, to provide a time series analysis of how the sector has progressed since the baseline (2017) and subsequent annual studies.

The cyber security sector remains fast-moving, and continually subject to changes in products, services, and market approaches. For this year's study, we have therefore further refined the methodology to ensure improved identification of businesses offering cyber security products and services in the UK. This includes:

- An updated and refined taxonomy to better identify and classify cyber security activity
- A new partnership with leading data intelligence firm [glass.ai](#) (using Artificial Intelligence, or AI, techniques¹ to identify businesses using web data)
- Updated telephone and online survey of cyber security businesses

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.

The process by which we identify and measure the economic contribution of cyber security activity reflects a best estimate by the Ipsos, Perspective Economics, glass.ai and Centre for Secure Information Technologies team, using agreed parameters for the inclusion of respective firms considered to be active in the field.

The key stages below are consistent with previous Cyber Security Sectoral Analysis exercises to enable a time series comparison.

¹ All firms identified using glass.ai were also subject to human review by the Perspective Economics analyst team for final inclusion in the cyber security sectoral dataset.

Stage 1: Desk Research

The research team conducted initial desk research to explore how the cyber security market had changed within the last 12 months. This included:

- Engagement with UK cyber security regional networks and clusters, to gather local intelligence
- A review of published reports regarding the output or activities of the sector (e.g. UK Cyber Security Exports Strategy and associated annual export statistics)
- Recent investments or initiatives in the cyber security sector (including review of investments and acquisitions, and identification of new industry initiatives and cohorts, e.g. Cyber Runway)
- Any emerging trends in the market (including supply side and demand side), e.g. enhanced demand attributable to cloud security or working from home, or new product innovations requiring specific cyber security requirements

Stage 2: Initial Data Collection & Gap Analysis

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

- A review of firms previously identified in the sectoral analysis (identifying 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 and updated taxonomy, informed through workshops with industry and academic stakeholders in the cyber security community
- An updated taxonomy has been used to inform a long list of firms (identified through use of glass.ai web data and by Perspective Economics). This list was subject to automated and manual review, and refined to a final cyber security business list for analysis (n = 1,838)

The business metrics include (but are not limited to):

- Company name, registered number, company status, and date of incorporation
- Registered and trading locations (using official and web data)
- Company website and contact details
- Core description of company activities related to cyber security
- Company size² (large / medium / small / micro)

Stage 3: Cyber Security Sectoral Survey

Ipsos conducted a representative survey of 248 cyber security firms from May to July 2021. The survey used the list of firms established in Stage 2 of this study as a sample frame. The purpose of the survey was to understand firm-level performance, barriers, and collaboration in further detail.

² Full size definitions: **Large:** Employees ≥ 250 and Turnover $> \text{€}50$ million or Balance sheet total $> \text{€}43$ million // **Medium:** Employees > 50 and < 250 And Turnover $\leq \text{€}50$ million or Balance sheet total $\leq \text{€}43$ million // **Small:** Employees > 10 and < 50 And Turnover $\leq \text{€}10$ million or Balance sheet total $\leq \text{€}43$ million // **Micro** Employees < 10 And Turnover $\leq \text{€}2$ million or Balance sheet total $\leq \text{€}2$ million

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 2)
- Extent of export activity, or international collaboration
- Perceived barriers to growth
- Understanding areas of collaboration and reasons for working with cyber security partners

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

Stage 4: Qualitative Consultations

This research has also been supported through 25 one-to-one consultations with cyber security firms, buyers of cyber security products and services, and investors in the cyber security sector. Participants were purposively sampled to reflect variation in size, location, product or service focus, and maturity, with participating cyber security firms being recruited from the Ipsos survey recontact sample. Larger cyber buyers were purposively sampled to capture feedback on how demand was evolving to address new challenges.

Stage 5: Data Blending

In August 2021, the results of the cyber security sector survey were used to inform gaps within the list of identified cyber security sector firms e.g. the extent to which a firm provided cyber security products or services and attributed revenues accordingly. This stage involved data cleaning and joining to provide a final dataset of cyber security firms, including the development of firm-level metrics used for analysis within the report.

Stage 6: 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 data sources used to underpin the sectoral analysis included:

- **glass.ai:** this year's study has partnered with web-scale intelligence providers [glass.ai](https://www.glass.ai) to use web data to help identify and map new providers of cyber security products and services, and match these to the cyber security taxonomy
- **Bureau van Dijk FAME** (and Companies House Data Product): This platform collates Companies House data and financial statements from all registered businesses within the UK
- **Beauhurst:** Beauhurst is a leading investment analysis platform, which 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 (glass.ai and Perspective Economics) has used web scraping³ to extract and parse key company descriptions, locations, and contact details from identified company websites
- **Representative survey of cyber security firms:** in Summer 2021, Ipsos conducted a representative survey of cyber security firms. The feedback from 248 providers has been useful to understand the financial performance, growth drivers, and challenges for firms within the market
- **One-to-one qualitative consultations:** further, the team has also conducted 25 one-to-one consultations with investors and market providers, to gather feedback on the growth and performance of the cyber security sector in the UK

1.2 Consistency with the 2021 Cyber Security Sectoral Analysis

Our approach remains consistent with previous reports (and builds upon the methodology to identify and measure the contribution of the sector). As per previous studies, 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, or individual contractors (non-registered) – all excluded for analysis purposes

It also draws upon consistent sources, i.e. company accounts, longitudinal survey data, and Beuhurst for investment data. The financial analysis of firms is also consistent, as it uses company information from the most recent financial year of accounts (analysis undertaken in late 2021, with financial year 2020/21 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).

The identification of firms related to the industry has been improved through the partnership with glass.ai, and subject to manual review to identify a full list of firms included in the UK cyber security sectoral database.

The inclusion of glass.ai (and enhanced engagement with third parties) has helped to identify more businesses at an early/micro stage, and those diversified firms with a cyber security presence. This has helped to boost the number of active firms from 1,483 to 1,838.

³ Note: web scraping has observed robots.txt – i.e. where access is permitted.

However, this also demonstrates that previous studies have captured the most prevalent providers of cyber security products and services - as the firms identified last year cover 94% of the revenue, 93% of the GVA, and 94% of the employment identified within this year's study.

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 is based on a sample of cyber sector firms rather than the entire population. Therefore, they are subject to sampling tolerances. The overall margin of error for the sample of 248 firms (within a population of 1,838 firms) is between c.3 and c.6 percentage points. The lower end of this range (3 percentage points) is used for survey estimates closer to 10% or 90%. The higher end (6 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 44% to 56%.⁴

By contrast, the data from the 25 qualitative consultations is intended to be illustrative of the key themes affecting the cyber security sector, as a whole, rather than a statistically representative view of cyber sector businesses or investors.

1.4 Acknowledgements

The authors would like to thank the DCMS team 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 industry survey, the regional cyber security clusters, consultations, and shared data, knowledge, and feedback to help underpin this study.

Note: The cyber security sector continues to increase in size, scope, and specialisms. We are happy to receive comments and feedback regarding the methodology or findings herein, through contacting cybersecurity@dcms.gov.uk

⁴ 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 2022](#), 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 previous studies, this analysis is focused upon organisations that include all of the following attributes:

- 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 an active website / social media presence)
- Provide cyber security products or services to the market (i.e. sell or enable the selling of cyber solutions to other customers) – aligned to the taxonomy set out below
- Have identifiable revenue or employment within the UK related to cyber security
- 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 services 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

We estimate that there are currently 1,838 firms active within the UK providing cyber security products and services. This reflects a glass.ai and Perspective Economics estimate as of Autumn 2021.

Whilst this reflects an increase in the number of firms offering cyber security products and services (1,483 identified in the previous study), the research team emphasise that this is one metric among many to gauge the health of the sector. For example, this increase includes:

- Newly registered companies offering cyber security products and services (often very early / small start-ups)
- Previously registered companies that did not previously offer such services, but have established a product or team to do so recently (e.g. consultancies offering IT risk services)
- Businesses now identified as providing a relevant cyber security product or service (e.g. identified through provision of an accredited scheme such as Cyber Essentials) where previous web-data matching did not flag such products or services.
- Businesses with limited web data reporting the provision of cyber security products or services, but which have been flagged through engagement with other sources (e.g. consultation with regional clusters).

Throughout this study, the report authors stress the need to draw upon a wide range of existing sources, alongside the development and deployment of a cyber security taxonomy against Companies House data, analysis of relevant website domains, and in-depth regional engagement.

Within the process, a 'long list' of several thousand businesses in the UK was identified as potentially relevant to the cyber security sector using keywords and web data. However, this long list was subsequently filtered to ensure each business demonstrated sufficient alignment to the research parameters and the market taxonomy.

For example, web data can identify firms that may have an active registration with Companies House, have a website or social media presence, and meets the parameters of the taxonomy. However, further review of the presence may indicate a lagging status (e.g. the business may have no true employees or may not appear to be active for several years). The team therefore reviewed more than 3,000 firms in detail, removing organisations that may have mentioned security (e.g. offering a secure data centre service) but did not appear to tangibly offer cyber security products or services to the end-market.

This yielded the 1,838 firms in scope, and the research team considers this to be an appropriate figure to gauge the health and composition of the sector whilst ensuring consistency with previous analysis.

We do however note, that as with all emerging sectors, subtle differences in definition can result in varying interpretations of the size and composition of activity. In this respect, there may be other relevant

cyber security use cases, which could in future meet the short list requirements (i.e. the 6 conditions set at the beginning of Section 2.1) and could therefore be included in future analysis. This might include, for example, firms involved in areas such as FinTech, RegTech or SafetyTech. However, we provide these parameters to avoid duplication, and provide DCMS with a health check regarding the overall cyber security market.

There are also businesses operating within the UK that may, for example, resell cyber security solutions (anti-virus, anti-malware, spam filtering etc) through a broader package of managed IT support. As this cyber security spend should be reflected in the revenues of those providing rather than reselling these solutions, we place less focus on the role of resellers within the sectoral analysis (although do include a small number of larger resellers that offer cyber security advisory services and implementation support).

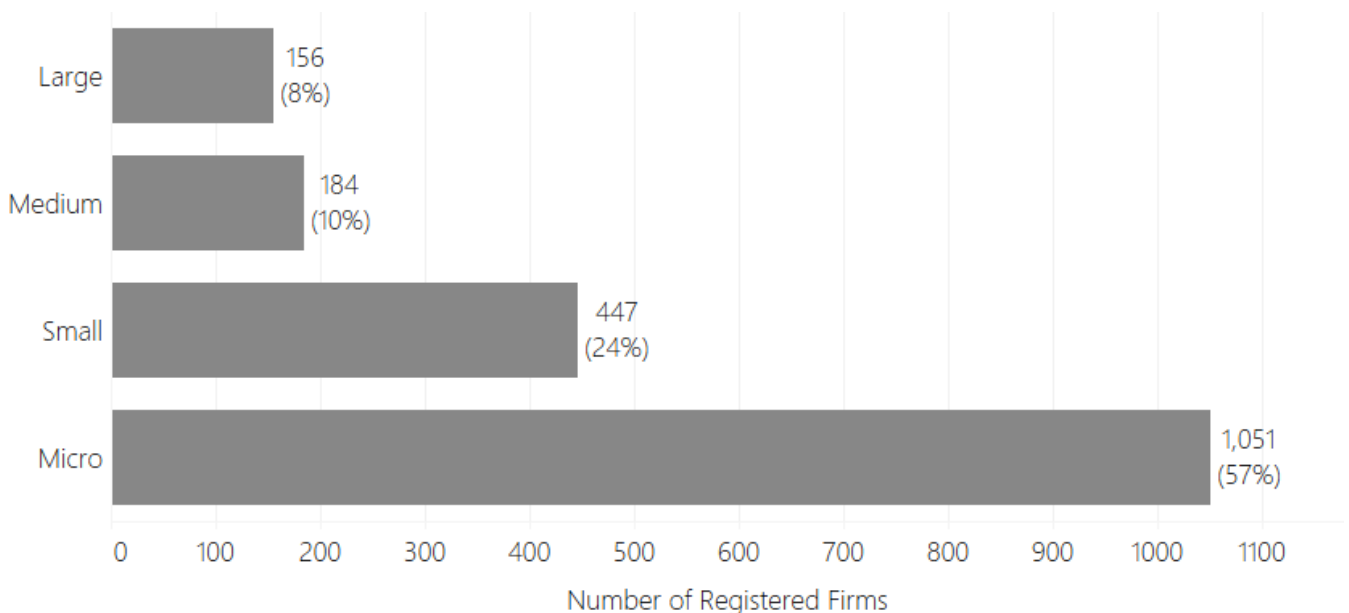
Overall, this process means that the 1,838 firms for analysis within this report have been assessed and verified as providers of cyber security products and solutions. We provide a high-level breakdown of this provision in subsequent chapters. Given the breadth of 'cyber security' as a term, we endeavour to be clear regarding what is in scope, what is being measured, and why this matters, for the sector and for the wider economy and society.

The following sub-sections set out an overview of the number of companies by size; the breakdown between companies that appear dedicated or diversified; and the products and or services provided by each company.

Number of Registered Firms by Size

For the 1,838 cyber security firms identified, Figure 2.1 and Table 2.1 demonstrate the breakdown by size.⁵

Figure 2.1: Number of Registered Cyber Security Firms by Size



Source: Perspective Economics, glass.ai (n = 1,838)

⁵ Full size definitions: **Large:** Employees ≥ 250 and Turnover $> \text{€}50$ million or Balance sheet total $> \text{€}43$ million // **Medium:** Employees > 50 and < 250 And Turnover $\leq \text{€}50$ million or Balance sheet total $\leq \text{€}43$ million // **Small:** Employees > 10 and < 50 And Turnover $\leq \text{€}10$ million or Balance sheet total $\leq \text{€}43$ million // **Micro** Employees < 10 And Turnover $\leq \text{€}2$ million or Balance sheet total $\leq \text{€}2$ million

Within the UK, the vast majority of all businesses are Small and Medium Enterprises (SMEs), and it is therefore to be expected that the majority of registered businesses within the cyber security sector are small (24%) or micro (57%) in size.

As this study focuses upon businesses with at least one member of staff, the following comparison is noted between the UK's cyber security sector, and the broader UK business population. This highlights that, despite the cyber security sector containing a considerable proportion of micro and small businesses, there are many providers of scale operating within the UK market (i.e. 18% of businesses offering cyber security products and services to market are medium or large, compared to 4% of all businesses in the UK).

Table 2.1 Comparison of the Size of Cyber Security Firms and Wider Business Population

Size	UK Business Population Estimates (2021)	Percentage	Cyber Security Sectoral Analysis	Percentage ⁶
Large (250+ employees)	7,655	1%	156	8%
Medium (50-249)	35,620	3%	184	10%
Small (10-49)	210,550	15%	447	24%
Micro (1-9)	1,162,155	82%	1,051	57%
All Businesses with at least 1 employee	1,415,980	100%	1,838	100%

Change in Size

Following last year's sectoral analysis, we have tracked the performance of each firm (n = 1,483 in the previous study) to understand how the size of cyber security firms has changed (where applicable) in the last 12 months.

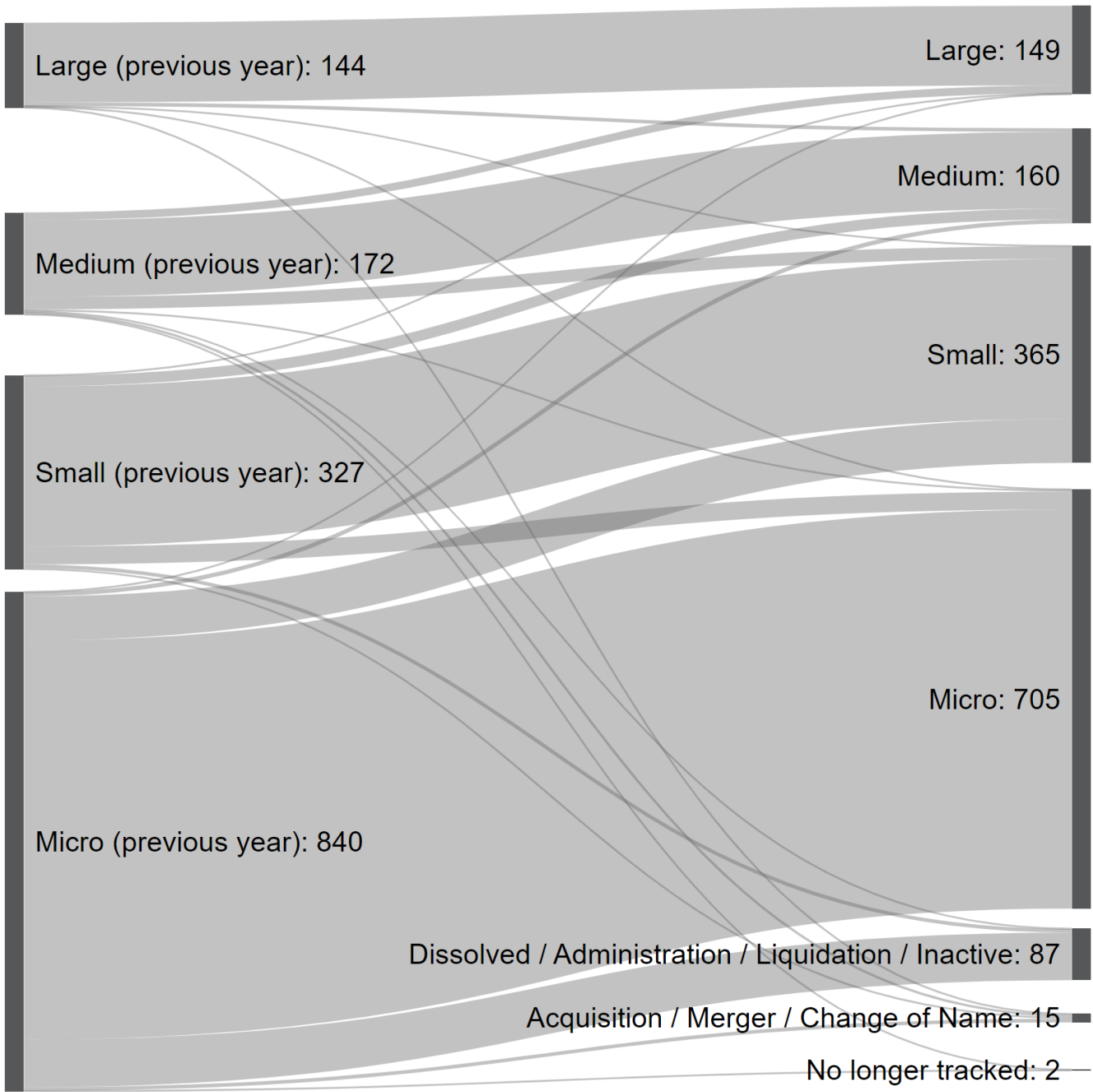
The left side of the Sankey diagram (Figure 2.2) shows the size of cyber security firms as identified in the 2021 study, with the right side showing their updated size currently. As this is a brief time period, the size composition of firms remains fairly static.

However, this does highlight that 5.9% of firms⁷ appear to have closed or are no longer fully trading within the last 12 months. This is a higher closure rate than identified within the previous study (4.6%), potentially reflecting a challenging couple of years for many micro firms, or the potential for market acquisitions and mergers.

⁶ Figures may not sum due to rounding

⁷ Number of firms dissolved, in administration, or liquidation (87 / 1,483) = 5.9%

Figure 2.2: Sankey Flow Chart – Size (2020 – 2021)



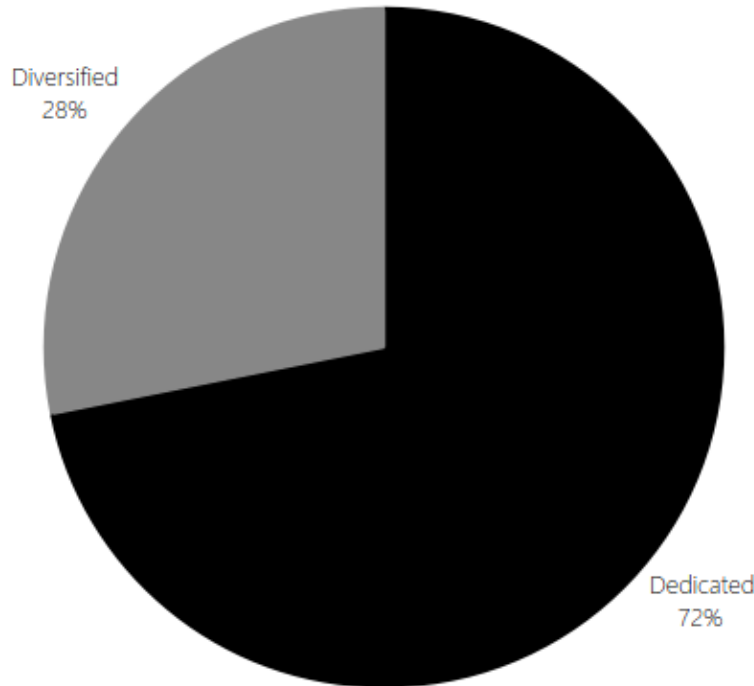
Source: Perspective Economics (n = 1,483)

Dedicated and Diversified Providers of Cyber Security Products and Services

Within this research, we attempt to categorise firms by whether they are either:

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

Figure 2.3: Dedicated and Diversified Providers



Source: *Perspective Economics* (n = 1,838)

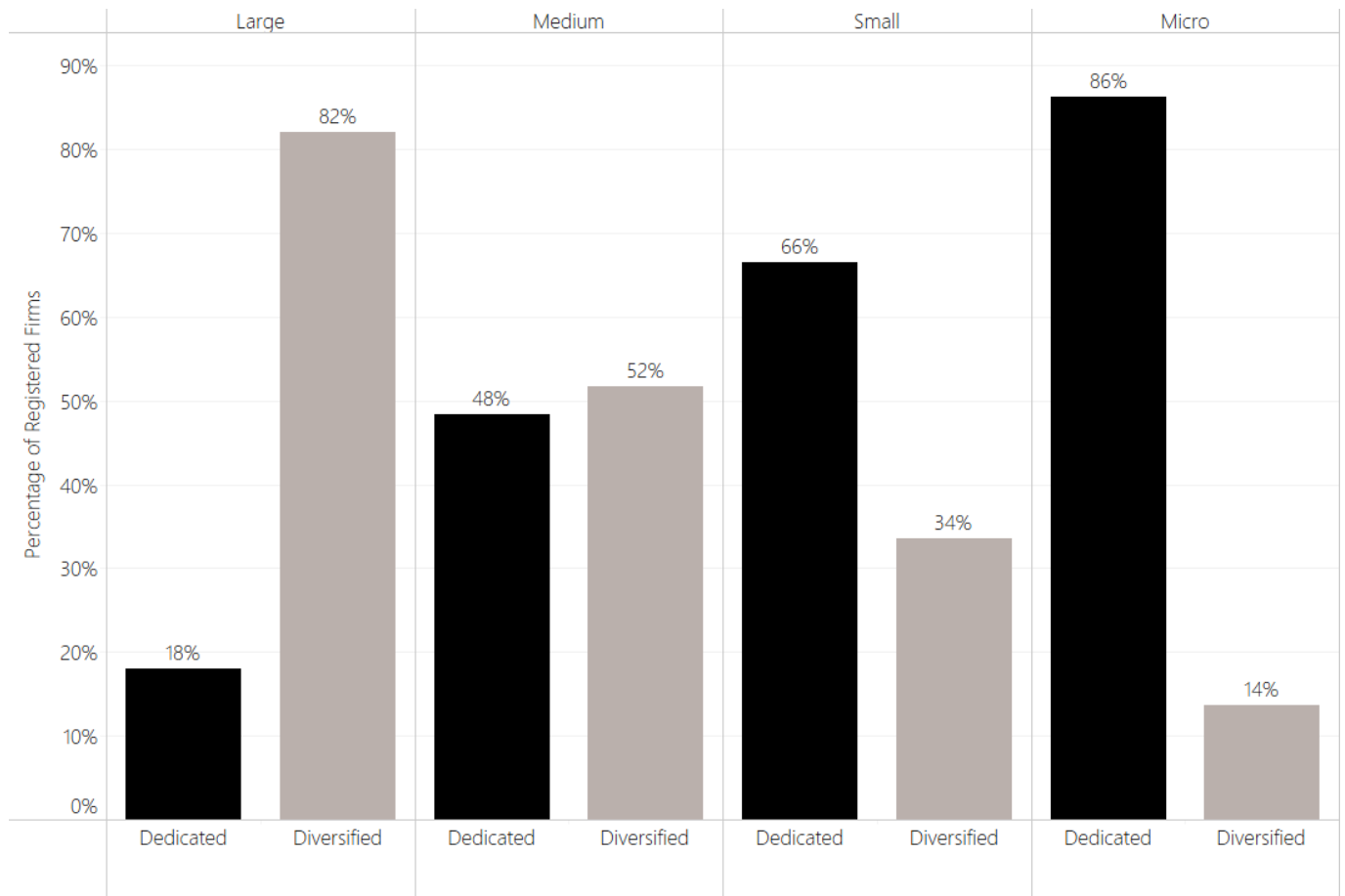
The rationale underpinning the need to provide this distinction is attributable to seeking to **understand how firms either set up to solely provide cyber security, or firms that provide cyber security as one product or service among others** vary with respect to size, scale, growth, and market activity.

Within the current dataset, almost three-quarters (72%) of firms are dedicated providers of cyber security products and services. This reflects no change from the previous study.

Disaggregating these firms by size (as below in Figure 2.4) also highlights that micro and small firms within this analysis are much more likely to be dedicated (86% and 66% respectively), whereas there are few large dedicated cyber security firms (18%).

In other words, this reflects the tendency for 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 2.4: Dedicated / Diversified Cyber Security Firms by Size



Source: Perspective Economics (n = 1,838)

2.3 Products and Services Provided by the UK Cyber Security Sector

In order to understand the products and services provided by the UK cyber security sector, DCMS and the research team use a taxonomy (as summarised below) to categorise each of the products and services offered. This provides a high-level overview of the UK's cyber security product and service offer.

This taxonomy remains broadly consistent with previous years; however, the underlying keywords and terms have been revisited and updated. Further, the use of web data and manual review means that firms can be classified into taxonomy areas through both the text available, and the analyst decision regarding key products and services. This means that the following data reflects an interpretation of the key products and services offered. It is therefore indicative of the main solutions provided by the UK cyber security sector.

In previous studies, the cyber security business survey had asked respondents which products and services they provide (against the taxonomy areas); however, this found that many respondents report to offer all or most of these products and services, which made delineation between specialisms difficult to measure. Therefore, we take a top-down review of products and services using the text data available through web data review.

Taxonomy Definitions:

Taxonomy Category	Agreed Definition (Short)
Cyber professional services	<p>Providing trusted contractors or consultants to advise on, or implement, cyber security products, solutions, or services for others</p> <p>Within this year's study, we also have identified a marker for:</p> <ul style="list-style-type: none"> - Risk and Compliance Support (e.g. support with GDPR, ISO27001, Cyber Essentials) - Cyber Security Design & Advisory Services (e.g. support with cyber security architecture) - Managed Security Service Providers (MSSPs)
Endpoint and mobile security	Hardware or software that protects devices when accessing networks
Identification, authentication, and access controls	Products or services that control user access, for example with passwords, biometrics, or multi-factor authentication
Incident response and management	Helping other organisations react, respond, or recover from cyber attacks
Information risk assessment and management	Products or services that support other organisations to manage cyber risks, for example around security compliance or data leakage
Internet of Things	Products or services to embed or retrofit security for Internet of Things devices or networks
Network security	Hardware or software designed to protect the usability and integrity of a network
SCADA and Information Control Systems	Cyber security specifically for industrial control systems, critical national infrastructure, and operational technologies

Taxonomy Category	Agreed Definition (Short)
Threat intelligence, monitoring, detection, and analysis	Monitoring or detection of varying forms of threats to networks and systems
Awareness, training, and education ⁸	Products or services in relation to cyber awareness, training, or education

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

Further, we also classify each company by whether they provide (as their main cyber security offering) products, services, managed security services, or act as a cyber security specific reseller.

- 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
- Resellers: i.e. the business packages and resells cyber security solutions (usually through licencing agreements)

This approach helps policymakers, industry, and investors understand how many companies there are focusing on a particular subsector of the market or offering new products or solutions accordingly.

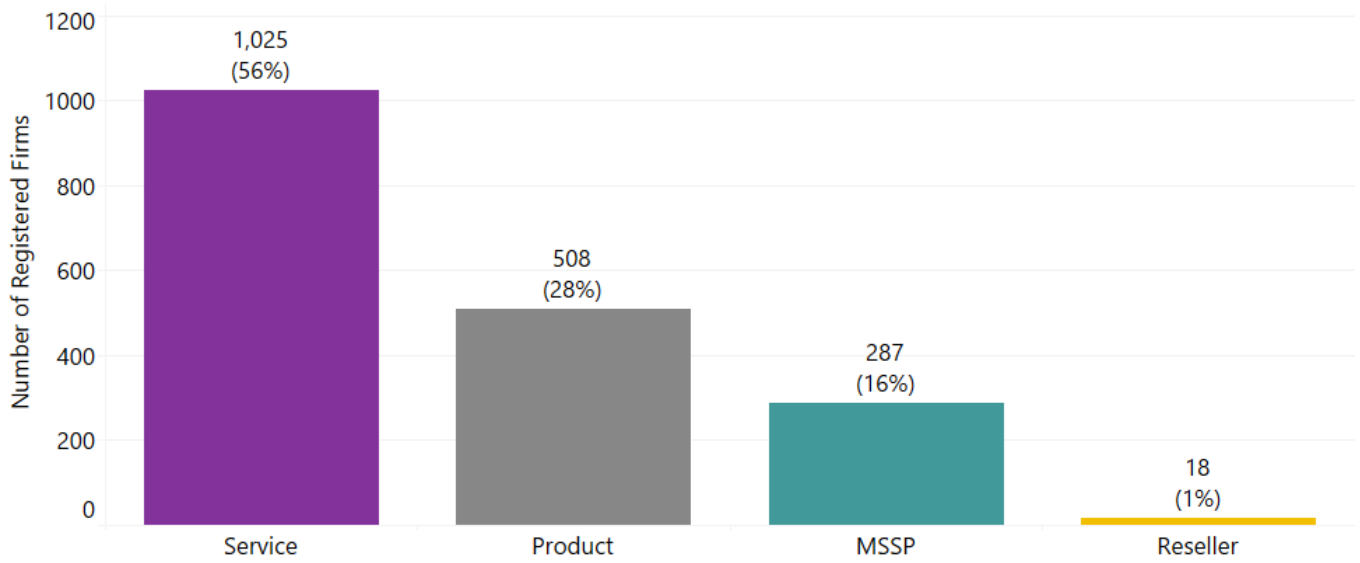
Product and Service Provision

Figure 2.5 sets out an analysis of how many companies appear to be focused upon product or service provision. It is worth noting that in reality, there will be some overlap where firms provide both products and services; however, this approach selects one category per firm.

Overall, analysis of company trading descriptions suggests that over 7 in 10 (72%) of firms are mainly involved in service provision (including managed services and reselling⁹), and just under 3 in 10 (28%) are mainly involved in cyber security product development.

⁸ The keywords underpinning Awareness, Training and Education have been broadened to include firms offering awareness or training courses without formal accreditation (e.g. online modules in cyber security awareness).

⁹ 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. We do not include, for example, high street or online retailers.

Figure 2.5: Number of Registered Cyber Security Firms by Product/Service Focus

Source: Perspective Economics (n = 1,838)

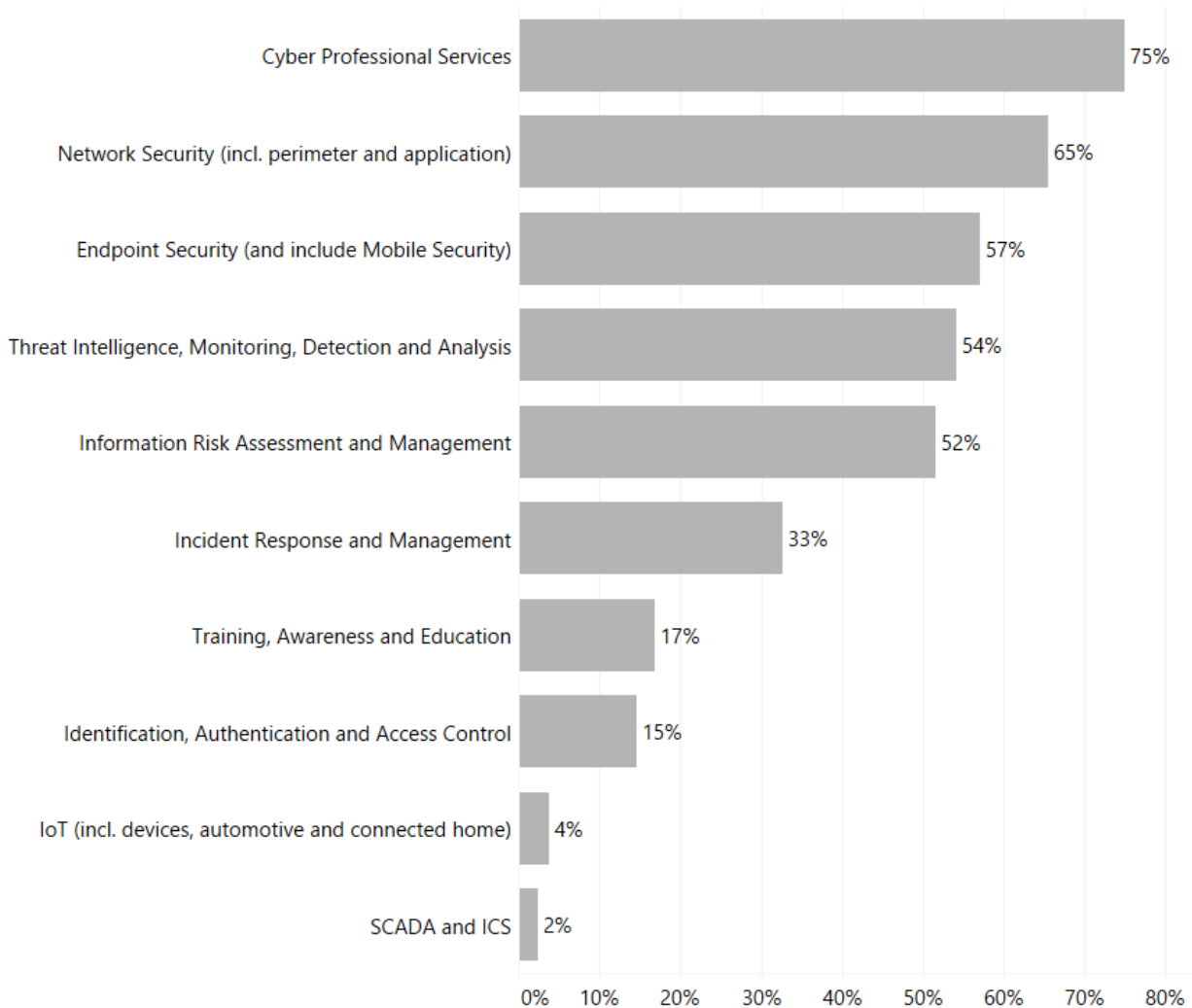
Taxonomy Breakdown

Within this study, we have matched company descriptions (in their own words through website analysis) 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. Please note that the increase in company text data, and slight change to the taxonomy structure may impact the figures below from previous years.

On this basis, Figure 2.6 is based upon our analysis of trading descriptions. It demonstrates that ‘Cyber Professional Services’ remains the most commonly provided taxonomy category (75% of businesses, up from 72% last year), 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.

Within the Cyber Professional Services category, we have also identified 561 firms (31%) offering support with GDPR compliance, ISO 27001 or Cyber Essentials accreditation, 215 firms (12%) providing cyber security design or advisory services (with respect to infrastructure etc) and 316 MSSPs (17%).

Figure 2.6: Number of Registered Cyber Security Firms by Taxonomy Offering



Source: Perspective Economics, glass.ai (n = 1,838)

3 Location of Cyber Security Firms (UK)

3.1 Introduction

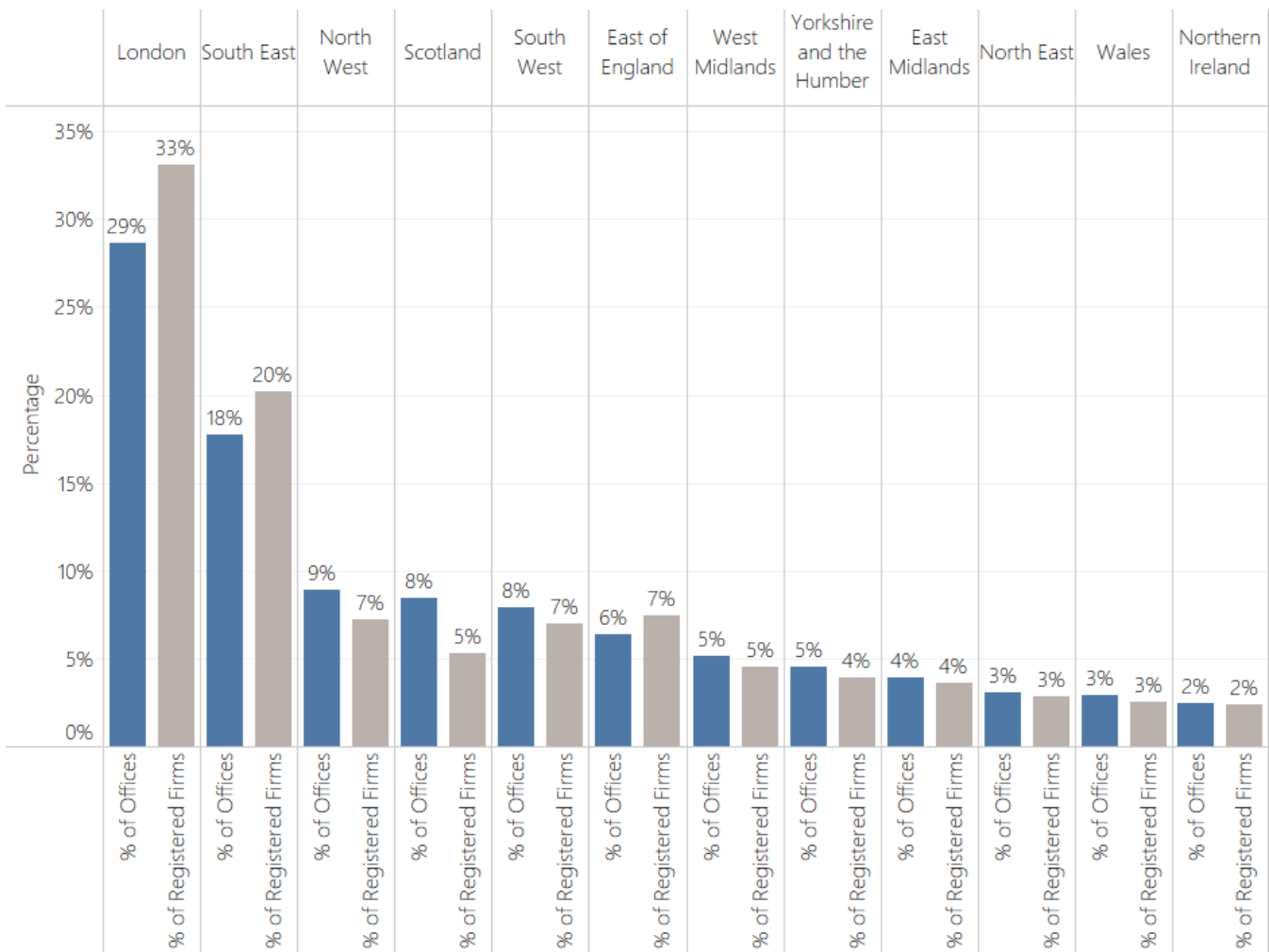
This chapter explores the registered location (i.e. where each business has located its registered address with Companies House), and the active office locations (i.e. where each business has a trading presence or office across the UK) of cyber security firms.

Understanding the registered and trading addresses of cyber security firms in the UK enables regional analysis and supports the evidence-based identification of notable clusters or hotspots of activity. **We have identified 3,818 office locations for the 1,838 firms identified within this study.** In other words, on average, each firm has over two office locations across the UK (of which, one will be a ‘registered’ location with Companies House).

3.2 Location of UK Cyber Security Firms

Figure 3.1 sets out the breakdown of firms by number of UK office locations identified in each of the twelve regions. This highlights the importance of identifying local units of activity in the UK (marked in blue below) when seeking to understand regional activity, as registered locations can be skewed towards London and the South East.

Figure 3.1: Percentage of Cyber Security Firms by Location



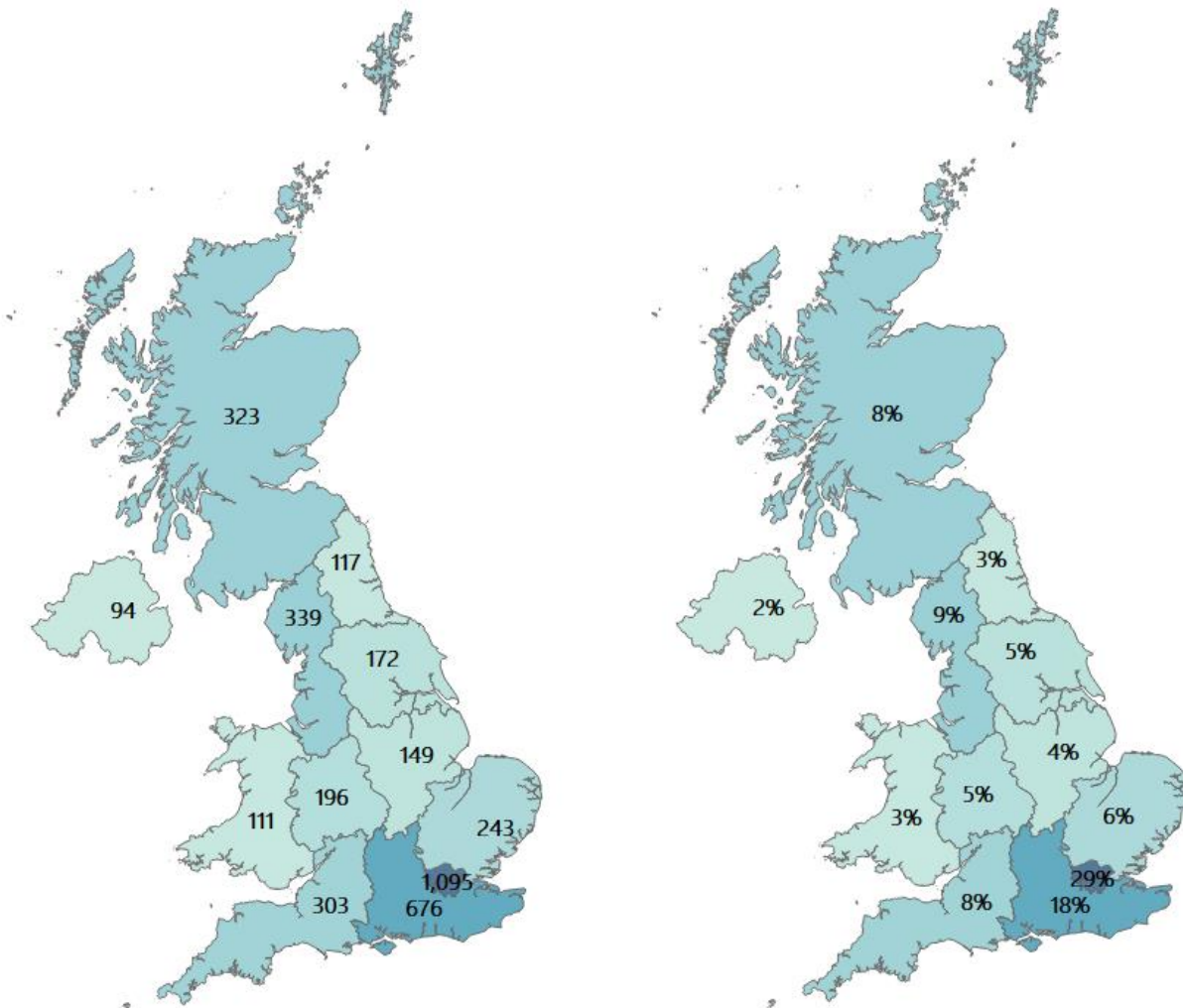
Source: Perspective Economics (n = 3,818 (all offices); n = 1,838 (registered offices))

Active (Local Offices)

Figure 3.2 sets out the number of active offices identified within this study by UK region. Overall, the data suggests a continuation of last year’s trend in that a slight majority of firms (53%) are based outside of London and the South East regions (compared to 54% last year). Further exploration of regional office data suggests no significant changes at the regional level; albeit with some growth noted in areas such as the North East (from 2% to 3% of offices) and the East Midlands (from 4% to 5%).

This may suggest that, as discussed in last year’s analysis, a recent shift to working-from-home practices, as a result of the COVID-19 pandemic may help to increase regional opportunities across the UK. Further, the DCMS [Cyber Skills in the UK Labour Market research](#) (2021) also highlights the significant increase in remote job postings advertised in cyber security roles across the UK. In other words, the presence of local offices (or remote presence) could yet further expand as employers’ increasing neutrality towards staff location may allow for firms to enter new geographical regions (e.g. a cyber security practice based in London recruiting staff working from home in Cardiff).

Figure 3.2: Active Cyber Security Offices by Region

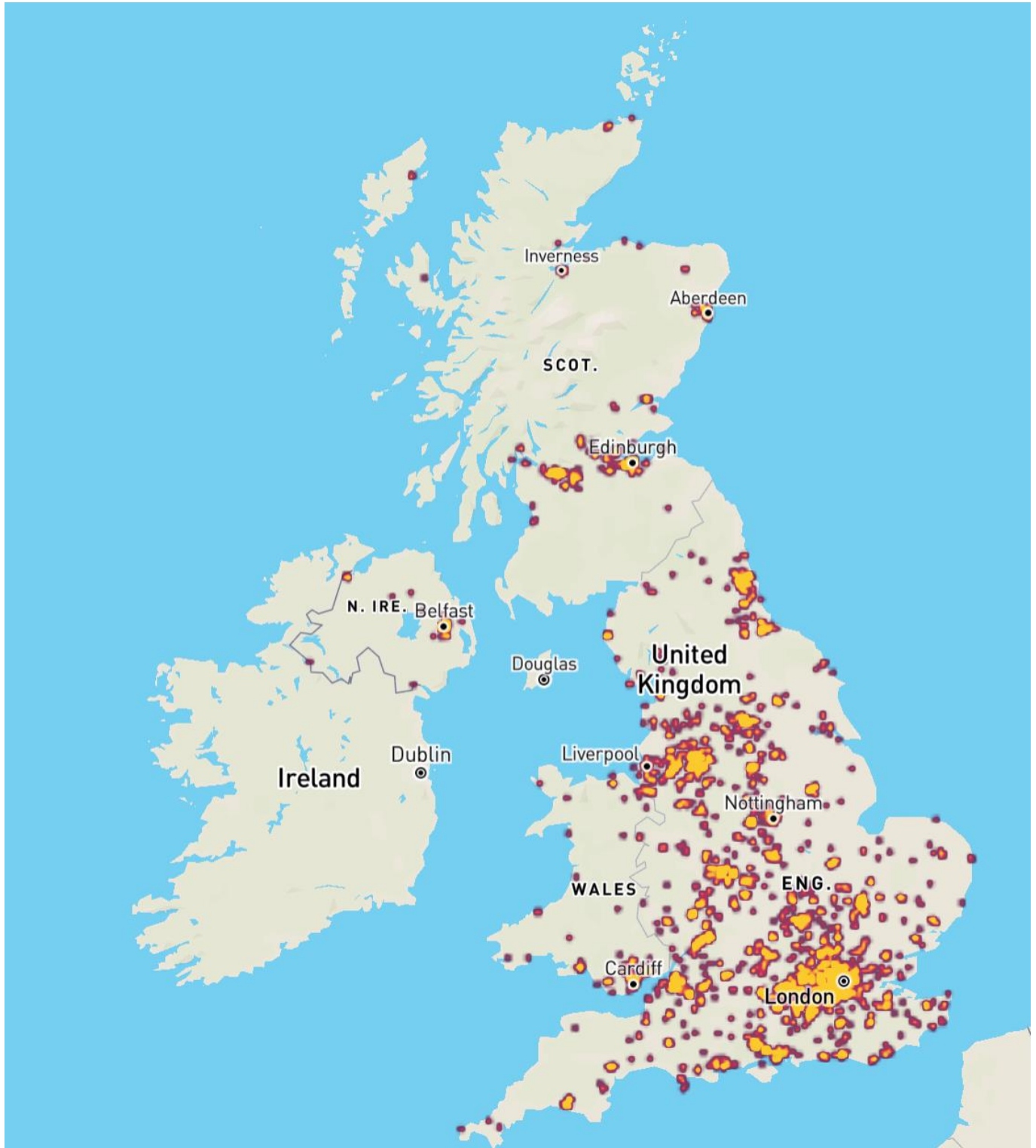


Source: Perspective Economics (n = 3,818)

3.3 UK Cyber Security Heatmap

In addition to understanding the number of offices across the UK for cyber security businesses, the research has identified the location of each office, and identified commercial clusters emerging. Heatmaps for each UK region are set out within the report annex.

Figure 3.3: Cyber Security Firm Level Heatmap



Source: Perspective Economics (n = 3,818)

3.4 Role of Cyber Security Clusters

DCMS works closely with regional cyber security clusters, supporting their development and improving reach and insight into local and regional cyber security sector ecosystems and opportunities for growth. Each of these clusters, and a regional snapshot is included within the annex of this report.

In July 2021, DCMS announced £850,000 of funding to support the establishment and activities of a new organisation called [UK Cyber Cluster Collaboration \(UKC3\)](#), which aims to support economic growth and skills development in the UK cyber security industry. UKC3 has a number of recognised clusters including Bristol & Bath Cyber Cluster, Cyber North, Cyber Wales, CyNam (Cyber Cheltenham), East of England Cyber Security Cluster, ScotlandIS Cyber, South West Cyber Security Cluster, Yorkshire Cyber Security Cluster, Midlands Cyber, North West, Swindon and Wiltshire, and NI Cyber, and this list is actively expanding across the UK's regions.

Section 6.4 explores the level of business engagement with cyber security clusters and regional support bodies across the UK in further detail.

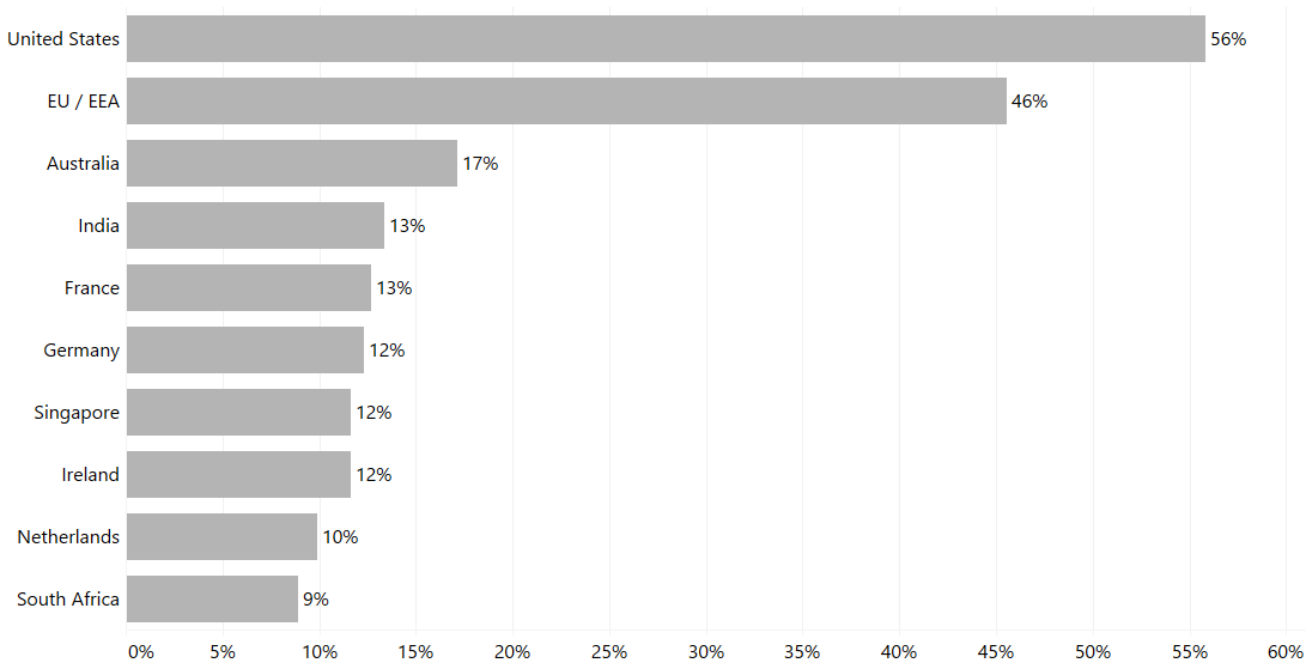
3.5 International Activity

This section outlines where UK registered cyber security firms have an established physical presence in another country. This helps to inform a further understanding of where firms are exporting, are engaged in international markets, or where multinational firms have a presence in the UK. For the 1,838 providers of cyber security products and services, we have identified:

- 292 UK-headquartered cyber security businesses with a physical presence in international markets (denoted by an office presence); and
- A further 281 cyber security businesses active in the UK appear to be headquartered or originate from outside the UK

For the 292 UK-headquartered cyber security businesses, the following chart sets out the main trading regions (totalling to more than 100%, since firms have offices across multiple locations):

Figure 3.4: Regions with an international presence (by UK-Headquartered Cyber Security Firms)



Source: *Perspective Economics (n = 292 UK-headquartered firms with an international office presence)*¹⁰

This suggests considerable growth in the number of UK firms operating with a presence in the United States (increased from 109 firms in last year’s study to 163). The European Union remains a key market, and 133 UK headquartered businesses have offices present across the European Union. In the last 12 months, there has also been increased activity by UK firms in India, Singapore, and South Africa.

In recent years, the UK has also been a clear international destination for foreign direct investment (FDI) in cyber security. We have identified where internationally headquartered firms (n = 281) have set up a presence in the UK (related to cyber security). In total, we have identified 183 firms from the United States that have set up an office in the UK (an increase from 167 last year). This accounts for 10% of all cyber security firms in the UK and highlights the importance of US-UK collaboration in this area. This is followed by 51 firms from across the European Union and European Economic Area (3% of cyber security firms operating in the UK), followed by 14 firms from Israel, 8 from Australia, and 6 from Canada.

¹⁰ Please note the EU/EEA figure (46%) includes all EU / EEA countries identified and is a total estimate.

4 Economic Contribution of the UK Cyber Security Sector

4.1 Estimated Revenue

In the most recent financial year, annual cyber security revenue within the sector is estimated at £10,146 million (rounded to £10.1 billion). This reflects an increase of 14%¹¹ from last year's study (£8.9 billion).

Please note that:

- The inclusion of glass.ai (and enhanced engagement with third parties) has helped to identify more businesses at an early/micro stage, and those diversified firms with a cyber security presence. This has helped to boost the number of active firms from 1,483 to 1,838
- However, this also demonstrates that previous studies have captured the most prevalent providers of cyber security products and services - as the firms identified last year cover **94% of the revenue, 93% of the Gross Value Added (GVA), and 94% of the employment**
- The **1,386 firms within last year's study that remain active today have grown their estimated cyber related revenues from £8.2 billion to £9.5 billion (increase of 16%)** - i.e. we perceive that sectoral revenue growth is being driven by these established providers
- **Therefore, we are confident in the estimated 14% increase in cyber security sector revenues (i.e. from £8.9 billion to £10.1 billion)**

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 2021
- 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. Please note that as the analysis was undertaken in late 2021. We use the most recent financial year reporting data where possible, which means that much of the revenue will have been achieved through work delivered and billed in 2020 (e.g. if a company has a financial year ending March 2021, those accounts will reflect billed work from April 2020 – March 2021).

¹¹£8,878 million to £10,146 million, CAGR of 14%.

In this respect, these figures can be considered relevant to the financial impact of COVID-19, and may reflect the receipt of government support, and potential for increased revenues (through clients moving to remote working etc.), and potentially reduced costs (e.g. through reduced travel, office costs, rates subsidies). This is also reflected in the increase in GVA estimate (Section 4.3).

Revenue by Firm Size

We estimate that three-quarters (£7.6 billion, 75%) of all UK cyber security revenue is earned by **large firms** (which further demonstrates the earning power of these firms given that they reflect 8% 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.

Medium firm revenues have softened (14% of the sector's revenues), with a slight decline from £1.56 billion (18%) to £1.38 billion (14%). However, this may also be attributable to some existing medium firms scaling from medium to large. This continues to suggest that a competitive mid-market is in place, particularly where firms in receipt of external investment have been able to scale and service the market accordingly.

Small and micro firms have experienced considerable relative growth in the previous year.

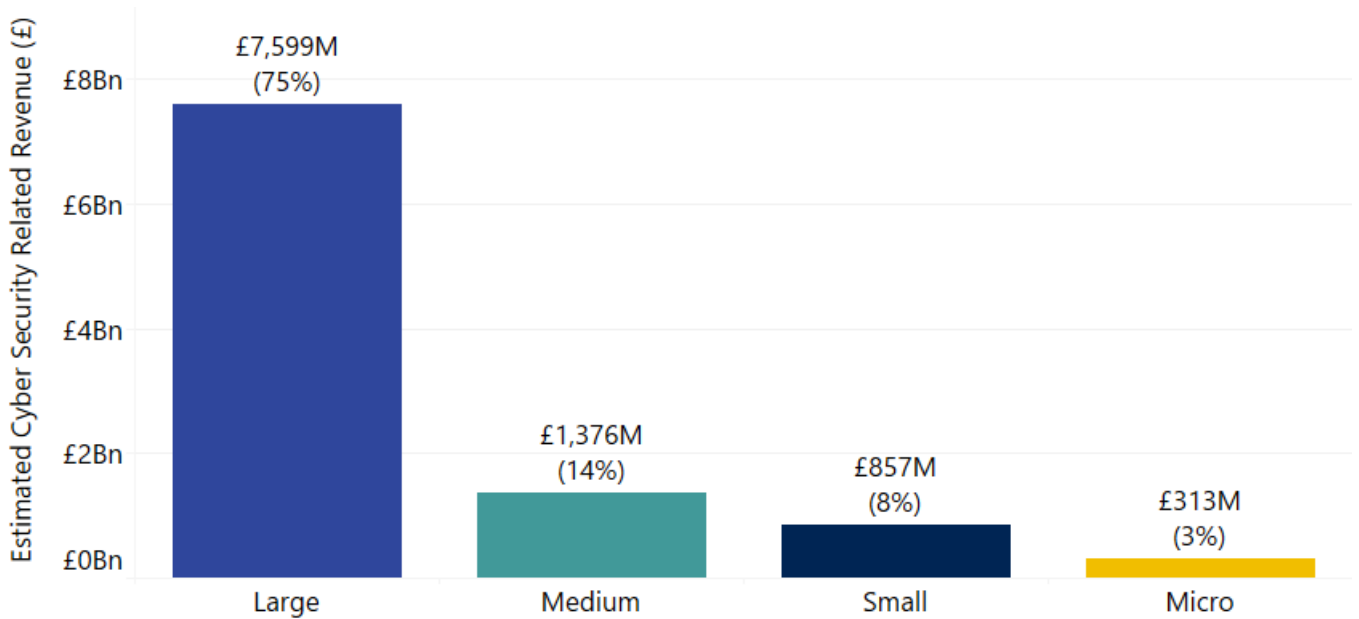
Small firms have increased their cyber security related revenues from £527 million (then 6% of revenues) to £857 million (now 8% of revenues). Further, average small firm cyber security related revenues have grown from approximately £1.6 million¹² to £1.9 million (i.e. on average, small cyber security firms have experienced an increase of 19% in revenue within the last financial year, and their annual growth has outstripped that of the wider market).

Micro firms have also increased their cyber security related revenues from £217 million (then 2% of revenues) to £313 million (now 3% of revenues). Average micro firm cyber security related revenues have grown from approximately £260,000¹³ to £300,000 (i.e. on average, micro cyber security firms have experienced an increase of 15% in revenue within the last financial year).

¹² 327 small firms identified in the previous year's study, with aggregate cyber security related revenues of £527 million (average of £1.6 million)

¹³ 840 micro firms identified in the previous year's study, with aggregate cyber security related revenues of £217 million (average of c. £260,000)

Figure 4.1: Total Cyber Security Revenue by Size of Firm

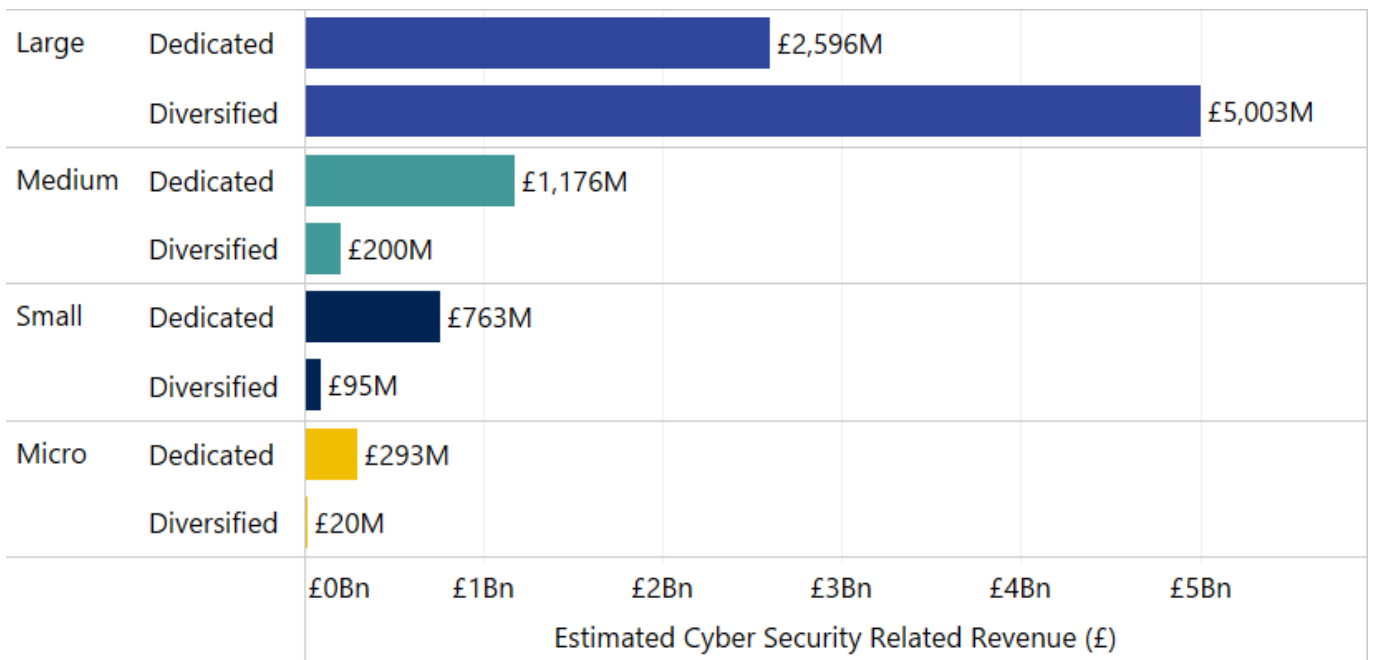


Source: Perspective Economics (n = 1,838)

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.

This highlights that ‘diversified’ firms continue to generate significant revenues through their cyber security offer. For Small and Medium Enterprises (SMEs), dedicated cyber security firms generate the greatest proportional revenue (e.g. 85% of revenues for medium firms, 89% for small, and 94% for micro firms).

Figure 4.2: Total Cyber Security Revenue by Size by Dedicated/Diversified Status



Source: Perspective Economics (n = 1,838)

This suggests that the UK market remains home to:

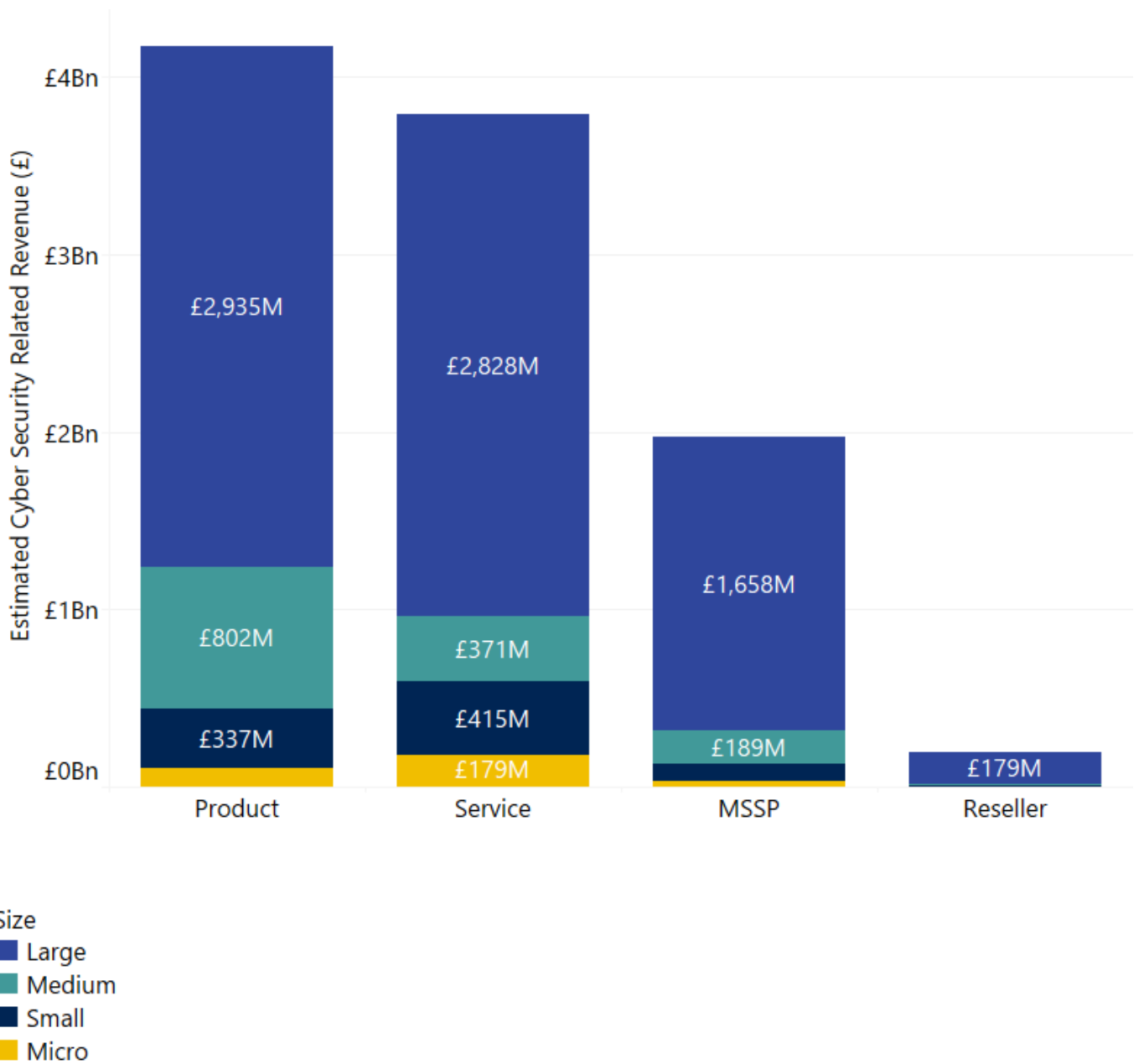
- Approximately 20 'anchor' large and diversified firms, which are estimated to generate over £50 million each in cyber security revenues. This can often be a very small proportion of the firm's revenues (often in £ billions) but reflects a significant proportion of the UK's cyber sector
- A significant 'dedicated' and growing middle market: There are now 84 firms (an increase from 72 last year) that we have identified as dedicated providers of cyber security with over £10 million in annual revenues

Finally, segmentation of revenues by size and by those companies that either provide (as a core role) cyber security products, services, managed security services, or resell (set out in Figure 4.3) also provides some useful insight.

Overall, service providers (including Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs)) are generating approximately £5.8 billion in cyber security related revenues. This reflects an increase of c. 12% since last year's study.

Product companies have continued to perform strongly in the last 12 months, with respective revenues increasing from c. £3.4 billion to c. £4.2 billion (an increase of 19%). This suggests a sustained trend of companies towards product / subscription-based solutions in the market.

Figure 4.3: Total Cyber Security Revenue by Size and by Offering



Source: Perspective Economics (n = 1,838)¹⁴

¹⁴ Note: Smaller values include **Product, Micro** £105 million, **MSP/MSSP, Small** £102 million, **Micro** £29 million, **Reseller, Medium** £14 million, **Small** £4 million, **Micro** £1 million

4.2 Estimated Employment

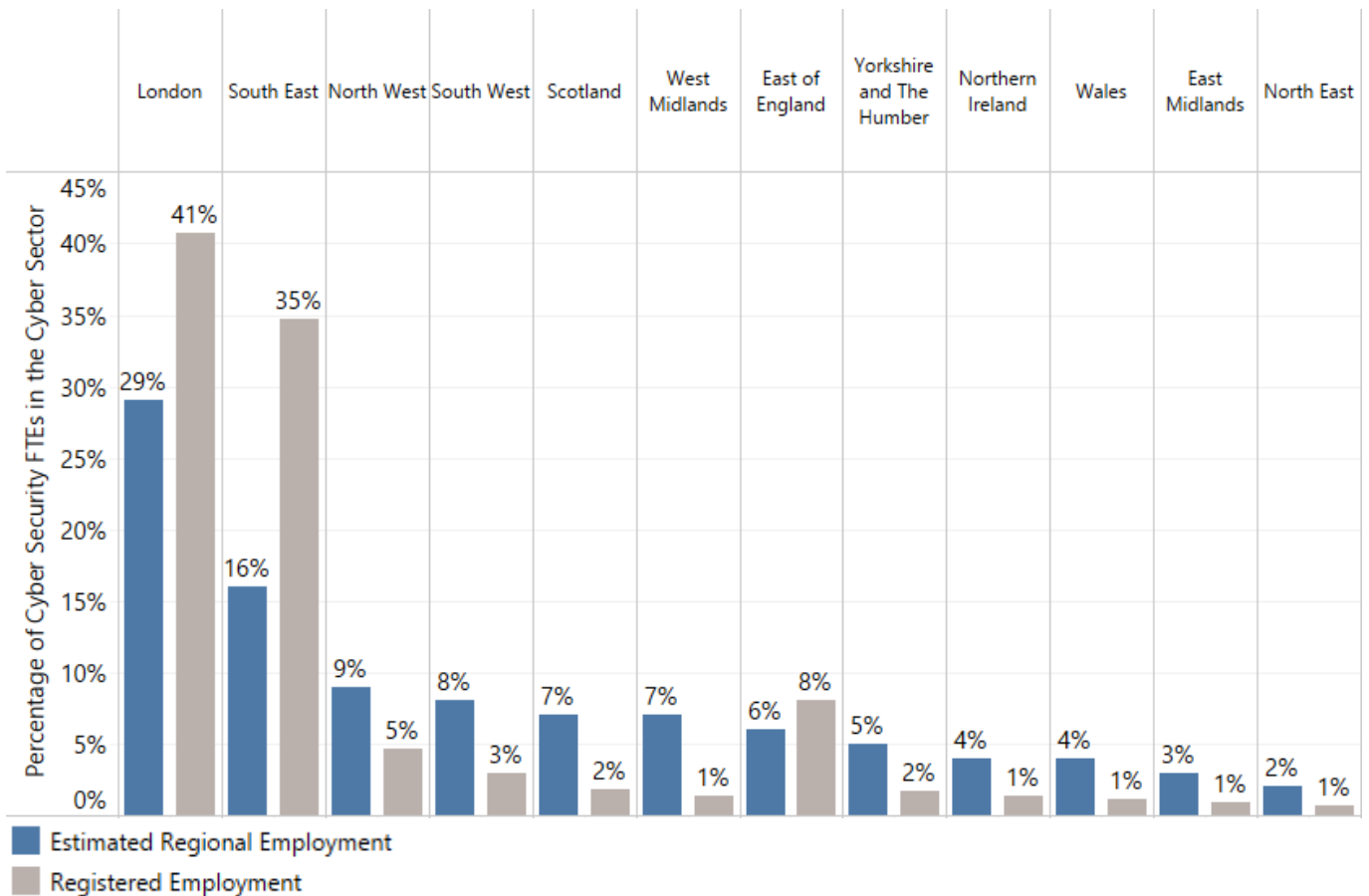
We estimate that there are 52,727 Full Time Equivalent (FTEs) working in a cyber security related role across the 1,838 cyber security firms identified. Please note that this figure only relates to the number of estimated FTE cyber security professionals working within cyber security sector firms.

This reflects an increase of 13% (up from 46,673 last year) in employee jobs within the last 12 months (and the rate of this increase is higher than the previous year’s employment growth figure of 9%). In other words, the sector has added over 6,000 FTEs in the past year.

This suggests that the number of employees working within the cyber security sector has grown significantly in 2020/21 and is also reflected in the considerable growth in cyber security job posting rates identified in the [Cyber Skills in the UK Labour Market research](#).

Company level employment is initially estimated at the registered level (i.e. this suggests concentrated employment within Greater London and the South East is 76% of the UK figure). However, as this reflects employment at a registered level, **this has the effect of underestimating employment for the other regions**, whereby employers have employees across the UK. For example, firms registered in Northern Ireland hire an estimated c. 600-700 people within cyber security, but the region is home to an estimated c. 2,300 cyber security professionals. As such, in Figure 4.4, we provide the registered and estimated actual employment breakdown by region. This estimate draws upon Perspective Economics modelling of key regional employers.

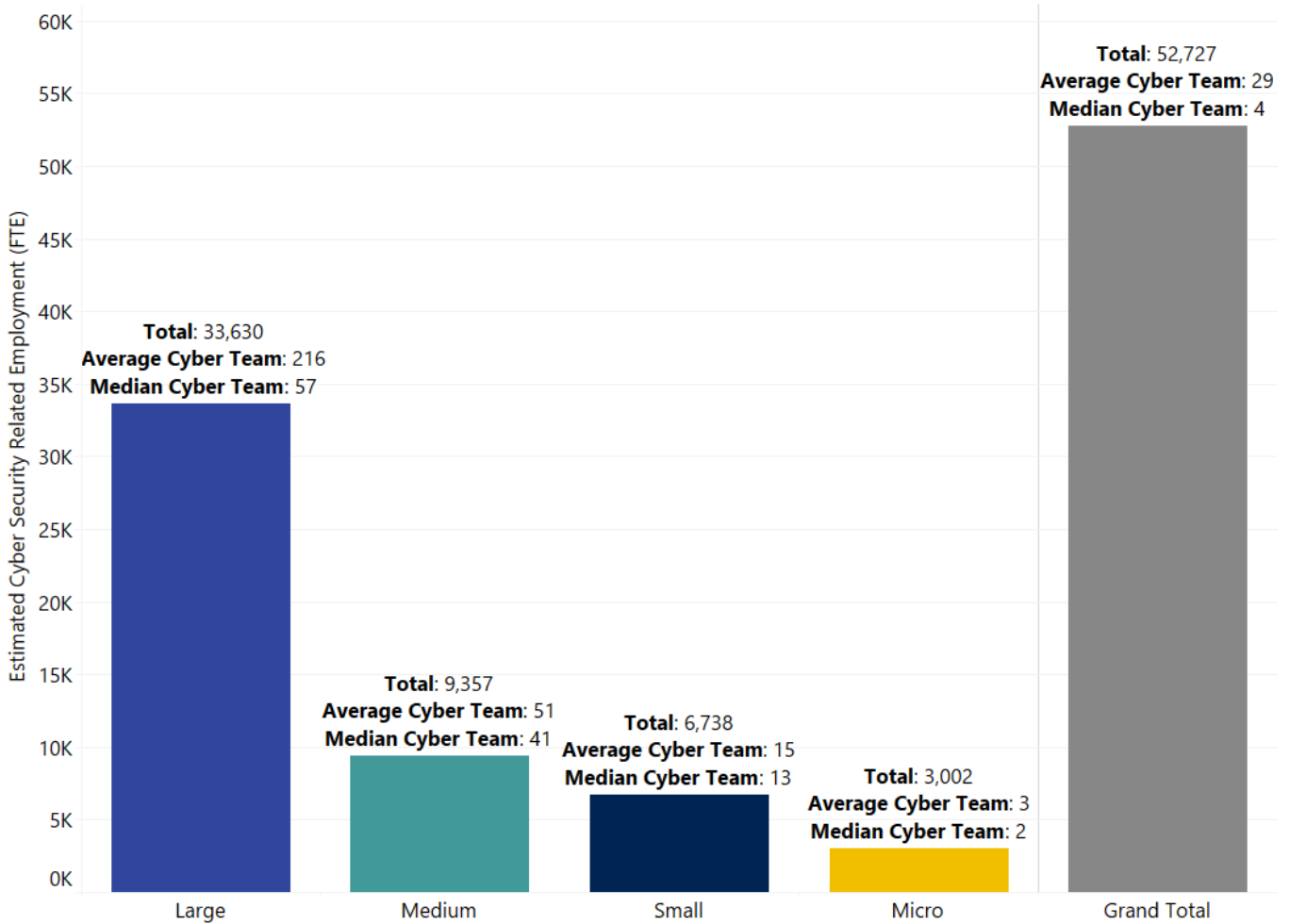
Figure 4.4: Estimated Cyber Security Employment by Region



Source: Perspective Economics (n = 52,727 FTEs, estimate)

Analysis of estimated cyber security employment by company size (Figure 4.5) demonstrates that, in line with last year’s findings, most cyber security employment remains concentrated within large firms (64%). The average size of a cyber security team has fallen slightly this year from 31 staff to 29 staff. Indeed, across the size brackets, average team size has remained consistent with last year’s figures. This suggests that whilst the total workforce has increased, there may be a tightening labour pool and enhanced competition among employers for new talent.

Figure 4.5: Estimated Cyber Security Employment by Size of Firm



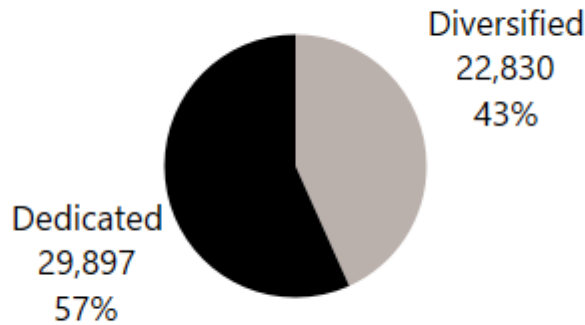
Source: Perspective Economics (n= 52,727)

Figure 4.6 sets out employment segmented by ‘Dedicated’ and ‘Diversified’ firms. This suggests that employment growth has been most pronounced within ‘dedicated’ firms.

When compared to last year’s estimates, the number of cyber security jobs within dedicated providers has increased from 25,241 FTEs to 29,897 (an increase of 4,656, or +18%), compared to a lower relative increase for diversified firms from 21,262 FTEs to 22,830 FTEs (an increase of 1,568, or +7%).

This may suggest an increased demand for additional resource and talent among some of the dedicated cyber security providers in the UK, and it will be important to explore this trend in future years.

Figure 4.6: Estimated Cyber Security Employment by Dedicated / Diversified

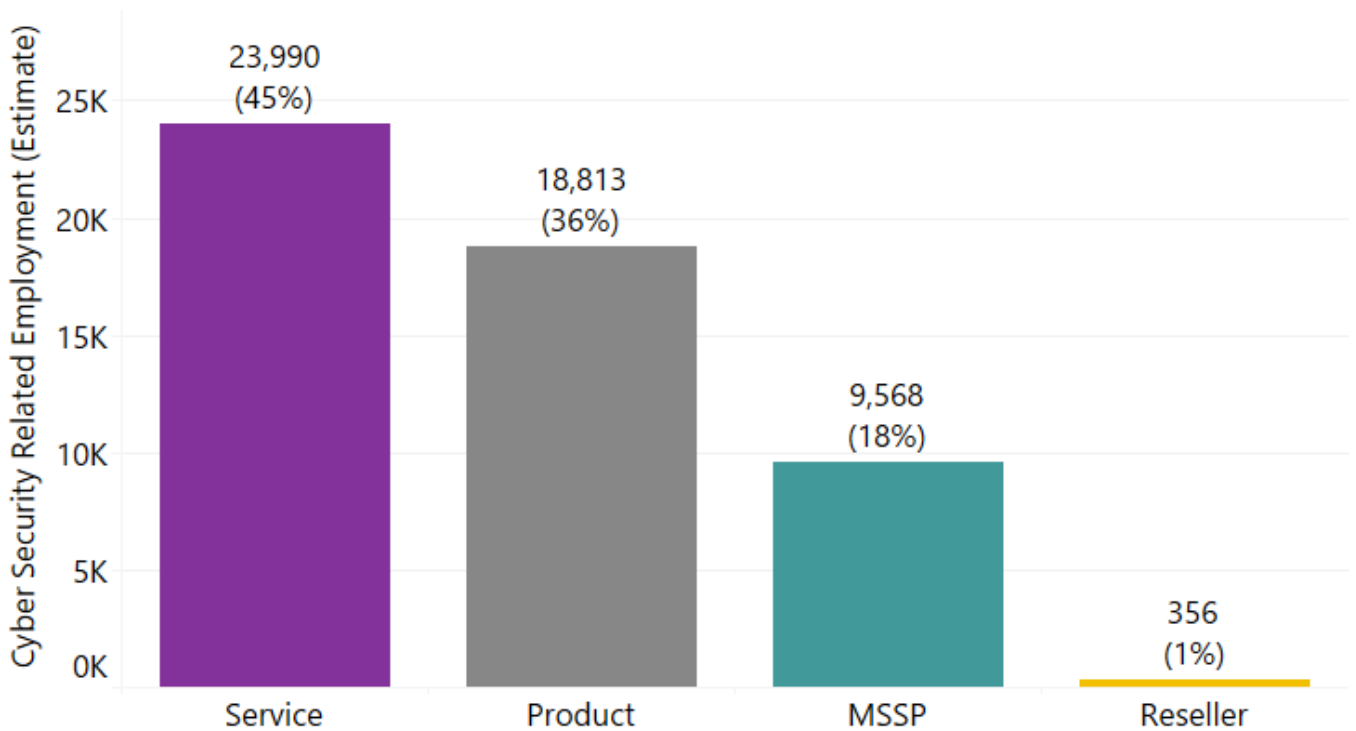


Source: Perspective Economics (n = 52,727)

Finally, Figure 4.7 sets out employment segmented by company core offering. Just under two-thirds (63%) of employees work within a company that primarily offers cyber security services or managed services, compared to 36% that work primarily within a product environment.

The number of staff working within product companies has increased from 15,278 last year (33% of all staff) to 18,813 (36% of this year’s employment figure). This reflects previous year’s trends and may highlight a drive for increased employment within dedicated product firms in the UK.

Figure 4.7: Estimated Cyber Security Employment by Offering



Source: Perspective Economics (n = 52,727)

4.3 Estimated Gross Value Added (GVA)

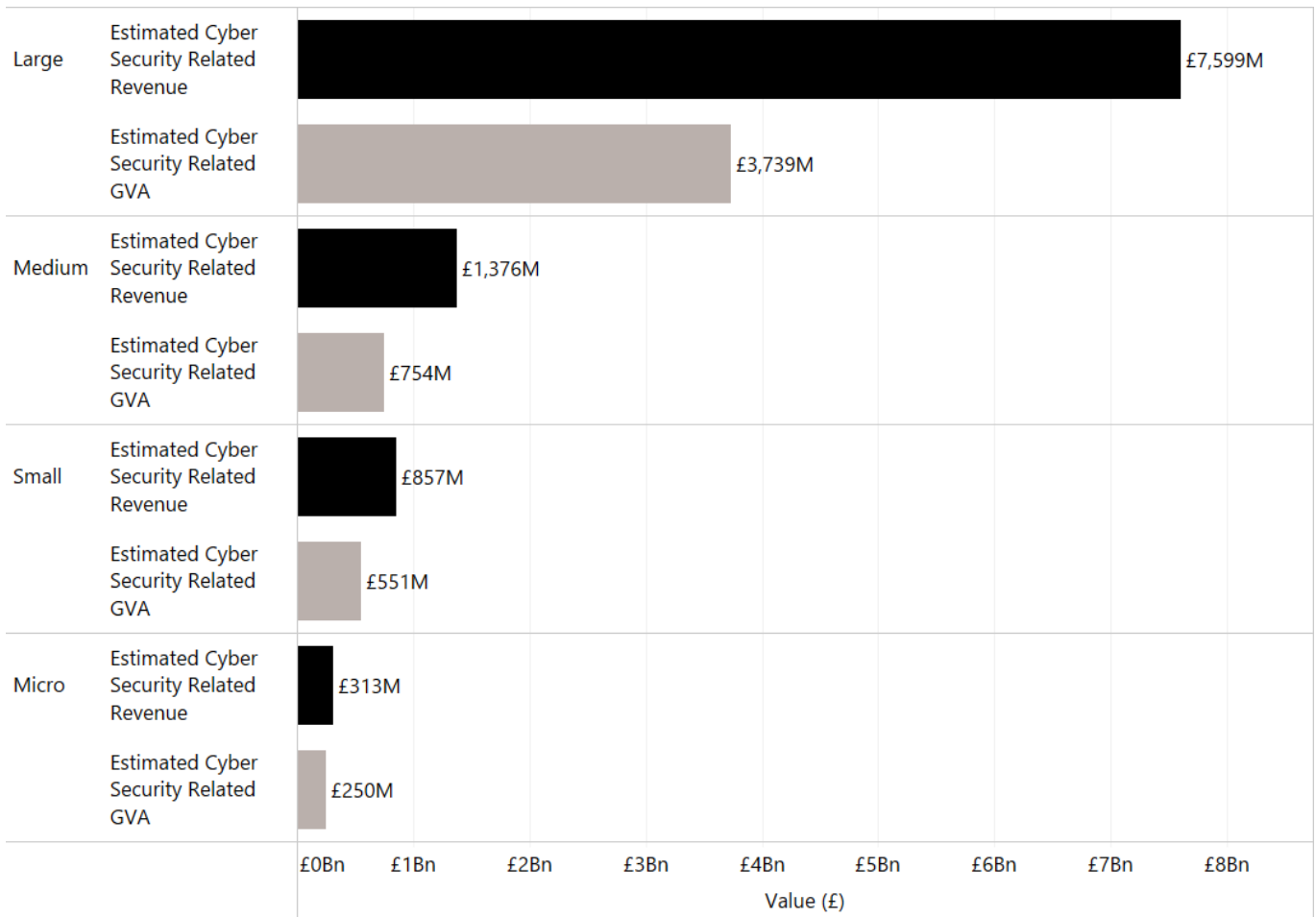
Gross Value Added (GVA) is used as a measure of productivity (at a firm level, or above). It captures the sum of a firm’s Gross Profit, Employee Remuneration, Amortisation and Depreciation. In this respect, any increase in GVA can highlight an improvement in the performance of a firm or a sector, as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

We estimate that within the most recent financial year, cyber security related GVA (for the 1,838 firms) has reached £5.3 billion (an increase of 33% since last year). This is a substantial increase and reflects improved profitability and remuneration across the firms.

Figure 4.8 sets out an overview of GVA (compared to revenue) by size of firm.

Overall, this data suggests an improved GVA-to-turnover ratio of 0.52:1 (i.e. for every £1 of revenue the sector generates, 52p in direct GVA is generated, compared to 46p last year).

Figure 4.8: Total Cyber Security Revenue and GVA by Size of Firm



Source: Perspective Economics (n = 1,838)

4.4 Summary of Economic Contribution

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

Size	Number of Firms	Estimated Revenue (Cyber Security Related)	Estimated GVA (Cyber Security Related)	Estimated Employment (FTE) (Cyber Security Related)	Estimated Revenue per employee	Estimated GVA per employee
Large	156	£7,599m	£3,739m	33,630	£225,959	£111,180
Medium	184	£1,376m	£780m	9,357	£147,086	£83,341
Small	447	£857m	£556m	6,738	£127,235	£82,542
Micro	1,051	£313m	£251m	3,002	£104,364	£83,762
Grand Total	1,838	£10,146m	£5,326m	52,727	£192,423	£101,019

Overall, since last year's study, the following changes to the key metrics are noted:

- The number of active cyber security firms (tracked in this study) has increased from 1,483 to 1,838
- Cyber security related revenues for these firms has increased from £8.9 billion to £10.1 billion (an increase of 13%)
- Cyber security related GVA for these firms has increased from £4 billion to £5.3 billion (an increase of 33%)
- Estimated revenue per employee has increased slightly, from c. £190,000 to c. £192,000 (an increase of 1%)
- Estimated GVA per employee has increased from c. £86,000 to c. £101,000 (an increase of 17%). This is higher than the current estimated GVA per employee for the DCMS Digital Sector (DCMS Economic Estimates) of £95,000 per employee.¹⁵

¹⁵ Digital GVA (£147.5 billion) / Employment (1,557,000) = £95,000

(Sources: DCMS (2020) 'DCMS Economic Estimates 2019: Gross Value Added'. Available at: <https://www.gov.uk/government/statistics/dcms-economic-estimates-2019-gross-value-added> and DCMS (2020) 'DCMS Economic Estimates 2019: Employment'. Available at: <https://www.gov.uk/government/statistics/dcms-sectors-economic-estimates-2019-employment>)

5 Investment in the UK Cyber Security Sector

5.1 Introduction

This section draws upon the [Beauhurst](#) platform which tracks announced and unannounced investments in high-growth companies from across the UK. Our team has matched Company Registration Numbers and Company Names identified within this current analysis with the platform to identify **976 investments¹⁶ in 322 tracked companies.**

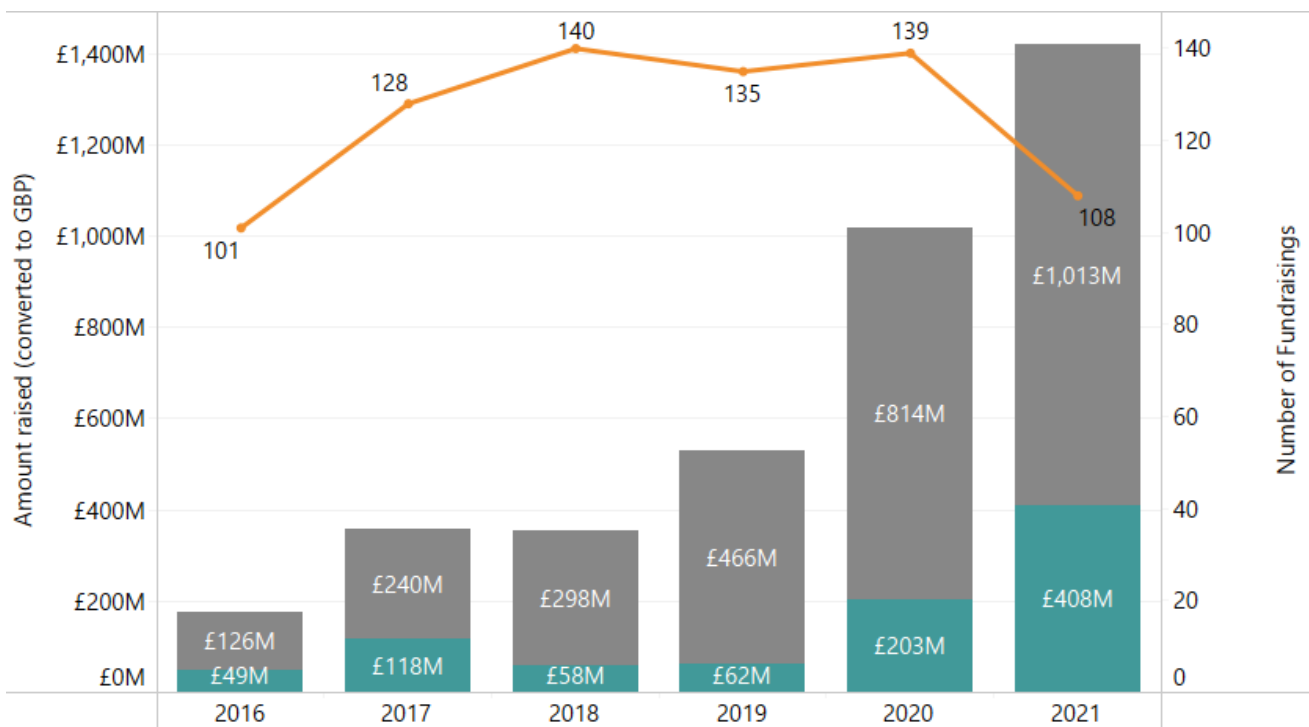
In other words, approximately 1 in every 6 firms identified within our analysis has received some form of external investment. This chapter focuses on investment activity within the full year of 2021 (1st January – 31st December).

5.2 Investment to Date

The investment timeline (Figure 5.1) demonstrates that 2021 has been a record year for cyber security investment, with over £1.4 billion raised in 2021 across 108 deals. **This includes £1,013 million raised across 84 deals within dedicated cyber security firms, which we focus on subsequently.**

Further, the total amount raised by the sector has almost doubled in 2020 compared to 2019 for dedicated cyber security firms (£814 million in 2020 and £466 million in 2019). Please note all following analysis focuses upon investment in dedicated cyber security firms.

Figure 5.1: Investment Timeline



Source = *Beauhurst* (note, blue = diversified, grey = dedicated, orange = number of deals)

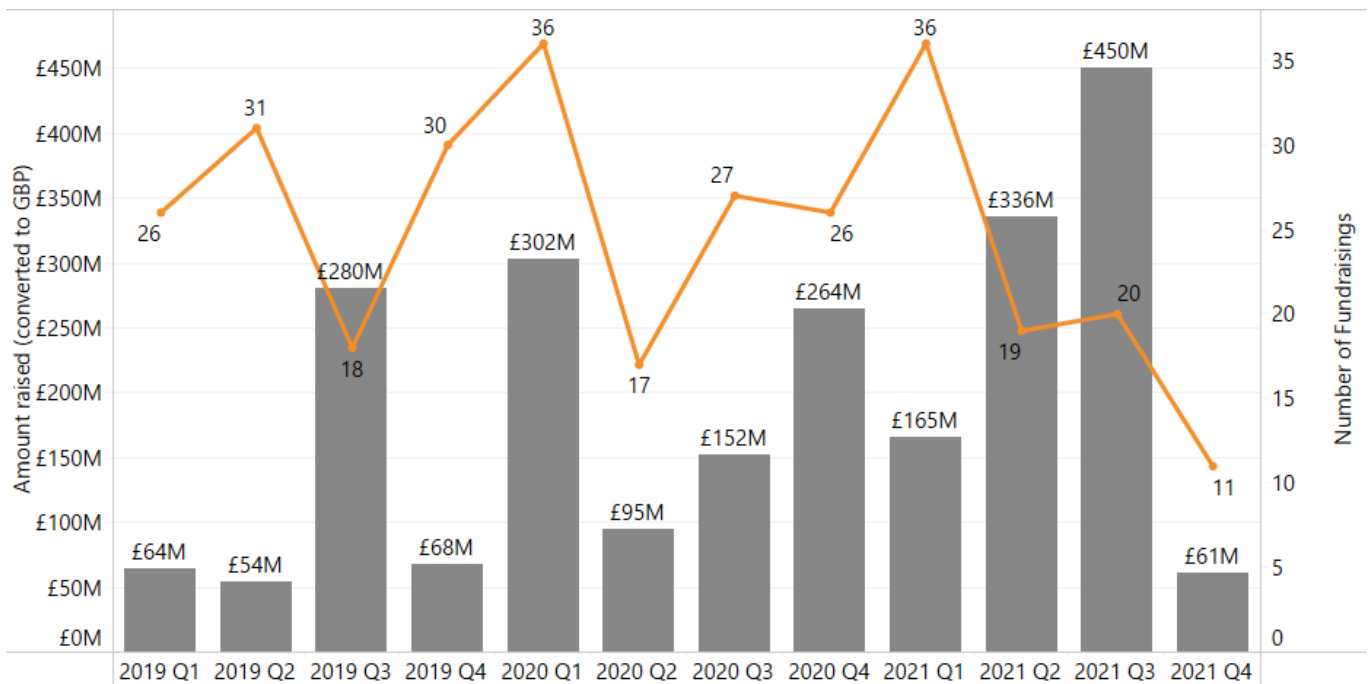
¹⁶ The Beauhurst platform tracks investments in these companies from 2006– 2021.

Within 2021, there were a number of notable investments raised by dedicated cyber security companies in the UK. Some examples include:

- **Snyk**, an application and developer security platform, raised two investments in 2021, including a \$530 million (c. £400 million) Series F investment co-led by Sands Capital and Tiger Global. This gives the company a post-money valuation of c. \$8.5 billion
- **OneTrust**, a privacy, security, and governance platform. announced a \$210 million Series C extension in April 2020
- **Immersive Labs**, based in Bristol provides online training and gamified labs for cyber security education. In June 2021, they raised £53.5 million in external investment
- **Tessian** develops software to detect phishing, unauthorised emails and prevent cyber security threats, and raised over £52 million in 2021
- **B-Secur** develops technology designed to enable the reading of an individual's heartbeat pattern through their fingerprint, enabling the verification of their identity. They announced an equity fundraising of £8.8 million in November 2021

Figure 5.2 also highlights that Q2 and Q3 2021 were particularly strong, with £336 million and £450 million raised by dedicated cyber security companies, respectively.

Figure 5.2: Investment Timeline (Quarterly, Dedicated Cyber Security Investment)



Source: *Beauhurst*

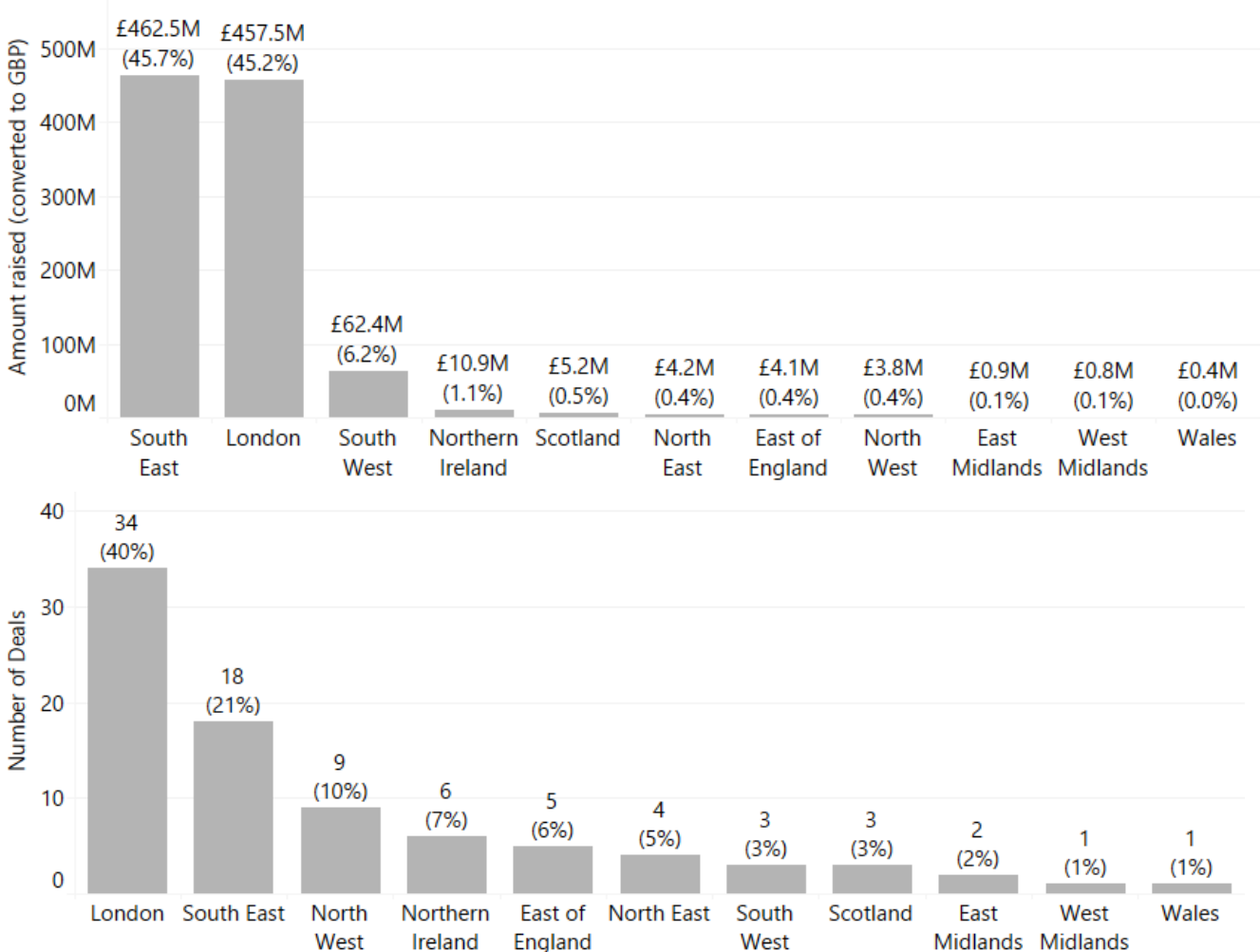
5.3 Investment by Location

External investment is a key indicator for business performance, as investment can help businesses to build their platforms, secure talent, and continue to grow, thereby helping to increase economic prosperity. It is crucial that businesses across the UK are able to secure investment where desired, in order to help provide the capital to scale and grow.

Figure 5.3 sets out an overview of investment performance within cyber security by UK region, with respect to value and volume of investment. This highlights that, as with previous years, the majority of investment raised (91%) is within cyber security firms based in London and the South East. Indeed, as with the previous study, 8 of the UK regions generate less than 1% of the UK total each, which highlights significant disparity with respect to large scale investments.

However, some of the regions continue to demonstrate multiple early-stage cyber security deals in their area, suggesting that sustained support for these start-ups may help to increase the value of rounds raised by cyber security firms across the regions. This is starting to be seen in areas such as the South West, where only 3% of the UK’s investment deals took place, but these deals represented 6.2% of the total value raised in 2021 (due to the significant growth in Bristol-based Immersive Labs). In this respect, many of the regions may be home to early-stage companies that could be feasibly supported to secure Series A (or higher) level investment in the upcoming years.

Figure 5.3: Total Investment (Value and Volume, 2021)



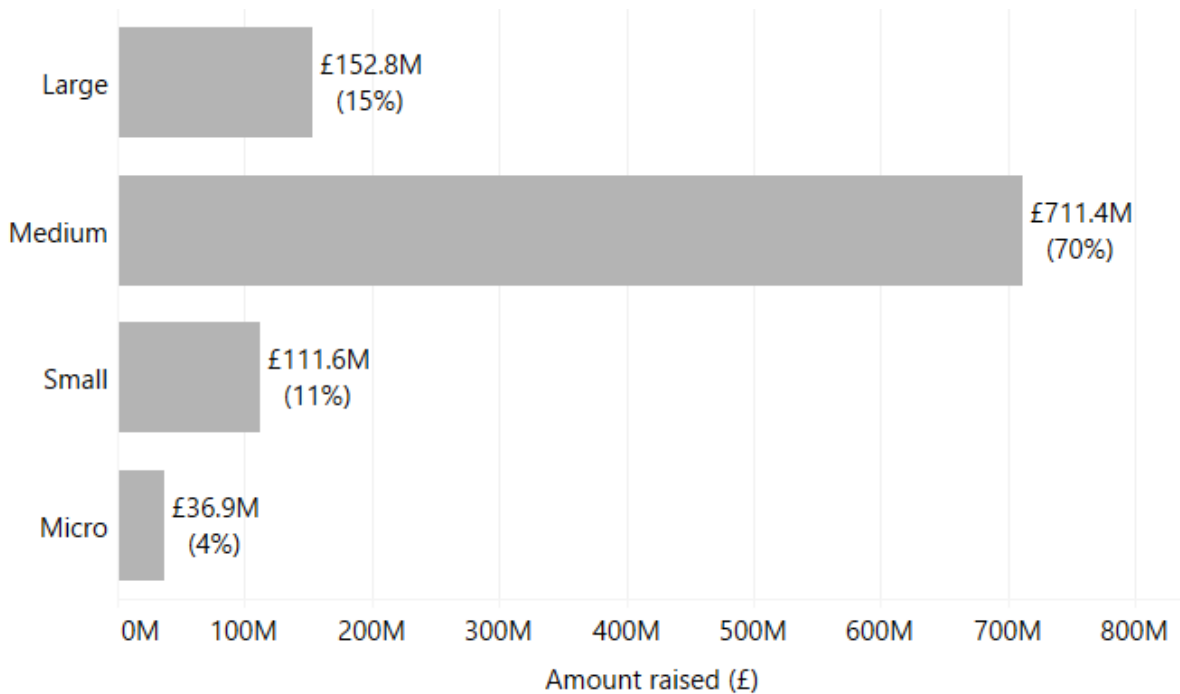
Source: Beauhurst (2021)

5.4 Investment by Size

Figure 5.4 sets out the volume of investment by (current) company size within the cyber security sector in 2021. The previous study set out that in 2020, only 7% of investment was raised by small and micro level firms (i.e. fewer than 50 staff). In 2021, this has increased to 15% of total investment raised, reflecting increased demand among investors for backing early-stage UK cyber security firms. For example, in 2021, firms such as Hack the Box (£7.7 million), Cado Security (£7.3 million) and Venari Security (£4.2 million) have all successfully raised investment.

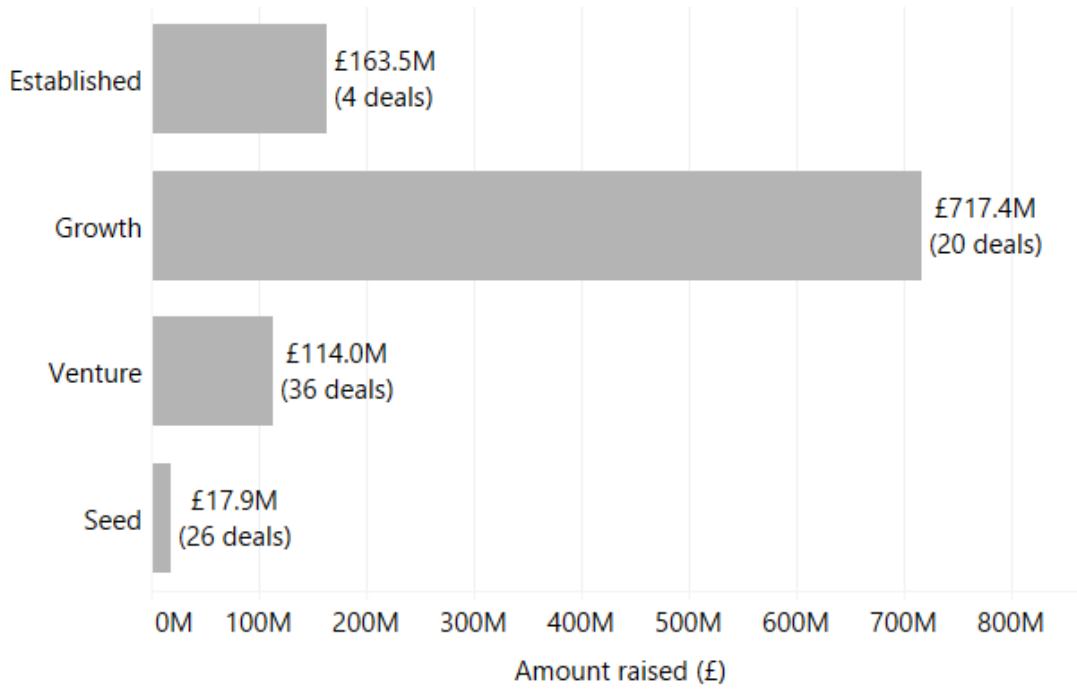
This is further highlighted in Figure 5.5, which highlights the growth in the amount of investment secured for venture stage companies (from £41.7 million across 32 deals in 2020, to £114 million across 36 deals in 2021). This suggests signs of a sustained maturity within the UK’s cyber security investment ecosystem, with high-growth firms able to secure investment and use this as a catalyst to expand their teams and operations.

Figure 5.4: Total Investment by Company Size (2021)



Source: Beauhurst (2021)

Figure 5.5: Total Investment by Stage of Evolution¹⁷ (2021)

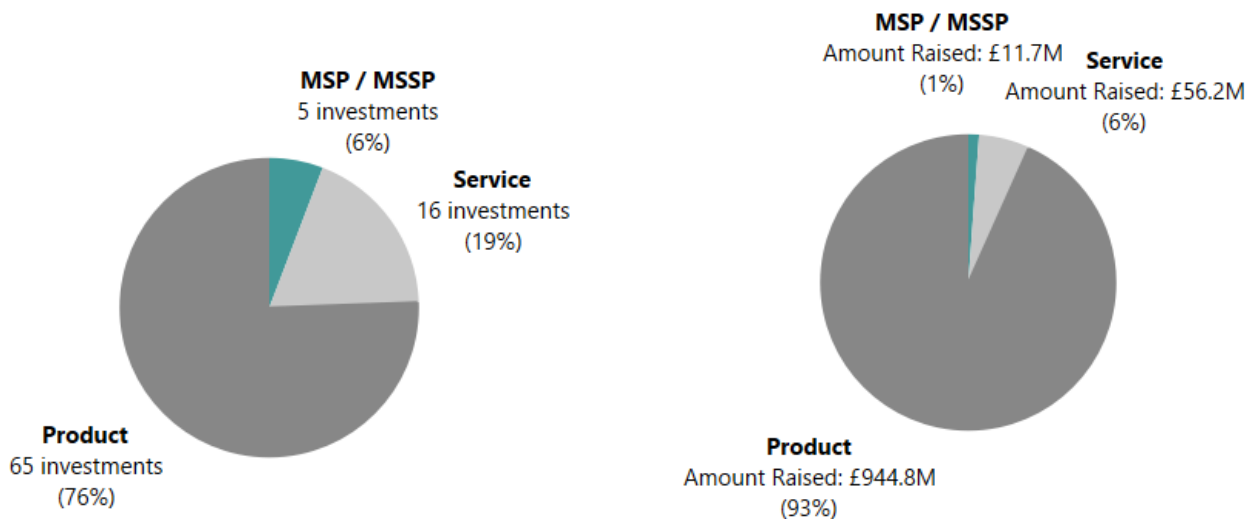


Source: Beauhurst (2021)

5.5 Investment by Company Type

Figure 5.6 highlights how investment preference for companies that primarily offer cyber security products has continued in 2021, with 76% of the volume of investments, and 93% (£945 million) of the respective investment value.

Figure 5.6: Investment by Product / Service Offer (2021)



Source: Beauhurst (2021)

¹⁷ The definitions for seed, venture, growth, and established categories are set out in Appendix D.

5.6 Investors and Sources of Funding

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

- Within all the historic cyber security fundraising data, there have been 513 funds involved, of which 83% are still active. This is a substantial increase from the 2017 baseline report (whereby 68 funds were identified), and from last year, where 283 funds were involved within the historic fundraising data. This suggests that as the UK's cyber security investment ecosystem has matured and scaled, many fundraisings contain multiple investment funders to provide this capital
- Further, within last year's analysis, there were 24 funds that could provide more than £25 million (based upon typical investment activity or known sector / investment restrictions). This has since increased to 35 funds, again reflecting further maturity within the investment landscape

Within the UK, some of the most significant investors continue to include (by value / volume¹⁸):

- 24Haymarket
- Accel
- AlbionVC
- British Patient Capital
- Amadeus Capital Partners
- IQ Capital
- Mercia Asset Management
- Octopus Ventures
- Paladin Capital Group

¹⁸ Granular figures not provided due to disclosive nature.

5.7 Market Dynamics: Qualitative Feedback

In August and September 2021, the research team held a series of qualitative consultations with a range of industry investors to gather views about what investors are looking for in UK cyber security, and perceptions of the investment landscape.

Main factors driving investment

Investors spoke of a number of factors driving their investment decisions.

One factor was **market opportunity**. The investors that participated in this research looked for products or services that they considered to be **innovative** and **in growth areas**, such as Internet of Things, cloud computing, supply chain security and smart cities.

“We will turn down very good businesses even if we think they are \$100 million to \$500 million. They don’t fit with the investment mandate of future public companies with multi-billion revenues.” Cyber security investor

There were investors who felt other areas such as network and endpoint security were already crowded markets, or that some areas such as hardware security and quantum computing needed ‘de-risking’ through government support. In terms of exports, there was little consistent feedback, although one investor felt that UK businesses were more ‘investment-ready’ if they exported to the US specifically, given the size and importance of the US market.

Different investors in the cyber investment market focused on different **growth stages** or levels of **maturity**. For example, one investor who focused on late-stage investment looked for companies that had already raised seed and series A and B funding, and that had potential to become multi-billion revenue public companies; while another investor focused on those looking for seed or series A funding, and so looked for companies with much lower revenues.

However, regardless of maturity, investors reported wanting to see businesses with a **strong roadmap for growth**. One investor commented that they like to see companies where intellectual property (IP) rights have already been granted.

“Good companies are those with a really strong product roadmap and the potential to move into adjacent markets and industries with a broader offer. Coming with a vision for how they can build a very large business is key.” Cyber security investor

The **experience** of the company’s team was also important to investors who focused on more mature businesses. Investors reported looking for businesses that did not just have technically gifted teams (in terms of technical cyber security skills), but who were also exceptional entrepreneurs. This involved businesses being able to demonstrate **commercial traction**, for example, having experience of attracting large or established customers and an exceptional rate of attraction.

However, investors reported it was also key for a business to have **validation of their product or service** from sophisticated buyers. This was important to investors due to the **challenges with validating the uniqueness and defensibility of cyber technologies** given the number of companies and products in the ecosystem.

“In cyber, we’re prepared to drop the £500,000 limit [lower revenue limit] and even go pre-revenue provided they have validation from sophisticated buyers and companies with sophisticated procurement processes who have engaged with and used the product in pilot or full-scale implementation and can vouch for the team and that the product works.” Cyber security investor

How investors support cyber sector businesses

Investors described supporting cyber sector businesses in various ways.

Investors emphasised the importance of **getting the right people** into the organisation, both in terms of **technical talent** and **sales talent**. The investors that participated in this research noted that start-ups can find it challenging to access technical talent as they are unable to compete with established businesses or in Big Tech and in the Fin Tech sector.

“Access to talent is still a huge issue. There is lots of talent, but start-ups are finding it hard to compete on compensation, stability, and risk. Software engineering, AI and machine learning are in hot demand from Big Tech, FinTech, etc.” Cyber security investor

Investors also noted that many founders struggle with sales and scaling their business. Investors with in-house teams reported **supporting scaling and recruitment** (of both technical and sales talent) through headhunting, advising on recruitment practices and culture, and advising on business structure to facilitate growth.

Larger investors reported offering **mentoring and networking support**. For example, one investor typically joined the Board of Directors to provide experience, act as a “strategic sounding board” for founders and allow cyber businesses to access the network of their portfolio around the world. This facilitated business development through customer introductions and connecting entrepreneurs with peers. This visibility – connecting successful entrepreneurs – was suggested as another way the government could support the cyber sector.

“I think it would be great for the government to continue to celebrate success stories.” Cyber security investor

Views of the UK as an investment landscape for cyber security

Investors were positive about the UK as an investment landscape for cyber security, although they identified some economic challenges facing the sector.

Investors viewed the UK cyber security sector as a **high growth sector attracting a lot of investment**, particularly compared to the rest of Europe, though it was still felt to be behind the US and Israel.

“I think the UK is probably the best place in Europe [for cyber security investments], but I feel it’s behind Israel and behind the US in terms of opportunities ... The UK is far ahead of the rest of Europe in terms of scale-up potential companies.” Cyber security investor

“On the whole I think it’s a sector which is well supported, and investors are excited to be supporting.” Cyber security investor

However, the UK cyber security sector was also described as being **heavily crowded**, meaning that high visibility, and strong sales and marketing were particularly important.

This reflects the global picture, with [recent research](#) suggesting the world's largest cyber security firms are spending 41% on average of their revenue on their commercial activities. As this external research highlights, the **information asymmetry** between vendors and buyers presents an economic (rather than a technological) challenge: buyers find it difficult to evaluate cyber security technologies, which incentivises vendors to bring sub-optimal solutions to the market. To counter this, **independent regulation** and **transparent efficacy assessments** of technologies are suggested to reduce the information asymmetry and build customer **trust and confidence** in cyber security solutions.

In our interviews, there were some investors who felt the government could do **more to support businesses working in fundamental technology** where development timescales are too long to be appealing to the traditional venture market.

“Government help is particularly needed on companies which are maybe not a traditional venture case and that could, for example, be around fundamental technology – hardware innovation, deep technology – which takes years to develop before it has any commercial implications. I think that's where the traditional venture market is not well set up to support.” Cyber security investor

Similarly, [recent research](#) suggests that UK investment in cyber security research is well below major competitors, and that the UK needs to be **more strategic in research funding**. This may be, for example, by developing clusters of excellence to compete with large long-term investment models in the US, France, and Germany.

There were also investors who felt more support was needed to help start-up companies reach ‘unicorn’ status (i.e. a valuation of over \$1 billion), though this was considered less important than very early-stage support.

“I think the Series A and B landscape is pretty supportive ... What we want to see more of is more funders who are looking to take these companies from £200 million valuations all the way through to unicorn one billion plus valuations.” Cyber security investor

Perceived changes in the investment landscape within the last 12 months

Investors were positive about changes in the investment landscape within the last 12 months.

There was a feeling that the cyber security investment landscape had been **resilient**, with little or no negative impact to date from the COVID-19 pandemic or EU Exit. In fact, there was **optimism** that the COVID-19 pandemic would encourage greater awareness and use of technological solutions, which would in turn present opportunities for the cyber security sector.

“COVID-19 has not impacted [investment]. In fact, we have seen the cyber sector being particularly resilient, so we are doubling down rather than changing tack.” Cyber security investor

More widely, investors reported an **increase in ambitions and late-stage capital** (Series B and C funding) into Europe and the UK over the past six months (the first half of 2021), which would allow more companies to remain independent.

“Many more investors are willing to write \$50 million plus cheques into the UK. Those companies are more likely now to remain independent than to be acquired given they have been able to grow so far. The scale of investment means there is less pressure on founders to exit or merge with others.” *Cyber security investor*

6 Government Support for the Cyber Security Sector

6.1 Introduction

In August 2021, the research team held a series of qualitative consultations with a range of cyber security businesses, businesses with dedicated cyber security teams and leads of accelerator schemes to gather views about funding and support received, regional engagement, growth, and support needs in the UK cyber security sector. Section 6.3 presents findings around engagement with cyber sector accelerator schemes and Section 6.4 presents findings around engagement with other regional bodies and organisations.

6.2 Recent Investments and Support Initiatives

The [National Cyber Strategy 2022](#) sets out how the Government has sought to support the growth of the cyber security sector, through a blend of direct investment in accelerators and growth initiatives, skills and profession support, investment in regions and clusters, and as a key buyer of cyber security products and services.

Some of these initiatives¹⁹ are summarised below:

Growing the sector and exports, and promoting regional growth:

- Helping cyber businesses find international markets. [The UK exported](#) £4.2 billion of cyber services in 2020
- Running [Cyber Exchange](#), a portal for cyber security businesses across all regions of the UK
- techUK's [Cyber Growth Partnership](#) has been bringing government and industry together to break barriers to growth
- [The UK Cyber Cluster Collaboration](#) (UKC3) is building partnerships between industry, academia and local government to ensure opportunities and expertise are available across the regions

Supporting businesses to grow and scale:

- Running initiatives such as [NCSC for Startups](#) to help address some of the most important strategic challenges in cyber security
- Providing funding for schemes such as [LORCA](#) (which has helped 72 cyber innovators raise over £200 million in investment and earn over £37 million in revenue), [Cyber Runway](#), which supports innovators to launch, grow and scale their business – building on the success of HutZero, Cyber101 and the Tech Nation Cyber Programme
- Supporting the commercialisation of academic research in cyber security through the [CyberASAP](#) (Cyber Security Academic Startup Accelerator Programme), led by the Knowledge Transfer Network (KTN)

¹⁹ Please note that these are examples, and not an exhaustive list of initiatives supported by government and devolved administrations.

Encouraging new entrants into the cyber security sector to help tackle the skills gap:

- [The CyberFirst bursary scheme](#) supports undergraduate students and is delivering hundreds of individuals, with work experience, into the cyber workforce every year
- The [CyberFirst](#) courses and Discovery programme have engaged nearly 300,000 young people aged 11-17 in the last five years
- [There are now four cyber apprenticeship standards](#) that have been designed by industry and three cyber offerings for initial learning outcomes offered through the DfE 'Courses for Jobs' initiative
- There have been nine [cyber bootcamps](#) supported through the recent National Skills Fund, taking people into cyber careers

Professionalising the cyber security workforce:

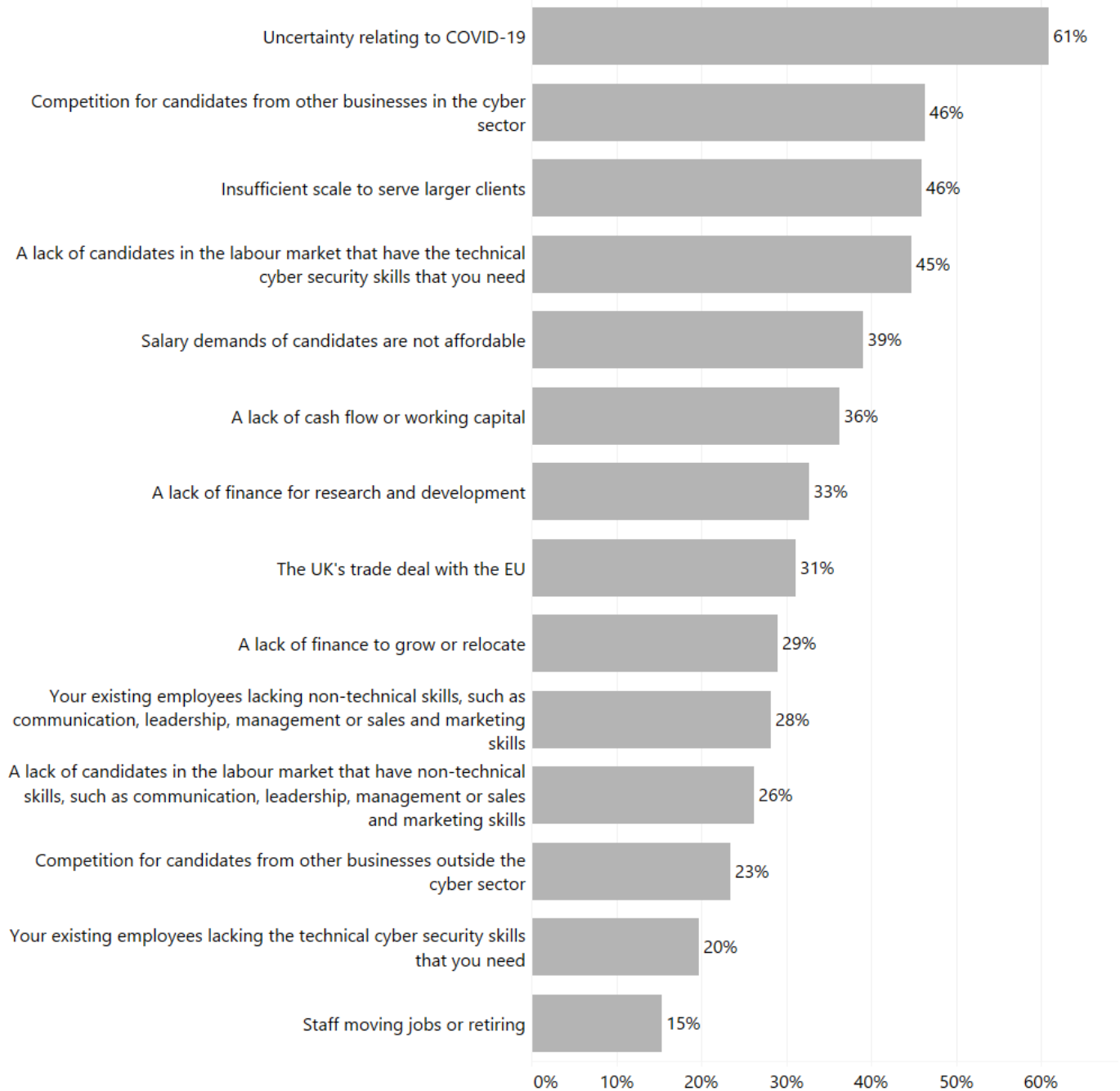
- [The UK Cyber Security Council](#) is a world-first professional authority for cyber security. It has begun to set clear and consistent professional standards, building on all the work that existing professional bodies have done to date. The Council will look to clearly identify effective qualifications from the myriad currently available
- The [Cyber Security Body of Knowledge \(CyBOK\)](#) informs and underpins education and professional training for the cyber security sector

6.3 Engagement with Cyber Sector Accelerator Schemes

Reasons for approaching accelerators

Within the business survey, we asked businesses the extent to which the following factors affected their ability to meet their business goals (to a great or large extent). Figure 6.1 sets out some of the key challenges, underpinning reasons for engaging with initiatives.

Figure 6.1: Barriers reported by cyber security businesses (“to a great extent / to some extent”)



Source: Ipsos (n = 248)

In the qualitative consultations, cyber security businesses reported a range of reasons for approaching accelerator schemes, especially to receive support with business strategy, networking, and sales and marketing.

They reported feeling confident about the product or service they were developing, but less confident about **business development** and **marketing strategies**. While their technological knowledge was good, there were founders who wanted more advice on the commercial side of the cyber security space – for example, knowledge of how their business, product or service fitted into the market and an awareness of what their competitors were doing.

There were also founders who wanted support on **human resources (HR)** and various **financial or legal aspects** of their product. They felt this was important to give them a good general understanding of how to run a business, since there were several businesses with no prior entrepreneurial experience. While this was particularly relevant to first-time founders, there were some experienced entrepreneurs who also viewed coverage of these aspects in accelerator schemes as a helpful refresher.

*“When I looked at [the accelerator scheme], it looked useful to get a 360-view of what to look at.”
Cyber security business*

Generating new business was an important reason for engagement with accelerator schemes. Businesses felt the accelerator schemes would offer them opportunities to present to buyers, generate leads and increase sales, for example, through **attendance at events** like the RSA Conference in San Francisco, **access to large client portfolios**, or simply **through association** with a prestigious and competitive accelerator scheme.

Accelerator scheme leads reported a similar picture, saying that businesses approached accelerator schemes to support their business development, and the commercialisation of their product or service. However, they also noted that cyber security firms were often unaware of the accelerator schemes or did not realise how much support they needed. The **lack of a captive audience** meant it was often necessary to seek out participants, although cyber businesses also came to accelerator schemes via other sources, for example, **word-of-mouth** and **recommendations** from existing relationships with accelerator leads, business mentors and universities.

“Someone I knew was involved as one of the mentors [on the accelerator scheme] and they recommended it.” Cyber security business

Perceived value of accelerator schemes

Cyber security businesses in the consultation interviews reported a range of benefits and added value as a result of participating in accelerator schemes, although there was also some criticism where accelerator schemes did not meet businesses' expectations.

For some businesses, participating in an accelerator scheme was considered a form of **endorsement** (or government endorsement by proxy) of their product or service, which gave the business added **validity** and **credibility**. This helped them stand out from competitors and facilitated networking, which led to further opportunities. Some businesses also benefited from having office space in London during accelerator participation.

“Just being on [the accelerator scheme] has opened opportunities for us, including an invitation to NCSC Cyber Innovation Den, which in turn led to two big opportunities.” Cyber security business

Accelerator schemes were also considered helpful in supporting businesses to think more about **commercialisation, marketing, and sales**.

“We used to be too embedded in product development. The schemes lifted our heads and said, in order to succeed, you have to play a better role in convincing people to use the product.” Cyber security business

In some cases, this had led businesses to change direction by **refocusing the business plan** or pivoting the product or service offered by the firm.

“[The accelerator scheme] helped us to ask those questions and gave us that introspective look – what is your model, and what are you doing that is different from others?” Cyber security business

Businesses cited **mentoring** as a valuable part of accelerator schemes, even if this was general **business advice** rather than advice on running a cyber security business specifically. Advice included help to create an action plan, doing a Strength, Weakness, Opportunity, Threat (SWOT) analysis to identify what to concentrate on and other potential areas to consider, gaining a better idea of how the business fits into the wider cyber sector landscape, and individualised feedback through discussions.

“It was really useful getting advice from experienced business owners. It was more general business advice rather than really targeted cyber information ... Some mentors suggested looking at different areas, e.g. compliance and Internet of Things – made us think about these early on – which was helpful.” Cyber security business

Networking was also felt to be a valuable part of accelerator schemes. The schemes gave businesses an opportunity to speak to other cyber security **companies at similar growth stages** to themselves and to embed themselves in the **cyber security ecosystem**. They felt this allowed them to **share knowledge, information, and perspectives** effectively and to learn from the practical experience of their peers.

“The workshop gave a sense of community – lots of people in the room all coming at tech from different angles.” Cyber security business

Some accelerator scheme leads also highlighted the importance of **building the ecosystem** to ensure market feedback was available earlier, in the research and development stages. For example, they observed cases where industry was telling academia that their research was usually delivered in a format which meant it could not be adopted, even if the idea was good.

“We’ve tried to fix that by building the ecosystem, that community that feeds in, and give that feedback earlier on.” Accelerator scheme lead

However, there was also some **criticism** where accelerator schemes did not meet businesses’ **expectations**, especially around the amount of marketing and sales support.

“I felt the marketing support was too light-touch, and there was not enough opportunity to meet with buyers.” Cyber security business

Another participant felt that some accelerators had become quite **London-centric**, as travelling to and from London was time-consuming and potentially off-putting to others. While the increased amount of virtual support during the pandemic has gone some way to mitigating this, there were also participants who highlighted the benefits of physical networking, which were hard to replicate through video calling.

Some participants also felt that existing accelerator schemes were **not fully geared towards businesses at their stage of maturity**. There were suggestions that accelerator schemes could be improved through having follow-up workshops. These would offer an opportunity to ask more questions, share experiences of how businesses are doing, and provide further networking.

“I don’t think [the accelerator] was sufficiently geared towards very small companies – we needed to be further along the line. We were hitting the same hurdles. We were told we need to ask customers about our product, but we were too early to have customers. We were then told to ask prospective customers, but that wasn’t particularly helpful advice because we needed help with our market positioning.” Cyber security business

These criticisms and suggestions highlight the importance among participants for accelerator schemes setting clear expectations, having support appropriate to the maturity of the business, and continuing to provide support to companies throughout the various stages of their growth.

Accelerator scheme leads noted that the accelerator landscape is more mature than it was, with a greater number of cyber security businesses and a greater number of businesses with potential to expand. They felt a key challenge was for businesses to secure medium and longer-term funding. This would mean moving towards 5 to 10-year funding brackets to ensure a more sustained support presence, and to allow greater awareness of accelerator schemes to develop.

6.4 Engagement with Other Regional Bodies and Organisations

Types of partnerships and engagement

Cyber security businesses in the consultation interviews reported a range of partnerships and engagement with other organisations in their region, including other cyber organisations, and universities and colleges. These came about through several sources, such as industry connections, research connections, local organisational groups (see below) and personal contacts.

Some businesses engaged with their local **Cyber Security Clusters** or with **local business organisations**, such as Local Enterprise Partnerships, business hubs and local Chambers of Commerce, as well as more informal networks around IT and artificial intelligence (AI). In some cases, businesses sought out such networks when looking for opportunities to increase their presence or sales, while in other cases, businesses were invited through personal or industry contacts to participate or attend events. As a result of these connections, some businesses reported partnering with **vendors**. In some cases, vendors approached the business, while in others the business approached the vendors. This was important for businesses to generate sales further along the supply chain, with vendors helping to convince clients of the need and value for new cyber technology.

“We work with companies further along the supply chain, e.g. device manufacturers, to bring down the costs of the equipment that’s essential for our technology. And once we cross that price threshold, it will open up a much more substantial market for us to sell tech.” Cyber security business

Businesses also described partnerships or engagement with **universities** and **colleges** to varying degrees. One business was approached by a university and a college to sponsor a course. This involved the business **updating and designing course content**, training lecturers to ethical hacker standards, sponsoring prizes for the best student, and partnering with certification bodies. Other businesses had

less formal engagement, for example, feeding into university courses through personal connections with the relevant university faculties. There were also those who were not involved in developing courses, but who would give talks, run events, or conduct demonstrations (e.g. live hackathons) at local universities, colleges, and schools.

Within the business survey, 54% of cyber security businesses stated that they were aware of local cyber security clusters or UKC3, and 59% of cyber security businesses had engaged with other cyber security businesses in a collaborative way (e.g. on products, R&D, or skills) in the last 12 months. This highlights the importance of clusters and initiatives where businesses can engage with each other (as well as other bodies and education providers).

Benefits and challenges

Cyber security businesses described a number of benefits to partnerships and engagement with other local organisations, as well as several challenges.

One benefit of engaging with local **Cyber Security Clusters** was having access to the **latest information and knowledge**, as well as **networking** with people engaged in cyber activities from a range of sectors. For example, as a result of being part of their local Cluster, one participant formed partnerships with local universities and police forces who were starting their ‘cyber journeys,’ i.e. looking to collaborate with local cyber security businesses. More generally, some participants felt these Clusters helped to raise awareness of cyber security among local businesses.

“All these little connections end up taking you in a different direction. But you’ve got to have a community that’s open to sharing and key individuals to bring people together.” Cyber security business

Similarly, businesses described engagement with **local business organisations** as good opportunities for **networking**, ‘soft’ **marketing** (e.g. informally talking about their business or handing out business cards) and **facilitating potential partnerships**. Building these networks allowed businesses to raise their profile, marketing and sales through endorsements or sponsorship, as well as allowing businesses to respond to new contract opportunities alongside potential partners in a more agile way.

“When partnerships come through personal connections, it removes some of the bureaucracy ... Having a sponsor makes things faster than cold calling.” Cyber security business

Businesses found partnerships with **vendors** particularly useful for **effectively expanding their client offering** in a cost-effective way, for example, providing specialist cyber security technology or expertise alongside a larger IT services company. It also helped in offering a **better stream of work**, as organisations could refer potential clients to a partner organisation.

“From a business perspective, partnering is a massive contribution, particularly offering services that other service providers need.” Cyber security business

Businesses that engaged with **universities** considered this a good way to **access graduates as future employees**, either via placement years or post-graduation, while some also noted that it provided a useful way for **bridging the gap between industry and academia**. In addition, businesses felt that partnering with universities helped to bolster their **credibility** and **promote themselves**, for example,

one business mentioned collaborating on academic research and journal articles to lend their business credibility through association with the university brand.

However, businesses also described a number of challenges associated with partnerships or local engagement.

One business described a potential challenge relating to **regional government funding schemes**. They noted that, if a business had funding from a regional scheme, it could potentially clash with the terms and conditions of national funding schemes, limiting their eligibility. This was considered particularly problematic for large parent companies with regional offices, where there would need to be significant coordination between offices so as not to fall foul of any eligibility criteria.

Businesses described a **lack of understanding of cyber security among the general business population**. In some cases, this lack of understanding made it difficult to establish partnerships, as it was challenging to identify how cyber businesses could complement existing service providers, or there was a perceived threat to reputations. One participant with a product designed to expose vulnerabilities described how potential partners felt there was a reputational risk that the product would expose breaches among the employees of those potential partners.

There were also reports from participants of larger IT service companies claiming to offer comprehensive cyber security whilst actually implementing low-quality cyber solutions. This **assurance issue** either meant cyber security businesses were spending a lot of time fixing mistakes caused by other providers, which gave them less time to develop their own business offer, and that cyber security businesses were finding it increasingly difficult to encourage clients to buy higher-quality products or services.

“I don’t do IT support, so why do [MSPs] think they can do cyber security?” Cyber security business

When talking about partnerships with universities, businesses described challenges around the **misalignment between academic curricula and industry needs**. For example, partnerships designed to support the development of a new curriculum for cyber security faced challenges with the **speed of change**. It could take several years to design a new curriculum, approve it, and implement it, and additional time for such changes to bear fruit, for example, graduates with the desired skills. In addition, in a fast-evolving area such as cyber security, businesses noted universities were not typically agile enough to respond to the changing needs of industry, with the problem even more pronounced in colleges. This was because college curricula for the entire academic year were considered fixed from early on, meaning business needs could only be reflected in the next academic year’s course, by which time it was too late.

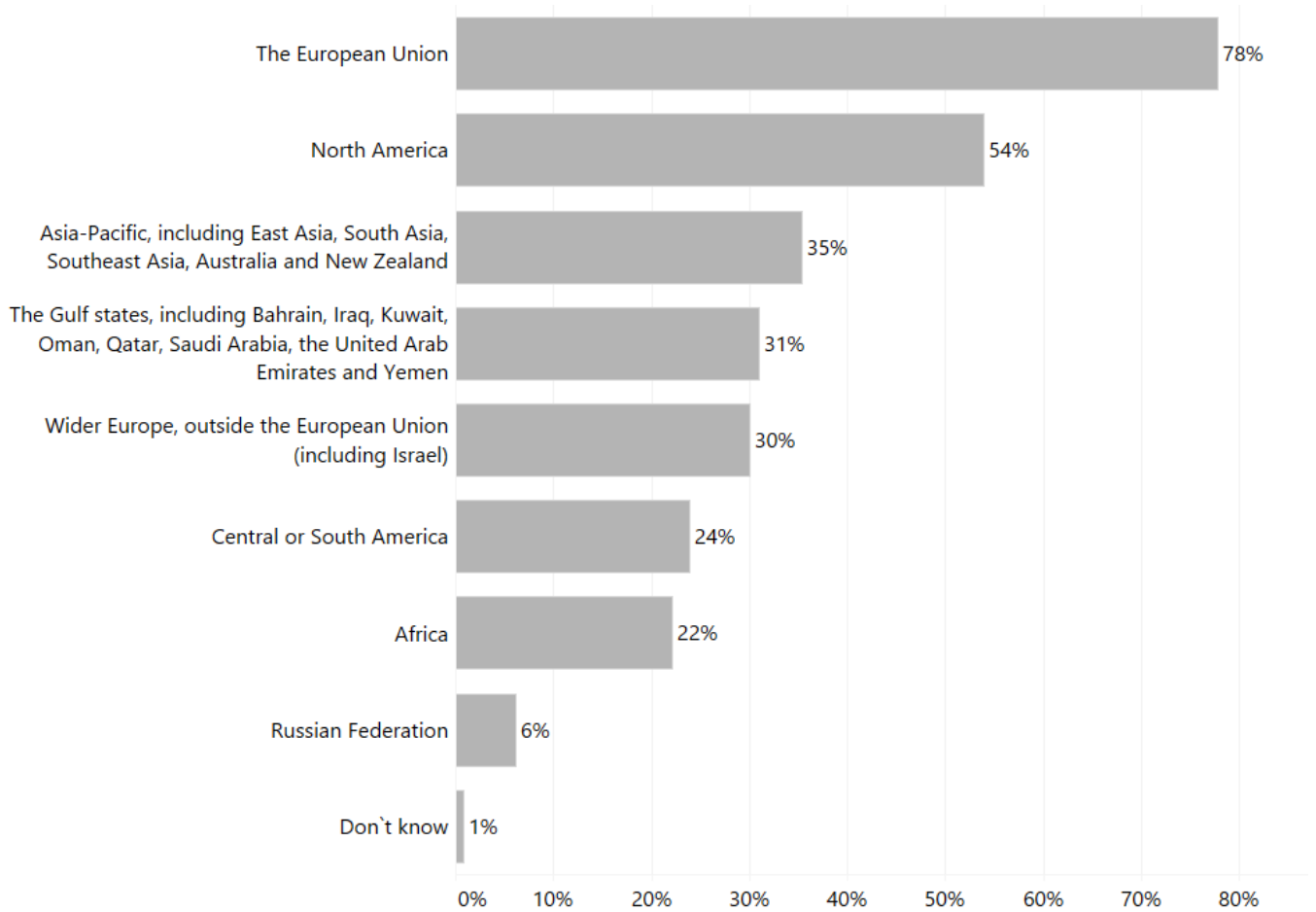
“The wheels turn very slowly in colleges; it’s hugely more challenging than unis ... It’s just too hard, not because of the students or lecturers, but we get push back on it always being too late and it becomes ‘next semester,’ too much lead-in time needed, and course changes are not agile or flexible. They have to advertise the course a year in advance, then the process is super slow to get colleges to gear up and be ready for it.” Cyber security business

6.5 Cyber Security Exports

In October 2021, the Department for International Trade published updated [UK Defence and Security Export Statistics](#) for 2020. This suggested that UK cyber security exports have grown from approximately £3.96 billion in 2019 to £4.24 billion in 2020 (an increase of c. 7%).

Within this year’s survey, cyber security businesses were asked if they exported, and if so, what and to which regions. In Figure 6.2, just under half of businesses (46%) reported that they exported products or services, of which the majority exported to the European Union (78% of exporters), and North America (54% of exporters).

Figure 6.2: Export Regions (for businesses that export)

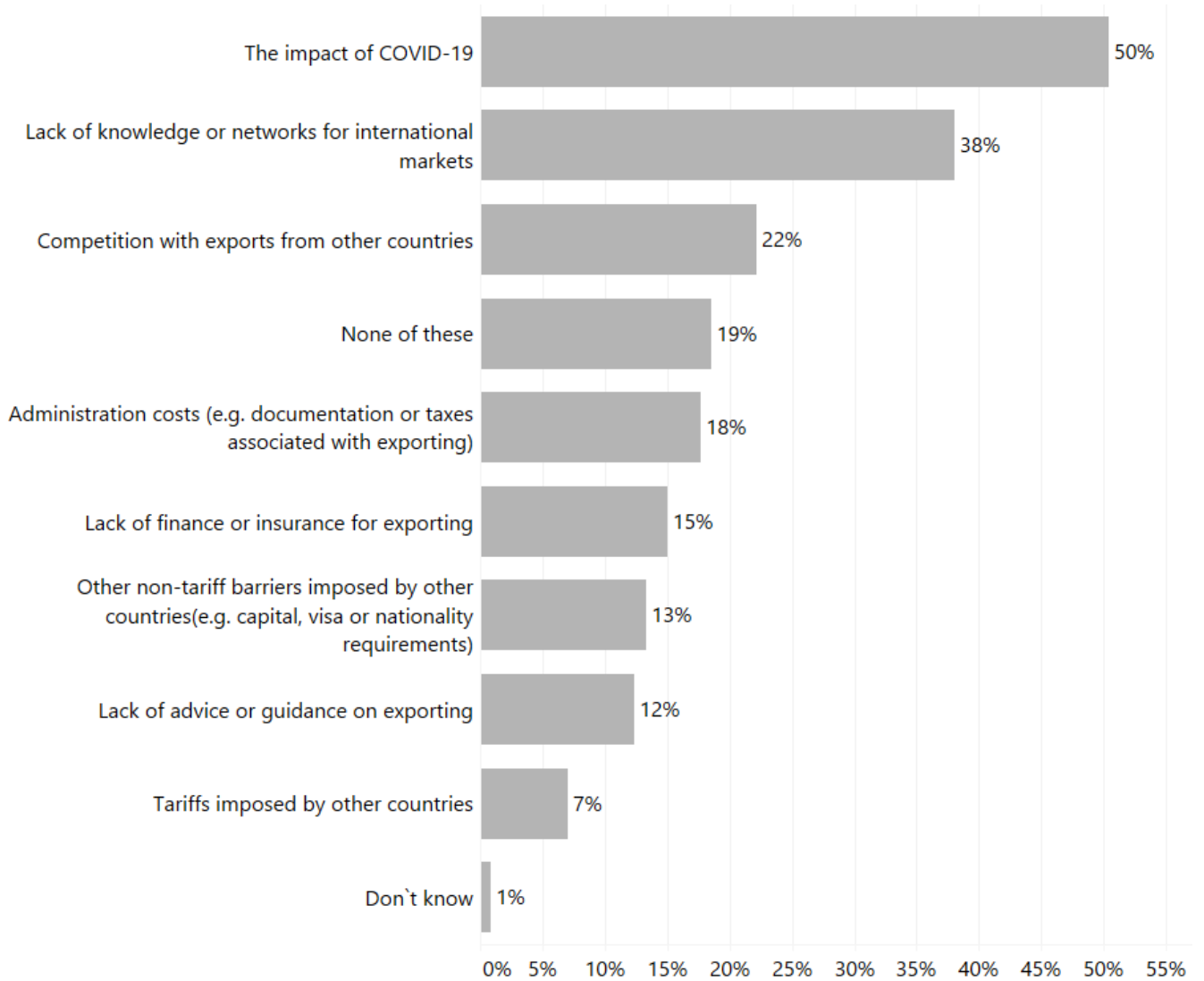


Source: Ipsos (n = 113)

Cyber security businesses that export were also asked about some of the key barriers that held them back from further maximising the value of their export business. Figure 6.3 sets out some of the key reasons, including the impact of COVID-19 (faced by 50% of exporters), limited knowledge or networks in international markets (38%), and competition with domestic traders in other countries (22%).

Figure 6.3: Challenges in exporting

“Which of the following, if any, have prevented you from maximising the value of your cyber security export business over the last 12 months?”



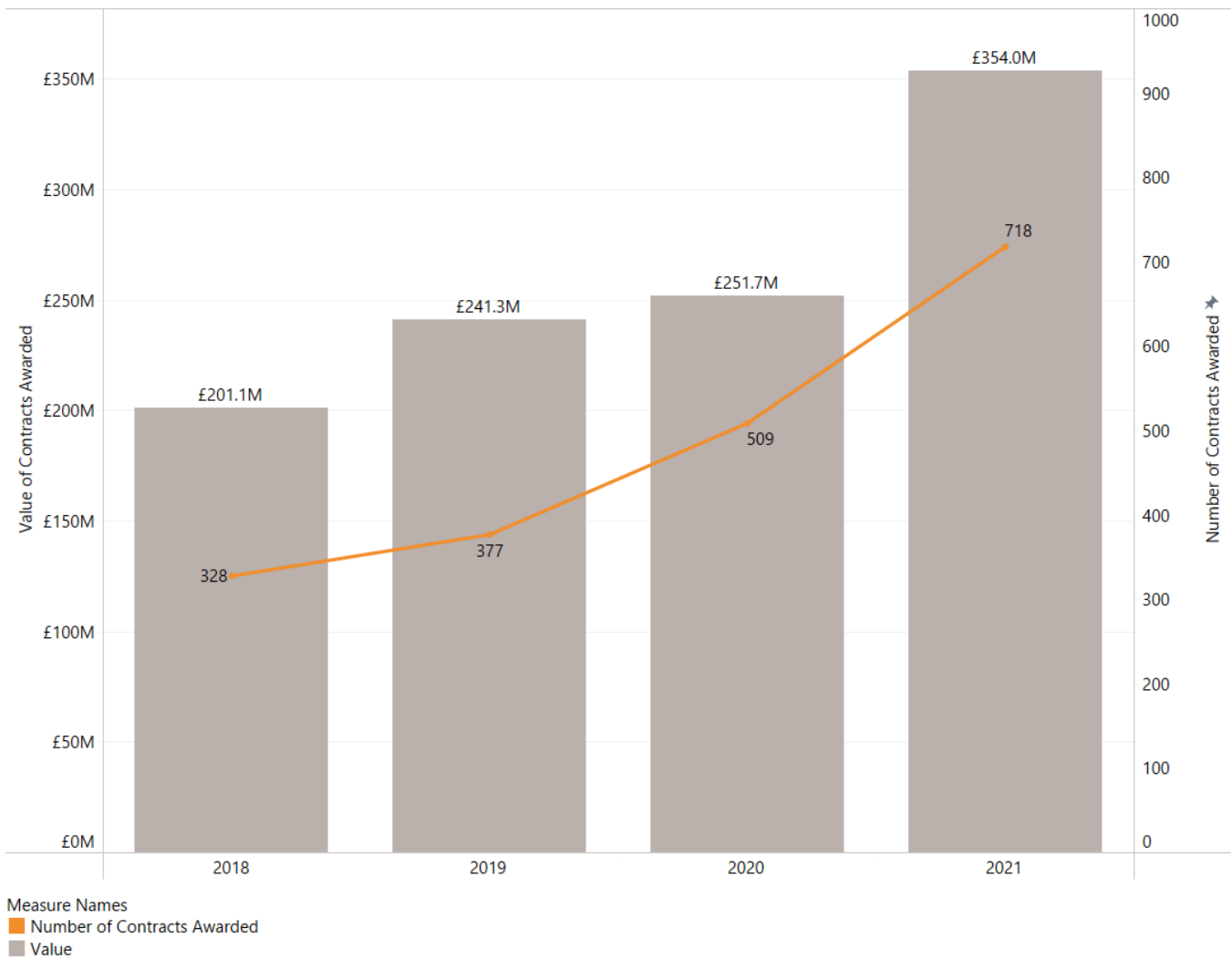
Source: Ipsos (n = 113)

6.6 Public Procurement

Public procurement plays a crucial role in the health of the cyber security sector, and for improving public sector engagement with innovative cyber security start-ups and techniques. In previous years, we have used Tussell data to identify cyber security related contract notices. For transparency, this measures the number and value of public contracts awarded to UK registered firms related to cyber security. It excludes the award of framework contracts as these can be difficult to identify exact government spending, where the contract value is the same as the framework maximum budget.

Figure 6.4 demonstrates that in 2021, the number of public contract awards relating to cyber security increased by 41%, and the value of awards also increased by 41%, reaching £354 million in 2021. This suggests a significant increase in demand by the public sector for cyber security products and services in the past 12 months.

Figure 6.4: Cyber Security Contracts (Value and Volume)



Source: Tussell²⁰ (data source on UK government spend and contracts).

²⁰ See www.tussell.com

Within the consultations with cyber security Small and Medium Enterprises (SMEs), many businesses mentioned the key role of procurement and working with government in helping to grow and scale their operations:

“Small companies really look up to these companies who are blazing a trail and being recognised for it. The fast-growing companies are providing a public service to the whole of the UK and their founders should be recognised accordingly.” Cyber security investor

“GDPR and Cyber Essentials are like the perfect salesman – businesses are worried about breaches and fines.” Cyber security business

“[Cyber Security Clusters] are good intelligence gathering for what may be going on, for what tenders may be coming out.” Cyber security business

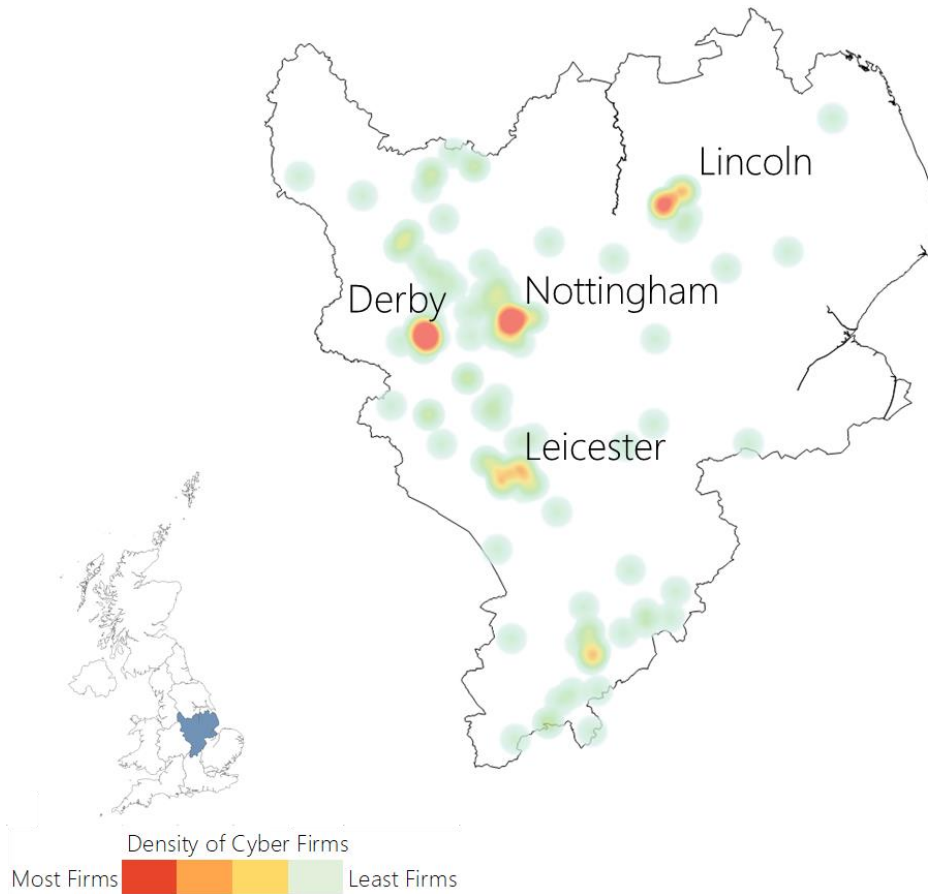
“COVID for us brought us a massive surge in the requirement for IT people because everyone wanted to do remote working ... particularly in the last six months because the backlog has been supercharged, including some large government contracts.” Cyber security business

Regional Snapshots

Introduction

Whilst this report focuses upon the cyber security sector across the entire UK, we set out snapshots²¹ of the number of cyber security firms, offices, and estimated share of UK activity (weighted for revenue, employment, and number of firms).

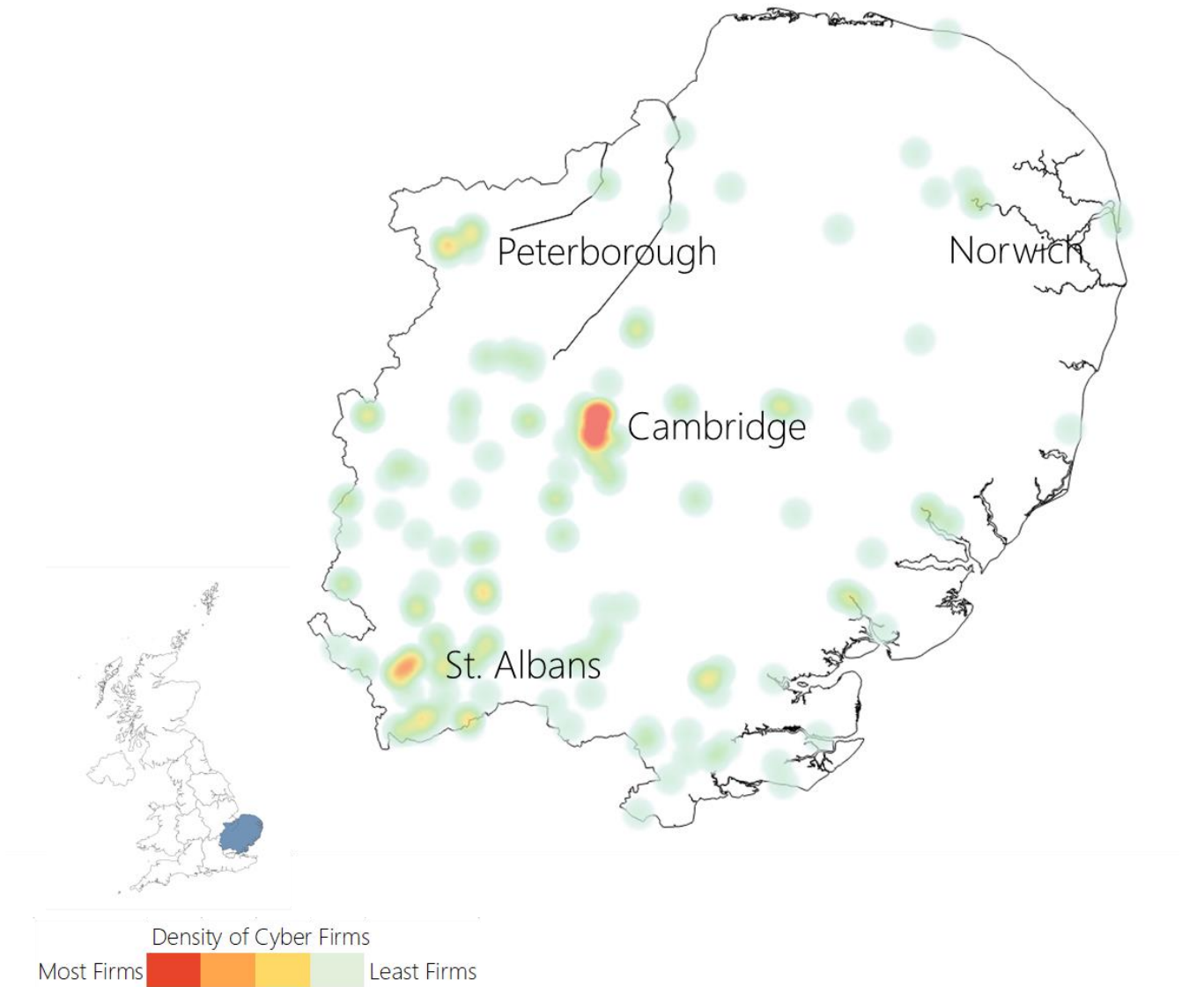
East Midlands



East Midlands	Number of Registered Offices	Total Number of Active Offices
	66	149
Percentage of UK cyber security offices	Estimated percentage of UK based cyber security employment	Average Advertised Salaries (2021) in core cyber security roles
4%	3%	£47,000

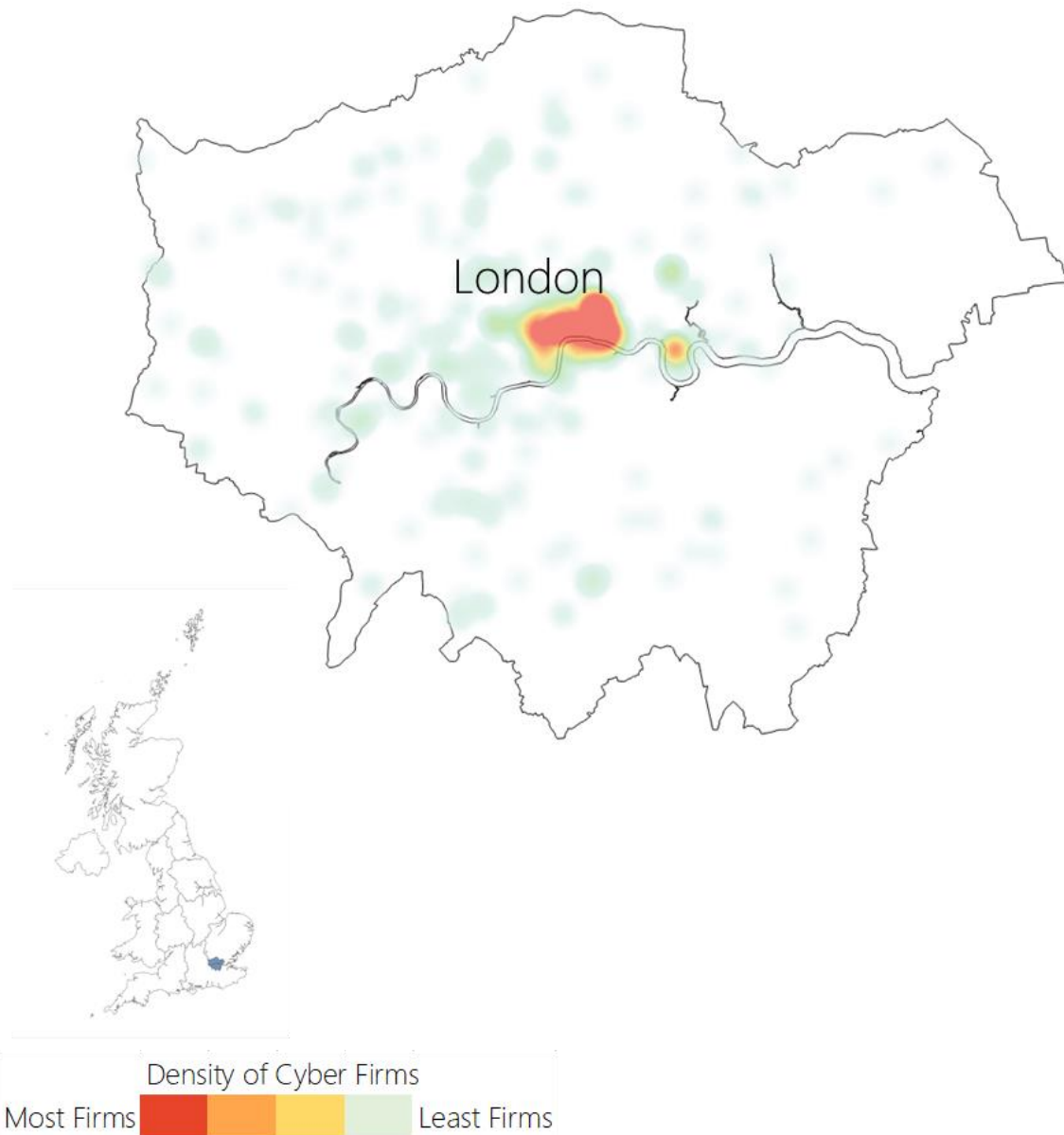
²¹ Each of the sections below sets out a heatmap of the active offices within each region (darker red intensity signals a cluster of firms), count of registered cyber firms, count of active cyber offices in the region, percentage of active UK cyber security offices within the region (i.e. number of active offices in the region divided by the total number of active cyber offices in the UK), and an estimated percentage of UK cyber security sectoral employment within the region. The average advertised salary is derived for 2021 using the Burning Glass Technologies Labour Insight tool. This is consistent with the methodology from the Cyber Skills in the UK Labour Market research (published in 2021, with data and analysis from 2020), and updates the figures from that report using labour market data from 2021.

East of England



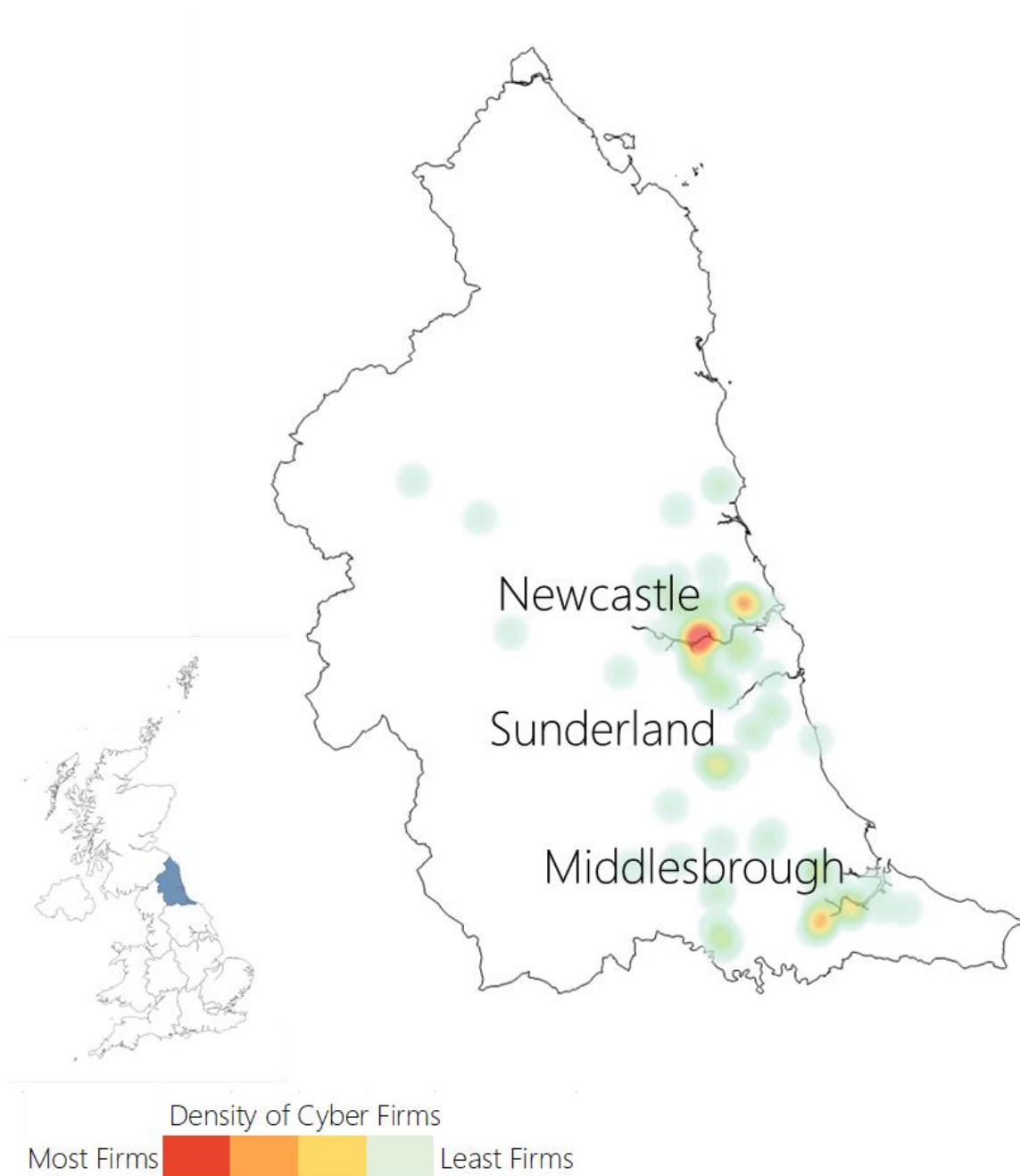
East of England	Number of Registered Offices	Total Number of Active Offices
	137	243
Percentage of UK cyber security offices	Estimated percentage of UK based cyber security employment	Average Advertised Salaries (2021) in core cyber security roles
6%	6%	£52,200

Greater London



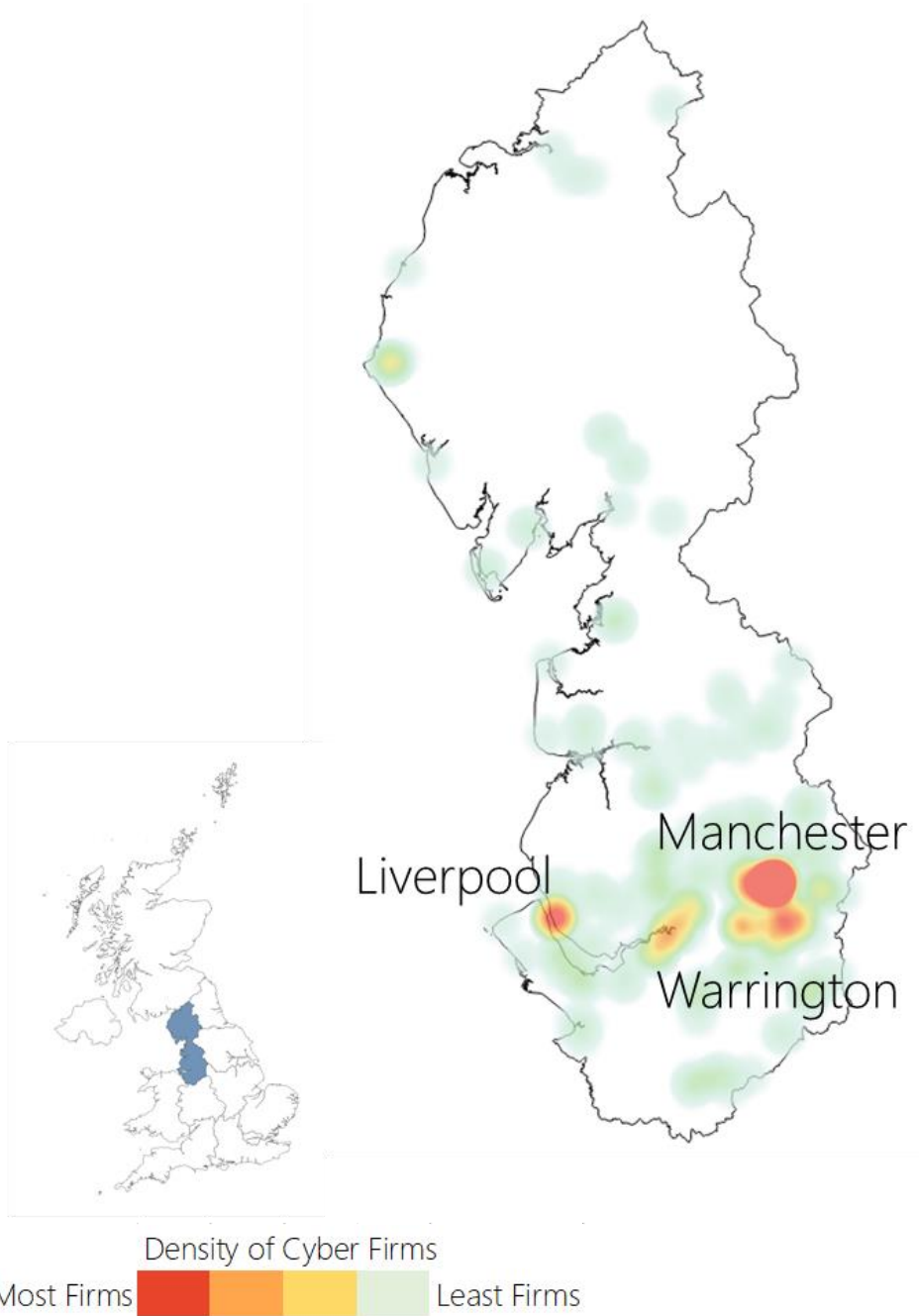
Greater London	Number of Registered Offices	Total Number of Active Offices
	609	1,095
Percentage of UK cyber security offices	Estimated percentage of UK based cyber security employment	Average Advertised Salaries (2021) in core cyber security roles
29%	29%	£69,700

North East



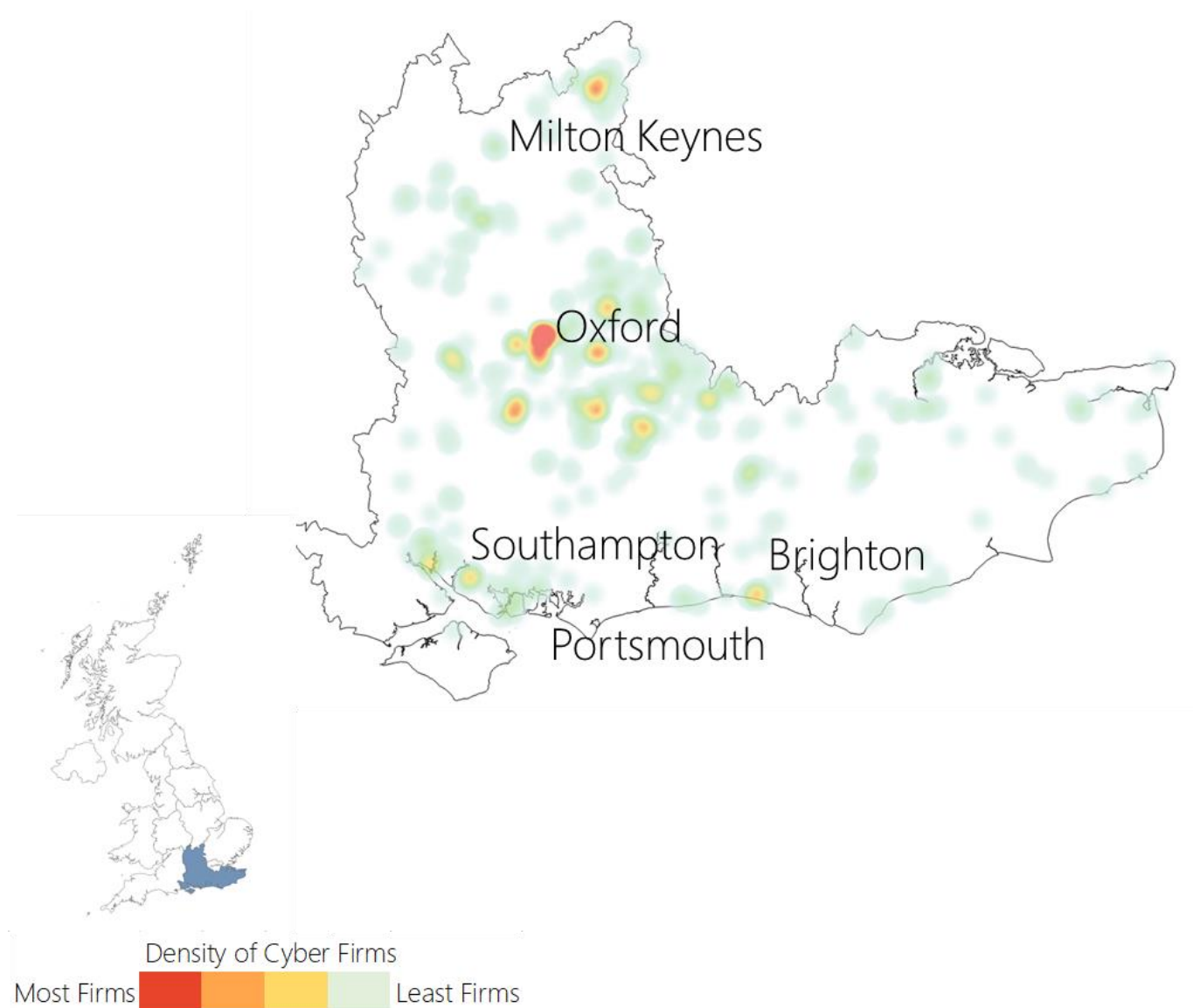
North East	Number of Registered Offices	Total Number of Active Offices
	52	117
Percentage of UK cyber security offices	Estimated percentage of UK based cyber security employment	Average Advertised Salaries (2021) in core cyber security roles
3%	2%	£46,500

North West



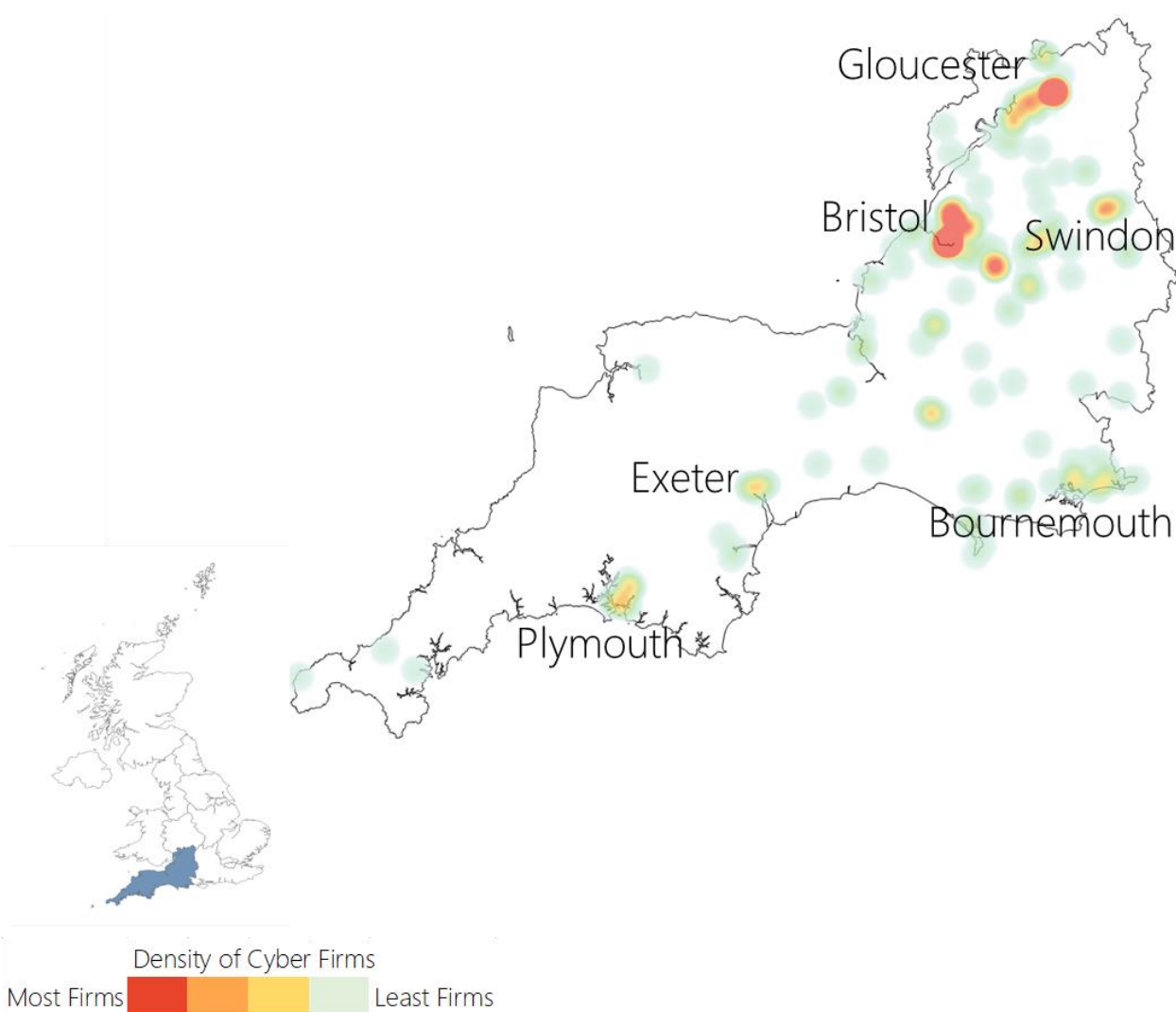
North West	Number of Registered Offices	Total Number of Active Offices
	132	339
Percentage of UK cyber security offices	Estimated percentage of UK based cyber security employment	Average Advertised Salaries (2021) in core cyber security roles
9%	9%	£54,600

South East



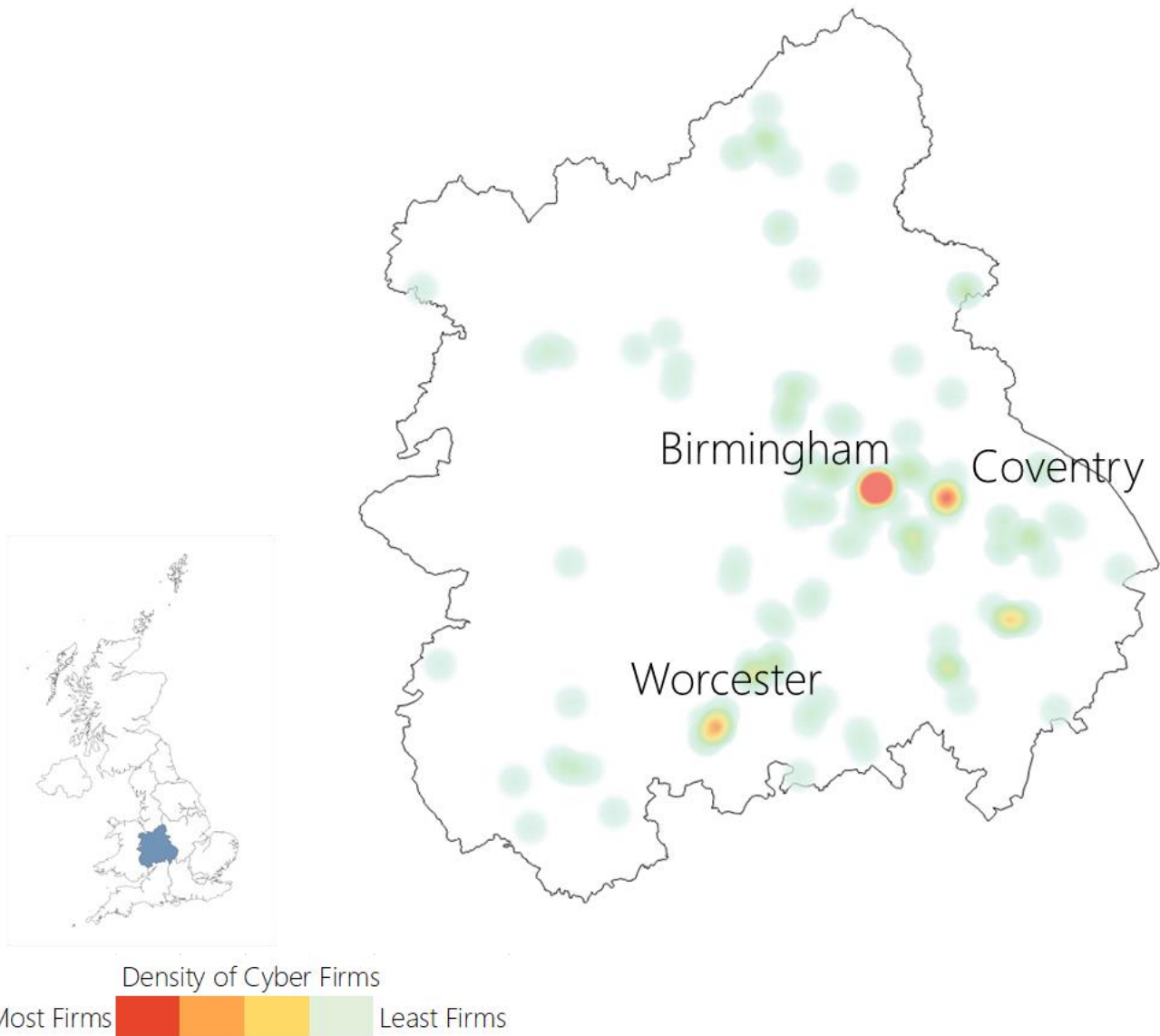
South East	Number of Registered Offices	Total Number of Active Offices
	371	676
Percentage of UK cyber security offices	Estimated percentage of UK based cyber security employment	Average Advertised Salaries (2021) in core cyber security roles
18%	16%	£59,700

South West



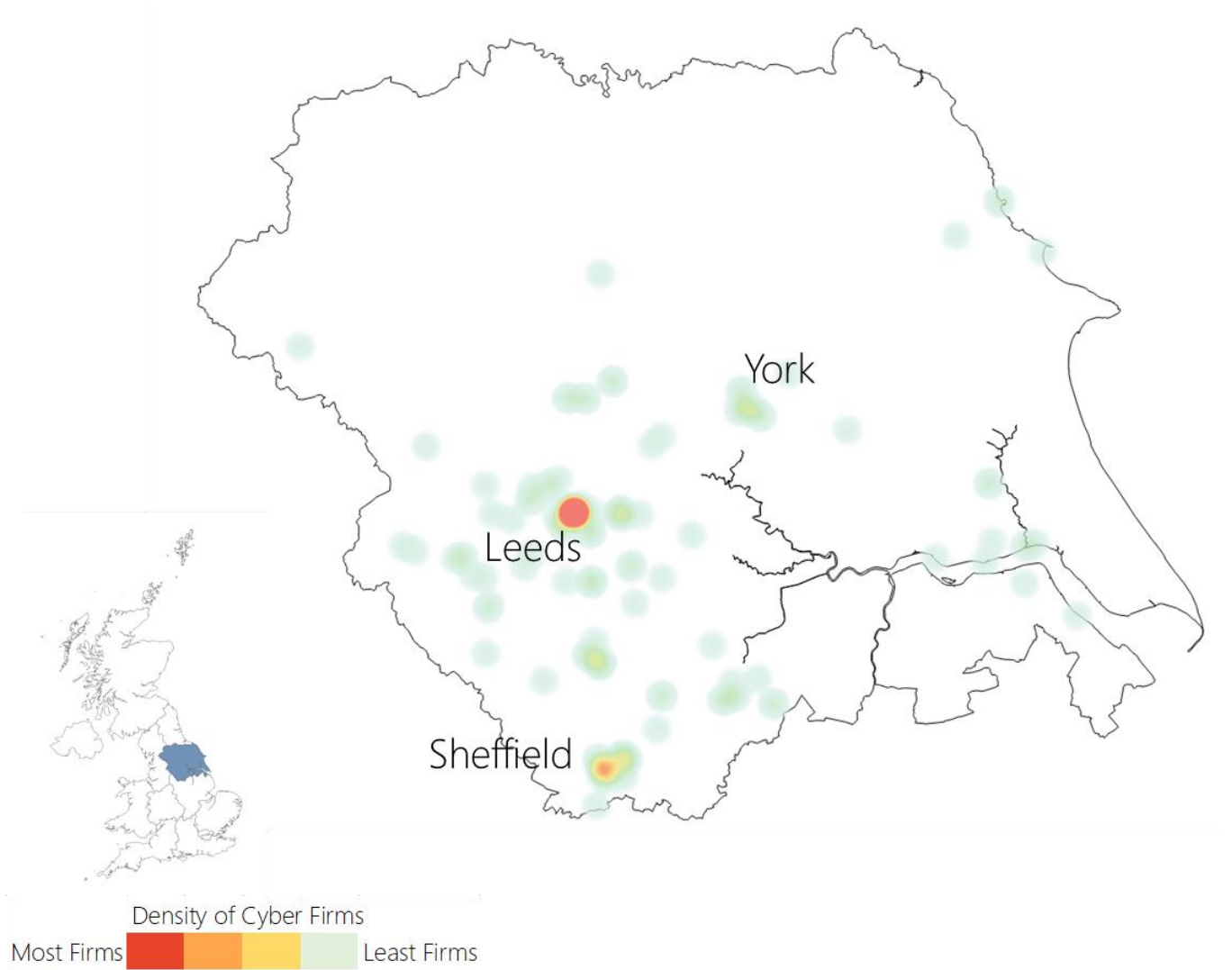
South West	Number of Registered Offices	Total Number of Active Offices
	129	303
Percentage of UK cyber security offices	Estimated percentage of UK based cyber security employment	Average Advertised Salaries (2021) in core cyber security roles
8%	8%	£58,000

West Midlands



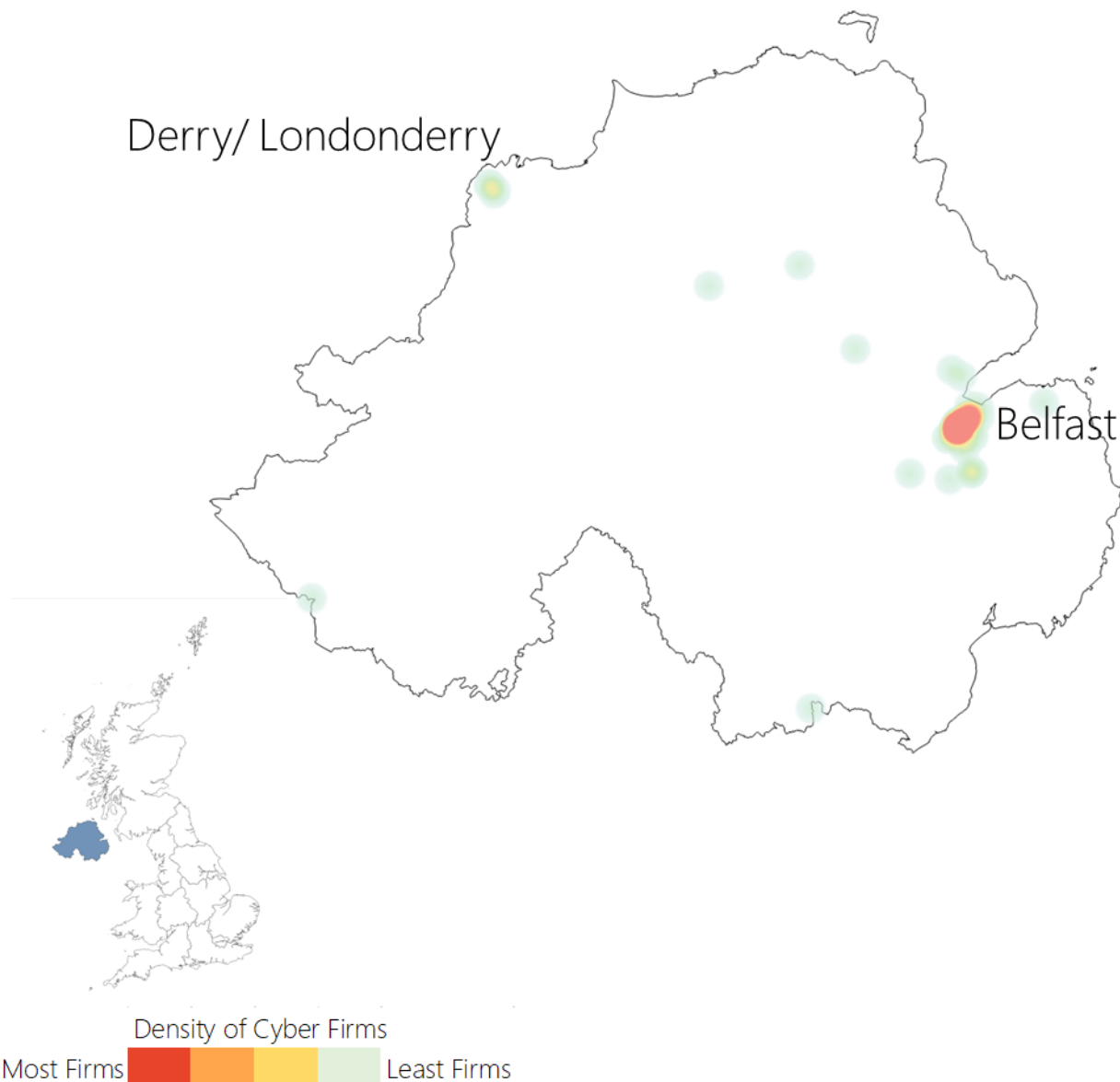
West Midlands	Number of Registered Offices	Total Number of Active Offices
	83	196
Percentage of UK cyber security offices	Estimated percentage of UK based cyber security employment	Average Advertised Salaries (2021) in core cyber security roles
5%	7%	£55,900

Yorkshire and the Humber



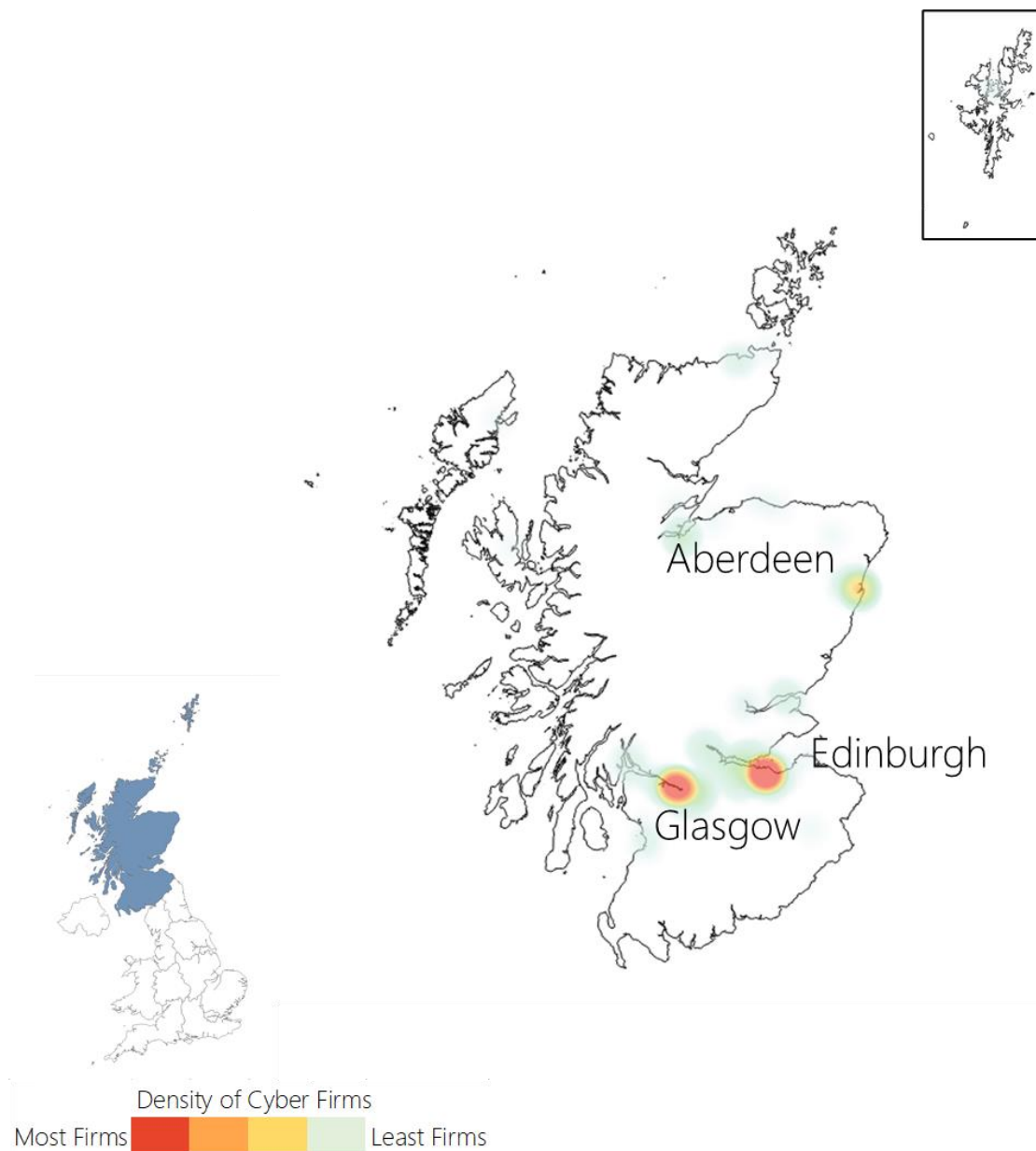
Yorkshire and the Humber	Number of Registered Offices	Total Number of Active Offices
	72	172
Percentage of UK cyber security offices	Estimated percentage of UK based cyber security employment	Average Advertised Salaries (2021) in core cyber security roles
5%	5%	£51,800

Northern Ireland



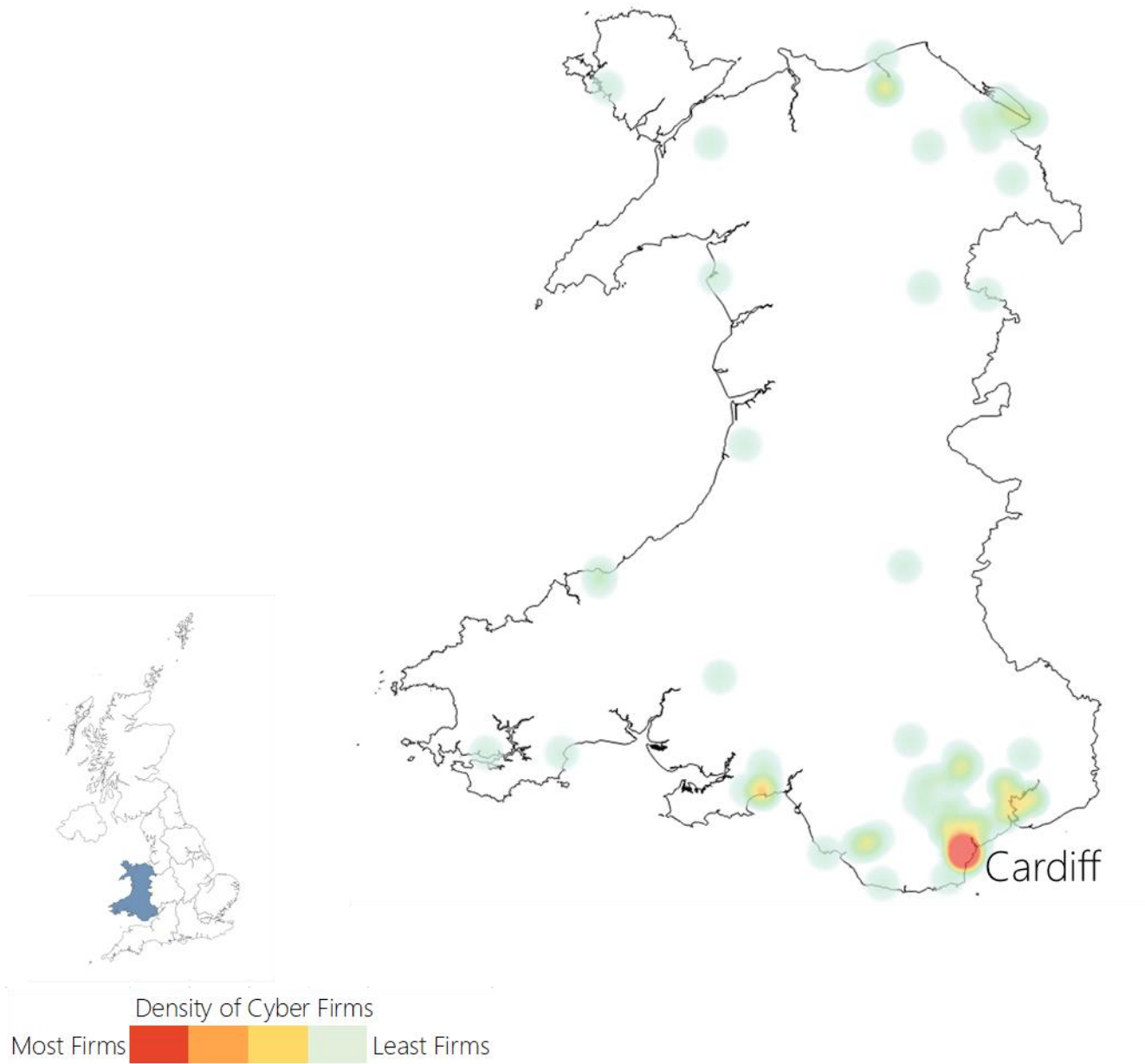
Northern Ireland	Number of Registered Offices	Total Number of Active Offices
	44	94
Percentage of UK cyber security offices	Estimated percentage of UK based cyber security employment	Average Advertised Salaries (2021) in core cyber security roles
2%	4%	£49,100

Scotland



Scotland	Number of Registered Offices	Total Number of Active Offices
	97	323
Percentage of UK cyber security offices	Estimated percentage of UK based cyber security employment	Average Advertised Salaries (2021) in core cyber security roles
8%	7%	£56,800

Wales



Wales	Number of Registered Offices	Total Number of Active Offices
	46	111
Percentage of UK cyber security offices	Estimated percentage of UK based cyber security employment	Average Advertised Salaries (2021) in core cyber security roles
3%	4%	£49,600

Appendices

A: Overview of Sources

The data sources used to underpin the sectoral analysis included:

- **glass.ai:** This year's study has partnered with web-scale intelligence providers [glass.ai](https://www.glass.ai) to use web data to help identify and map new providers of cyber security products and services, and match these to the cyber security taxonomy.
- **Bureau van Dijk FAME:** (and Companies House Data Product): This platform collates Companies House data and financial statements from all registered businesses within the UK
- **Beahurst:** Beahurst is a leading investment analysis platform, which 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 (glass.ai and Perspective Economics) has used web scraping²² to extract and parse key company descriptions, locations, and contact details from identified company websites
- **Representative survey of cyber security firms:** In Summer 2021, Ipsos conducted a representative survey of cyber security firms. The feedback from 248 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 25 one-to-one consultations with investors and market providers, to gather feedback on the growth and performance of the cyber security sector in the UK

²² Note: web scraping has observed robots.txt – i.e. where access is permitted.

B: Taxonomy and Definitions

Taxonomy Category	Agreed Definition
Cyber professional services	<p>Providing trusted contractors or consultants to advise on, or implement, cyber security products, solutions, or services for others.</p> <p>Within this year's study, we also have identified a marker for:</p> <ul style="list-style-type: none"> - Risk and Compliance Support (e.g. support with GDPR, ISO27001, Cyber Essentials) - Cyber Security Design & Advisory Services (e.g. support with cyber security architecture) - Managed Security Service Providers (MSSPs)
Endpoint and mobile security	Hardware or software that protects devices when accessing networks
Identification, authentication, and access controls	Products or services that control user access, for example with passwords, biometrics, or multi-factor authentication
Incident response and management	Helping other organisations react, respond, or recover from cyber attacks
Information risk assessment and management	Products or services that support other organisations to manage cyber risks, for example around security compliance or data leakage
Internet of Things	Products or services to embed or retrofit security for Internet of Things devices or networks
Network security	Hardware or software designed to protect the usability and integrity of a network
SCADA and Information Control Systems	Cyber security specifically for industrial control systems, critical national infrastructure, and operational technologies
Threat intelligence, monitoring, detection, and analysis	Monitoring or detection of varying forms of threats to networks and systems
Awareness, training, and education ²³	Products or services in relation to cyber awareness, training, or education

²³ The keywords underpinning Awareness, Training and Education have been broadened to include firms offering awareness or training courses without formal accreditation (e.g. online modules in cyber security awareness).

C: Survey Methodology and Interpretation

Response rate

The primary data collection was by a telephone survey carried out by Ipsos interviewers, from 7 June to 23 July 2021. This followed a random-probability approach, with interviewers making a minimum of 10 calls to each record (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.

One adjustment to the methodology for this year was to also allow respondents to complete the survey online, or partially online, alongside the telephone interviews. A total of 27 cyber firms responded online (i.e. just under 11% of the total achieved interviews). This measure was adopted in recognition of the much more challenging business survey environment as a result of the COVID-19 pandemic and the resulting restrictions placed on businesses.

We included all the identified cyber sector businesses in our original sample (i.e. 1,838 businesses). The unadjusted response rate for the survey is 13% (248/1,838). However, this does not account for the fact that a proportion of the sample did not have telephone numbers, or where the sampled telephone numbers were unusable (e.g. wrong numbers, disconnected). Over the course of the survey, Ipsos attempted wherever possible to find (alternative) numbers, including alternatives to office numbers whilst working remotely.

The adjusted response rate, based on the total usable sample, was 18% (248/1,415). This is lower than the response rate for last year's sectoral analysis (30%), which reflects the more challenging environment. Nevertheless, the sample composition achieved this year is broadly comparable to last year, suggesting the survey results provide reliable and representative estimates for the sector as a whole.

D: Investment Definitions

The definitions below are sourced from [Beaumont's Glossary of Terms](#).

Seed

A seed-stage company is a young start-up, with low employee count, valuation, and total equity investment raised. There may still be uncertainty as to whether its product or service has an adequate market, or it may be working to gain regulatory approval. The most common sources of funding for this stage of company are grant-awarding bodies, crowdfunding platforms, and angel investors.

Venture

Venture-stage companies have developed their business models and technology over multiple years, typically securing investment and a valuation in the millions. They'll likely have some revenue, and may be expanding their initial product range. Venture rounds typically involve private equity and venture capital funds, although may tap into crowdfunding.

Growth

When a company has been operating for more than five years, and has grown to multiple offices, they're more likely to have reached the Growth stage of evolution. A growth-stage company will also have

regulatory approval and is likely bringing in significant revenue and investment, with a valuation in the millions. It will be continuing to expand its product range and international activities.

Established

An established-stage company has been trading for 15+ years, or 5-15 years with a three-year consecutive profit of £5m+ or turnover of £20m+. As you may expect, these businesses usually have several offices and a widely recognised brand. Funding at this stage is often deployed by corporates, private equity firms, banks and specialist debt funds, or major international investors.

Exited

Exited companies are those that have exited the private market, by listing on a stock exchange or being acquired. We do not consider management buyouts (MBOs) as exits, but rather a trigger to start tracking a company as high growth on the Beauhurst platform.

Our standards and accreditations

Ipsos' standards and accreditations provide our clients with the peace of mind that they can always depend on us to deliver reliable, sustainable findings. Our focus on quality and continuous improvement means we have embedded a "right first time" approach throughout our organisation.



ISO 20252

This is the international market research specific standard that supersedes BS 7911/MRQSA and incorporates IQCS (Interviewer Quality Control Scheme). It covers the five stages of a Market Research project. Ipsos was the first company in the world to gain this accreditation.



Market Research Society (MRS) Company Partnership

By being an MRS Company Partner, Ipsos endorses and supports the core MRS brand values of professionalism, research excellence and business effectiveness, and commits to comply with the MRS Code of Conduct throughout the organisation. We were the first company to sign up to the requirements and self-regulation of the MRS Code. More than 350 companies have followed our lead.



ISO 9001

This is the international general company standard with a focus on continual improvement through quality management systems. In 1994, we became one of the early adopters of the ISO 9001 business standard.



ISO 27001

This is the international standard for information security, designed to ensure the selection of adequate and proportionate security controls. Ipsos was the first research company in the UK to be awarded this in August 2008.



The UK General Data Protection Regulation (GDPR) and the UK Data Protection Act (DPA) 2018

Ipsos is required to comply with the UK GDPR and the UK DPA. It covers the processing of personal data and the protection of privacy.



HMG Cyber Essentials

This is a government-backed scheme and a key deliverable of the UK's National Cyber Security Programme. Ipsos was assessment-validated for Cyber Essentials certification in 2016. Cyber Essentials defines a set of controls which, when properly implemented, provide organisations with basic protection from the most prevalent forms of threat coming from the internet.



Fair Data

Ipsos is signed up as a "Fair Data" company, agreeing to adhere to ten core principles. The principles support and complement other standards such as ISOs, and the requirements of Data Protection legislation.

For more information

3 Thomas More Square
London
E1W 1YW

t: +44 (0)20 3059 5000

www.ipsos.com/en-uk
<http://twitter.com/IpsosUK>

About Ipsos Public Affairs

Ipsos Public Affairs works closely with national governments, local public services, and the not-for-profit sector. Its c.200 research staff focus on public service and policy issues. Each has expertise in a particular part of the public sector, ensuring we have a detailed understanding of specific sectors and policy challenges. Combined with our methods and communications expertise, this helps ensure that our research makes a difference for decision makers and communities.

